ZX-Calculi for Quantum Computing and their Completeness

Renaud Vilmart

▶ **To cite this version:**

Renaud Vilmart. ZX-Calculi for Quantum Computing and their Completeness. Logic in Computer Science [cs.LO]. Université de Lorraine, 2019. English. NNT : 2019LORR0130 . tel-02395443

HAL Id: tel-02395443
https://hal.science/tel-02395443

Submitted on 5 Dec 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITÉ DE LORRAINE

École doctorale IAEM Lorraine

ZX-Calculi for Quantum Computing and their Completeness

THÈSE

présentée et soutenue publiquement le 19 septembre 2019

pour l'obtention du

Doctorat de l'Université de Lorraine

(mention informatique)

par

Renaud Vilmart

Composition du jury

Président :	Stephan Merz	Inria, Loria, Université de Lorraine
Rapporteurs :	Bob Coecke	University of Oxford, UK
	Peter Selinger	Dalhousie University, Halifax, Canada
Examinatrices :	Elham Kashefi	CNRS, LIP6, Sorbonne Université
	Christine Tasson	IRIF, Université Paris-Diderot
Directeurs :	Emmanuel Jeandel	Loria, Université de Lorraine
	Simon Perdrix	CNRS, Loria, Université de Lorraine

Laboratoire Lorrain de Recherche en Informatique et ses Applications — UMR 7503

Remerciements

J'aimerais tout d'abord remercier mes directeurs de thèse Emmanuel Jeandel et Simon Perdrix pour tout le temps qu'ils m'ont accordé, et pour l'aide précieuse et indéfectible qu'ils m'ont prodiguée. Il sont parvenus à m'intéresser dans ce sujet peu orthodoxe des langages graphiques pour le quantique, et cette thèse n'aurait pu aboutir sans eux.

À ce sujet, je remercie Bob Coecke et Peter Selinger pour avoir accepté de rapporter ma thèse, ainsi que le reste de mon jury : Elham Kashefi, Christine Tasson et Stephan Merz.

Je remercie tous les cobureaux thésards que j'ai eu pendant ces trois années : Pierre, Titouan, Sylvain et Hubert. Merci également à Henri, qui fut presque un cobureau pendant son passage en stage dans l'équipe.

Travailler dans l'équipe Mocqua fut un plaisir. Je remercie tous ses membres pour leur entrain et leur bienveillance : Romain, Emmanuel, Mathieu, Frédéric, Nazim et Vladimir.

J'aimerais remercier également mes amis des Mines et ceux que je me suis fais pendant la thèse, et dont l'intersection est non-nulle: Thomas, Florian, David, Baptiste, Adrien, Jean-Charles, Pierre, Charles, Matthieu, Prisca, Margaux et Joséphine.

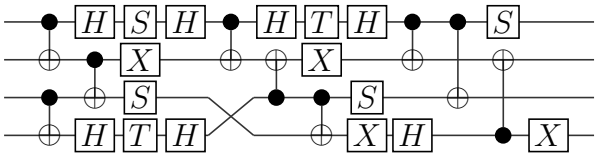
Je remercie bien évidemment mes parents, mon frère, ma soeur, et mes grands-parents pour leur soutien. Enfin, je remercie particulièrement chaleureusement Cynthia, qui a été à mes côtés et a su me supporter pendant ces trois années.

Introduction (fr)

L'informatique quantique est un modèle de calcul capable de supplanter un ordinateur classique pour effectuer certaines tâches. L'exemple le plus probant est l'algorithme de Shor qui permet de factoriser un nombre en ses facteurs premiers en un temps exponentiellement moins long que le meilleur algorithme classique connu. L'algorithme de Grover permet également un gain quadratique pour la recherche d'un élément dans une structure de données non-triée, et pléthore d'algorithmes dérivés de celui-ci permettent une même amélioration pour le problème qu'ils résolvent. Une des principales attentes de ce modèle, étant lui-même quantique, est de permettre de simuler efficacement d'autres systèmes quantiques. On peut encore trouver des applications dans la recherche d'un optimum, ou encore dans la cryptographie.

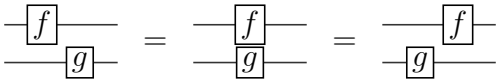
Pour pouvoir raisonner dans ce modèle de calcul, et effectuer des tâches complexes, il est nécessaire d'avoir des langages de plus haut niveau que l'implémentation physique du processus. Un parallèle est possible avec l'informatique classique: Les circuits booléens, qui utilisent des portes logiques telles que ET, OU, OUexclusif…, ont été une abstraction nécessaire à l'électronique sous-jacente. Une telle abstraction a plusieurs avantages. Premièrement, elle permet à l'utilisateur de se débarasser d'une certaine surcharge de travail inutile, tout en réduisant sa propension à faire des erreurs. Qui plus est, plus un langage est bas-niveau, et plus il voit ses paradigmes dictés par la nécessité de l'implémentation physique. À ce titre, un langage de plus haut niveau utilisera des paradigmes jugés plus utiles et compréhensibles par l'utilisateur (d'où la simplicité d'utilisation déjà remarquée), mais en plus il sera plus portable, le langage ne changeant pas entre les différents processeurs.

Les circuits quantiques sont un langage graphique qui permet une première abstraction. Les unités du calcul quantique, appelés bits quantiques ou qubits, sont représentés comme parcourant un fil, et des portes quantiques qui permettent le calcul altèrent leur valeur. Ces portes peuvent être combinées comme dans cet exemple (lu par convention de gauche à droite):

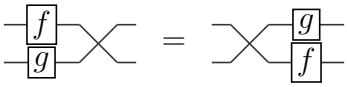


Le langage reste assez bas-niveau: son utilisation sur des projets d'envergure est lourde, et les choix dans ses opérateurs restent fortement dictés par la physique. On voit toutefois apparaître des éléments intéressants pour un langage graphique. Notamment, que deux processus indépendants, c'est-à-dire agissant sur des qubits différents, peuvent

commuter, peu importe celui qui est appliqué en premier:



ou encore comment réagissent les processus lorsque l'on échange les qubits sur lesquels ils sont appliqués:



Ces transformations sont évidentes dans le langage graphique, plus qu'elles ne le sont dans le langage algébrique:

$$(f \otimes id) \circ (id \otimes g) = f \otimes g = (g \otimes id) \circ (id \otimes f)$$

et

$$(g \otimes f) \circ \sigma = \sigma \circ (f \otimes g)$$

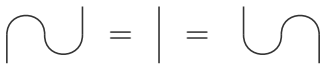
où σ représente l'échange de qubits.

Ce sont les equations qui sous-tendent les PROPs, un cas particulier des catégories monoïdales, issue de la théorie des catégories et qui permet de formaliser la notion de langage graphique. C'est justement de considérations catégoriques dont naquit le ZX-Calculus, le langage graphique qui est au centre de cette thèse.

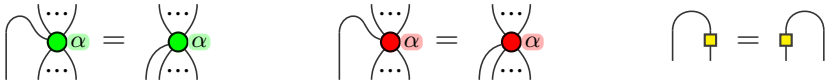
Il a été introduit en 2008 par Bob Coecke et Ross Duncan [CD11] avec pour fondement la complémentarité d'observables quantiques, un paradigme a priori indépendent de l'implémentation physique des évolutions quantiques représentées. Là aussi, les qubits sont représentés comme traversant des fils qui relient les générateurs du langage pour former ce que l'on appelle un diagramme. Dans toute la thèse, les diagrammes sont lus du haut vers le bas.

Le langage contient trois générateurs dont deux sont duaux l'un-de-l'autre et peuvent avoir un paramètre sous la forme d'un angle:  et  . Ceux-ci peuvent prendre un nombre arbitraire de fils en entrée et en sortie. Le troisième générateur est binaire, et permet de transformer l'un des deux précédents opérateurs en l'autre.

Dans ce langage, un fil, lorsqu'il est droit représente l'identité , mais il peut aussi être courbé: et . Ces diagrammes ont une signification particulière. Le premier représente l'état EPR $|00\rangle + |11\rangle$, tandis que le second représente le projecteur associé $\langle 00| + \langle 11|$, qui physiquement correspond à l'un des résultats possibles lors d'une mesure de Bell sur deux qubits. L'un des atouts du ZX-Calculus est justement l'existence de ces deux diagrammes, qui forment ce que l'on appelle une structure compacte:



Qui plus est, ces deux diagrammes réagissent bien avec les autres générateurs:



Grâce à cela en particulier, on peut considérer n'importe quel diagramme du ZX-Calculus comme un graphe ouvert (les entrées et les sorties sont fixées), tel que n'importe quel

isomorphisme de graphe (qui préserve entrées et sorties) préserve l'évolution quantique qui est représentée. C'est un des très gros avantages du ZX-Calculus, et qui en fait un langage plus haut-niveau que les circuits quantiques.

Les applications du langage graphique connues à ce jour sont très variées. Il peut être utilisé pour raisonner sur un modèle d'informatique quantique appelé MBQC (Measurement-Based Quantum Computing) [DP10, Dun13, Hor11] ou sur la correction d'erreurs quantiques [DL14, DG18, CKR+16]. Il se trouve notamment que les générateurs du langage sont très proches des primitives du "lattice surgery", un modèle pour la réalisation d'ordinateurs quantiques universels avec correction d'erreur [dBH17, dBDHP19]. Le ZX-Calculus a permis des améliorations dans la simplification de circuits quantiques [DKPvdW19, KvdW19] dans le projet PyZX [KvdW18], et peut être utilisé pour faire de la vérification, par exemple de protocoles [Hil11, Zam12].

Comme on l'a vu, différents diagrammes peuvent représenter la même évolution quantique, de la même façon que différentes compositions de matrices peuvent donner le même résultat. Dans le calcul matriciel, on sait réduire n'importe quelle composition de matrices obtenue avec $\circ$ et $\otimes$ à une unique matrice. Une telle réduction ne sera pas possible dans le ZX-Calculus, car un générateur seul n'est pas suffisamment expressif. On peut néanmoins donner un ensemble de transformations autorisées entre un diagramme du ZX-Calculus et un autre. Idéalement, ces règles devraient être intuitives et suffisamment peu nombreuses pour qu'un être humain puisse les retenir.

Les règles fondamentales du ZX-Calculus sont issues de la théorie des catégories, et utilisent des structures bien connues du domaine, telles les *algèbres de Frobenius* ou les *algèbres de Hopf*. Cette démarche est également utilisée pour décrire des structures tout aussi fondamentales en algèbre linéaire, pour représenter par exemple des flots de signal [BE15], avec un langage nommé **IH**, un proche parent du ZX-Calculus [BSZ17, Zan15]. Pour être plus précis, le premier formalise une restriction du second.

Pour s'assurer de la véracité d'une dérivation (une suite d'applications des règles de transformation), on peut utiliser un assistant de peuve appelé Quantomatic [KDD+11, KZ15] développé par la communauté et qui permet de manipuler des diagrammes de cordes tels que ceux du ZX-Calculus ainsi que de spécifier les règles de calcul autorisées.

Se pose alors la question de la complétude : Si deux diagrammes représentent la même évolution quantique, est-il possible de transformer l'un en l'autre en utilisant uniquement les transformations graphiques autorisées ? Un tel résultat est essentiel. Il implique que la théorie quantique est entièrement capturée par le langage, le rendant ainsi autosuffisant. Il n'est alors plus nécessaire de garder en tête la théorie mathématique des espaces de Hilbert sous-jacente, et tout raisonnement sur le quantique peut être mené au sein du langage uniquement.

C'est à cette question qu'essaie de répondre cette thèse. Le problème étant ardu, il a été étudié pour des restrictions du langage, appelés fragments. On appelle "fragment $\frac{\pi}{p}$" la restriction du ZX-Calculus où les paramètres de  et  sont des multiples de $\frac{\pi}{p}$. Bien sûr, des axiomatisations différentes peuvent être donnés pour différentes restrictions. On va donc distinguer les diagrammes du fragment $\frac{\pi}{p}$, aussi noté $\mathbf{ZX}[\frac{\pi}{p}]$, et les axiomatisations R. En les combinant, on obtient $\mathbf{ZX}[\frac{\pi}{p}]/R$, le langage obtenu en quotientant le fragment $\frac{\pi}{p}$ du ZX-Calculus par la théorie équationnelle R.

Le premier fragment pour lequel un résultat de complétude a été donné est $\mathbf{ZX}[\frac{\pi}{2}]$ [Bac14a], aussi appelé le stabiliseur du ZX-Calculus, ou encore Clifford. Un résultat ana-

logue existe pour les circuits [Sel15]. S'est ensuivi un résultat similaire pour le fragment π du langage $\mathbf{ZX}[\pi]$ [DP14], avec un ensemble d'axiomes légèrement différent. Malheureusement, ces fragments ne sont pas universels, ni même approximativement (certaines évolutions quantiques ne peuvent être représentées, même de façon approchée, par des diagrammes de ces fragments). Ceux-ci sont même simulables efficacement par un ordinateur classique[AG04].

L'intérêt s'est donc ensuite porté vers le fragment $\mathbf{ZX}[\frac{\pi}{4}]$, aussi appelé Clifford+T, qui lui, est approximativement universel [Shi03]. Un premier résultat a été donné pour le cas particulier de diagrammes sur un seul fil [Bac14b], lui-même dérivé du résultat sur les circuits [MA08]. Dans les circuits, on peut également citer la complétude des diagrammes "CNot-dihedraux" [ACR18] qui sont une restriction de Clifford+T, et la complétude des circuits Clifford+T sur deux qubits [SB15], redémontré dans le ZX-Calculus mais en sortant du fragment [CW18].

Parallèlement au développement du ZX-Calculus, un autre langage graphique, proche cousin du premier, a vu le jour : le ZW-Calculus [CK10]. Celui-ci jouit également d'une structure compacte, et donc de ce résultat puissant sur la conservation de la sémantique par isomorphisme de graphe. Ce langage se base lui sur l'interaction entre deux classes d'états quantiques fondamentalement différents, à savoir les états GHZ et les états W. Une autre différence flagrante avec le ZX-Calculus, est que le ZW-Calculus jouit d'une forme normale relativement naturelle. Cela a notamment permis la recherche d'axiomatisations complétes pour des fragments du langages [Had15, Had17, HNW18].

Dans cette thèse, nous faisons le lien entre les deux langages graphiques, ce qui permet notamment de simplifier la recherche d'axiomatisation complète pour le ZX-Calculus. Le premier résultat présenté dans cette thèse concerne $\mathbf{ZX}[\frac{\pi}{4}]$ [JPV18a], dont la complétude est obtenue par un système de traduction de $\mathbf{ZX}[\frac{\pi}{4}]$ vers une extension du ZW-Calculus notée $\mathrm{ZW}_{1/\sqrt{2}}$, ce qui permet le transport de la propriété de complétude. Pour ce faire, nous passons par un langage intermédiaire appelé $\Delta\mathbf{ZX}$, qui est une extension du ZX-Calculus avec un générateur supplémentaire  [Vil19]. Celui-ci est intéressant en lui-même car $\Delta\mathbf{ZX}[\pi]$ capture le fragment "Toffoli-Hadamard" de la mécanique quantique.

Nous montrons ensuite que l'axiomatisation utilisée avec $\mathbf{ZX}[\frac{\pi}{4}]$ est en réalité plus forte que cela, car elle permet aussi la complétude pour une restriction plus large des diagrammes du ZX-Calculus, appelés diagrammes linéaires à constantes dans Clifford+T, et dénotée $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$ [JPV18b]. Encore une fois, nous passons par le langage intermédiaire $\Delta\mathbf{ZX}[\vec{\alpha}, \pi]$, et la combinaison des deux permet d'obtenir une axiomatisation complète pour $\Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$. Ce résultat puissant de complétude sur les diagrammes linéaires, bien que non constructif, permet de déterminer pour un grand nombre d'égalités dans des fragments plus grands que $\mathbf{ZX}[\frac{\pi}{4}]$ qu'elles sont dérivables.

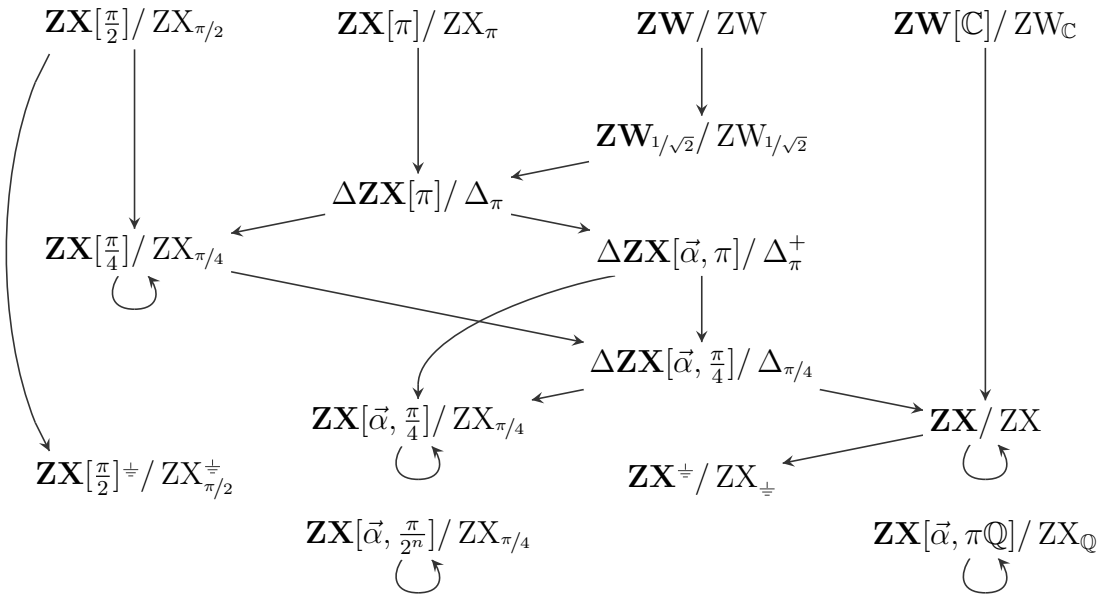
En utilisant ce résultat, un autre système de traduction entre le ZX-Calculus et un fragment plus grand du ZW-Calculus, ainsi qu'une méthode de réduction de certains diagrammes vers leur décomposition en valeurs singulières (SVD) [Vil18], nous prouvons ensuite la complétude du langage sans restriction $\mathbf{ZX}$ pour un ensemble d'axiomes étonnament plus petit que celui de $\mathbf{ZX}[\frac{\pi}{4}]$.

Il est bon de noter que les langages graphiques évoqués jusqu'à présent sont faits pour la mécanique quantique *pure*, c'est à dire sans interaction avec l'extérieur. Pour prendre en compte cette interaction, on représente les évolutions quantiques par des

CPM (completely positive maps), et on peut rajouter au langage un générateur $\perp\!\!\!\!\!\!\perp$ qui représente la trace partielle. Nous montrons comment rendre un langage graphique complet pour les CPM s'il l'est déjà pour la mécanique quantique pure. En particulier, on peut trouver aisément des axiomatisations complètes pour $\mathbf{ZX}^{\perp\!\!\!\!\!\!\perp}$ et sa restriction à Clifford $\mathbf{ZX}^{\perp\!\!\!\!\!\!\perp}[\frac{\pi}{2}]$ [CJPV19].

Enfin, en dernier lieu, nous donnons une construction pour une forme normale, valable dans n'importe quel fragment du ZX-Calculus qui contient $\frac{\pi}{4}$ [JPV18c]. Cela nous permet de reprouver les deux précédents résultats de complétude sans utiliser le ZW-Calculus, mais également de trouver des axiomatisations complètes pour d'autres fragments, notamment $\mathbf{ZX}[\frac{\pi}{2^n}]$ le fragment des dyadiques, et $\mathbf{ZX}[\pi\mathbb{Q}]$ le fragment des rationnels.

Le diagramme suivant représente les différents langages (constitués d'un fragment et d'une théorie équationnelle) considérés dans la thèse, les flèches représentant les dépendances pour la preuve de complétude. Les résultats de complétude obtenus par forme normale sont représentés avec une flèche qui boucle sur le langage. Les langages dont la complétude est considérée comme acquise sont les quatre du haut, vers lesquels ne pointe aucune flèche.



Durant cette thèse, j'ai participé à la conception du langage graphique appelé Y-Calculus [JPV18d], une variante du ZX-Calculus confinée à la représentation d'évolutions quantiques réelles. Nous avons donné un ensemble complet d'axiomes pour le stabiliseur. Puisqu'il existe un système de traduction entre le ZX-Calculus et le Y-Calculus, il est tout-à-fait possible de compléter ce dernier pour d'autres fragments, maintenant que les résultats analogues existent dans le ZX-Calculus. Toutefois, nous ne traiterons pas le cas du Y-Calculus dans cette thèse.

J'ai également participé à [JPVW17], qui introduit deux équations du ZX-Calculus qui seront évoqués voire utilisés comme axiomes dans la thèse, mais là encore nous ne nous attarderons pas sur les aspects traités dans le papier.

Contents

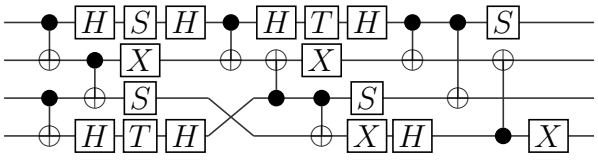
List of Figures

Introduction

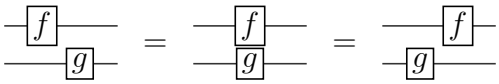
Quantum computing is a computational model capable of supplanting a conventional computer to perform certain tasks. The most convincing example is Shor's algorithm, which allows for number factoring into its prime factors in an exponentially shorter time than the best known classical algorithm. Grover's algorithm also allows a quadratic gain for searching for an element in a unsorted data structure, and a plethora of algorithms derived from it allow the same improvement for the problem they solve. One of the main expectations of this model, being itself a quantum model, is to allow other quantum systems to be effectively simulated. Applications can still be found in the search for an optimum, or in cryptography.

To be able to reason in this calculation model, and perform complex tasks, it is necessary to have languages of a higher level than the physical implementation of the process. A parallel is possible with classical computing: Boolean circuits, which use logic gates such as AND, OR, XOR..., have been a necessary abstraction to the underlying electronics. Such an abstraction has several advantages. First, it allows the user to get rid of a certain amount of unnecessary overload, while reducing the user's propensity to make mistakes. Moreover, the lower the level of a language, the more it sees its paradigms dictated by the need for physical implementation. As such, a higher level language will use paradigms considered more useful and understandable by the user (hence the simplicity of use already noted), but in addition it will be more portable, the language not changing between different processors.

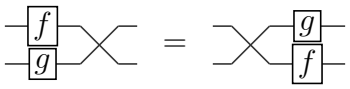
Quantum circuits are a graphical language that allows for a first abstraction. The units of quantum computation, called quantum bits or qubits, are represented as running through a wire, and quantum gates that allow computation alter their value. These gates can be combined as in this example (read by convention from left to right):



The language remains fairly low-level: its use on large-scale projects is heavy, and the choices in its operators remain strongly dictated by physics. However, there are some interesting elements for a graphical language. In particular, that two independent processes, i.e. acting on different qubits, can commute, no matter which one is applied first:



or how the processes react when exchanging the qubits on which they are applied:



These transformations are evident in the graphical language, more so than they are in the algebraic language:

$$(f \otimes id) \circ (id \otimes g) = f \otimes g = (g \otimes id) \circ (id \otimes f)$$

and

$$(g \otimes f) \circ \sigma = \sigma \circ (f \otimes g)$$

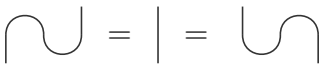
where σ represents the exchange of qubits.

These are the equations that underlie PROPs, a particular case of monoidal categories, stemming from category theory and which formalises the notion of graphic language. It was precisely from categorical considerations that ZX-Calculus, the graphical language that is at the heart of this thesis, was born.

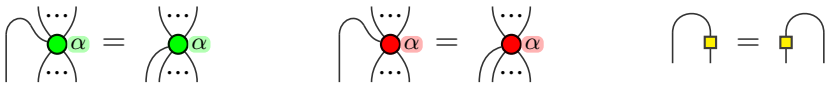
It was introduced in 2008 by Bob Coecke and Ross Duncan [CD11], based on the complementarity of quantum observables, a priori a paradigm independent of the physical implementation of the quantum evolutions represented. Again, qubits are represented as passing through wires that connect the language generators to form what is called a diagram. Throughout the thesis, the diagrams are read from top to bottom.

The language contains three generators, two of which are dual and can have a parameter in the form of an angle:  and  . These can take an arbitrary number of input and output wires. The third generator  is binary, and allows to transform one of the two previous operators into the other.

In this language, a wire, when straight, represents the identity , but it can also be curved:  and  . These diagrams have a particular meaning. The first represents the EPR state $|00\rangle + |11\rangle$, while the second represents the associated projector $\langle 00| + \langle 11|$, which physically corresponds to a possible result of a Bell measurement on two qubits. One of the advantages of the ZX-Calculus is precisely the existence of these two diagrams, which form what is called a compact structure:



Moreover, these two diagrams react well with the other generators:



Thanks to these equations in particular, we can consider any diagram of the ZX-Calculus as an open graph (inputs and outputs are fixed), such that any graph isomorphism (which preserves inputs and outputs) preserves the quantum evolution that is represented. This is one of the very big advantages of the ZX-Calculus, a feature that makes it a higher level language than quantum circuits.

The applications of the graphic language known to date are very varied. It can be used to reason about a quantum computing model called MBQC (Measurement-Based

Quantum Computing) [DP10, Dun13, Hor11] or about quantum error correction [DL14, DG18, CKR+16]. In particular, the language generators are very close to the primitives of "lattice surgery", a model for the realization of universal quantum computers with error correction [dBH17, dBDHP19]. The ZX-Calculus has allowed improvements in quantum circuit simplification [DKPvdW19, KvdW19] in the PyZX project [KvdW18], and can be used to perform verification, for example of protocols [Hil11, Zam12].

As we have seen, different diagrams can represent the same quantum evolution, in the same way that different matrix compositions can yield the same result. In matrix calculation, we know how to reduce any matrix composition obtained with $\circ$ and $\otimes$ to a single matrix. Such a reduction will not be possible in the ZX-Calculus, as a single generator is not sufficiently expressive. However, a set of allowed transformations can be given between one diagram of the ZX-Calculus and another. Ideally, these rules should be intuitive and sufficiently sufficiently limited in number to be remembered by the user.

The fundamental rules of ZX-Calculus are derived from category theory, and use structures well known in the field, such as Frobenius algebras or Hopf algebras. This approach is also used to describe equally fundamental structures in linear algebra, for example to represent signal flows [BE15], with a language named **IH**, a close relative of the ZX-Calculus [BSZ17, Zan15]. To be more precise, the former formalises a restriction of the latter.

To ensure the soundness of a derivation (a sequence of application of transformation rules), we can use a proof assistant called Quantomatic [KDD+11, KZ15] developed by the community and which allows to handle string diagrams such as those of the ZX-Calculus as well as to specify the allowed calculation rules.

The question of completeness then arises: If two diagrams represent the same quantum evolution, is it possible to transform one into the other using only the authorised graphical transformations? Such a result is essential. It implies that quantum theory is entirely captured by the language, making it self-sufficient. It is then no longer necessary to keep in mind the mathematical theory of the underlying Hilbert spaces, and any reasoning about quantum can be conducted within the language alone.

This thesis attempts to answer this question. The problem being difficult, it has been studied first for language restrictions, called fragments. The restriction of the ZX-Calculus where the parameters of  and  are multiples of $\frac{\pi}{p}$ is called a "$\frac{\pi}{p}$-fragment". Of course, different axiomatisations can be given for different restrictions. We will therefore distinguish the diagrams of the $\frac{\pi}{p}$-fragment, also denoted $\mathbf{ZX}[\frac{\pi}{p}]$, and the axiomatisations R. By combining them, we obtain $\mathbf{ZX}[\frac{\pi}{p}]/R$, the language obtained by quotienting the $\frac{\pi}{p}$-fragment of the ZX-Calculus by the equational theory R.

The first fragment for which a completeness result has been given is $\mathbf{ZX}[\frac{\pi}{2}]$ [Bac14a], also called the stabiliser ZX-Calculus, or Clifford ZX-Calculus. A result for the analogous fragment exists for the circuits [Sel15]. A similar result followed for the π-fragment of the ZX-Calculus [DP14], with a slightly different set of axioms. Unfortunately, these fragments are not universal, not even approximately (some quantum evolutions cannot be represented, even approximately, by diagrams of these fragments). Moreover, these fragments can even be efficiently simulated by a classical computer.

Interest then turned to the fragment $\mathbf{ZX}[\frac{\pi}{4}]$, also called Clifford+T, which is approximately universal [Shi03]. A first result was given for the particular case of diagrams on a single wire [Bac14b], itself derived from the result on quantum circuits [MA08].

As for circuits, we can also mention the completeness of the "CNot-dihedral" diagrams [ACR18] which are a restriction of Clifford+T, as well as the completeness of the Clifford+T circuits on two qubits [SB15], restated in the ZX-Calculus but with axioms that require the derivation to be carried outside the fragment [CW18].

In parallel with the development of the ZX-Calculus, another graphical language, close cousin of the first, has emerged: ZW-Calculus [CK10]. It also has a compact structure, and therefore the same powerful result on the conservation of semantics by graph isomorphism. This language is based on the interaction between two fundamentally different classes of quantum states, namely GHZ states and W states. Another obvious difference with ZX-Calculus is that ZW-Calculus has a relatively natural notion of normal form. This made it possible to search for complete axiomatisations for fragments of the language [Had15, Had17, HNW18].

In this thesis, we make the link between the two graphical languages, which simplifies the search for complete axiomatisations for the ZX-Calculus. The first result presented in this thesis concerns $\mathbf{ZX}[\frac{\pi}{4}]$ [JPV18a], whose completeness is obtained by a translation system of $\mathbf{ZX}[\frac{\pi}{4}]$ towards an extension of the ZW-Calculus $\mathrm{ZW}_{1/\sqrt{2}}$ and back, which allows the transport of the completeness property. To do this, we go through an intermediate language called $\Delta\mathbf{ZX}$, which is an extension of the ZX-Calculus with an additional generator  [Vil19]. This one is interesting in itself because $\Delta\mathbf{ZX}[\pi]$ captures the "Toffoli-Hadamard"-fragment of quantum mechanics.

We then show that the axiomatisation used with $\mathbf{ZX}[\frac{\pi}{4}]$ is actually stronger than that, because it also allows completeness for a broader restriction of the ZX-Calculus diagrams, called linear diagrams with constants in Clifford+T, and denoted $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$ [JPV18b]. Once again, we go through the intermediate language $\Delta\mathbf{ZX}[\vec{\alpha}, \pi]$, and the combination of the two allows us to obtain a complete axiomatisation for $\Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$. This powerful result of completeness on linear diagrams, although not constructive, allows to determine for a large number of equations in fragments broader than $\mathbf{ZX}[\frac{\pi}{4}]$ that they are derivable.

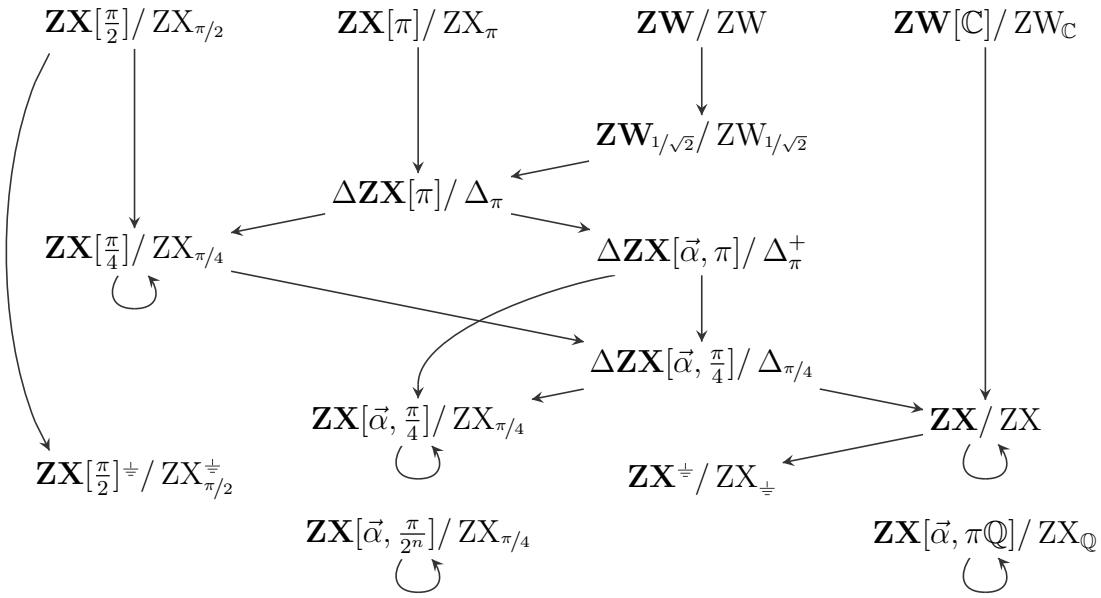
Using this result, another translation system between the ZX-Calculus and a larger fragment of the ZW-Calculus, as well as a method for reducing some diagrams to their singular value decomposition (SVD) [Vil18], we then prove the completeness of the unrestricted language $\mathbf{ZX}$, surprisingly with a smaller set of axioms than that of $\mathbf{ZX}[\frac{\pi}{4}]$.

It is worth noting that the graphical languages mentioned so far are designed for *pure* quantum mechanics, i.e. without interaction with the outside world. To take into account this interaction, we can add to the language a generator  which represents the partial trace. We show how to make a graphical language for CPMs complete if it is already complete for pure quantum mechanics. In particular, complete axiomatisations for $\mathbf{ZX}^{\div}$ and its restriction to Clifford $\mathbf{ZX}^{\div}[\frac{\pi}{2}]$ [CJPV19] can be easily found.

Finally, we give a construction for a normal form, valid in any fragment of the ZX-Calculus that contains $\frac{\pi}{4}$ [JPV18c]. This allows us to recover the two previous completeness results without using the ZW-Calculus, but also to find complete axiomatisations for other fragments, including $\mathbf{ZX}[\frac{\pi}{2^n}]$, the dyadic fragment, and $\mathbf{ZX}[\pi\mathbb{Q}]$, the rational fragment.

The following diagram represents the different languages (consisting of a fragment and an equational theory) considered in the thesis, the arrows representing the dependencies for the proofs of completeness. The completeness results obtained by normal

form are represented with an arrow looping on the language. The languages whose completeness is taken for granted are the top four, to which no arrows point, for they were proven in the literature [Bac14a, DP14, Had15, Had17].



During this thesis, I participated in the design of the graphical language called Y-Calculus [JPV18d], a variant of ZX-Calculus confined to the representation of real quantum evolutions. We have given a complete set of axioms for its stabiliser fragment. Since there is a translation system between the ZX-Calculus and the Y-Calculus, it is absolutely possible to complete the latter for other fragments, now that similar results exist in the ZX-Calculus. However, we will not deal with the case of the Y-Calculus in this thesis.

I also participated in [JPVW17], which introduces two equations of the ZX-Calculus that will be mentioned or even used as axioms in the thesis, but here again we will not dwell on the aspects treated in the paper.

Part I

Background

Chapter 1

Standard Quantum Mechanics

Quantum mechanics [FLSL66] is one of the two prominent physical models that arose during the first decades of the XXth century, the other being relativity. It was created to explain experiments where the now called classical physics fell short, such as black body radiation, or the photoelectric effect [Pla01, Ein05]. The core difference with the classical model is that some quantities of a system – such as energy, momentum ... – are restricted to discrete values, as opposed to continuous ones in the classical model. So far, this theory has proven to be extremely robust and precise [NC10].

It has already had applications in several domains of physics, and can also be used to perform transistor and laser computations. Indeed, these can be used to store, process and communicate information. We review in this chapter the fundamentals of quantum mechanics, which we can find e.g. in [vN32] or [NC10].

1.1 Pure Quantum States

⌜ **Definition 1.1.1** (Hilbert Space)**:** A Hilbert space $\mathcal{H}$ is a vector space over $\mathbb{K}$ (where $\mathbb{K}$ is either $\mathbb{C}$ or $\mathbb{R}$), equipped with an inner product, that is, a function $\langle . \,|\, . \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{K}$ with the following properties:

- $\langle x \,|\, y \rangle = \overline{\langle y \,|\, x \rangle}$
- It is linear in its first argument:

$$\langle x_1 + \lambda x_2 \,|\, y \rangle = \langle x_1 \,|\, y \rangle + \lambda \langle x_2 \,|\, y \rangle$$

- $x \mapsto \langle x \,|\, x \rangle$ is positive definite:

$$\langle x \,|\, x \rangle > 0 \text{ if } x \neq 0$$
$$\langle x \,|\, x \rangle = 0 \text{ if } x = 0$$

In this context, it is conventional to define a norm by $\|.\| := x \mapsto \sqrt{\langle x \,|\, x \rangle}$, which is real-valued. The inner product makes $\mathcal{H}$ a metric space, in which we can define the distance between two elements a and b as $d(a, b) := \|a - b\|$. A Hilbert space is further assumed to be complete, i.e. any sequence $(a_n)_{n \in \mathbb{N}}$ such that $\lim_{n \to \infty} d(a_n, a_{n+1}) = 0$ converges in $\mathcal{H}$. ⌟

Postulate 1.1.2. *Each physical system is associated with a complex Hilbert space $\mathcal{H}$ with inner product $\langle . \,|\, . \rangle$, and topologically separable in the sense that it admits a countable orthonormal basis. Rays (that is, subspaces of complex dimension 1) in $\mathcal{H}$ are associated with quantum states of the system.*

Hence, any quantum state ψ can be represented by a vector over the Hilbert space $\mathcal{H}$, of norm one i.e. $\langle \psi \,|\, \psi \rangle = 1$. Two such vectors are equivalent if they only differ by a phase factor: Indeed, if $|\psi_1\rangle$ is equivalent to $|\psi_2\rangle$ by definition of rays, there exists $\lambda \in \mathbb{C}$ such that $|\psi_1\rangle = \lambda \,|\psi_2\rangle$. However the constraint on the norm gives:

$$1 = \langle \psi_1 \,|\, \psi_1 \rangle = |\lambda|^2 \,\langle \psi_2 \,|\, \psi_2 \rangle = |\lambda|^2$$

which implies $\lambda = e^{i\theta}$ for some $\theta \in \mathbb{R}$.

Example 1.1.3. In $\mathbb{C}^2$, $\frac{1}{2}\begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix} \sim \frac{e^{i\phi}}{2}\begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix}$ where $\phi \in \mathbb{R}$ is an arbitrary angle, and $\sim$ is the equivalence relation.

A useful notation, introduced by Dirac, and consistent with the inner product notation is the so-called *Dirac notation*, or *braket* notation. In this notation, a vector is denoted with $|.\rangle$, called *ket*, and its dagger (in finite dimension, the conjugate transpose) is $\langle .| := |.\rangle^\dagger$, called *bra*, and defined for every element of $\mathcal{H}$ as:

$$\langle \psi| : \begin{array}{ccc} \mathcal{H} & \to & \mathbb{K} \\ |\phi\rangle & \mapsto & \langle \psi \,|\, \phi \rangle \end{array}$$

Hence, $\langle \psi| \circ |\phi\rangle = \langle \psi \,|\, \phi \rangle$.

A building block of finite-dimensional quantum mechanics is a quantum object of dimension d, called a *qudit*. A qudit state will be represented as a vector of $\mathbb{C}^d$. It is fairly easy to see that the set of vectors $(\vec{e_i})_{0 \leq i < d}$ – where $\vec{e_i} \in \mathbb{C}^d$ is the vector with 0s everywhere except for the ith component which is a 1 – forms a basis for $\mathbb{C}^d$. The vectors $\vec{e_i}$ will be denoted in the Dirac notation $|i\rangle := \vec{e_i}$. This forms the so-called *canonical basis* or *standard basis*. Then, any qudit state can be expressed as a linear combination of the vectors in this basis: $|\psi\rangle = \sum_{i=0}^{d} \alpha_i \,|i\rangle$.

The vectors of the canonical basis can be seen as classical states. Any state that is not a basis vector is then said to be in a *superposition* of the (or some) classical states. The coefficients in the linear combination are called *amplitudes*, and are linked to the measurement outcomes of the system, as we will describe later.

Of primary interest for us will be the case where $d = 2$. The base component is then called *qubit*, and it is a linear combination of $|0\rangle$ and $|1\rangle$. Several very simple quantum objects are qubits: the electron spin, the photon polarisation, the fermion position ... [NC10, BK02] Moreover, the two classical states $|0\rangle$ and $|1\rangle$ can be identified with the states of a classical bit. A bit is hence a qubit which is not allowed superposition.

When working with qubits, we may also consider two other bases: $(|+\rangle\,, |-\rangle)$ and $(|i\rangle\,, |-i\rangle)$ where:

$$|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$
$$|i\rangle := \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}} \qquad |-i\rangle := \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}$$

It is to be noted that the three bases $(|0\rangle, |1\rangle)$, $(|+\rangle, |-\rangle)$ and $(|i\rangle, |-i\rangle)$ are all orthonormal.

1.2 Composite Systems

Postulate 1.2.1. *The state space of a composite physical system is the tensor product (denoted $.\otimes.$) of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$.*

The tensor product is a bilinear operator from $\mathcal{H}_A \times \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$:

$$(\varphi_1 + \lambda\varphi_2) \otimes \psi = \varphi_1 \otimes \psi + \lambda\varphi_2 \otimes \psi$$
$$\psi \otimes (\varphi_1 + \lambda\varphi_2) = \psi \otimes \varphi_1 + \lambda\psi \otimes \varphi_2$$

If two systems A and B have corresponding Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, then the combination of the subsystems is a system of corresponding Hilbert space $\mathcal{H}_{A\otimes B} := \mathcal{H}_A \otimes \mathcal{H}_B$. The elements of $\mathcal{H}_{A\otimes B}$ are linear combinations of tensor products $|\psi_A\rangle \otimes |\psi_B\rangle$ of elements $|\psi_A\rangle$ of $\mathcal{H}_A$ and $|\psi_B\rangle$ of $\mathcal{H}_B$.

If $\{|i_A\rangle\}$ and $\{|i_B\rangle\}$ are bases of respectively $\mathcal{H}_A$ and $\mathcal{H}_B$, then $\{|i_A\rangle \otimes |i_B\rangle\}$ is a basis of $\mathcal{H}_{A\otimes B}$. In particular, if $\mathcal{H}_A$ and $\mathcal{H}_B$ are finite dimensional, then $\dim(\mathcal{H}_{A\otimes B}) = \dim(\mathcal{H}_A) \times \dim(\mathcal{H}_B)$.

In the Dirac notation, when there is no ambiguity, it is customary to write a tensor product as the concatenation of the two kets: $|\psi\phi\rangle := |\psi\rangle \otimes |\phi\rangle$. For instance, in the qubit case, $|01\rangle$ represents a state on two qubits, the first of which is in state 0 and the second in state 1. In terms of vectors, if $|j\rangle \in \mathcal{H}_B$, then $|ij\rangle := |i\rangle \otimes |j\rangle = \vec{e}_{i\times\dim(\mathcal{H}_B)+j}$, i.e. the vector with 0 entries everywhere except 1 for the $(i \times \dim(\mathcal{H}_B) + j)$th. By bilinearity of $\otimes$, this completely defines the tensor product. For instance, in $\mathbb{C}^2 \otimes \mathbb{C}^3$:

$$(\vec{e}_0 + 2\vec{e}_1) \otimes (\vec{e}_0 + \vec{e}_2) = \vec{e}_0 \otimes \vec{e}_0 + \vec{e}_0 \otimes \vec{e}_2 + 2\vec{e}_1 \otimes \vec{e}_0 + 2\vec{e}_1 \otimes \vec{e}_2 = \vec{e}_0 + \vec{e}_2 + 2\vec{e}_3 + 2\vec{e}_5$$

i.e.

$$\begin{pmatrix}1\\2\end{pmatrix} \otimes \begin{pmatrix}1\\0\\1\end{pmatrix} = \begin{pmatrix}1\\0\\1\\2\\0\\2\end{pmatrix}$$

A state on a composite system cannot always be decomposed as a tensor product of the two subsystems. When this is the case, the composite state is called *entangled*. The easiest and most famous example is the state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. It can be shown that there is no pair of one-qubit states $|\psi_1\rangle$ and $|\psi_2\rangle$ such that $\frac{|00\rangle+|11\rangle}{\sqrt{2}} = |\psi_1\rangle \otimes |\psi_2\rangle$.

This particular state has a special name: it is called the EPR state. It is due to Einstein, Podolsky and Rosen, who thought they had found a paradox in the theory of quantum mechanics [EPR35]. The two particles in this state are dependant to one-another and any

operation on one of them affects the state as a whole. Specifically, during a measurement in the standard basis (see Section 1.4), if the measurement of the first qubit yields $x \in \{0, 1\}$, then the measurement of the second one automatically yields the same result x, no matter how far the two particles are from one another. This violates the principle of locality.

The EPR state is one of the four Bell states, which are the four maximally entangled two qubit states: $\frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$ and $\frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$ [Bel64]. It is also a particular case of the GHZ states, of the form $\frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$ where $|x^n\rangle$ represents a register of n qubits in the state $|x\rangle$ [GHZ89].

1.3 Operators

The state of a quantum system can evolve through time. This is modelled as applying a linear map to the state: $|f\psi\rangle := f(|\psi\rangle)$. The neutral element for the composition of maps $\circ$ is the identity. We denote by $id_{\mathcal{H}}$ the identity on $\mathcal{H}$. Notice that if $\dim(\mathcal{H}) = 1$, then $\mathcal{H} = \mathbb{C}$, so $id_{\mathbb{C}} = (1)$. The subscript of id can be neglected when it is clear from the context.

⌜ **Definition 1.3.1** (Linear Map)**:** A linear map $f : \mathcal{H}_1 \to \mathcal{H}_2$ is a map such that:

$$\forall x, y \in \mathcal{H}_1, \forall \lambda \in \mathbb{C}, \quad f(x + \lambda y) = f(x) + \lambda f(y)$$ ⌟

One can define a norm on linear maps [AB06].

⌜ **Definition 1.3.2** (Norm)**:** Let f be a linear map. We define $\|f\|$ as:

$$\|f\| := \sup_{|\psi\rangle \neq 0} \left(\frac{\|f\,|\psi\rangle\,\|}{\|\,|\psi\rangle\,\|} \right)$$ ⌟

Linear maps can be composed by the tensor product. If f_A and f_B act respectively on Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, then $f_A \otimes f_B$ acts on the composite space $\mathcal{H}_{A\otimes B}$, such that, if $|\psi_A\rangle$ and $|\psi_B\rangle$ are elements of respectively $\mathcal{H}_A$ and $\mathcal{H}_B$, then $(f_A \otimes f_B)\,|\psi_A\,\psi_B\rangle = (f_A\,|\psi_A\rangle) \otimes (f_B\,|\psi_B\rangle)$.

Similarly to quantum states, maps on finite dimensional Hilbert spaces can be expressed using the Dirac notation: $f = \sum |\psi_i\rangle\langle\phi_j|$, where $|\psi_i\rangle\langle\phi_j| := |\psi_i\rangle \circ \langle\phi_j|$ and $\circ$ is the matrix composition. If $f_A = \sum \left|\psi_i^{(A)}\right\rangle\!\left\langle\phi_j^{(A)}\right|$ and $f_B = \sum \left|\psi_i^{(B)}\right\rangle\!\left\langle\phi_j^{(B)}\right|$, then the tensor product is expressed $f_A \otimes f_B = \sum \left|\psi_i^{(A)}\psi_k^{(B)}\right\rangle\!\left\langle\phi_j^{(A)}\phi_\ell^{(B)}\right|$.

Example 1.3.3. Given (x_i) an orthonormal basis of the finite dimensional Hilbert space $\mathcal{H}$, the identity id in $\mathcal{H}$ can be expressed as $id = \sum |x_i\rangle\langle x_i|$.

It is convenient to work with an orthonormal basis (x_i) since:

$$\langle x_i \,|\, x_j\rangle = \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

Hence, if $f : \mathcal{H}_1 \to \mathcal{H}_2 = \sum \alpha_{ij}\,|x_i\rangle\langle y_j|$ and $g : \mathcal{H}_2 \to \mathcal{H}_3 = \sum \beta_{k\ell}\,|z_k\rangle\langle x_\ell|$ with (x_i) an orthonormal basis of $\mathcal{H}_2$, then the composition $g \circ f$ has a simple expression:

$$g \circ f = \left(\sum_{k,\ell} \beta_{k\ell}\,|z_k\rangle\langle x_\ell| \right) \left(\sum_{i,j} \alpha_{ij}\,|x_i\rangle\langle y_j| \right) = \sum_{i,j,k,\ell} \alpha_{ij}\beta_{k\ell}\,|z_k\rangle\underbrace{\langle x_\ell \,|\, x_i\rangle}_{\delta_{i,\ell}}\langle y_j|$$

$$= \sum_{i,j,k} \alpha_{ij}\beta_{ki} \left|z_k\right\rangle\!\left\langle y_j\right|$$

The next postulate dictates how a closed quantum system evolves, and needs the following notions:

⌜ **Definition 1.3.4** (Adjoint and Unitary Operator)**:** Let $A : \mathcal{H}_1 \to \mathcal{H}_2$ be a linear operator. The adjoint map $A^\dagger : \mathcal{H}_2 \to \mathcal{H}_1$ is uniquely defined as the linear map such that for all $x, y \in \mathbb{C}$, $\langle Ax \,|\, y\rangle = \langle x \,|\, A^\dagger y\rangle$.

A unitary operator $U : \mathcal{H} \to \mathcal{H}$ on a Hilbert space $\mathcal{H}$ is a linear map such that $UU^\dagger = U^\dagger U = id$. ⌟

Notice that for any $|x\rangle$, $\|U|x\rangle\| = \||x\rangle\|$, which implies that $\|U\| = 1$ for any unitary U.

Postulate 1.3.5. *The evolution of a* closed *quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the closed system at time t_0 is related to the state $|\psi'\rangle$ of the system at time t_1 by a unitary operator U:*

$$|\psi'\rangle = U|\psi\rangle$$

During a computation, it could be interesting to initialise new qubits on the fly. The system cannot be seen as evolving unitarily in this case, since one would end up with more qubits than at the start. Instead, this can be modelled as making the system undergo an *isometry*.

⌜ **Definition 1.3.6** (Isometry)**:** An isometry $f : \mathcal{H}_1 \to \mathcal{H}_2$ is a linear map such that $\forall x, y,\ \langle fx \,|\, fx\rangle = \langle x \,|\, x\rangle$, or equivalently, such that $f^\dagger \circ f = id$. ⌟

Notice that if f is an isometry, then in general $f^\dagger$ is not. For instance $|0\rangle$ is an isometry: $\langle 0 \,|\, 0\rangle = 1 = id_0$ but clearly not a unitary transformation: $|0\rangle\langle 0| \neq id$.

An interesting set of operators on qubits that is useful to point out is the set of controlled operators (on qubits). Let U be an operator on n qubits. The operator "controlled U", denoted ΛU, is an operator on $n+1$ qubits, uniquely defined as:

$$\Lambda U = |0\rangle\langle 0| \otimes id + |1\rangle\langle 1| \otimes U$$

The first qubit in ΛU is called the control qubit. Indeed, if a classical bit is sent on this qubit, U is applied on the n other qubits iff the control bit is 1. Conversely, if an operator V is such that $V \circ (|0\rangle \otimes id) = |0\rangle \otimes id$ and $V \circ (|1\rangle \otimes id) = |1\rangle \otimes v$, then V is a controlled operator ($V = \Lambda v$).

1.4 Observables and Measurements

Not all quantities in a quantum state can be measured. Those that can be are called observables. For instance, the polarisation of a photon, the spin of an electron, the position and the momentum of a particle are all observables [KDT95, Dir28, CHT05].

Postulate 1.4.1. *The observables of a quantum system are the self-adjoint ($A = A^\dagger$) operators on $\mathcal{H}$.*

A very important set of observables for the qubit case are the Pauli matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Linear combinations of Pauli matrices with the identity and real coefficients ($x_0 id + x_1 X + x_2 Y + x_3 Z$ with $x_i \in \mathbb{R}$) can represent any 2×2 self-adjoint matrix, i.e. they span all the one-qubit observables. Also, the group generated by the Pauli matrices using the composition $\circ$ is called the Pauli group. This group is easily extended to n qubits:

⌜ **Definition 1.4.2** (Pauli Group)**:** The Pauli group G_1 is defined as $G_1 := \langle X, Y, Z\rangle$, the group generated by $(\{X, Y, Z\}, \circ)$. For any $n \in \mathbb{N}^* := \{n \in \mathbb{N} \mid n \neq 0\}$, the Pauli group on n qubits G_n is defined as $G_n := \{O_1 \otimes \cdots \otimes O_n \mid O_i \in G_1\}$. ⌟

Remark 1.4.3. The Pauli matrices of G_1 can be expressed using the Dirac notation:

$$X = \sum_{k\in\{0,1\}} |k \oplus 1\rangle\langle k| \qquad Y = i \sum_{k\in\{0,1\}} (-1)^k |k \oplus 1\rangle\langle k| \qquad Z = \sum_{k\in\{0,1\}} (-1)^k |k\rangle\langle k|$$

where $\oplus$ is the XOR operation.

Then, given an observable, one can perform the measurement of a quantum state, in the following way [NC10]:

Postulate 1.4.4. *Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These operators act on the state space of the system being measured, and satisfy*

$$\sum_m M_m^\dagger M_m = id$$

The index m in M_m refers to the measurement outcome that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ before the measurement then the probability that result m occurs is given by

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$$

and the state collapses to

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}}$$

Notice that the operators $M_m^\dagger M_m$ are observables, since $(M_m^\dagger M_m)^\dagger = M_m^\dagger M_m$.

Example 1.4.5. Consider the measurement of the state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ in the computational basis $(|0\rangle, |1\rangle)$, i.e. with the measurement operators $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Then $p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = (\overline{\alpha}\langle 0| + \overline{\beta}\langle 1|)|0\rangle\langle 0|(\alpha|0\rangle + \beta|1\rangle) = |\alpha|^2$. Similarly, $p(1) = |\beta|^2$.

As explained in the postulate, the quantum state collapses after measurement in a new state that depends on the outcome of the measurement.

Example 1.4.6. Consider a series of two measurements of the same qubit, the first in the diagonal basis $(|+\rangle, |-\rangle)$ and the second in the computational basis $(|0\rangle, |1\rangle)$. After the first measurement, the qubit will either be in the state $|+\rangle := \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ or $|-\rangle := \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, with some probability. However, both $|+\rangle$ and $|-\rangle$ will have probabilities $\frac{1}{2}$ to collapse to state $|0\rangle$ and $\frac{1}{2}$ to collapse to state $|1\rangle$ after the second measurement. Hence, all information has been erased after the two measurements.

We have now presented all the postulates of quantum mechanics, that are valid in finite dimensions as well as in infinite dimensions. In the rest of the thesis, we will only consider finite dimensional systems.

1.5 Non-Isolated Systems

Up to Section 1.3, we had described how a quantum system behaves in the ideal case, when it is isolated. When parts of the system are measured, it is not isolated any more. In particular, when measuring parts of an entangled pure state (as described in Section 1.1), we end up with a state that is not pure any more, but is rather a probabilistic distribution over pure quantum states, called a mixed state. Mixed states can be modelled by density matrices. This requires that the rest of the formalism adapts to this generalisation of quantum states.

⌜ **Definition 1.5.1** (Mixed States)**:** A mixed state ρ is of the form $\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$. The coefficient p_i represents the probability that the system is in the pure state $|\psi_i\rangle$. In order to represent a probability distribution, all the p_i must be non-negative and add up to 1. ⌟

Of course, a pure state $|\psi\rangle$ in this formalism is a particular case of mixed state, and will be represented by $|\psi\rangle\langle\psi|$. Notice that ρ is a Hermitian matrix: $\rho^\dagger = (\sum p_i |\psi_i\rangle\langle\psi_i|)^\dagger = \sum p_i |\psi_i\rangle\langle\psi_i| = \rho$.

A composite system of two mixed states, $\rho_1 = \sum p_i |\psi_i\rangle\langle\psi_i|$ and $\rho_2 = \sum q_j |\phi_j\rangle\langle\phi_j|$, is again the tensor product of the two: $\rho_1 \otimes \rho_2 := \sum p_i q_j |\psi_i\phi_j\rangle\langle\psi_i\phi_j|$.

Pure operators (i.e. operators that map a pure state to another pure state) can still be applied to a mixed state, in the form of a *superoperator*, i.e. a linear operator that maps a linear map to another linear map.

⌜ **Definition 1.5.2:** The pure operator U defines the superoperator $\rho \mapsto U \circ \rho \circ U^\dagger$ for mixed states. ⌟

Notice that the operator preserves the Hermitian structure of the state.

The measurement postulate can be logically extended as follows:

⌜ **Definition 1.5.3:** The expectation value of an observable A for a system in a mixed state $\rho = \sum p_i |\psi_i\rangle\langle\psi_i|$ is given by the weighted sum of inner products: $\sum p_i \langle\psi_i| A |\psi_i\rangle$. ⌟

This value can be computed as being $\mathrm{tr}(A\rho)$, where tr is the trace operator. The trace operator is complex-valued and linear. It has the property that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ whenever AB and BA are square matrices, and if id is the identity in $\mathcal{H}$, then $\mathrm{tr}(id) = \dim(\mathcal{H})$.

$$\begin{aligned}\sum p_i \langle\psi_i| A |\psi_i\rangle &= \mathrm{tr}\left(\sum p_i \langle\psi_i| A |\psi_i\rangle\right) = \sum p_i \,\mathrm{tr}\left(\langle\psi_i| A\psi_i\rangle\right) \\ &= \sum p_i \,\mathrm{tr}\left(|A\psi_i\rangle\langle\psi_i|\right) = \mathrm{tr}\left(A\left(\sum p_i |\psi_i\rangle\langle\psi_i|\right)\right) = \mathrm{tr}(A\rho)\end{aligned}$$

This time, the trace can be expressed as a superoperator, using the Dirac notation. Given (x_i) an orthonormal basis of the considered finite Hilbert space:

$$\mathrm{tr} = \rho \mapsto \sum \langle x_i| \rho |x_i\rangle$$

It is possible to trace out only part of the system. If $\mathcal{H} = \mathcal{H}_{A\otimes B\otimes C}$, then tr_B is defined on $\mathcal{H}$ as $id_A \otimes \mathrm{tr} \otimes id_C$ where id_A and id_C are identities in respectively A and C. tr_B traces out the subsystem B. It is called *partial trace* [NC10].

Given a mixed state, it is always possible to see it a pure state that underwent a partial trace.

Theorem 1.5.4 (Purification). *Let $\rho : \mathcal{H}_A \to \mathcal{H}_A$ be a mixed state. Then, there exists a Hilbert space $\mathcal{H}_B$ and a pure state $|\psi\rangle \in \mathcal{H}_{A\otimes B}$ such that $\rho = \mathrm{tr}_B(|\psi\rangle\langle\psi|)$. We say that $|\psi\rangle$ purifies ρ.*

1.6 Pure Quantum Circuits

Similarly to boolean circuits, quantum circuits were introduced both as a model for the potential physical implementations of quantum processes, as well as a means to reason on said processes.

We give here a presentation of the circuits for pure qubit quantum mechanics. Hence, the maps we are going to represent are unitaries from $\mathcal{H}$ to $\mathcal{H}$ where $\dim(\mathcal{H})$ is a power of 2.

The qubits will be represented as wires, and quantum gates will be applied on them. The operations applied to a quantum state have to be unitary, so some gates usually employed in quantum circuits are derived from reversible boolean circuits, such as the Not gate, the CNot gate and the Toffoli gate. To these are added phase-inducing gates such as the Hadamard gate or the R_Z gate. The usual quantum gates used in quantum circuits are summarised in Table 1.1.

The map $[\![.]\!]$ associates to any quantum gate a linear map from and to Hilbert spaces. The gates can then be composed in parallel or in sequence. The parallel composition corresponds to the tensor product $\otimes$:

$$\left[\!\!\left[\begin{array}{c} \vdots \\ D_1 \\ \vdots \\ D_2 \\ \vdots \end{array} \right]\!\!\right] = [\![\vdots\, D_1 \,\vdots]\!] \otimes [\![\vdots\, D_2 \,\vdots]\!]$$

while the sequential composition corresponds to the usual composition of maps $\circ$:

$$[\![\vdots\, D_1 \,\vdots\, D_2 \,\vdots]\!] = [\![\vdots\, D_2 \,\vdots]\!] \circ [\![\vdots\, D_1 \,\vdots]\!]$$

Notice that all the gates whose names begin with "C" are controlled operators: CNot represents a controlled Not, CZ a controlled $R_Z(\pi)$, CCNot a controlled controlled Not (that is an operator that controls CNot), and CSwap a controlled Swap.

All these gates and the two compositions are used to represent unitaries. However, one can extend the formalism with qubit initialisations. Here, some qubits can be given the value $|0\rangle$ at the beginning of the computation. We represent it as $|0\rangle$—, with interpretation $[\![|0\rangle\text{—}]\!] = |0\rangle$. Notice that other states can be obtained by composition of $|0\rangle$ and unitary gates. For instance, $|+\rangle$ can be obtained with $|0\rangle$–H–, while the EPR pair (seen in Section 1.2) can be constructed with the following circuit:

$$\begin{array}{l} |0\rangle\text{–}H\text{–}\bullet\text{–} \\ |0\rangle\text{———}\oplus\text{–} \end{array}$$

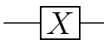
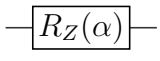
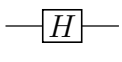
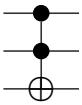
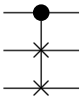
Gate	Representation	Interpretation $[\![.]\!]$
Identity		$\sum_{x\in\{0,1\}} \|x\rangle\langle x\|$
X, Not		$\sum_{x\in\{0,1\}} \|x\oplus 1\rangle\langle x\|$
Z-rotation, R_Z		$\sum_{x\in\{0,1\}} e^{ix\alpha} \|x\rangle\langle x\|$
Hadamard, H		$\frac{1}{\sqrt{2}} \sum_{x,y\in\{0,1\}} (-1)^{xy} \|x\rangle\langle y\|$
Swap		$\sum_{x,y\in\{0,1\}} \|y\ x\rangle\langle x\ y\|$
CNot, CX		$\sum_{x,y\in\{0,1\}} \|x\ x\oplus y\rangle\langle x\ y\|$
CZ		$\sum_{x,y\in\{0,1\}} (-1)^{xy} \|x\ y\rangle\langle x\ y\|$
Toffoli, CCNot		$\sum_{x,y,z\in\{0,1\}} \|x\ y\ xy\oplus z\rangle\langle x\ y\ z\|$
Fredkin, CSwap		$\sum_{x,y,z\in\{0,1\}} \|x\ x(y\oplus z)\oplus y\ x(y\oplus z)\oplus z\rangle\langle x\ y\ z\|$

Table 1.1: The usual gates for quantum circuits.

As already noticed, using qubit initialisation allows one to represent not only unitary transformations but actually isometries.

Now back to the unitary transformations. All the gates in Table 1.1 (with the two compositions) are enough to represent any unitary $f : \mathcal{H} \to \mathcal{H}$ (where $\dim(\mathcal{H})$ is a power of two).

⌜ **Definition 1.6.1** (Universality)**:** A set of gates sufficient to represent any unitary is called *universal*. A set of gates that can approximate any unitary with arbitrary precision is called *approximately universal*.

In other words, a set of gates S is universal if, for any unitary U, there exists a circuit D composed only of gates of S such that $U = [\![D]\!]$. S is approximately universal if, for any unitary U and any $\epsilon > 0$ there exists a circuit D composed of gates of S and such that $\|U - [\![D]\!]\| \leq \epsilon$. ⌟

Actually, the set of gates in Table 1.1 is more than you need to get the universality. Indeed, the gate set (CNot, R_Z, H) is universal [NC10]. Notice that the gate R_Z is parametrised by an angle α which can take values in $\mathbb{R}$. Hence, there is actually an infinite number of gates in the gate set.

One can restrict these angles. For instance, by only allowing rotations of angle $\frac{\pi}{2}$, one gets the gate set (CNot, $R_Z(\frac{\pi}{2})$, H), also called Clifford, for it exactly represents the

Clifford group, defined as:

⌜ **Definition 1.6.2** (Clifford group, Stabiliser group)**:** The Clifford group, also called stabiliser group, is the set of unitaries that stabilise the Pauli group:

$$C_n := \{f : \mathcal{H} \to \mathcal{H} \mid \forall x \in G_n,\ f \circ x \circ f^\dagger \in G_n,\ ff^\dagger = f^\dagger f = id\}$$

where $\mathcal{H} := \mathbb{C}^{2^n}$. ⌟

However, the Clifford group is not universal, even approximately, and can be efficiently simulated on a classical computer [AG04].

There is an in-between, though. There exist finite sets of gates that are approximately universal. For instance, the gate set (CNot, $R_Z(\frac{\pi}{4})$, H) [Shi03]. The gate $R_Z(\frac{\pi}{4})$ is often referred to as the T gate. Since $T^2 := T \circ T = R_Z(\frac{\pi}{2})$, one can see this new gate set as the Clifford gate set to which the T gate has been added. As such, it is commonly referred to as Clifford+T.

There exist other interesting universal gate sets. For instance, the Toffoli gate (with ancillae) is already universal for reversible boolean circuits, and it so happens that adding any basis-changing single-qubit real gate (e.g. Hadamard) to Toffoli makes the resulting gate set approximately universal for *encoded* quantum computing [Shi03]. This new notion of encoded (approximate) universality is slightly different from the one defined in Definition 1.6.1, in that there is an encoding of data in the usual framework (complex numbers), in a less expressive setting (here the real numbers).

1.7 Encoding

In [Aha03], it is shown how to encode a complex quantum state with a real quantum state. Any quantum state $|\psi\rangle$ can be decomposed as its real and imaginary parts $|\psi\rangle = |\psi_\Re\rangle + i\,|\psi_\Im\rangle$ with respect to the computational basis. We can then embed this in a larger real quantum state $|\psi_{\text{enc}}\rangle := |\psi_\Re\rangle \otimes |0\rangle + |\psi_\Im\rangle \otimes |1\rangle$.

This can also be done for operators, where $U := U_\Re + iU_\Im$ is encoded in $U_{\text{enc}} := U_\Re \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + U_\Im \otimes (|1\rangle\langle 0| - |0\rangle\langle 1|)$. It is then shown that (Toffoli, H) represent exactly the encoded versions of a complex approximately universal gate set, namely ($\Lambda R_Z(\frac{\pi}{2})$, H), and hence encodes it.

This idea of encoding data of a certain type (actually a ring) with data of a more restrictive type (a smaller ring) can be generalised. In the following, we restrict to the finite dimensional case.

⌜ **Definition 1.7.1** (Linear Maps over a Ring)**:** Let R be a subring of $\mathbb{C}$. We denote $\mathcal{M}_{n,m}(R)$ the set of linear maps from R^n to R^m for $n, m \in \mathbb{N}$. Any element of $\mathcal{M}_{n,m}(R)$ can be represented as a matrix over the ring R. ⌟

Now we can give a definition of an encoding:

⌜ **Definition 1.7.2:** Let $R_1 \subseteq R_2$ be two subrings of $\mathbb{C}$. We say that R_1 encodes R_2 if there exists a homomorphism $\psi : R_2 \to \mathcal{M}_{n,n}(R_1)$ (called the encoding) with a left inverse Θ, i.e. $\Theta \circ \psi = id$ (called the decoding). ⌟

The homomorphism ψ, even though defined only on R_2, extends naturally to a family of homomorphisms $\psi_{mp} : \mathcal{M}_{m,p}(R_2) \to \mathcal{M}_{mn,pn}(R_1)$. This amounts to replacing every component c in $M \in \mathcal{M}_{m,p}(R_2)$ by the $n \times n$ matrix $\psi(c)$.

Even though the encoding is defined on rings, we will extensively use fields for intermediate results.

A common occurrence of an encoding is when the second ring is an algebraic extension of the first one. Let R be a subring of $\mathbb{C}$, and α be an R-algebraic integer: We denote $P_\alpha \in R[X]$ the smallest monic (its leading coefficient is 1) polynomial such that $P_\alpha(\alpha) = 0$. We denote d_α the degree of the polynomial P_α. R_2 here is $R[\alpha]$, that is, the smallest ring containing both R and α.

Let K be the smallest field containing R. Then it is well known that $K[\alpha]$ is also a field. $K[\alpha]$ can be seen as a vector space over K of dimension d_α, where $(\alpha^i)_{0 \leq i < d_\alpha}$ constitutes a basis, i.e. any element x of $K[\alpha]$ can be expressed as a linear combination of powers of α, with coefficients in K.

For all $x \in K[\alpha]$, we define $\psi_0(x) = (y \mapsto xy)^T$. The map $y \mapsto xy$ being linear, it can be represented as a $d_\alpha \times d_\alpha$ matrix, and can be transposed. The transpose does not change much, it merely makes the decoding part more natural (see the example below). The map $\psi_0(1)$ is obviously the identity matrix. More interestingly,

$$\psi_0(\alpha) = M := \begin{pmatrix} 0 & 1 & & \\ & & \ddots & \\ & & & 1 \\ a_0 & a_1 & \cdots & a_{d_\alpha\text{-}1} \end{pmatrix}$$

where $P_\alpha(X) = X^{d_\alpha} - \sum_{k=0}^{d_\alpha - 1} a_k X^k$.

Lemma 1.7.3. *ψ_0 is a homomorphism, i.e. for any $x, y \in K[\alpha]$, $\psi_0(x+y) = \psi_0(x)+\psi_0(y)$ and $\psi_0(xy) = \psi_0(x) \circ \psi_0(y)$.*

One first consequence of this lemma is that $\psi_0(\alpha^k) = \psi_0(\alpha)^k = M^k$.

Lemma 1.7.4. *Any $x \in K[\alpha]$ can be uniquely written $x = \sum_{k=0}^{d_\alpha - 1} x_k \alpha^k$ with $x_k \in K$.*

Together, the last two lemmas imply that any element $x = \sum_{k=0}^{d_\alpha - 1} x_k \alpha^k$ of $K[\alpha]$ maps to $\psi_0(x) = \sum_{k=0}^{d_\alpha - 1} x_k M^k$.

Let us now show that ψ_0 has a left inverse Θ_0. First, notice that, inductively, $M^k = \begin{pmatrix} 0_{(d_\alpha\text{-}k)\times k} & I_{d_\alpha\text{-}k} \\ A_k & B_k \end{pmatrix}$, where $0_{(d_\alpha\text{-}k)\times k}$ is the zero matrix of dimension $(d_\alpha\text{-}k) \times k$, and A_k and B_k are not important. Hence, $e_0^T M^k = e_k^T$ where e_k is the vector where the sole non null component is component k, which is 1. Let us denote θ the vector $\theta := \sum_{k=0}^{d_\alpha - 1} \alpha^k e_k$.

Then, for all $x = \sum_{k=0}^{d_\alpha - 1} x_k \alpha^k \in K[\alpha]$:

$$e_0^T \psi_0(x)\theta = e_0^T \psi_0 \left(\sum_{k=0}^{d_\alpha - 1} x_k \alpha^k \right) \theta = \sum_{k=0}^{d_\alpha - 1} x_k e_0^T M^k \theta = \sum_{k=0}^{d_\alpha - 1} x_k e_k^T \theta = \sum_{k=0}^{d_\alpha - 1} x_k \alpha^k = x$$

$\Theta_0 := X \mapsto e_0^T X \theta$ is then a left inverse of ψ_0, in the sense that $\Theta_0 \circ \psi_0 = id$.

These results can be generalised to $\mathcal{M}(K[\alpha])$ in the following way. Any X in $\mathcal{M}(K[\alpha])$ can be written $X = \sum_{k=0}^{d_\alpha - 1} X_k \alpha^k$ where $X_k \in \mathcal{M}(K)$. We define

$$\psi : \sum_{k=0}^{d_\alpha - 1} X_k \alpha^k \mapsto \sum_{k=0}^{d_\alpha - 1} X_k \otimes M^k$$

Again, ψ is a homomorphism, and it has a left inverse Θ, defined as

$$\Theta : X \mapsto (I \otimes e_0^T) \circ X \circ (I \otimes \theta)$$

where I are identity matrices of adequate dimension.

Actually, we have a slightly stronger result:

Lemma 1.7.5. *For any element $X \in \mathcal{M}(K[\alpha])$, we have $\psi(X) \circ (I \otimes \theta) = X \otimes \theta$.*

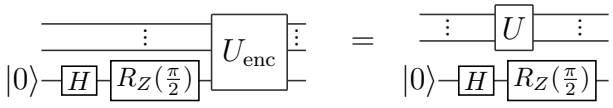
It is pretty obvious that restricting ψ to $\mathcal{M}(R[\alpha])$, and Θ accordingly, the results hold, and ψ becomes an encoding, with decoding Θ. Hence, $\mathcal{M}(R[\alpha])$ can be encoded by $\mathcal{M}(R)$.

Example 1.7.6. $\mathbb{C}$ can be encoded by $\mathbb{R}$, since $\mathbb{C} = \mathbb{R}[i]$. The encoding ψ is:

$$\psi : A + iB \mapsto A \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + B \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

since i is a root of $X^2 + 1$. We recover the transpose of the encoding defined in [Aha03] and presented at the beginning of the section. θ is given by $\theta = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$.

In terms of circuits, we have $\psi\left(\begin{array}{c}\vdots\\ \boxed{U}\\ \vdots\end{array}\right) = \begin{array}{c}\vdots\\ \boxed{U_{\text{enc}}}\\ \vdots\end{array}$ and Lemma 1.7.5 translates as:



Hence we can recover U from U_{enc} by applying the appropriate state on the additional qubits, and then discarding them. This is the reason why we used the transpose in the definition of ψ_0.

This shows how the gate set (Toffoli, H), which can only represent real quantum evolutions, can have encoded approximate universality.

Chapter 2

Categorical Quantum Mechanics

Categorical Quantum Mechanics was introduced in 2004 by Samson Abramsky and Bob Coecke [AC04, AC09]. The purpose of Category Theory is to study "universal" properties and constructions, i.e. that only depend on the structure – the category – and not on the particular elements (objects and arrows) inside the category. Hence, the aim of Categorical Quantum Mechanics is to reveal the fundamental structures of quantum mechanics and quantum computation, as well as to provide powerful tools for the study and development of quantum information technologies.

In this chapter we describe some usual notions in category theory [ML13, BW95]. We then present results of categorical quantum mechanics, as well as the state of the art of the ZX and ZW Calculi at the beginning of the thesis.

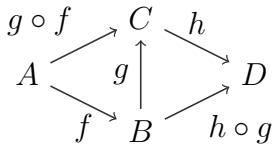
2.1 Categories

⌜ **Definition 2.1.1** (Category)**:** A *category* consists of a collection of *objects* and *arrows* between objects, with a binary operator $\circ$ between some arrows. Let f be an arrow from A to B. We may write $f : A \to B$ or $A \xrightarrow{f} B$. A is called the *domain* of f, and B its *codomain*. To qualify for being a category, the following axioms must be met:

- The operator $. \circ .$ maps any pair of arrows $(B \xrightarrow{g} C, A \xrightarrow{f} B)$ (notice that the domain of g and the codomain of f coincide) to a third arrow $g \circ f : A \to C$ called their composite.
- For any object A in the category, there exists an arrow $id_A : A \to A$, called the *identity* on A, such that:
  - $\forall A \xrightarrow{f} B,\ f \circ id_A = f$
  - $\forall B \xrightarrow{g} A,\ id_A \circ g = g$
- The composition is associative: in the configuration $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, we have $(h \circ g) \circ f = h \circ (g \circ f)$. ⌟

Example 2.1.2. Taking sets as objects and functions between sets as arrows forms a category, named **Set**.

When reasoning about categories, it is customary to draw diagrams, that is, oriented graphs where the vertices are objects and edges are arrows. A diagram is said to be commutative if, for any pair of vertices a and b, any two directed paths from a to b are equal. For instance, the associativity of $\circ$ can be stated as saying that the following diagram commutes:



Arrows in a category will be referred to as morphisms. We can define the collection of morphisms between two objects in a category: $\mathrm{Hom}_{\mathbf{C}}(A, B)$ or $\mathbf{C}[A, B]$.

It may be useful to define the collection of objects of a category $\mathbf{C}$: $\mathrm{Ob}(\mathbf{C})$. Also, the collection of arrows of $\mathbf{C}$ is referred to as $\mathrm{Ar}(\mathbf{C})$.

Arrows that have a left and right inverse are of particular interest.

⌜ **Definition 2.1.3** (Isomorphism)**:** Let $\mathbf{C}$ be a category, and $A, B \in \mathrm{Ob}(\mathbf{C})$. If $f : A \to B$ and $g : B \to A$ are such that $g \circ f = id_A$ and $f \circ g = id_B$, then f and g are *isomorphisms*, g is an *inverse* of f (and vice-versa). Both f and g can be called *invertible*, and A and B are said to be *isomorphic*. g can be written f^{-1}. ⌟

Notice that for any object A of a category, id_A is an isomorphism.

To more easily define some concepts, it is customary to introduce the product category and the dual of a category.

⌜ **Definition 2.1.4** (Product Category)**:** Let $\mathbf{C}$ and $\mathbf{D}$ be two categories. The *product category* $\mathbf{C} \times \mathbf{D}$ is the category where:

- Objects are ordered pairs (A, B) with A an object of $\mathbf{C}$ and B an object of $\mathbf{D}$.
- Morphisms are ordered pairs $(f : A \to A', g : B \to B')$ where f is a morphism of $\mathbf{C}$ and g of $\mathbf{D}$.
- Composition is such that $(f, g) \circ (f', g') := (f \circ f', g \circ g')$ whenever it makes sense. ⌟

⌜ **Definition 2.1.5** (Dual of a Category)**:** Let $\mathbf{C}$ be a category. The category $\mathbf{C}^{\mathrm{op}}$, called *dual* or *opposite* category of $\mathbf{C}$, is defined as:

- $\mathrm{Ob}(\mathbf{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathbf{C})$.
- If $f : A \to B$ is in $\mathbf{C}$, then $f^{\mathrm{op}} : B \to A$ is in $\mathbf{C}^{\mathrm{op}}$.
- The composition is such that $g^{\mathrm{op}} \circ f^{\mathrm{op}} := (f \circ g)^{\mathrm{op}}$. ⌟

The dual of a category is basically the category where all the arrows are reversed. Then, some concepts can simply be defined as some other concepts in the dual category (they are dual concepts). For instance, initial and terminal objects:

⌜ **Definition 2.1.6** (Initial and Terminal Objects)**:** An object T of a category $\mathbf{C}$ is called terminal if, for every object A in $\mathbf{C}$, there is exactly one arrow $A \to T$.

An initial object of a category $\mathbf{C}$ is a terminal object in $\mathbf{C}^{\mathrm{op}}$. It is an object which has exactly one arrow to each of the objects of $\mathbf{C}$. ⌟

Notice that the only arrow to a terminal object (resp. from an initial object) is the identity.

If a category has no terminal object, it is possible to construct one (either add a terminal object, or make an object that is already in the category terminal).

⌜ **Definition 2.1.7** (Affine Completion)**:** Let $\mathbf{C}$ be a category with no terminal object. The category $\mathbf{C}^!$, called *affine completion*, is defined as:

- The objects of $\mathbf{C}^!$ are the objects of $\mathbf{C}$ with an (additional) object T.
- All arrows of $\mathbf{C}$ are arrows of $\mathbf{C}^!$.
- For all objects A in $\mathbf{C}^!$, we add an arrow $!_A : A \to T$.
- We impose $!_T = id_T$ and $!_B \circ f = \ !_A$ for all $f : A \to B$. ⌟

This construction makes the object T terminal. Indeed, let $f : A \to T$ be a morphism. We can show that f is necessarily $!_A$:

- If $T \notin \mathrm{Ob}(\mathbf{C})$, then by construction, $!_A$ is the only morphism from A to T, so $f = !_A$.
- If $T \in \mathrm{Ob}(\mathbf{C})$: $f = id_T \circ f = \ !_T \circ f = \ !_A$.

Hence, there is exactly one arrow from any object to T.

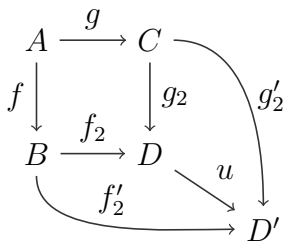
⌜ **Definition 2.1.8** (Pushout)**:** Let f, g be two arrows of a category $\mathbf{C}$ in the configuration $B \xleftarrow{f} A \xrightarrow{g} C$. A pushout of (f, g) is a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{g} & C \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g_2} \\ B & \xrightarrow{f_2} & D \end{array}$$

such that for any other commutative diagram built on (f, g)

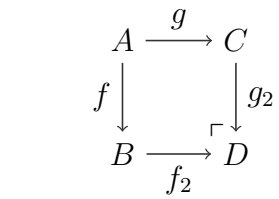
$$\begin{array}{ccc} A & \xrightarrow{g} & C \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g'_2} \\ B & \xrightarrow{f'_2} & D' \end{array}$$

there exists a unique arrow $u : D \to D'$ such that $u \circ g_2 = g'_2$ and $u \circ f_2 = f'_2$ i.e. such that the following diagram commutes:



⌟

The object D in the pushout is uniquely defined up to isomorphism. It may be referred to as the coproduct of B and C over A, and written $B \sqcup_A C$. Also, if a diagram is a pushout, it is customary to signal it with the symbol ⌜ over the coproduct:



If A, B and C are sets in the category $\mathbf{Set}$, let us define the relation R' as:

$$\forall b \in B, c \in C, \quad bR'c \text{ if } \exists a \in A,\ (b = f(a)) \wedge (c = g(a))$$

and let R be the smallest equivalence relation containing R' (i.e. its transitive closure). Then, $B \sqcup_A C$ can be taken to be the disjoint union of B and C, where $b \in B$ and $c \in C$ are identified if bRc.

In particular, if A is the intersection of B and C, and if f and g are the usual inclusions, the pushout can be taken as the union of B and C.

A pullback is the dual of a pushout, i.e. a pullback in a category $\mathbf{C}$ is a pushout in $\mathbf{C}^{\mathrm{op}}$. We will not define the concept further, for we do not need it in the following.

2.2 Functors

So far, we have seen what constitutes a category, as well as some constructions on categories. We will now see how to link different categories together.

A morphism between categories that preserves the structure is called a functor:

⌜ **Definition 2.2.1** (Functor)**:** A functor $F : \mathbf{C} \to \mathbf{D}$ between the categories $\mathbf{C}$ and $\mathbf{D}$ is a map that:

- Assigns to each object A of $\mathbf{C}$ an object $F(A)$ of $\mathbf{D}$
- Assigns to each arrow $A \xrightarrow{f} B$ of $\mathbf{C}$ an arrow $F(A) \xrightarrow{F(f)} F(B)$ of $\mathbf{D}$
- Preserves identities: for each object A of $\mathbf{C}$, $F(id_A) = id_{F(A)}$
- Preserves composition: $F(g \circ f) = F(g) \circ F(f)$ whenever $g \circ f$ is defined in $\mathbf{C}$ ⌟

We call a *bifunctor* a functor from a product category to a category. For instance, $\mathrm{Hom}_{\mathbf{C}}$ actually defines a bifunctor $\mathrm{Hom}_{\mathbf{C}}(\cdot,\cdot) : \mathbf{C}^{\mathrm{op}} \times \mathbf{C} \to \mathbf{Set}$, as follows:

- objects (A, B) of $\mathbf{C}^{\mathrm{op}} \times \mathbf{C}$ i.e. pairs of objects A and B of $\mathbf{C}$ are mapped to $\mathrm{Hom}_{\mathbf{C}}(A, B)$
- morphisms $(f^{\mathrm{op}} : A \to A',\ g : B \to B')$ of $\mathbf{C}^{\mathrm{op}} \times \mathbf{C}$ are mapped to the morphisms $\mathrm{Hom}_{\mathbf{C}}(A, B) \to \mathrm{Hom}_{\mathbf{C}}(A', B') : q \mapsto g \circ q \circ f$

Since we are going in the following to consider several different categories, we will end up using functors a lot to go from one to the other. Two properties of functors we will largely be interested in are fullness and faithfulness:

⌜ **Definition 2.2.2** (Fullness)**:** A functor $F : \mathbf{C} \to \mathbf{D}$ is full if:

$$\forall A, B \in \mathrm{Ob}(\mathbf{C}),\ \forall g : F(A) \to F(B),\ \exists f : A \to B,\ g = F(f)$$ ⌟

This property can be seen as a kind of surjectivity: for any arrow of $\mathbf{D}$ *whose domain and codomain are attained by* F, there exists at least one preimage by F in $\mathbf{C}$. Of course, if B is not attained by F, none of the arrows in $\mathrm{Hom}(A, B)$ and $\mathrm{Hom}(B, C)$ can have a preimage by F, for any objects B and C in $\mathbf{D}$.

⌜ **Definition 2.2.3** (Faithfulness)**:** A functor $F : \mathbf{C} \to \mathbf{D}$ is faithful if:

$$\forall A, B \in \mathrm{Ob}(\mathbf{C}),\ \forall f, g : A \to B,\ F(f) = F(g) \implies f = g$$ ⌟

Again, faithfulness is a bit more subtle than injectivity. Two arrows *between the same objects* are equal in the image of F if and only if they are equal in $\mathbf{C}$. However, it can happen that $f : A \to B$ and $g : C \to D$ are mapped to the same arrow if either $A \neq C$ or $B \neq D$.

⌜ **Definition 2.2.4** (Subcategory)**:** A subcategory $\mathbf{S}$ of the category $\mathbf{C}$ is a category with the same composition $(. \circ .)$, such that all the objects of $\mathbf{S}$ are objects of $\mathbf{C}$ (with the same identities), and that all the arrows of $\mathbf{S}$ are arrows of $\mathbf{C}$. ⌟

There is an obvious functor I from $\mathbf{S}$ to $\mathbf{C}$ which maps the objects and arrows of $\mathbf{S}$ to the same objects and arrows in $\mathbf{C}$, called the inclusion functor. Notice that this functor is necessarily faithful.

Now, suppose we want to consider some categories as objects, and functors between the categories as arrows. We would then end up with a "meta category" (functors can be composed, the composition is associative, and the identity functor exists for any category). Although, one has to be careful when doing so, for we want to avoid the category version of Russell's paradox: should the category of all categories be an object of itself?

To avoid this problem, we only define $\mathbf{Cat}$ as the category of all *small* categories, a small category being a category where both the collections of objects and arrows constitute sets.

Now, interestingly, the constructions of the previous section can be applied to categories of small categories. Indeed, it is sometimes possible to perform the pushout of two functors, or to consider some categories as terminal objects in some larger categories. For instance the category, often denoted $\mathbf{1}$, with a single object 1 and single arrow $id_1 : 1 \to 1$, is a terminal object in the category of categories $\mathbf{Cat}$.

2.3 PROPs

The categories we are going to consider in the next section and in Part II are called PROPs (for **pro**duct and **p**ermutations). These are strict monoidal categories generated by a single object. The reason monoidal categories are interesting for us is that they benefit from a very natural graphical interpretation. In these categories, we have two compositions: the usual composition of categories $\circ$, which performs the sequential composition, and a new composition called *tensor product* and denoted $\otimes$, which performs a kind of parallel composition. In general (for so-called *relaxed* monoidal categories), the tensor product is not directly associative, but only up to isomorphism. We will not consider the relaxed monoidal categories, but only the *strict* monoidal categories, where $\otimes$ really is associative.

⌜ **Definition 2.3.1** (Monoidal Category)**:** A (strict) *monoidal category* $\mathbf{C}$ is a category with additional bifunctor $(.\otimes.) : \mathbf{C}\times\mathbf{C}\to\mathbf{C}$ called tensor product (we may denote $A\otimes B$ the objects of $\mathbf{C}\times\mathbf{C}$), and a particular object I such that:

- $\otimes$ is associative: $(A\otimes B)\otimes C = A\otimes(B\otimes C)$ and $(f\otimes g)\otimes h = f\otimes(g\otimes h)$
- I is the neutral element for $\otimes$: $A\otimes I = I\otimes A = A$
- $(f_2\otimes g_2)\circ(f_1\otimes g_1) = (f_2\circ f_1)\otimes(g_2\circ g_1)$ where the left hand side is defined if the right hand side is

$\mathbf{C}$ is a strict *braided* monoidal category if moreover, for any objects A and B, there is an isomorphism $\sigma_{A,B} : A\otimes B\to B\otimes A$, called *braiding*, such that:

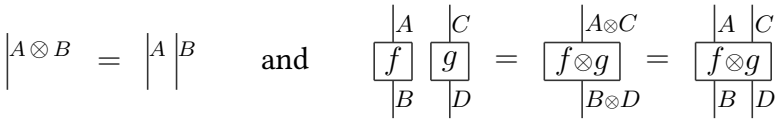
- $\forall f : A\to B, g : C\to D,\ (g\otimes f)\circ\sigma_{A,C} = \sigma_{B,D}\circ(f\otimes g)$
- $\sigma_{A\otimes B,C} = (\sigma_{A,C}\otimes id_B)\circ(id_A\otimes\sigma_{B,C})$
- $\sigma_{A,B\otimes C} = (id_B\otimes\sigma_{A,C})\circ(\sigma_{A,B}\otimes id_C)$

$\mathbf{C}$ is called strict *symmetric* monoidal category if moreover:

- $\forall A, B\in \mathrm{Ob}(\mathbf{C}),\ \sigma_{B,A}\circ\sigma_{A,B} = id_{A\otimes B}$ ⌟

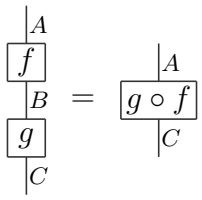
As announced, monoidal categories benefit from a nice graphical presentation, i.e. with *string diagrams* [Sel10]. In string diagrams, objects are represented as wires (with the object variable written as a label on the wires), and morphisms are represented as a distinct symbol with input wires the domain and with output wires the codomain. The generic symbol will simply be a box with the name of the morphism variable. For instance, a morphism $f : A\to B$ can be written:

Notice, first, that we took the convention that the diagrams are read from top to bottom. Secondly, notice that we label wires and boxes by respectively object *variables* and morphism *variables*. This meta-notation allows us to treat for instance $A\otimes B$ as either two objects side by side (which is the string-diagrammatic representation of the tensor product), or as a single object. More generally, we have:

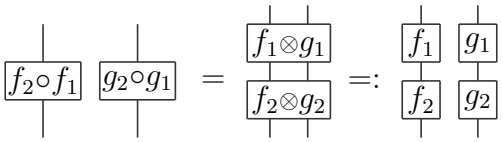


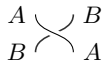
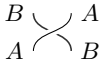
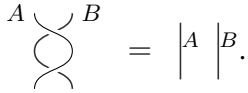
Since I is a neutral element for $\otimes$, one can interpret it as "no wire". I can be seen as the empty space between and around wires. If a morphism $h : I\to A$ has domain I, it can be represented as:

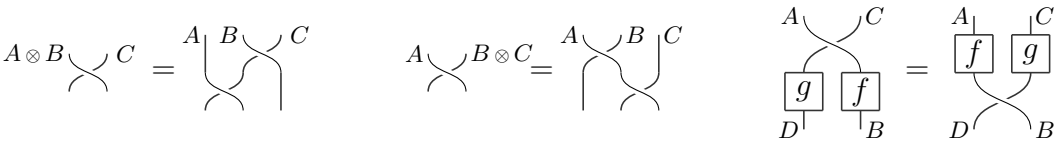
Of course, the composition $\circ$ amounts to plugging two processes if the type matches:

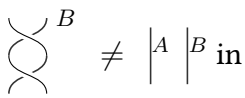
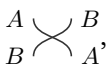
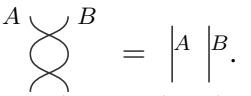


The last axiom of the monoidal category is called the bifunctorial law or interchange law and states that:



In a braided monoidal category, the braiding $\sigma_{A,B}$ is usually represented by  and its inverse $\sigma^{-1}_{A,B}$ by  , so that  . The axioms of the braiding are given by:



Notice however that  in general. When it does, we are precisely in the case of a symmetric monoidal category. In this case, $\sigma_{A,B}$ is represented by  , so that  .

To use the graphical representation for computation, we have to make sure that it does not allow to do less or more than the category itself. This is called coherence and shown in [JS91, Sel10].

Theorem 2.3.2 (Coherence for Monoidal, Braided and Symmetric Categories)**.** *A well-formed equation between morphisms in the language of monoidal (resp. braided monoidal, resp. symmetric monoidal) categories follows from the axioms of monoidal (resp. braided monoidal, resp. symmetric monoidal) categories if and only if it holds, up to planar isotopy (resp. up to isotopy in 3 dimensions, resp. up to isomorphism of diagrams), in the language of string diagrams.*

The graphical language is very interesting for making some axioms obvious. A first example is the interchange law above. We give another example (which actually also uses the interchange law):

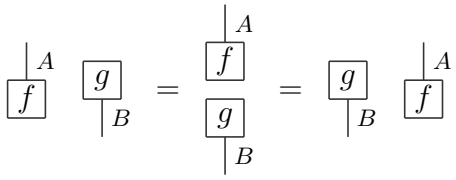
Proposition 2.3.3. *Let* $\mathbf{C}$ *be a monoidal category, and to morphisms* $f : A \to I$ *and* $g : I \to B$*. Then:*

$$f \otimes g = g \circ f = g \otimes f$$

Proof ▶ Using the axioms of monoidal categories, we have:

$$\begin{aligned} f \otimes g &= (id_I \circ f) \otimes (g \circ id_I) = (id_I \otimes g) \circ (f \otimes id_I) \\ &= g \circ f = (g \otimes id_I) \circ (id_I \otimes f) = (g \circ id_I) \otimes (id_I \circ f) \\ &= g \otimes f \end{aligned}$$

Pictorially, thanks to the coherence Theorem 2.3.2, we directly have:



◀

In an arbitrary strict monoidal category, the objects can be very different, so it is important to keep track of the objects on all the wires, to make sure we are not mistyping. This can quickly be cumbersome, although there is a case where this becomes useless: if the strict monoidal category $\mathbf{C}$ is generated by a single object. This is the case for instance in quantum circuits, where the wires can only represent a qubit.

These are, in a sense, the "smallest interesting (non-trivial) monoidal categories". Let us have a glimpse of what they look like. Let $\mathbf{C}$ be such a strict monoidal category. First, as a monoidal category, it has an identity object I. For $\mathbf{C}$ to be non-trivial (since $I \otimes I = I$), it should also have an additional object X. By the axioms of monoidal category, $X \otimes X$ should also be in $\mathbf{C}$. Inductively, $\overbrace{X \otimes \cdots \otimes X}^{n}$ for any $n \in \mathbb{N}^*$ should be in $\mathbf{C}$. We may denote $X^{\otimes n} := \overbrace{X \otimes \cdots \otimes X}^{n}$. Recall that I is "no wire", whereas $X^{\otimes n}$ represents n parallel wires. Hence, it is customary to identify I with $X^{\otimes 0}$. Such a monoidal category, if it is strict symmetric, is called a PROP [Lac04].

⌜ **Definition 2.3.4** (PROP)**:** A PROP is a strict symmetric monoidal category whose objects are freely generated by a single object and $\otimes$.

Equivalently, a PROP can be defined as a strict symmetric monoidal category whose objects are all natural integers $\mathbb{N}$. ⌟

Indeed, it suffices to identify $X^{\otimes n}$ with n. This is made even clearer with the convention that denotes the generating object by 1. Then $n := \overbrace{1 \otimes \cdots \otimes 1}^{n}$, and the morphisms are of the form $f : n \to m$ with $n, m \in \mathbb{N}$. The identity on the object n is denoted id_n. From now on we will not label the wires that represent 1. However, we may still use $\Big|^n$ to represent a bundle of n wires.

Example 2.3.5. The collection of quantum circuits can be seen as a PROP if the Swap gate is allowed and taken to be $\sigma_{1,1}$. For instance, take the gate set (CNot, Swap, H, $R_Z(\alpha)$). The quantum circuits built with it constitute a PROP where the morphisms are CNot : $2 \to 2$, Swap : $2 \to 2$, $H : 1 \to 1$, $R_Z(\alpha) : 1 \to 1$, and all the parallel and sequential compositions of these gates. Notice that stating that it constitutes a PROP gives an equational theory on the circuits. For instance, we have Swap $\circ$ Swap $= id_2$.

We are getting closer to the focus of the thesis, since we can already define a category whose graphical interpretation is a language for quantum mechanics. We can specify even further though. Notice that even though the following definitions are refinements over PROPs, many of the concepts are valid in some more general categories.

⌜ **Definition 2.3.6** (†-PROP)**:** A category $\mathbf{C}$ is a †-PROP if it is a PROP such that for any morphism $f : n \to m$ there exists a morphism $f^\dagger : m \to n$, and such that:

- $id_A^\dagger = id_A$
- $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$
- $(g \otimes f)^\dagger = g^\dagger \otimes f^\dagger$
- $(f^\dagger)^\dagger = f$
- $\sigma_{n,m}^\dagger = \sigma_{m,n}$

Equivalently, $\mathbf{C}$ is a †-PROP if there is a functor $\dagger : \mathbf{C}^{\mathrm{op}} \to \mathbf{C}$, compatible with $\otimes$, which is the identity on the objects and which is an involution, i.e., $\dagger \circ \dagger = id_{\mathbf{C}}$. ⌟

There is now enough background to *categorically* define unitary morphisms, which is in the core of quantum mechanics, as well as self-adjoint morphisms.

⌜ **Definition 2.3.7** (Unitary Morphism)**:** A morphism f in a †-PROP is called *unitary* if it is an isomorphism and if $f^\dagger = f^{-1}$. ⌟

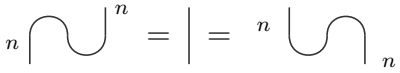
⌜ **Definition 2.3.8** (Self-Adjoint Morphism)**:** A morphism f in a †-PROP is called *self-adjoint* if $f = f^\dagger$. ⌟

The axioms of PROP (or symmetric monoidal category) allow us to move things around, or loosing and straightening wires, but they do not allow us to bend them backwards for instance. If we want to have real freedom on how to move morphisms around, we should be able to perform something like this:  . This is allowed by compact-closed PROPs.

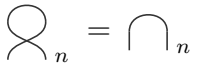
⌜ **Definition 2.3.9** (†-Compact PROP)**:** A compact-closed †-PROP is a †-PROP with two morphisms $\epsilon_n : 2n \to 0$ and $\eta_n : 0 \to 2n$ for each object n, such that:

- $\epsilon_n = \eta_n^\dagger$
- $(id_n \otimes \epsilon_n) \circ (\eta_n \otimes id_n) = id_n = (\epsilon_n \otimes id_n) \circ (id_n \otimes \eta_n)$
- $\sigma_{n,n} \circ \eta_n = \eta_n$
- $\eta_{n+1} = (id \otimes \eta_n \otimes id) \circ \eta_1$ ⌟

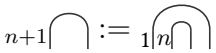
The last three equations are worth stating out using string diagrams. ϵ_n is usually represented as $\cup^{\,n}$ and η_n as $\cap_{\,n}$. The ante-penultimate equation becomes



called the *snake equations*. The penultimate equation becomes



and the last one becomes



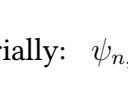
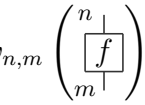
The presence of a compact structure, i.e. two morphisms ϵ_n and η_n that satisfy the snake equations, allow for a very important result, called the *map/state duality*.

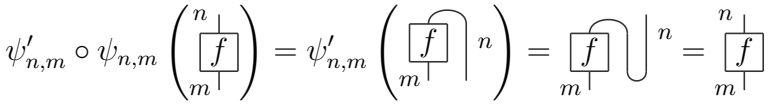
Proposition 2.3.10 (Map/State Duality)**.** *In any †-compact PROP, there exists an isomorphism from $n \to m$ maps to $0 \to n + m$ states.*

Proof ▶ Since we are in a †-compact PROP, there exist two morphisms η_n and ϵ_n for any $n \in \mathbb{N}$, which satisfy the snake equations. Then, for $n, m \in \mathbb{N}$, we define:

$$\begin{array}{rccc} \psi_{n,m} : & \mathrm{Hom}(n,m) & \to & \mathrm{Hom}(0, m+n) \\ & f & \mapsto & (f \otimes id_n) \circ \eta_n \end{array}$$

$$\begin{array}{rccc} \psi'_{n,m} : & \mathrm{Hom}(0, m+n) & \to & \mathrm{Hom}(n,m) \\ & f & \mapsto & (id_m \otimes \epsilon_n) \circ (f \otimes id_n) \end{array}$$

Pictorially: $\psi_{n,m}$  and $\psi'_{n,m}$  . We then check that $\psi_{n,m}$ and $\psi'_{n,m}$ are inverse to each other (i.e. $\psi'_{n,m} = \psi^{-1}_{n,m}$), making them isomorphisms:



for any $f : n \to m$, thanks to snake equations. We similarly have $\psi_{n,m} \circ \psi'_{n,m} = id$. ◀

We now have all the overall structure we need. Before we dive into the different interesting internal structure, we define functors between the different categories we handle.

⌜ **Definition 2.3.11** (PROP Functors)**:** A PROP-functor $F : \mathbf{C} \to \mathbf{D}$ is a functor between PROPs which is compatible with $\otimes$, that is:

- $F(0) = 0$
- $\forall n, m \in \mathbb{N},\ F(n+m) = F(n) + F(m)$
- $\forall f : n \to m, g : p \to q,\ F(f \otimes g) = F(f) \otimes F(g)$
- $F(\sigma_{n,m}) = \sigma_{F(n),F(m)}$

A †-PROP-functor F is a PROP-functor which "commutes" with the †-functor, i.e.:

- $\forall f : n \to m,\ F(f^\dagger) = F(f)^\dagger$

A †-compact-PROP-functor further preserves the compact structure:

- $\forall n \in \mathbb{N},\ F(\eta_n) = \eta_{F(n)}$

⌟

Here, we did not describe how the functor transforms the object 1. In particular, it is not necessary that $F(1) = 1$, as one might want the functor F to act on objects as $F(n) = 2n$ for instance.

2.4 Monoids, Comonoids, and their Interactions

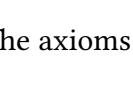
We are now interested in some particular structures that one can have in a PROP. All the structures presented in this section are pretty common in monoidal category theory [ML13]. The simplest are the monoid and its dual, the comonoid.

⌜ **Definition 2.4.1** (Monoid)**:** Let $\mathbf{C}$ be a PROP. A monoid is a pair of morphisms (μ, υ), where $\mu : 2n \to n$ is called *multiplication*, and $\upsilon : 0 \to n$ is called *unit*, and such that:

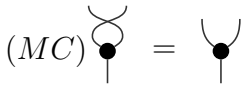
- $\mu \circ (\mu \otimes id_n) = \mu \circ (id_n \otimes \mu)$
- $\mu \circ (\upsilon \otimes id_n) = id_n$
- $\mu \circ (id_n \otimes \upsilon) = id_n$

The monoid is called *commutative* if moreover:

- $\mu \circ \sigma_{n,n} = \mu$ ⌟

With string diagrams, we usually represent the pair (μ, υ) by  . The axioms of a monoid are given by:

and the monoid is commutative if:

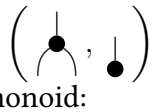


Example 2.4.2. Let $\mathbb{B} := \{\mathsf{true}, \mathsf{false}\}$ be the set of booleans. Let $\mathbf{B}$ be the full monoidal subcategory of $\mathbf{Set}$ generated by $\mathbb{B}$. This constitutes a PROP, where $1 := \mathbb{B}$, and with σ the usual swap of boolean variables: $\forall x, y : 0 \to 1,\ \sigma_1 \circ (x \otimes y) = y \otimes x$. In this PROP, we have in particular two arrows: $\oplus : 2 \to 1$ which is the boolean XOR operation, and $\mathsf{false} : 0 \to 1$ the boolean value false. Then, $(\oplus, \mathsf{false})$ forms a commutative monoid.

Remark 2.4.3. Notice that if $\left[\left(\mu_i : 2n_i \to n_i, \upsilon_i : 0 \to n_i\right)\right]_{1 \leq i \leq n}$ is a list of monoids, then $\left(\mu_1 \otimes \dots \otimes \mu_n : 2\sum n_i \to \sum n_i,\ \upsilon_1 \otimes \dots \otimes \upsilon_n : 0 \to \sum n_i\right)$ is a commutative monoid.

A very important notion for the following is the the monoid in the dual category.

⌜ **Definition 2.4.4** (Comonoid)**:** Let $\mathbf{C}$ be a PROP. A pair of morphisms (ν, τ) forms a *comonoid* if it forms a monoid in $\mathbf{C}^{\mathrm{op}}$. If moreover the monoid is commutative, the comonoid is called *cocommutative*. ⌟

In terms of string diagrams, a pair of morphisms  is a comonoid if they respect the upside-down version of the axioms of a monoid:

Example 2.4.5. In the PROP $\mathbf{B}$ defined in Example 2.4.2, we have two arrows: $\mathrm{copy} : 1 \to 2$ and $\mathrm{discard} : 1 \to 0$, such that

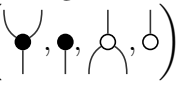
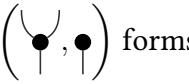
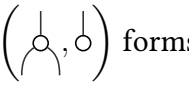
$$\forall x : 0 \to 1, \ \ \mathrm{copy} \circ x = x \otimes x \text{ and } \mathrm{discard} \circ x = id_0$$

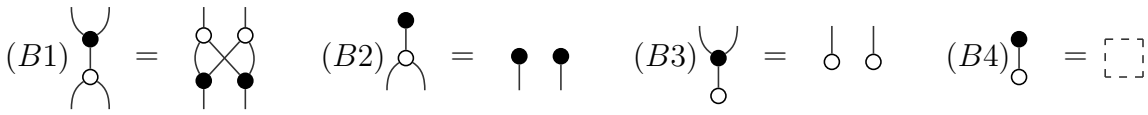
The pair $(\mathrm{copy}, \mathrm{discard})$ forms a cocommutative comonoid.

We now have two very essential structures in a PROP. In the following we are interested in how such structures can interact. The first is when they form a *bialgebra*.

⌜ **Definition 2.4.6** (Bialgebra)**:** A *bialgebra* in a PROP is a quadruple $(\mu, \upsilon, \nu, \tau)$ such that:

- (μ, υ) forms a monoid
- (ν, τ) forms a comonoid
- $\nu \circ \mu = (\mu \otimes \mu) \circ (id \otimes \sigma_{n,n} \otimes id) \circ (\nu \otimes \nu)$
- $\nu \circ \upsilon = \upsilon \otimes \upsilon$
- $\tau \circ \mu = \tau \otimes \tau$
- $\tau \circ \upsilon = id_0$ ⌟

With string diagrams, when they form a bialgebra, it is common to distinguish the monoid and the comonoid by using two different colours. The quadruple  is a bialgebra if  forms a monoid,  forms a comonoid, and:



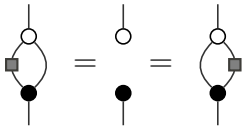
Example 2.4.7. In the PROP $\mathbf{B}$ described in Examples 2.4.2 and 2.4.5, the quadruple $(\oplus, \mathsf{false}, \mathrm{copy}, \mathrm{discard})$ forms a bialgebra. Indeed, xoring two booleans then copying the result is equivalent to copying the two booleans first and then xoring each pair of copies, copying the boolean false results in having two copies of false, xoring two booleans and discarding the result is equivalent to discarding both booleans, and finally, discarding a boolean that was just initialised to false amounts in doing nothing.

Refining further on the bialgebra structure, we get the concept of Hopf algebra.

⌜ **Definition 2.4.8** (Hopf Algebra)**:** A bialgebra $(\mu, \upsilon, \nu, \tau)$ is called a Hopf algebra if there exists $\alpha : n \to n$, called *antipode*, such that:

- $\mu \circ (\alpha \otimes id_n) \circ \nu = \upsilon \circ \tau = \mu \circ (id_n \otimes \alpha) \circ \nu$ ⌟

Using string diagrams, if we represent the antipode α by , then the axiom translates as:

(H) 

Example 2.4.9. The quadruple $(\oplus, \text{false}, \text{copy}, \text{discard})$ forms a Hopf algebra with antipode the identity. Indeed, we already know it forms a bialgebra, and if we xor two copies of the same value, the result is always false.

The other potential interaction of monoids and comonoids is the Frobenius algebra.

⌜ **Definition 2.4.10** (Frobenius Algebra)**:** A (commutative) Frobenius algebra in a PROP is a quadruple $(\mu, \upsilon, \nu, \tau)$ such that:

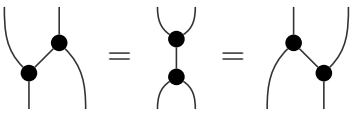
- (μ, υ) forms a (commutative) monoid
- (ν, τ) forms a (cocommutative) comonoid
- $(\mu \otimes id_n) \circ (id_n \otimes \nu) = \nu \circ \mu = (id_n \otimes \mu) \circ (\nu \otimes id_n)$

A Frobenius algebra is called *special* if moreover:

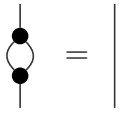
- $\mu \circ \nu = id_n$

In the case where the PROP is a †-PROP, one can define a (special) (commutative) †-Frobenius monoid as a pair (μ, υ) such that $(\mu, \upsilon, \mu^\dagger, \upsilon^\dagger)$ is a (special) (commutative) Frobenius algebra. ⌟

The last two axiom are made clearer when using string diagrams, where the colour is taken to be the same for the monoid and the comonoid (the reason for this is given by Theorem 2.4.17 in the following):

(F) 

and the specialness:

(Fs) 

Example 2.4.11. This time, let $\mathbf{B}'$ be the full sub-PROP of $\mathbf{Rel}$ generated by $\mathbb{B} := \{\text{true}, \text{false}\}$. Its morphisms are binary relations between tensors of $1 := \mathbb{B}$. One morphism of $\mathbf{B}'$ is $\text{copy} : 1 \to 2$ which relates any boolean to two copies of itself, i.e. $\forall x : 0 \to 1,\ (x, x \otimes x) \in \text{copy}$. Together with the morphism $\text{discard} : 1 \to 0$, for which $\forall x :$

$0 \to 1,\ (x, id_0) \in \text{discard}$, they form a comonoid (similarly to their counterparts in **Set**). However, there are two more morphisms in $\mathbf{B}'$, which we will denote respectively by copy^{op} and $\text{discard}^{\text{op}}$, defined by:

$$\forall x : 0 \to 1,\ (x \otimes x, x) \in \text{copy}^{\text{op}} \text{ and } (id_0, x) \in \text{discard}^{\text{op}}$$

The couple $(\text{copy}^{\text{op}}, \text{discard}^{\text{op}})$ forms a monoid, and actually, the tuple:

$$(\text{copy}^{\text{op}}, \text{discard}^{\text{op}}, \text{copy}, \text{discard})$$

forms a Frobenius algebra.

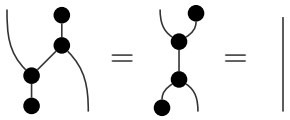
Remark 2.4.12. A commutative Frobenius algebra on object 1 induces a compact structure, that is some $\epsilon_n : 2n \to 0$ and $\eta_n : 0 \to 2n$ that satisfy the axioms $(id_n \otimes \epsilon_n) \circ (\eta_n \otimes id_n) = id_n = (\epsilon_n \otimes id_n) \circ (id_n \otimes \eta_n)$ and $\sigma_{n,n} \circ \eta_n = \eta_n$. Define for instance ϵ_n inductively as:

$\epsilon_1 := \tau \circ \mu$ i.e.  and $\epsilon_n := \epsilon_1 \circ (id \otimes \epsilon_{n-1} \otimes id)$

and similarly η_n as:

$\eta_1 := \nu \circ \upsilon$ i.e.  and $\eta_n := (id \otimes \eta_{n-1} \otimes id) \circ \eta_n$

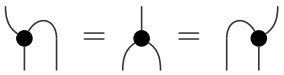
The axiom $\sigma_{n,n} \circ \eta_n = \eta_n$ is obviously satisfied by cocommutativity of ν. The axiom $id = (\epsilon_1 \otimes id) \circ (id \otimes \eta_1)$ is satisfied:



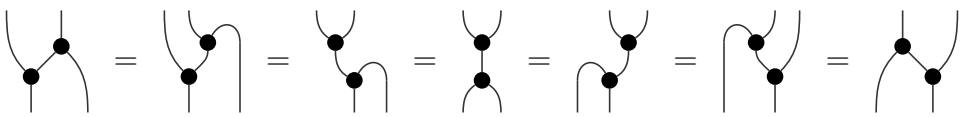
Similarly, the axiom $(id \otimes \epsilon_1) \circ (\eta_1 \otimes id) = id$ is satisfied. It is then routine to show that the generalised axiom $(id_n \otimes \epsilon_n) \circ (\eta_n \otimes id_n) = id_n = (\epsilon_n \otimes id_n) \circ (id_n \otimes \eta_n)$ is also satisfied.

Conversely, we can suppose we have a compact structure that reacts well with our multiplication and comultiplication, and see what we can get from here:

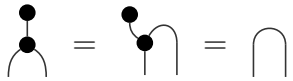
Remark 2.4.13. Suppose we have a monoid $(\mu : 2 \to 1, \upsilon : 0 \to 1)$, and there exists $\nu : 1 \to 2$ and $\eta : 0 \to 2$ (represented by $\frown$) such that:

$(\mu \otimes id) \circ (id \otimes \eta) = \nu = (id \otimes \mu) \circ (\eta \otimes id)$ i.e. 

Notice that so far, the only assumptions on ν are that it is a $1 \to 2$ morphism, and that it satisfies the two equations just above. Then the Frobenius axioms can be deduced from associativity of (μ, υ):



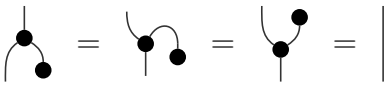
We can even show that $\eta = \nu \circ \upsilon$:



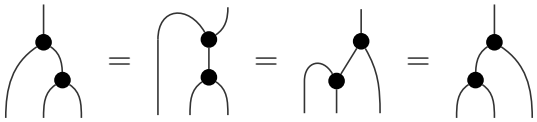
However we do not have a Frobenius algebra, for there is no counit (and hence no comonoid). This can be patched if there exists $\tau : 1 \to 0$ such that:

$$(\tau \otimes id) \circ \eta = \upsilon = (id \otimes \tau) \circ \eta \qquad \text{i.e.}$$

Then:

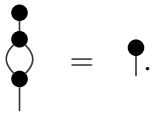


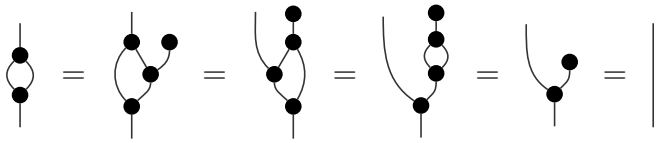
And similarly for the left counit. Coassociativity can be obtained thanks to:



Also, thanks to the previous remark, we can build a morphism $\epsilon : 2 \to 0$ such that it forms a compact structure together with η.

This shows how closely related associativity and the Frobenius axioms are.

Remark 2.4.14. A Frobenius algebra is special iff  $=$. Indeed, if the algebra is special, this equation is obvious, but we can also recover specialness from it:

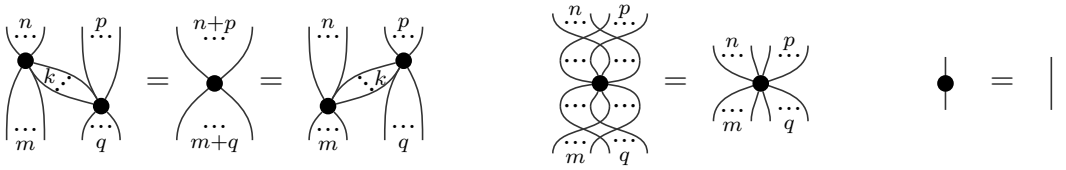


When working with a special commutative Frobenius algebra in a PROP – which is a strict monoidal category –, it is tempting to do some simplifications.

⌜ **Definition 2.4.15** (Spider)**:** In a PROP, the family $(s^{(n,m)} : n \to m)_{n,m \in \mathbb{N}}$ is called a *spider* if:

- $\forall k \geq 1,\ (id_m \otimes s^{(k+p,q)}) \circ (s^{(n,m+k)} \otimes id_p) = s^{(n+p,m+q)}$
- $\forall k \geq 1,\ (s^{(n+k,m)} \otimes id_q) \circ (id_n \otimes s^{(p,k+q)}) = s^{(n+p,m+q)}$
- $\sigma_{q,m} \circ s^{(p+n,q+m)} \circ \sigma_{n,p} = s^{(n+p,m+q)}$
- $s^{(1,1)} = id$ ⌟

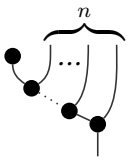
In string diagrams representation, if $s^{(n,m)}$ is represented by  , then, for $k \geq 1$:



It so happens that the spiders capture the special commutative Frobenius algebras, as spelt out in [Lac04] and graphically in [CP08].

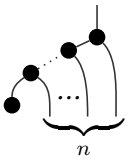
Proposition 2.4.16 (Normal Form). *Let μ_n be inductively defined as:*

$$\mu_0 = \upsilon, \qquad \mu_n = \mu \circ (\mu_{n-1} \otimes id) \qquad \textit{i.e.} \quad \mu_n =$$



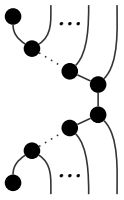
Similarly, ν_n is inductively defined as:

$$\nu_0 = \tau, \qquad \nu_n = (\nu_{n-1} \otimes id) \circ \nu \qquad \textit{i.e.} \quad \nu_n =$$



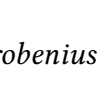
If $f : n \to m$ is a morphism generated from the special commutative Frobenius algebra $(\mu, \upsilon, \nu, \tau)$, and the symmetric monoidal structure maps $\sigma_{n,m}$, and if the graphical representation of f is connected, then we have:

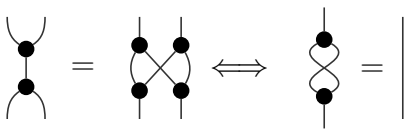
$$f = \nu_m \circ \mu_n \qquad \textit{i.e.} \quad f =$$



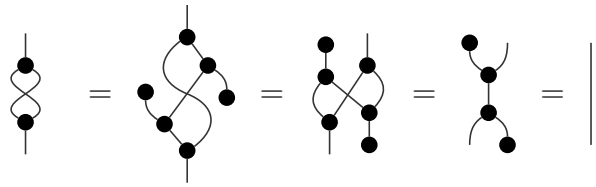
Theorem 2.4.17 (Spider $\leftrightarrow$ Special Commutative Frobenius Algebra).
The family $(\nu_m \circ \mu_n)_{n,m \in \mathbb{N}}$ forms a spider family. Conversely, given a spider family $(s^{(n,m)} : n \to m)_{n,m \in \mathbb{N}}$, the quadruple $(s^{(2,1)}, s^{(0,1)}, s^{(1,2)}, s^{(1,0)})$ forms a special commutative Frobenius algebra.

The axioms of a Frobenius algebra can be more powerful than $(B1)$. Under the right assumption, the axioms of Frobenius algebras implies $(B1)$:

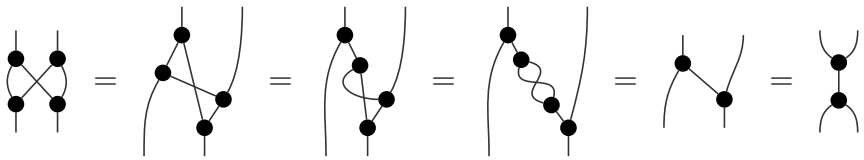
Proposition 2.4.18. *In a Frobenius algebra*  :



Proof ▶ [⇒]:



[⇐]:



◀

Notice that any special commutative Frobenius algebra meets the previous conditions, but it was already known from Theorem 2.4.17.

2.5 PROPs for Quantum Mechanics

It is now time to apply the introduced notions to quantum mechanics. In [AC09], the framework of choice was the †-compact PROPs. This follows from the observation that the Hilbert spaces of dimension the powers of some d and linear maps form a †-compact PROP.

⌜ **Definition 2.5.1 (FdHilb):** We define **FdHilb** as the monoidal category of finite dimensional Hilbert spaces. Its objects are $\mathbb{C}^n$ and its arrows are linear maps. The object $\mathbb{C}^n \otimes \mathbb{C}^m$ can be seen as $\mathbb{C}^{nm}$, and if $f = \sum a_i \left|x_i\right\rangle\!\left\langle y_i\right|$ and $g = \sum b_i \left|x'_i\right\rangle\!\left\langle y'_i\right|$ then $f \otimes g := \sum a_i b_j \left|x_i x'_j\right\rangle\!\left\langle y_i y'_j\right|$. ⌟

This monoidal category is symmetric: for any $n, m \in \mathbb{N}$, $\sigma_{\mathbb{C}^n,\mathbb{C}^m} := \sum_{\substack{i\in\{0,\dots,n-1\}\\ j\in\{0,\dots,m-1\}}} \left|ji\right\rangle\!\left\langle ij\right|$ are such that $\sigma_{\mathbb{C}^n,\mathbb{C}^m} \circ \sigma_{\mathbb{C}^m,\mathbb{C}^n} = id_{\mathbb{C}^{nm}}$.

This serves as the framework for the categories where the dimension of the Hilbert spaces are the powers of a single integer d.

⌜ **Definition 2.5.2 (Qudit, Qubit):** For a fixed d, **Qudit** is the subcategory of **FdHilb** restricted to objects of the form $\mathbb{C}^{d^k}$ with $k \in \mathbb{N}$. When $d = 2$, the category is denoted **Qubit**. ⌟

These are of course subcategories of **FdHilb**.

Proposition 2.5.3. **Qudit** *is a †-compact PROP.*

Proof ▶ The objects of the category are $\mathbb{C}^{d^k}$ for $k \in \mathbb{N}$. We denote $k := \mathbb{C}^{d^k}$, so that $n + m$ can be seen as $\mathbb{C}^{d^n} \otimes \mathbb{C}^{d^m}$. Hence, the objects can be seen as generated by $\mathbb{C}^d$. Let us also denote $B := \{0, \cdots, d-1\}$ so that $\{\left|0\right\rangle, \cdots, \left|d-1\right\rangle\}$ is an orthonormal basis of $\mathbb{C}^d$. The identity on n is given by:

$$id_n := \sum_{x \in B^n} \left|x\right\rangle\!\left\langle x\right|$$

The axioms of strict monoidal category are obviously satisfied. For the category to be symmetric, we need a braiding that is essentially self-inverse. We define $\sigma_{n,m}$ as:

$$\sigma_{n,m} := \sum_{\substack{x\in B^n \\ y\in B^m}} |y\ x\rangle\langle x\ y|$$

Then, if $f = \sum f_{xy}\,|y\rangle\langle x|$ and $g = \sum g_{zw}\,|w\rangle\langle z|$, we get (ignoring some subscripts for simplicity):

$$\begin{aligned}(g\otimes f)\circ\sigma &= \left(\sum f_{xy}g_{zw}\,|w\ y\rangle\langle z\ x|\right)\left(\sum |y\ x\rangle\langle x\ y|\right)\\ &= \sum f_{xy}g_{zw}\,|w\ y\rangle\langle x\ z|\\ &= \left(\sum |y\ x\rangle\langle x\ y|\right)\left(\sum f_{xy}g_{zw}\,|y\ w\rangle\langle x\ z|\right)\\ &= \sigma\circ(f\otimes g)\end{aligned}$$

The other axioms of braided and symmetric monoidal categories are more easily satisfied. It is then routine to show that **Qudit** is a †-PROP if $(\sum f_{xy}\,|y\rangle\langle x|)^\dagger := \sum \overline{f_{xy}}\,|x\rangle\langle y|$.

It remains to prove that **Qudit** is compact-closed. Take $\eta_n := \sum_{x\in B^n} |x\ x\rangle$. ϵ_n is imposed by $\epsilon_n = \eta_n^\dagger = \sum_{x\in B^n} \langle xx|$. The equation $\sigma_{n,n}\circ\eta_n = \eta_n$ is obviously satisfied. The snake equation also is:

$$(id_n\otimes\epsilon_n)\circ(\eta_n\otimes id_n) = \left(\sum_{x,y\in B^n} |x\rangle\langle x\ y\ y|\right)\left(\sum_{z,w\in B^n} |z\ z\ w\rangle\langle w|\right) = \sum_{x\in B^n} |x\rangle\langle x| = id_n$$

and similarly for the second equation. In conclusion, **Qudit** is a †-compact PROP. ◀

We can now discuss the different structures (monoid, Frobenius algebras and †-Frobenius monoids, bialgebras, Hopf algebras) in the category **Qudit**. A first result shows that any commutative †-Frobenius monoid exactly corresponds to an orthonormal basis in **Qudit** [CPV12].

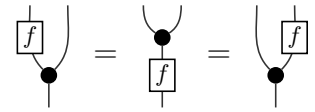
Theorem 2.5.4 (†-Frobenius Monoid ↔ Basis)**.** *Let $(|i\rangle)_{0\leq i<d}$ be an orthonormal basis of $\mathbb{C}^d$, and $\mu := \sum |i\rangle\langle i\ i|$ and $\upsilon := \sum |i\rangle$. Then (μ,υ) forms a special commutative †-Frobenius monoid.*

Conversely, if (μ,υ) forms any special commutative †-Frobenius monoid on object 1, then there exists an orthonormal basis $(|i\rangle)_{0\leq i<d}$ such that $\mu = \sum |i\rangle\langle i\ i|$ and $\upsilon = \sum |i\rangle$.

Hence, using the Spider Theorem 2.4.17, together with Theorem 2.5.4, one can deduce that spider families exactly represent orthonormal bases. We now want to extend the notion of spider family by integrating morphisms that react well with the underlying Frobenius algebra. This will lead to the notion of phase group. It is introduced in [CD11], but we take in the following approach a detour to what we call the diagonal morphisms (also called pre-phase in [DD16]).

⌜ **Definition 2.5.5** (Diagonal Morphisms)**:** Let (μ,υ) be a monoid on object n. A morphism $f : n \to n$ is called diagonal (with respect to (μ,υ)), if:

$$\mu\circ(f\otimes id_n) = f\circ\mu = \mu\circ(id_n\otimes f) \qquad \text{i.e.}$$



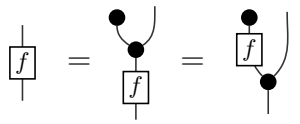
If f is a diagonal morphism that is unitary (i.e. $f \circ f^\dagger = id_n = f^\dagger \circ f$), then f is called a *phase shift.* ⌟

Proposition 2.5.6. *The set of diagonal morphisms (with respect to (μ, υ) on object n) forms a commutative monoid with $\circ$, i.e. for any diagonal morphisms f and g, $f \circ g$ is a diagonal morphism, we have $f \circ g = g \circ f$, id_n is a diagonal morphism, and obviously $f \circ id_n = f = id_n \circ f$ and $\circ$ is associative.*

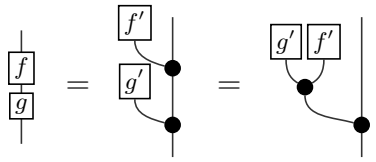
As a consequence, the set of invertible diagonal morphisms forms an abelian group (or commutative group).

The set of phase shifts (with respect to (μ, υ)) forms an abelian group, called phase group.

Proof ▶ First, notice that for any diagonal morphism $f : n \to n$ there is a morphism $f' : 0 \to n$ such that $f = \mu \circ (f' \otimes id_n)$. Indeed:



so $f' = f \circ \upsilon$. Conversely, it is easy to check that for any $f' : 0 \to n$, then $\mu \circ (f' \otimes id_n)$ is a diagonal morphism (by associativity). The identity is obviously a diagonal morphism, which is the neutral element for $\circ$. The composition of two diagonal morphisms is a diagonal morphism:



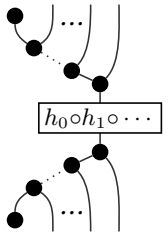
As a result, the set of diagonal morphisms forms a monoid with $\circ$. The monoid is commutative by commutativity of μ. The results for invertible and unitary diagonal morphisms directly follow. ◀

Through this proof, we actually get a characterisation of diagonal morphisms. These are exactly the morphisms that can be expressed as $\mu \circ (f' \otimes id_n)$ for $f' : 0 \to n$.

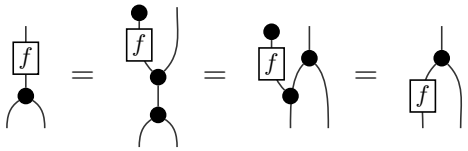
Now, back to the Frobenius algebras, it is fairly easy to see that we can extend the notion of normal form in a special commutative Frobenius algebra.

Corollary 2.5.7. *Let $(\mu, \upsilon, \nu, \tau)$ be a special commutative Frobenius algebra on object 1. If $f : n \to m$ is a morphism generated from the special commutative Frobenius algebra $(\mu, \upsilon, \nu, \tau)$, the set of diagonal morphisms $\{h_i\}_i$ and the symmetric monoidal structure maps $\sigma_{n,m}$, and if the graphical representation of f is connected, then we have:*

$$f = \nu_m \circ \left(\bigcirc_i h_i \right) \circ \mu_n \qquad \textit{i.e.} \quad f =$$



Proof ▶ The only technical point is to prove that if f is a diagonal morphism w.r.t. μ, then it is a "codiagonal morphism" w.r.t. ν:



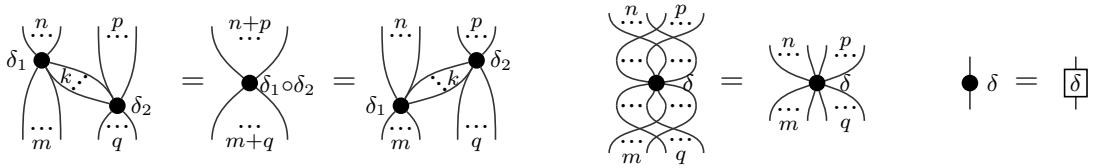
the rest is obvious by application of Proposition 2.4.16 and the axiom of diagonal morphisms and the result of "codiagonal" morphism. ◀

We therefore get a natural extension of the spider families that include diagonal morphisms.

⌜ **Definition 2.5.8** (Extended Spider)**:** Let Δ be the set of diagonal morphisms w.r.t. a monoid (μ, υ) on object 1. The family of morphisms $(s_\delta^{(n,m)} : n \to m)_{\substack{n,m\in\mathbb{N}\\ \delta\in\Delta}}$ is called an extended spider if:

- $\forall k \geq 1,\ (id_m \otimes s_{\delta_2}^{(k+p,q)}) \circ (s_{\delta_1}^{(n,m+k)} \otimes id_p) = s_{\delta_1\circ\delta_2}^{(n+p,m+q)}$
- $\forall k \geq 1,\ (s_{\delta_1}^{(n+k,m)} \otimes id_q) \circ (id_n \otimes s_{\delta_2}^{(p,k+q)}) = s_{\delta_1\circ\delta_2}^{(n+p,m+q)}$
- $\sigma_{q,m} \circ s_\delta^{(p+n,q+m)} \circ \sigma_{n,p} = s_\delta^{(n+p,m+q)}$
- $s_\delta^{(1,1)} = \delta$ ⌟

In string diagram representation, for $k \geq 1$:

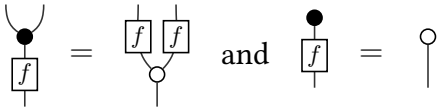


Corollary 2.5.9 (Extended Spider)**.**
The family $(\nu_m \circ \delta \circ \mu_n)_{\substack{n,m\in\mathbb{N}\\ \delta\in\Delta}}$*, where* Δ *is the set of diagonal morphisms w.r.t.* (μ, υ) *on object* 1*, forms an extended spider family.*

Conversely, given Δ *a set of morphisms, and an extended spider family* $(s_\delta^{(n,m)} : n \to m)_{\substack{n,m\in\mathbb{N}\\ \delta\in\Delta}}$*, the quadruple* $(s_{id}^{(2,1)}, s_{id}^{(0,1)}, s_{id}^{(1,2)}, s_{id}^{(1,0)})$ *forms a special commutative Frobenius algebra with* Δ *the set of diagonal morphisms w.r.t.* $(s_{id}^{(2,1)}, s_{id}^{(0,1)})$*.*

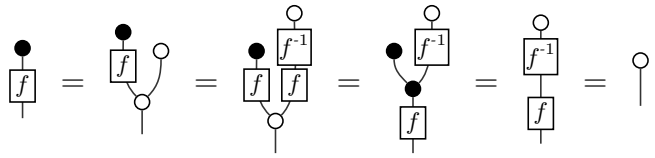
The notion of extended spider was led by a type of morphisms that interact well with a monoid. We give another example of morphisms that interact in a particular way with monoids.

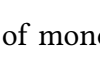
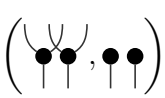
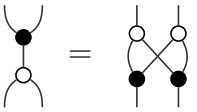
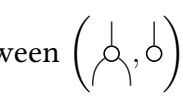
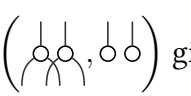
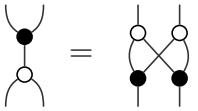
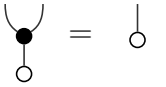
⌜ **Definition 2.5.10** (Morphism of Monoids)**:** Let (μ, υ) and (μ', υ') be two monoids on objects respectively n and m. A morphism $f : n \to m$ is called a morphism of monoids if:

$$f \circ \mu = \mu' \circ (f \otimes f) \quad \text{and} \quad f \circ \upsilon = \upsilon' \qquad \text{i.e.} \quad \text{  }$$

If moreover $n = m$ and $(\mu, \upsilon) = (\mu', \upsilon')$, we call f an endomorphism of monoids. ⌟

Notice that if f is invertible, one can express one monoid entirely as the other monoid together with f and f^{-1}. Moreover, in this case the second equality is provable:



Interestingly, we can recover the definition of bialgebra by means of morphism of monoids. Indeed, stating that  is a morphism of monoids between  and  gives  and  ; while stating that  is a morphism of comonoids between  and  gives  and  . We can recover the last axiom by stating that  is a morphism of monoids between and  .

We know how to characterise an orthonormal basis as a special commutative †-Frobenius monoid, we have defined a family of morphisms that react specifically well with a given orthonormal basis, and we have a compact way to express them by means of spiders. We will show in the next sections how to build two graphical languages for quantum computing: the so-called ZX-Calculus and ZW-Calculus; but before this we want to discuss a particular property that such a language can have, and which is directly related to the algebras explored previously.

2.6 Universality and Completeness

In the following, we are going to define and study *graphical languages* for quantum mechanics. A graphical language $\mathbf{L}$ is a PROP, where the morphisms are string diagrams, and are called *diagrams*.

⌜ **Definition 2.6.1** (Graphical Language)**:** A *graphical language* $\mathbf{L}/R$ is a PROP $\mathbf{L}$ presented by a set of *generators* and a set of *equations* R together with a function $[\![.]\!] : \mathbf{L} \to S$ called the *standard interpretation* of $\mathbf{L}/R$ in S.
$\mathbf{L}/R$ is said to represent S. $\mathbf{L}/R$ is said to be *sound* if $[\![.]\!]$ defines a functor $[\![.]\!] : \mathbf{L}/R \to S$. ⌟

Hence, a graphical language for quantum mechanics if there is a function $[\![.]\!]$ from the language to **Qudit**, which gives to all the diagrams an interpretation as a quantum operator. We always consider that the standard interpretation is the identity on the objects (i.o.o.).

If the language can represent any quantum operator, it is called *universal*.

⌜ **Definition 2.6.2** (Universality)**:** For a fixed d, a graphical language $\mathbf{L}$ for qudits is called *universal* if:

$$\forall f \in \mathbf{Qudit},\ \exists D \in \mathbf{L},\ \ [\![D]\!] = f$$

Equivalently, $\mathbf{L}$ is universal if the functor $\mathbf{L} \xrightarrow{[\![.]\!]} \mathbf{Qudit}$ is full. ⌟

Notice that $\mathbf{L}$ is universal should be equivalent to $[\![.]\!]$ is surjective. However, since the standard interpretation $[\![.]\!]$ is i.o.o., and since $\mathbb{N} = \mathrm{Ob}(\mathbf{L}) = \mathrm{Ob}(\mathbf{Qudit})$ by definition of PROPs, $[\![.]\!]$ is full $\iff$ $[\![.]\!]$ is surjective.

In general, two different morphisms can represent the same quantum operator. This is dealt with by the set R of equalities between diagrams, that can be applied locally. Such a set is called a *monoidal theory* or an *axiomatisation*, and it defines an equivalence relation between morphisms. If D_1 is equivalent to D_2 under this equivalence relation, we may denote $R \vdash D_1 = D_2$, and we have:

- $R \vdash D_1 \otimes D = D_2 \otimes D$
- $R \vdash D \otimes D_1 = D \otimes D_2$
- $R \vdash D_1 \circ D = D_2 \circ D$
- $R \vdash D \circ D_1 = D \circ D_2$

for any diagram D whenever it makes sense.

Obviously, for a given set of generators, different axiomatisations can yield different languages. This is why we denote a graphical language as $\mathbf{L}/R$. This can also be seen as the language obtained by taking the diagrams of $\mathbf{L}$ modulo the equivalence relation R.

The *completeness* is a crucial question for a graphical language.

⌜ **Definition 2.6.3** (Completeness)**:** Let $\mathbf{L}/R$ be a graphical language for quantum mechanics, with standard interpretation $[\![.]\!] : \mathbf{L}/R \to \mathbf{Qudit}$. We say that $\mathbf{L}/R$ is complete if for any two diagrams D_1 and D_2, we have:

$$[\![D_1]\!] = [\![D_2]\!] \implies R \vdash D_1 = D_2$$

Equivalently, the language $\mathbf{L}/R$ is complete if the functor $[\![.]\!]$ is faithful. ⌟

This is fundamental. If the language is complete, then whenever two diagrams represent the same quantum operator, they can be turned into one another solely using the axiomatisation R. It means the language completely captures quantum mechanics, and any computation can be conducted entirely inside the graphical language.

The notion of completeness can be extended to sub-PROPs of $\mathbf{Qudit}$ (i.e. subcategories of $\mathbf{Qudit}$ that are also PROPs). However, one has to be careful that some of these sub-PROPs do not allow approximate universality.

⌜ **Definition 2.6.4** (Approximately Universal Sub-PROP)**:**
Let $\mathbf{C}$ be a sub-PROP of $\mathbf{Qudit}$. $\mathbf{C}$ is approximately universal if:

$$\forall f : n \to m \in \mathbf{Qudit},\ \exists (g_p : n \to m)_{p \in \mathbb{N}} \in \mathbf{C}^{\mathbb{N}},$$
$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \ (p \geq N) \implies (\|f - \iota(g_p)\| < \varepsilon)$$

where $\iota : \mathbf{C} \to \mathbf{Qudit}$ is the inclusion functor, and with $\|.\|$ defined in Section 1.3. In other word, $\mathbf{C}$ is approximately universal if its morphisms can approach any morphism of $\mathbf{Qudit}$ with arbitrary precision. ⌟

This is permitted because the arrows of $\mathbf{Qudit}$ form a topological space.

In the thesis, we will mainly be interested in the category $\mathbf{Qubit}$ and languages that represent it. An important sub-PROP of $\mathbf{Qubit}$ is $\mathbf{Stab}$.

⌜ **Definition 2.6.5 (Stab):** $\mathbf{Stab}$ is defined as the sub-PROP of $\mathbf{Qubit}$ whose morphisms are generated by:

- $S^{(n,m)} : n \to m := |0^m\rangle\langle 0^n| + i\,|1^m\rangle\langle 1^n|$
- $H : 1 \to 1 := |+\rangle\langle 0| + |-\rangle\langle 1|$ ⌟

This PROP is a †-compact PROP (one can recover the compact structure of $\mathbf{FdHilb}$ for instance with $\eta := (S^{(1,1)} \otimes S^{(1,1)}) \circ S^{(1,2)} \circ S^{(0,1)}$ and $\epsilon := \eta^\dagger$) . It is very close to the stabiliser or Clifford group in the following sense: It is equivalent to a scaled stabiliser group with initialisation and post-selected measure.

Proposition 2.6.6.

$$\forall f : n \to m \in \mathbf{Stab},\ \exists g \in C_p, x \in \mathbb{C},\quad f = x\left(id_m \otimes \left\langle 0^{p-m}\right|\right) \circ g \circ \left(id_n \otimes \left|0^{p-n}\right\rangle\right)$$

Proof ► We are going to proceed by induction. We need to show the result on the two generators $S^{(n,m)}$ and H, and then on the two compositions $\circ$ and $\otimes$. Since the result will be proven to be preserved by compositions, we can break $S^{(n,m)}$ into smaller parts.

Let us first define the following morphisms:

$$\mu := \left(S^{(1,1)}\right)^3 \circ S^{(2,1)} \qquad \upsilon := \left(S^{(1,1)}\right)^3 \circ S^{(0,1)}$$
$$\nu := S^{(1,2)} \circ \left(S^{(1,1)}\right)^3 \qquad \tau := S^{(1,0)} \circ \left(S^{(1,1)}\right)^3$$

One can notice that $(\mu, \upsilon, \nu, \tau)$ forms a Frobenius algebra. We can define μ_n and ν_n for arbitrary n by:

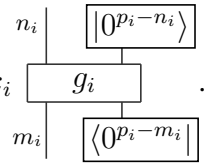
$$\mu_0 := \upsilon \qquad \mu_{n+1} := \mu \circ (\mu_n \otimes id)$$
$$\nu_0 := \tau \qquad \nu_{n+1} := (\nu_n \otimes id) \circ \nu$$

One can check that $\mu_n = |0\rangle\langle 0^n| + |1\rangle\langle 1^n|$ and $\nu_n = |0^n\rangle\langle 0| + |1^n\rangle\langle 1|$, so that $S^{(n,m)} = \nu_m \circ S^{(1,1)} \circ \mu_n$. Now instead of showing the result for $S^{(n,m)}$, we can show it for $S^{(1,1)}$, μ, ν, υ and τ.

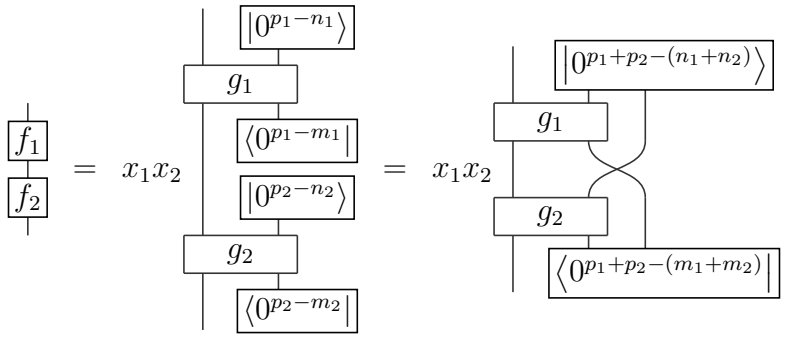
Remember that the gate set (CNot, $R_Z(\frac{\pi}{2})$, H) exactly synthesises the Clifford group. H and $S^{(1,1)}$ are already in C_1. One can check that:

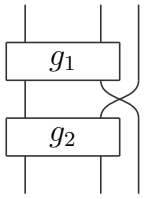
$$\mu = (id \otimes \langle 0|) \circ \text{CNot}$$
$$\nu = \text{CNot} \circ (id \otimes |0\rangle)$$
$$\upsilon = \sqrt{2} H\,|0\rangle$$
$$\tau = \sqrt{2}\,\langle 0|\,H$$

which means that H, $S^{(1,1)}$, μ, ν, υ and τ are of the form $x\ (id_m \otimes \langle 0^{p-m}|) \circ g \circ (id_n \otimes |0^{p-n}\rangle)$ with g Clifford. It remains to show that the two compositions preserve this structure.

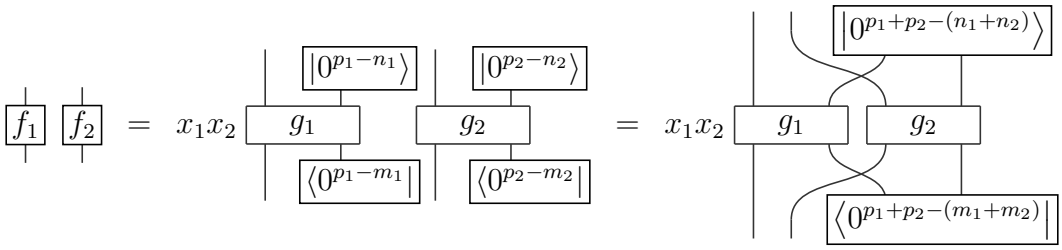
Suppose $f_i = x_i$ 

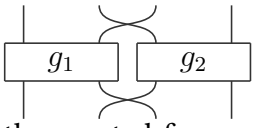
. Then:



where 

$\in C_{p_2+p_1-m_1}$ if $g_i \in C_{p_i}$.



where 

$\in C_{p_2+p_1}$ if $g_i \in C_{p_i}$. Hence, by composition, $S^{(n,m)}$ can be put in the wanted form, and by induction, any morphism of **Stab** can be put in this form. ◀

Stab is not approximately universal. If it were, then so would be the Clifford group. In this thesis we will also be interested in another sub-PROP of **Qubit**.

⌜ **Definition 2.6.7 (Clifford+T):** **Clifford+T** is defined as the sub-PROP of **Qubit** whose morphisms are generated by:

- $T^{(n,m)} : n \to m := |0^m\rangle\langle 0^n| + e^{i\frac{\pi}{4}} |1^m\rangle\langle 1^n|$
- $H : 1 \to 1 := |+\rangle\langle 0| + |-\rangle\langle 1|$ ⌟

Again, this PROP is †-compact, and it is equivalent to a scaled Clifford+T group with initialisation and post-selected measure. As we will show in Section 3.10 (Theorem 3.10.2), this sub-PROP is approximately universal, though it can be inferred from a analogous result on quantum circuits [NC10].

We can also define a whole family of sub-PROPs of **Qudit**, indexed by a ring R.

⌜ **Definition 2.6.8** ($\mathbf{Qudit}_R$)**:** Let R be a subring of $\mathbb{C}$. $\mathbf{Qudit}_R$ is the sub-PROP of $\mathbf{Qudit}$, such that its morphisms are linear maps of the form $\sum f_{xy} |y\rangle\langle x|$ where $f_{xy} \in R$. ⌟

Remark 2.6.9. If R is closed under conjugation, then $\mathbf{Qudit}_R$ is †-compact. Of course, if R is dense in $\mathbb{C}$, then $\mathbf{Qudit}_R$ is approximately universal.

Proposition 2.6.10. $\mathbf{Clifford{+}T} = \mathbf{Qubit}_{\mathbb{Z}\left[\frac{1}{2}, e^{i\frac{\pi}{4}}\right]}$

Notice that it makes $\mathbf{Clifford{+}T}$ approximately universal. Again, this proposition will be proven in Section 3.10.

In the two following sections, we are going to define two graphical languages for quantum computing, which will use the previous structures ((co)monoids, bialgebras, Hopf algebras, Frobenius algebras ...). Although these were defined in the general case on any object, in the following graphical languages, they are defined on object 1.

2.7 The ZX-Calculus

The premise of the ZX-calculus follows logically from the previous work on orthonormal basis. This language depicts how two such bases interact. To do so, we need to carefully select the them. Since we want to capture the most of quantum mechanics, it makes sense to take them as "far apart" from each other as possible.

⌜ **Definition 2.7.1** ([CD11] Unbiasedness, Complementarity)**:** Let $\{|i\rangle\}_i$ be an orthonormal basis of $\mathbb{C}^d$. A quantum state $|\psi\rangle$ on $\mathbb{C}^d$ is called *unbiased* w.r.t. $\{|i\rangle\}_i$ if:

$$\forall\, |i\rangle\,, |j\rangle\,, \quad |\,\langle i\,|\,\psi\rangle\,| = |\,\langle j\,|\,\psi\rangle\,|$$

Two orthonormal bases are *complementary* or *mutually unbiased* if each vector of one basis is unbiased w.r.t. the other. ⌟

More informally, a state is unbiased w.r.t. a basis if measuring the state in this basis yields all the states in said basis with equal probabilities. The two mutually unbiased bases each form a †-Frobenius monoid, and their interaction yields an interesting structure [CD11, DD16], which is a variant of structures seen in Section 2.4.

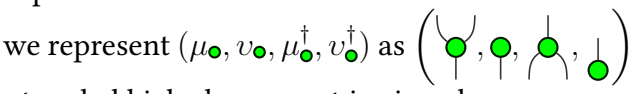
⌜ **Definition 2.7.2** (Scalar, Scaled Algebra)**:** In a PROP, we call any morphism $\kappa : 0 \to 0$ a *scalar*. It is called invertible if there exists a scalar κ^{-1} such that $\kappa \otimes \kappa^{-1} = id_0$.

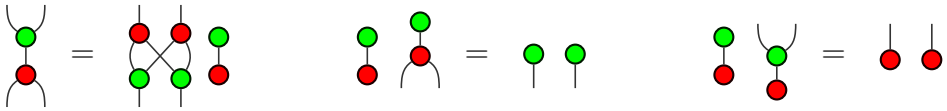
We say that some tuple $(f_0 \otimes \kappa_0, \cdots, f_n \otimes \kappa_n)$ of morphisms f_i with invertible scalars $\kappa_i : 0 \to 0$ forms a *scaled* algebra if $(f_0, \cdots, f_n)$ forms an algebra. Such an algebra can be a monoid, a bialgebra, a Hopf algebra, a Frobenius algebra, ... ⌟

Proposition 2.7.3 (Complementarity $\leftrightarrow$ Bialgebra/Hopf)**.** *Let* $(\mu_\bullet, \upsilon_\bullet)$ *and* $(\mu_\circ, \upsilon_\circ)$ *be two special commutative* †*-Frobenius monoids representing complementary bases in* $\mathbf{Qudit}$*. Then, both* $(\mu_\bullet, \upsilon_\bullet, \mu_\circ^\dagger, \upsilon_\circ^\dagger)$ *and* $(\mu_\circ, \upsilon_\circ, \mu_\bullet^\dagger, \upsilon_\bullet^\dagger)$ *form* scaled *bialgebras.*

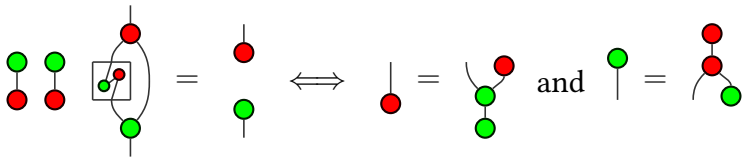
Furthermore, $\upsilon_\bullet = (\upsilon_\circ^\dagger \otimes id) \circ \mu_\circ^\dagger \circ \upsilon_\bullet$ *and* $\upsilon_\circ^\dagger = \upsilon_\circ^\dagger \circ \mu_\bullet \circ (\upsilon_\bullet \otimes id)$ *if and only if* $(\mu_\bullet, \upsilon_\bullet, \mu_\circ^\dagger, \upsilon_\circ^\dagger)$ *forms a* scaled *Hopf algebra with antipode* $\alpha = \Big((\upsilon_\circ^\dagger \circ \mu_\bullet) \otimes id\Big) \circ \Big(id \otimes (\mu_\circ^\dagger \circ \upsilon_\bullet)\Big)$.

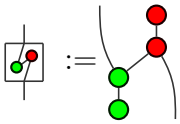
Let us first see what the resulting equations are, and we will try to fix the scalars in the morphisms afterwards.

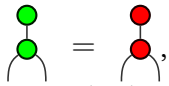
If we represent $(\mu_\bullet, \upsilon_\bullet, \mu_\bullet^\dagger, \upsilon_\bullet^\dagger)$ as  and similarly for $(\mu_\bullet, \upsilon_\bullet, \mu_\bullet^\dagger, \upsilon_\bullet^\dagger)$, the first scaled bialgebra we get is given by:



The second result of Proposition 2.7.3 states, with the right scalars, that:

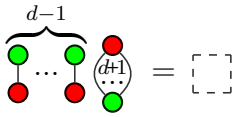


where  represents the antipode.

Notice that the compact structures induced by $(\mu_\bullet, \upsilon_\bullet)$ and $(\mu_\bullet, \upsilon_\bullet)$ are mixed in the condition for the Hopf algebra, as well as in the antipode. When the two coincide, that is when  , then we directly get that $(\mu_\bullet, \upsilon_\bullet, \mu_\bullet^\dagger, \upsilon_\bullet^\dagger)$ forms a scaled Hopf algebra with antipode the identity. However, the two do not coincide in general [CPP08], but if $d = 2$ (i.e. we are in **Qubit**), then they do.

Notice also that we ignored temporarily the scalar equation of the bialgebra. This is merely because it uses a non-trivial scalar. Let us define $\mu_{\bullet n}$ and $\mu_{\bullet n}^\dagger$ as in Proposition 2.4.16. Then define the scalar $\varsigma_n := \upsilon_\bullet^\dagger \circ \mu_{\bullet n} \circ \mu_{\bullet n}^\dagger \circ \upsilon_\bullet$. Using the spider notation, this scalar is represented as  .

Then, in **Qudit**, we have:

$$\varsigma_1^{\otimes d-1} \otimes \varsigma_{d+1} = id_0 \qquad \text{i.e.} \qquad$$ 

This equation basically gives an inverse of ς_1 for $\otimes$. Let us write $\varsigma_1^{\text{-}1} := \varsigma_1^{\otimes d-2} \otimes \varsigma_{d+1}$. Then, all of the scalars in the previous scaled bialgebras come from the fact that

$$(\mu_\bullet \otimes \varsigma_1, \upsilon_\bullet \otimes \varsigma_1^{\text{-}1}, \mu_\bullet^\dagger, \upsilon_\bullet^\dagger)$$

forms an actual bialgebra.

The ZX-Calculus is then a calculus of two interacting mutually unbiased bases, Z and X, with phases for both. The reason for taking phase shifts and not more generally diagonal morphisms is two-fold: first, it is driven by quantum mechanics, where the operators are unitary; second, the phases form a group, which is easier to manipulate than a monoid. Particularly, every phase shift has a dagger that is also a phase shift.

In the following, we restrict the language to the qubit case, that is, when $d := \dim(\mathcal{H}) = 2$. In this case, the two compact structures coincide, and the phase shifts

w.r.t. the basis $\{|0\rangle, |1\rangle\}$ are of the form $e^{i\gamma}(|0\rangle\langle 0| + e^{i\alpha}|1\rangle\langle 1|)$. The global phase $e^{i\gamma}$ is sometimes ignored, and it turns out, it can be represented otherwise:

$$e^{i\gamma} = \left(\langle +^3| + \langle -^3|\right)\left(|0^3\rangle + |1^3\rangle\right)\left(\langle +| + e^{i\pi}\langle -|\right)\left(|0\rangle\langle 0| + e^{i\gamma}|1\rangle\langle 1|\right)\left(|0\rangle + |1\rangle\right)$$

so we only give a generator for $|0\rangle\langle 0| + e^{i\alpha}|1\rangle\langle 1|$, and we identify it with α, the value of the phase shift. Of course, we do this for both bases.

Proposition 2.7.4. *Two mutually unbiased bases, $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, together with their respective phase shifts, are sufficient to create a language that can represent any linear map in* **Qubit**.

Proof ▶ First, notice that we can represent any complex number $\rho e^{i\theta} \in \mathbb{C}$: there exists $n \in \mathbb{N}$ and $\gamma \in \mathbb{R}$ such that $\rho e^{i\theta} = 2^{n+1}\cos(\gamma)\, e^{i\theta}$, which can be represented by:

$$[(\langle 0| + \langle 1|)(|0\rangle + |1\rangle)]^{\otimes n}\,(\langle +| + e^{-i\gamma}\langle -|)(|0\rangle + e^{i\gamma}|1\rangle)(\langle +| + e^{i\pi}\langle -|)(|0\rangle + e^{i\theta}|1\rangle)$$

Also, any unitary can be represented. (CNot, R_Z, H) is a universal set of gates for unitaries, and each of these gates can be implemented:

$$\text{CNot} = ((|0\rangle\langle 00| + |1\rangle\langle 11|) \otimes id \otimes (\langle 0| + \langle 1|))\,(id \otimes (|++\rangle\langle +| + |--\rangle\langle -|) \otimes (|+\rangle + |-\rangle))$$
$$R_Z(\alpha) = |0\rangle\langle 0| + e^{i\alpha}|1\rangle\langle 1|$$
$$H = e^{-i\frac{\pi}{4}}(|0\rangle\langle 0| + i|1\rangle\langle 1|)(|+\rangle\langle +| + i|-\rangle\langle -|)(|0\rangle\langle 0| + i|1\rangle\langle 1|)$$

Now, let $|\psi\rangle : 0 \to n$ be an n qubit state, i.e. $|\psi\rangle \in \mathbb{C}^{2^n}$. Then, there exists a unitary $U : n \to n$ such that $|\psi\rangle = \left(\frac{1}{\sqrt{2^n}}||\psi\rangle|\right) U\sqrt{2}^n |0^n\rangle$. It can be represented since $\left(\frac{1}{\sqrt{2^n}}||\psi\rangle|\right) \in \mathbb{C}$, U is unitary, and $\sqrt{2}^n|0^n\rangle = (|+\rangle + |-\rangle)^{\otimes n}$.
Finally, given an arbitrary map $D : n \to m$, we have $D = (id_n \otimes \epsilon_n)([(D \otimes id_n)\eta_n] \otimes id_n)$, where ϵ_n and η_n are the morphisms obtained from the two bases thanks to Remark 2.4.12 and the fact that in the qubit case, these compact structures coincide. Since $(D \otimes id_n)\eta_n$ is a state $0 \to n+m$, it is representable, so D is representable. ◀

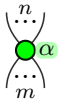
However, we add to the language one last generator: the Hadamard gate H. This generator comes in handy for it allows to transform one basis into the other. As seen in the proof of Proposition 2.7.4, it can be written as a composition of phase shifts [DP09]:

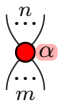
$$H := e^{-i\frac{\pi}{4}}(|0\rangle\langle 0| + i|1\rangle\langle 1|) \circ (|+\rangle\langle +| + i|-\rangle\langle -|) \circ (|0\rangle\langle 0| + i|1\rangle\langle 1|)$$

Notice that H qualifies as an involutive morphism of monoids: it allows to change the basis $\{|0\rangle, |1\rangle\}$ to $\{|+\rangle, |-\rangle\}$ and vice-versa, so $H^2 = id$.

We finally have all the generators of the ZX-Calculus, and we can now give a formal definition [CD11, CK17].

⌜ **Definition 2.7.5** (ZX-Calculus)**:** The qubit ZX-Calculus, or **ZX**, is a †-compact graphical language that represents **Qubit**, with the following set of generators and their string-diagram representation:

- $R_Z^{(n,m)}(\alpha) : n \to m ::$ 

- $R_X^{(n,m)}(\alpha) : n \to m ::$ 
- $H : 1 \to 1 ::$ 

Where $\alpha \in \mathbb{R}$. The PROP structure is provided by $\sigma : 2 \to 2 ::$  ; and the compact structure by $\epsilon : 2 \to 0 ::$  and $\eta : 0 \to 2 ::$  .

The functor † is such that:

- $\left(R_Z^{(n,m)}(\alpha)\right)^\dagger = R_Z^{(m,n)}(-\alpha)$
- $\left(R_X^{(n,m)}(\alpha)\right)^\dagger = R_X^{(m,n)}(-\alpha)$
- $H^\dagger = H$

The language comes with a PROP-functor $[\![.]\!] : \mathbf{ZX} \to \mathbf{Qubit}$, called the *standard interpretation*, and given by:

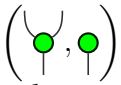
- $\left[\!\left[R_Z^{(n,m)}(\alpha)\right]\!\right] = |0^m\rangle\langle 0^n| + e^{i\alpha}\,|1^m\rangle\langle 1^n|$
- $\left[\!\left[R_X^{(n,m)}(\alpha)\right]\!\right] = |+^m\rangle\langle +^n| + e^{i\alpha}\,|-^m\rangle\langle -^n|$
- $[\![H]\!] = |+\rangle\langle 0| + |-\rangle\langle 1|$
- $[\![\sigma]\!] = \sum_{i,j\in\{0,1\}} |ji\rangle\langle ij|$
- $[\![\eta]\!] = |00\rangle + |11\rangle$
- $[\![\epsilon]\!] = \langle 00| + \langle 11|$

Whatever the axiomatisation chosen for the ZX-Calculus, we always consider that whenever two diagrams are isomorphic, then they are equal. ⌟

By convention, when the parameter of R_Z or R_X is 0, we may omit it.

Remark 2.7.6. We did not give a specific monoidal theory to the language yet. This omission is conscious. The axiomatisation varies from one restriction of the language to the other, hence several will be given throughout the thesis. Of course, the study of the algebras in what precedes was not done in vain. Most of the axioms for Frobenius algebras and Hopf algebras will be found in every axiomatisation.

What always appears in a ZX-axiomatisation is that two isomorphic diagrams are equal. Take it as a feature of the language so important that it is part of the "freest" version of the ZX-Calculus considered. This captures essential equations of †-compact PROPs, but also things like:

Remark 2.7.7. The ZX-Calculus does not only have a morphism of monoid, H, but also two non-trivial endomorphisms of monoid. Indeed  is an endomorphism of monoid for  and similarly  for  . This trait appeared in early axiomatisations, but was proven to be derivable from other axioms [BPW17a].

This language is universal for **Qubit** [CD11], although it is interesting to study some of its restrictions, called fragments.

⌜ **Definition 2.7.8** (Fragment of the ZX-Calculus)**:** Let F be an additive subgroup of $\mathbb{R}$. The *fragment* F of the ZX-Calculus is the restriction of the language where the morphisms are generated by $\{R_Z^{(n,m)}(\alpha), R_X^{(n,m)}(\alpha), H \mid \alpha \in F\}$. We may write the resulting language $\mathbf{ZX}[F]$. Also, if F is generated by a finite set of numbers $\{a_0, \cdots, a_n\}$, we may denoted $\mathbf{ZX}[a_0, \cdots, a_n]$ the resulting language. By contrast, $\mathbf{ZX}$ is the unrestricted ZX-Calculus, i.e. where the angles are in $\mathbb{R}$. ⌟

Of course, axiomatisations can be applied to fragments of the language, provided all the phase shifts in the set of rules are part of the fragment. We hence denote by $\mathbf{ZX}[F]/R$ the language resulting of the equivalence relation R applied to the fragment F of the ZX-Calculus. In this case, when an axiom of R displays unconstrained phase shifts (see e.g. (S) in Figure 2.1), it is assumed for all the phase shifts in the fragment F.

A first example of an axiomatisation of the ZX-Calculus is the set of rules $\mathrm{ZX}_{\pi/2}$, given in Figure 2.1. This axiomatisation, partially introduced in [CD11], completed in [DP09, Bac15], and simplified in [BPW17a], was proven to be complete for $\mathbf{ZX}[\frac{\pi}{2}]$ [Bac14a].

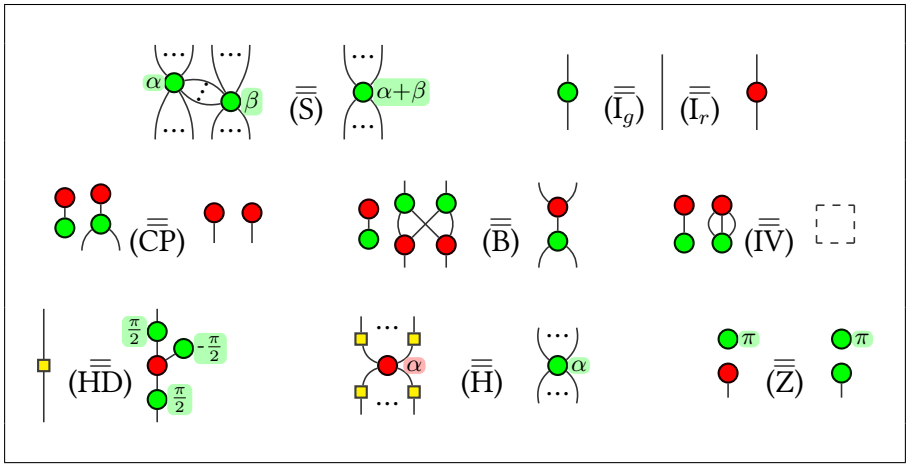


Figure 2.1: Set of rules $\mathrm{ZX}_{\pi/2}$ for the Clifford fragment of the ZX-Calculus. The right-hand side of (IV) is an empty diagram. (...) denotes zero or more wires, while $(\cdot^{\cdot})$ denotes one or more wires.

Theorem 2.7.9 (Clifford ZX)**.** *The language* $\mathbf{ZX}[\frac{\pi}{2}]/\mathrm{ZX}_{\pi/2}$ *is complete, i.e. the functor* $[\![.]\!] : \mathbf{ZX}[\frac{\pi}{2}]/\mathrm{ZX}_{\pi/2} \to \mathbf{Qubit}$ *is faithful.*

The proof uses a particular notion of states, known as *graph states* [EEC08].

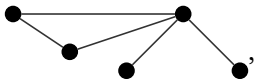
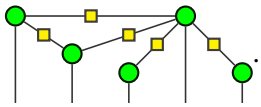
⌜ **Definition 2.7.10** (Graph States)**:** The set of graph states is a set of particular stabiliser states generated by

- $|+\rangle$
- Swap : $\sum |ji\rangle\langle ij|$
- CZ : $\sum (-1)^{ij} |ij\rangle\langle ij|$

Any graph state can be represented by a graph $G := (V, E)$ where V is the set of vertices and E the set of edges of G. Each vertex represents a qubit initialised in $|+\rangle$, and each edge between vertices v_1 and v_2 represents a CZ applied on the two qubits represented by v_1 and v_2. We denote the resulting state $|G\rangle$. ⌟

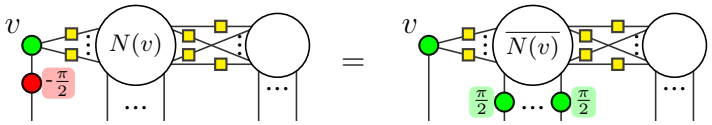
Sketch of Proof ▷ First, thank to the map/state duality, one can consider only the states in $\mathbf{ZX}[\frac{\pi}{2}]$. The graph states have a nice interpretation in ZX. If $G := (V, E)$ is a graph, we can build a ZX-diagram D_G as follows:

- Each vertex in G is a green node with scalar  in D_G connected to an output.
- Each edge between v_1 and v_2 in G is a wire with  between the corresponding nodes.

For instance, if $G =$  , then $D_G =$  . Of course, the diagram is built so that $[\![D_G]\!] = |G\rangle$.

Through a strategy known as *pivoting* [DP14] that uses the rules of $\mathrm{ZX}_{\pi/2}$, one can reduce a diagram of $\mathbf{ZX}[\frac{\pi}{2}]$ to a graph state with additional 1-qubit morphisms on the outputs. These morphisms are identified as being elements of C_1, i.e. the stabiliser of the one-qubit Pauli group G_1.

This reduced form is not unique, but it is up to *local complementations*, which are derivable using the rules in $\mathrm{ZX}_{\pi/2}$. In ZX, a local complementation is the following transformation:



where $N(v)$ denotes the neighbourhood of node v and $\overline{N(v)}$ the complementary of the subgraph $N(v)$, that is u_1 and u_2 share an edge in $\overline{N(v)}$ iff they do not in $N(v)$. ◁

$\mathbf{ZX}[\frac{\pi}{2}]/\,\mathrm{ZX}_{\pi/2}$ is complete, however the diagrams of $\mathbf{ZX}[\frac{\pi}{2}]$ exactly represent morphisms of **Stab** [Bac14a, Bac15].

Proposition 2.7.11. *The functor* $[\![.]\!] : \mathbf{ZX}[\frac{\pi}{2}]/\,\mathrm{ZX}_{\pi/2} \to \mathbf{Stab}$ *is full and faithful.*

Hence, this language is not (approximately) universal for quantum mechanics. Actually, it has been proven that this axiomatisation does not make the unrestricted ZX-Calculus complete [SdWZ14].

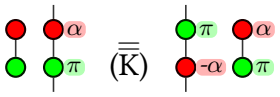
Theorem 2.7.12. *The functor* $\mathbf{ZX}/\,\mathrm{ZX}_{\pi/2} \to \mathbf{Qubit}$ *is not faithful.*

Because of this, one might want to find a middle ground: a complete axiomatisation for an approximately universal fragment of the ZX-Calculus. Such a fragment would allow for computational speed-ups, while at the same time simplifying the search for a

complete axiomatisation. A natural candidate for such a fragment would $\mathbf{ZX}[\frac{\pi}{4}]$, for the functor $\mathbf{ZX}[\frac{\pi}{2}] \to \mathbf{Clifford{+}T}$ is full, and $\mathbf{Clifford{+}T}$ is approximately universal.

A first partial answer was found, for one-qubit Clifford+T unitaries [Bac14b].

Proposition 2.7.13. *Consider two morphisms $f : 1 \to 1$ and $g : 1 \to 1$ generated by binary operators of $\mathbf{ZX}[\frac{\pi}{4}]$ i.e. by $(R_Z^{(1,1)}(\pi/4), R_X^{(1,1)}(\pi/4), H)$, and consider the equation:*

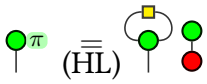


Then:

$$[\![f]\!] = [\![g]\!] \implies \mathrm{ZX}_{\pi/2}\text{+(K)} \vdash f = g$$

where $\mathrm{ZX}_{\pi/2}$+(K) *denotes the set of rules* $\mathrm{ZX}_{\pi/2}$ *enriched with the equation* (K).

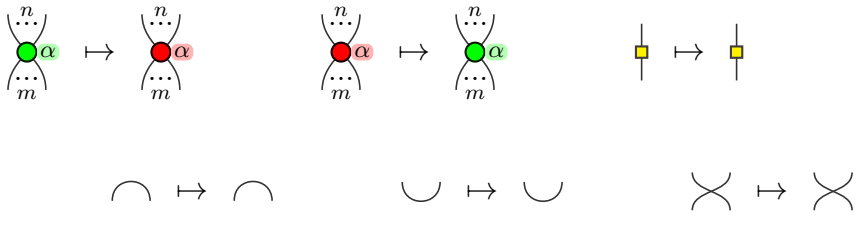
One of the main results of the thesis is to provide a complete axiomatisation for the many-qubit Clifford+T diagrams. We will also explore some other languages and axiomatisations. Every time, a first step towards completeness will be to recover one known axiomatisation from which some useful lemmas can be derived. The simplest axiomatisation of the ZX-Calculus is not for the Clifford fragment, but for the *real stabiliser* [DP14]. In this axiomatisation, denoted ZX_π, the only novelty is that (HD) is replaced by:



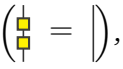
i.e. $\mathrm{ZX}_\pi := \mathrm{ZX}_{\pi/2} \setminus \{\text{(HD)}\} \cup \{\text{(HL)}\}$.

Most axiomatisations for the ZX-Calculus (all of those that are presented in this thesis) have the axiom (H), and are powerful enough to prove that  is involutive, i.e.  . In this case, colour-swapping preserves the equality.

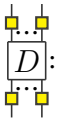
Proposition 2.7.14. *Let F be a fragment, and $[\![.]\!]^{\bullet\leftrightarrow\bullet} : \mathbf{ZX}[F] \to \mathbf{ZX}[F]$ the interpretation inductively defined as:*

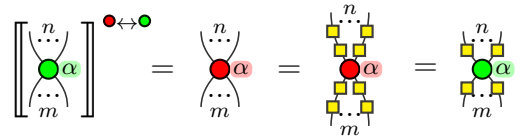
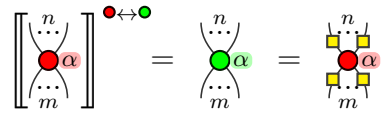
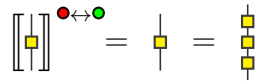
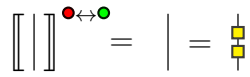
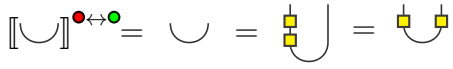
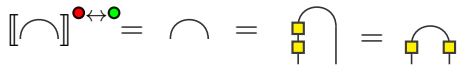
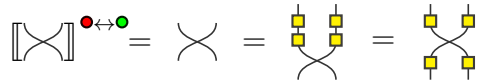
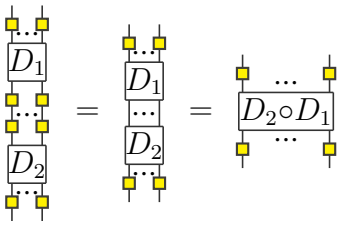
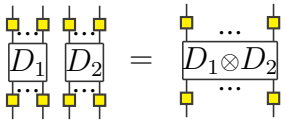


$$D_2 \circ D_1 \mapsto [\![D_2]\!]^{\bullet\leftrightarrow\bullet} \circ [\![D_1]\!]^{\bullet\leftrightarrow\bullet} \qquad D_1 \otimes D_2 \mapsto [\![D_1]\!]^{\bullet\leftrightarrow\bullet} \otimes [\![D_2]\!]^{\bullet\leftrightarrow\bullet}$$

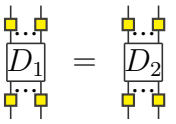
If an axiomatisation R is such that $R \vdash$ (H),  *, then:*

$$R \vdash D_1 = D_2 \iff R \vdash [\![D_1]\!]^{\bullet\leftrightarrow\bullet} = [\![D_2]\!]^{\bullet\leftrightarrow\bullet}$$

Proof ► We can show inductively that for any $\mathbf{ZX}[F]$-diagram D, $R \vdash [\![D]\!]^{\bullet\leftrightarrow\bullet} =$ 

- $R \vdash$ 
- $R \vdash$ 
- $R \vdash$ 
- $R \vdash$ 
- $R \vdash$ 
- $R \vdash$ 
- $R \vdash$ 
- $R \vdash \llbracket D_2 \circ D_1 \rrbracket^{\bullet\leftrightarrow\circ} = \llbracket D_2 \rrbracket^{\bullet\leftrightarrow\circ} \circ \llbracket D_1 \rrbracket^{\bullet\leftrightarrow\circ} =$ 
- $R \vdash \llbracket D_1 \otimes D_2 \rrbracket^{\bullet\leftrightarrow\circ} = \llbracket D_1 \rrbracket^{\bullet\leftrightarrow\circ} \otimes \llbracket D_2 \rrbracket^{\bullet\leftrightarrow\circ} =$ 

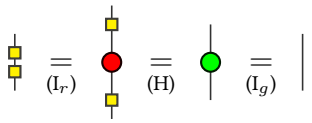
Then, if $R \vdash D_1 = D_2$, we obviously have:

$R \vdash \llbracket D_1 \rrbracket^{\bullet\leftrightarrow\circ} =$  $= \llbracket D_2 \rrbracket^{\bullet\leftrightarrow\circ}$

◀

This is the case when (H), (I_r) and (I_g) are given in the axiomatisation:

Lemma 2.7.15. *If $R \vdash$ (H), (I_r), (I_g), then colour-swapping preserves the equality, since:*



and thanks to Proposition 2.7.14.

In *all* the axiomatisations that we are going to give in this these, colour-swapping of diagrams generated by R_Z, R_X and H can always be proven. Hence, when referring to an axiom or a lemma, we will either signify the equation itself, or its colour-swapped version.

Then, we provide in Figure 2.2 some useful equations between ZX-diagrams as well as their dependencies. If there is an arrow $\mathrm{eq}_1 \to \mathrm{eq}_2$, it means that eq_1 is used to derive eq_2. The spider rules (S) and (I), the colour-change rule (H), which together with (I) allows for colour-swapping, and the biagebra rule (B), are always supposed to be in the axiomatisations.

Proposition 2.7.16. *In an oriented graph, let us denote* $\Gamma^-(v)$ *the incoming neighbourhood of vertex* v*. In Figure 2.2, for any* eq *in the set of vertices, either* $\Gamma^-(\mathrm{eq}) = \emptyset$ *and the equation is considered as an axiom for its neighbours, or* eq *is derivable using* $\Gamma^-(\mathrm{eq})$ *(assumed as axioms), and rules* (S), (B), (I) *and* (H)*, i.e.:* (S), (B), (I), (H), $\Gamma^-(\mathrm{eq}) \vdash \mathrm{eq}$.

Remark 2.7.17. Notice that having a cycle in the graph (between (CP) and (Hopf)) is not a problem. This simply means that in a setting where one has (S), (I), (B) and (H), then (CP) and (Hopf) are equivalent.

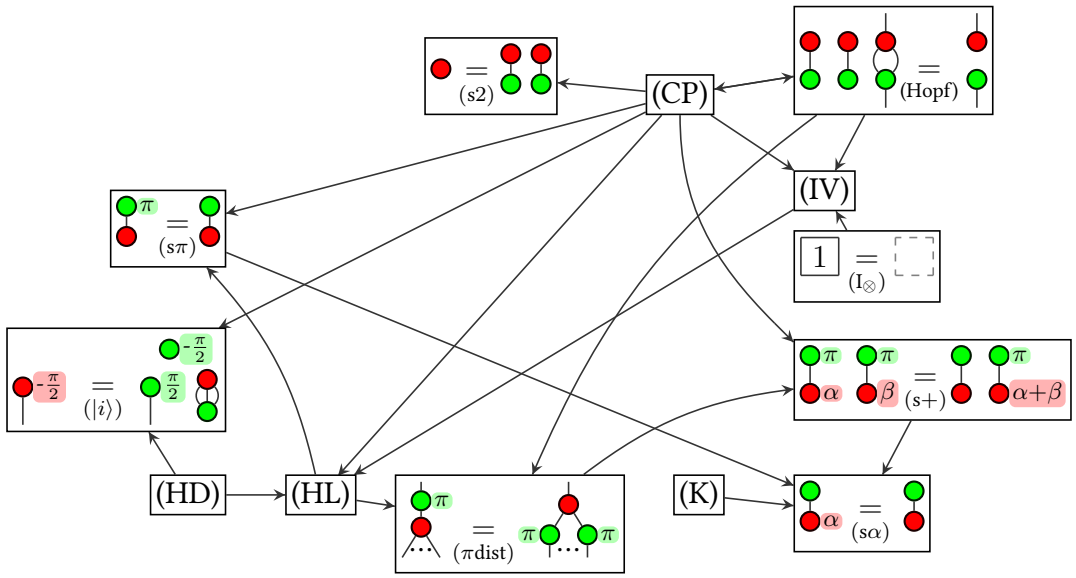
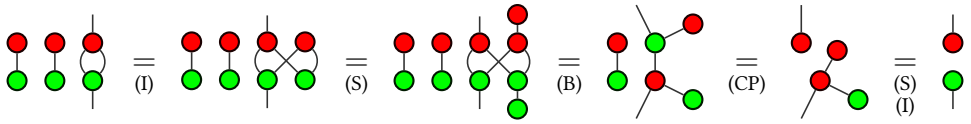
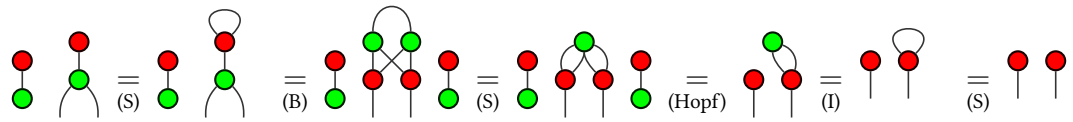


Figure 2.2: Lemmas and their dependencies. $\boxed{1}$ represents any non-empty diagram such that $[\![\boxed{1}]\!] = 1$. (S), (B), (I) and (H) are assumed.

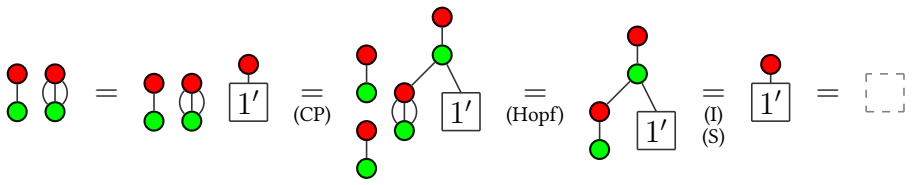
Proof *of Proposition 2.7.16* ▶
• (S), (I), (B), (CP) ⊢ (Hopf):



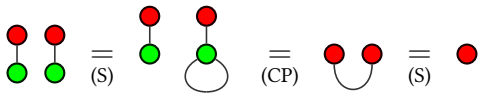
• (S), (I), (B), (Hopf) ⊢ (CP):



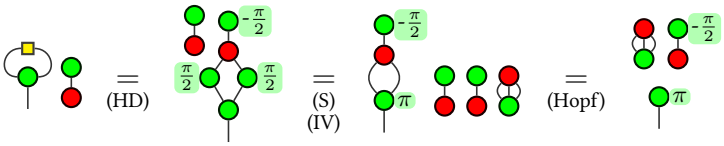
• For the proof that (S), (I), (CP), (Hopf), ($I_\otimes$) ⊢ (IV), notice that in ($I_\otimes$), if $\boxed{1}$ is non-empty, there exists a diagram $1'$ such that $\boxed{1} = \boxed{1'}$. Indeed, there is necessarily at least one wire in $\boxed{1}$, because the only non-empty, wireless scalars are $R_Z^{(0,0)}(\alpha)$ and $R_X^{(0,0)}(\alpha)$, both of which have interpretation $1 + e^{i\alpha} \neq 1$. Hence, one can use (I_r) and (S) to create the node : $= $. Then:



• (S), (CP) ⊢ (s2):

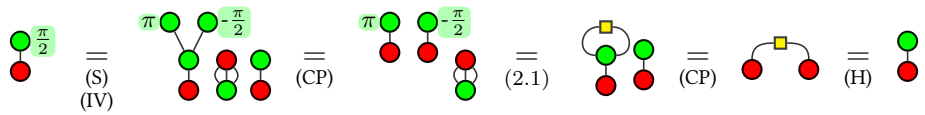


• (HD), (S), (IV), (Hopf), (H) ⊢ (HL):
First:



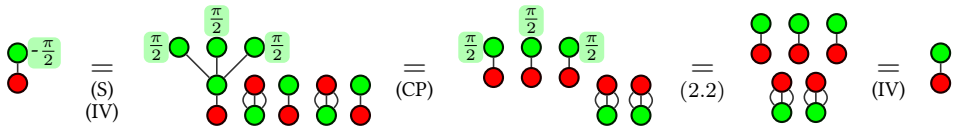
(2.1)

Then:



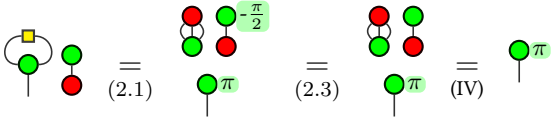
(2.2)

Hence:

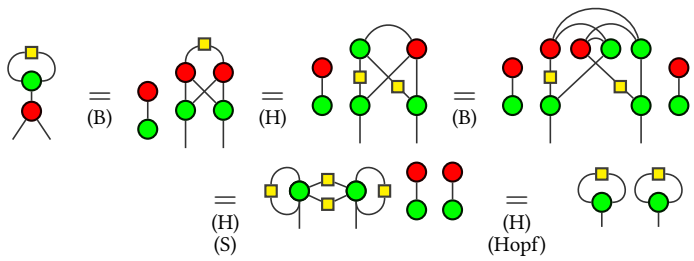


(2.3)

Finally:

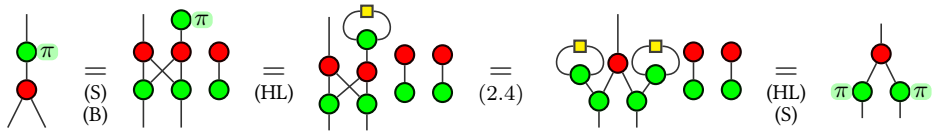


• (B), (H), (S), (Hopf), (HL) ⊢ (πdist):
First:

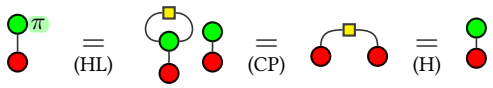


(2.4)

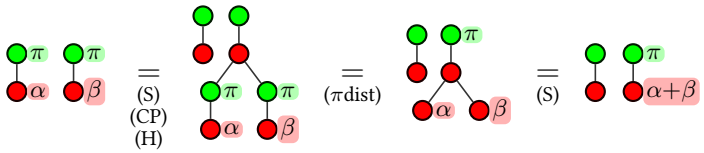
Then:



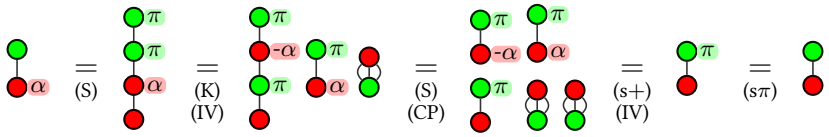
• (HL), (CP), (H) ⊢ (sπ):



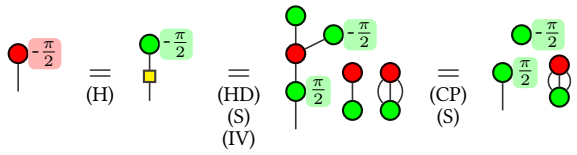
• (S), (CP), (H), (πdist) ⊢ (s+):



• (S), (K), (CP), (s+), (IV), (sπ) ⊢ (sα):



• (H), (HD), (S), (IV), (CP) ⊢ ($|i\rangle$):



◀

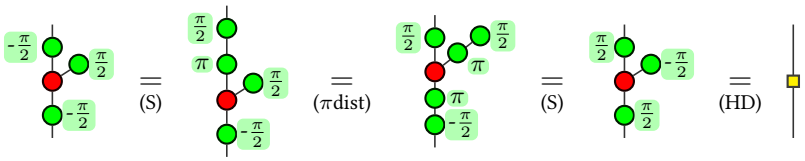
Moreover, the two axiomatisations $\mathrm{ZX}_{\pi/2}$ and ZX_{π} allow multiplication of all the phase shifts by -1:

Lemma 2.7.18. *For an arbitrary fragment F, let $[\![.]\!]_{-1} : \mathbf{ZX}[F] \to \mathbf{ZX}[F]$ be the interpretation that multiplies all the angles by -1. Then:*

$$\forall D_1, D_2 \in \mathbf{ZX}[\tfrac{\pi}{2}], \quad \mathrm{ZX}_{\pi/2} \vdash D_1 = D_2 \iff \mathrm{ZX}_{\pi/2} \vdash [\![D_1]\!]_{-1} = [\![D_2]\!]_{-1}$$

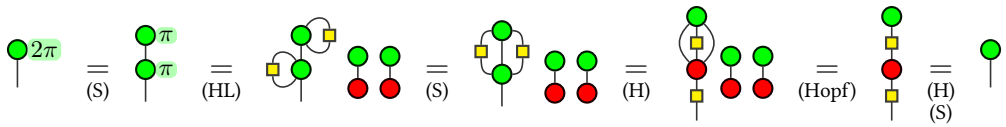
$$\forall D_1, D_2 \in \mathbf{ZX}[\pi], \quad \mathrm{ZX}_{\pi} \vdash D_1 = D_2 \iff \mathrm{ZX}_{\pi} \vdash [\![D_1]\!]_{-1} = [\![D_2]\!]_{-1}$$

Proof ▶ We can show that all the axioms hold under interpretation $[\![.]\!]_{-1}$. All cases except (HD) in $\mathrm{ZX}_{\pi/2}$ are trivial. Thanks to Proposition 2.7.16, $\mathrm{ZX}_{\pi/2} \vdash (\pi\mathrm{dist})$, hence:



◀

Remark 2.7.19. In the ZX-Calculus, we consider the angles to be in $\mathbb{R}/2\pi\mathbb{Z}$, although it is actually provable provided we have the adequate axioms or lemmas (in particular (HL) and (Hopf)):



2.8 The GHZ/W-Calculus

Contrarily to the ZX-Calculus, the two interacting monoids in the GHZ/W-Calculus are very different. The generators of the language are initially motivated by equivalence classes of entanglement on three qubits. It was later shown that it formed a fitting language for fermionic quantum computing [HdFN18].

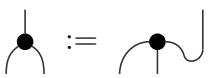
⌜ **Definition 2.8.1** (LOCC, SLOCC)**:** Let $|\psi\rangle$ and $|\phi\rangle$ be two states on n qubits. We say that $|\psi\rangle$ and $|\phi\rangle$ are LOCC-equivalent if one can be turned into the other by application of local unitaries, that is, the tensor product of one-qubit unitaries: $U = U_1 \otimes \ldots \otimes U_n$ with $U_i^\dagger U_i = id$ for all i.

If we drop the unitarity requirement (but keep invertibility), we get the SLOCC-equivalence: The two n-qubit states $|\psi\rangle$ and $|\phi\rangle$ are SLOCC-equivalent if they can be turned into one-another by invertible local operators: $O = O_1 \otimes \ldots \otimes O_n$ such that all the O_i are invertible. ⌟

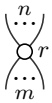
Notice that SLOCC is more permissive, and hence results in a smaller number of equivalence classes. Yet, this number is infinite for states on 4 qubits and more. A state on two qubits can either be entangled or not. There is only one equivalence class for each case. For a three-partite entangled state, however, there are two classes of states that are entangled on three qubits [DVC00]. Representatives of these two classes are the so-called GHZ state $|000\rangle + |111\rangle$, and W state $|001\rangle + |010\rangle + |100\rangle$.

The GHZ/W-Calculus was hence introduced as a graphical language making these two classes interact [CK10]. In [Had15], the language was made complete for a non-universal sub-PROP of **Qubit**, and later was made complete for **Qubit** (and actually also a lot of its sub-PROPs) [HNW18]. Although an embryo of the language exists for qudits [Had17], here, we only give its description for qubits.

First of all we need multiplications and co-multiplications, given by the states GHZ and W. It suffices to use the map/state duality to get them, e.g.:

 where  represents the W state, and  represents the projector $\langle 00| + \langle 11|$.

Concerning the GHZ state, notice that it yields an already known multiplication, represented  : $\mu := |0\rangle\langle 00| + |1\rangle\langle 11|$ after map/state duality. Together with $\upsilon := |0\rangle + |1\rangle$, represented  , it forms a †-Frobenius monoid. It also has diagonal morphisms of the form $s(|0\rangle\langle 0| + r\,|1\rangle\langle 1|)$. We ignore the global scalar s, and only give a generator for $|0\rangle\langle 0| + r\,|1\rangle\langle 1|$ that we identify with r. This leads to an extended spider of the form:



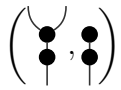
Notice here that the choice was made to take an arbitrary complex number r as argument (actually an arbitrary ring element), instead of a phase. As a result, the diagonal morphisms are not necessarily phase shifts, however this choice simplifies some calculations, such as the normal form of a ZW-diagram.

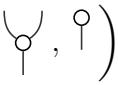
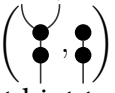
The second monoid is formed from the W state. Notice that the W state is the sum of the three 3-qubit states of Hamming weight 1:

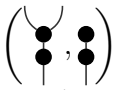
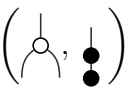
$$|001\rangle + |010\rangle + |100\rangle = \sum_{\substack{x\in\{0,1\}^3 \\ |x|=1}} |x\rangle$$

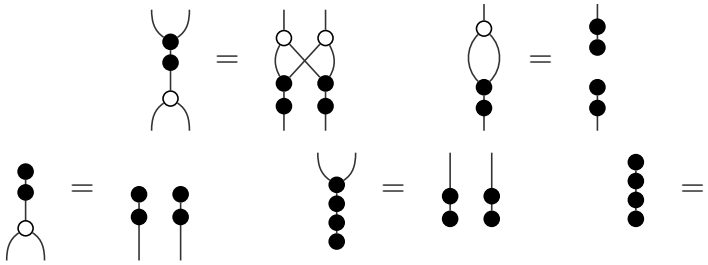
where the Hamming weight $|s|$ of a string s is the number of non-zero symbols in s. It is then fairly natural to define 1- and 2-qubit W states as $|1\rangle$ and $|01\rangle + |10\rangle$. These will help define a monoid. Indeed, if we take the following string diagram representations:

 : $|1\rangle$  : $|0\rangle\langle 1| + |1\rangle\langle 0|$  : $|0\rangle\langle 01| + |0\rangle\langle 10| + |1\rangle\langle 00|$

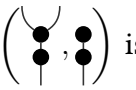
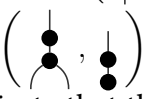
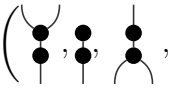
then the pair  forms a monoid. We also define the upside-down version of these three generators as representing the transpose of the associated linear map. It is actually possible to define a degenerate version of a spider family that fits the W states.

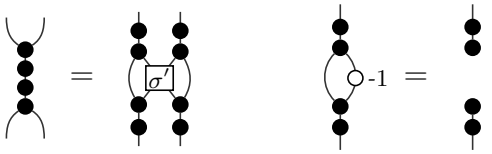
Notice that  is an involutive endomorphism for the monoid  , and more interestingly, for any complex number r,  is an endomorphism for  .

The W-monoid does not define a †-Frobenius monoid. This is a first hint to the fact that the interactions of the two structures are not usual. For instance, the two pairs  and  satisfy the axioms of Hopf algebras with identity as the antipode:

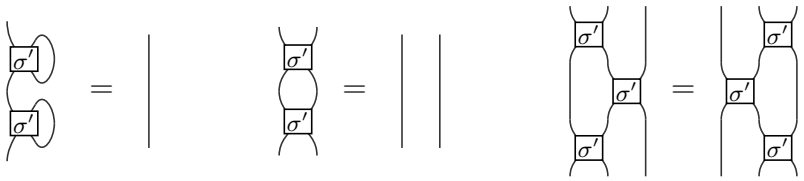


Notice however that it is not a proper Hopf algebra, for  is not a comonoid.

Now, because  is not a †-Frobenius monoid, we have not specified how it reacts with  , although two equations have already been found above. These seem to indicate that there is some sort of bialgebra between the two. However it does not function with the usual swap σ. Interestingly, there exists a "degenerate" swap $\sigma' : 2 \to 2$ such that  satisfies the axioms of Hopf algebra with antipode  :

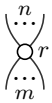


Again, this is not a proper Hopf algebra, for σ' cannot be considered as a proper swap. For the biagebra to function, σ' must represent the map $|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| - |11\rangle\langle 11| = \sum(-1)^{ij} |ji\rangle\langle ij|$, and it does not satisfy all the axioms of PROP. For instance, $\sigma' \circ \eta \neq \eta$ and in general $(id \otimes f) \circ \sigma' \neq \sigma' \circ (f \otimes id)$. It does satisfy, however, equalities that are known as the (modified) Reidemeister moves:



In the following, the morphism σ' will be denoted  .

⌜ **Definition 2.8.2** (ZW-Calculus)**:** The qubit ZW-Calculus, or **ZW**, is a †-compact graphical language, with the following set of generators:

- $Z^{(n,m)}(r) : n \to m ::$ 
- $W^{(n,m)} : n \to m ::$ 
- $\sigma' : 2 \to 2 ::$ 

where $r \in \mathbb{C}$. The PROP structure is provided by $\sigma : 2 \to 2 ::$; and the compact structure by $\epsilon : 2 \to 0 ::$ and $\eta : 0 \to 2 ::$.

The functor † is such that:

- $\left(Z^{(n,m)}(r)\right)^\dagger = Z^{(m,n)}(\overline{r})$
- $\left(W^{(n,m)}\right)^\dagger = W^{(m,n)}$

- $\sigma'^{\dagger} = \sigma'$

The language comes with a PROP-functor $[\![.]\!] : \mathbf{ZW} \to \mathbf{Qubit}$, called the *standard interpretation*, and given by:

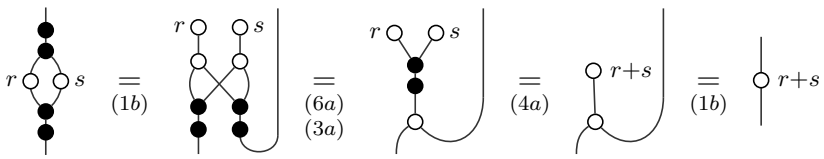
- $[\![Z^{(n,m)}(r)]\!] = |0^m\rangle\langle 0^n| + r\,|1^m\rangle\langle 1^n|$
- $[\![W^{(n,m)}]\!] = \sum_{\substack{x\in\{0,1\}^m \\ y\in\{0,1\}^n \\ |x\cdot y|=1}} |x\rangle\langle y|$
- $[\![\sigma']\!] = \sum_{i,j\in\{0,1\}} (-1)^{ij}\,|ji\rangle\langle ij|$
- $[\![\sigma]\!] = \sum_{i,j\in\{0,1\}} |ji\rangle\langle ij|$
- $[\![\eta]\!] = |00\rangle + |11\rangle$
- $[\![\epsilon]\!] = \langle 00| + \langle 11|$

where $x \cdot y$ is the concatenation of x and y, and $|.|$ is the Hamming weight, i.e. the number of non-zero symbols in a word. Hence, $|x \cdot y| = 1$ means that there is only one symbol 1 in *both* x and y.

We can consider fragments of the PROP where the parameters of $Z^{(n,m)}$ are restricted to a *ring* $R \subseteq \mathbb{C}$ that is closed under conjugation. Such a fragment will be denoted $\mathbf{ZW}[R]$. To each is associated an axiomatisation ZW_R, given in Figure 2.3. ⌟

Here, we cannot use the result that every graph isomorphism between diagrams preserves the semantics if we consider the nodes as non-oriented, precisely because σ' in some sense has to be considered as a swap. Particularly,  $\neq$  . However, what remains true is that any graph isomorphism between two σ'-free ZW-diagrams preserves the semantics. Alternatively, if σ' is understood to be an oriented node, any graph isomorphism *that respects the symmetries of* σ' preserves the semantics.

The axiomatisation presented here has been sightly simplified from the one found in [HNW18]. Particularly, the rule $4a$ allows us to derive:



The axiomatisation has the powerful property:

Theorem 2.8.3 (Completeness of the ZW-Calculus [HNW18]).
For any subring R of $\mathbb{C}$, $\mathbf{ZW}[R]/\,\mathrm{ZW}_R$ is complete, i.e. $[\![.]\!] : \mathbf{ZW}[R]/\,\mathrm{ZW}_R \to \mathbf{Qubit}$ is faithful.

Historically, the ZW-Calculus was not given with parameters in a ring, but merely in $\{-1, 1\}$ [Had15]. We denote this particular restriction $\mathbf{ZW}$. Of course the rule 4 has no meaning in this setting, and is replaced by the rule $4'$ give in Figure 2.4.

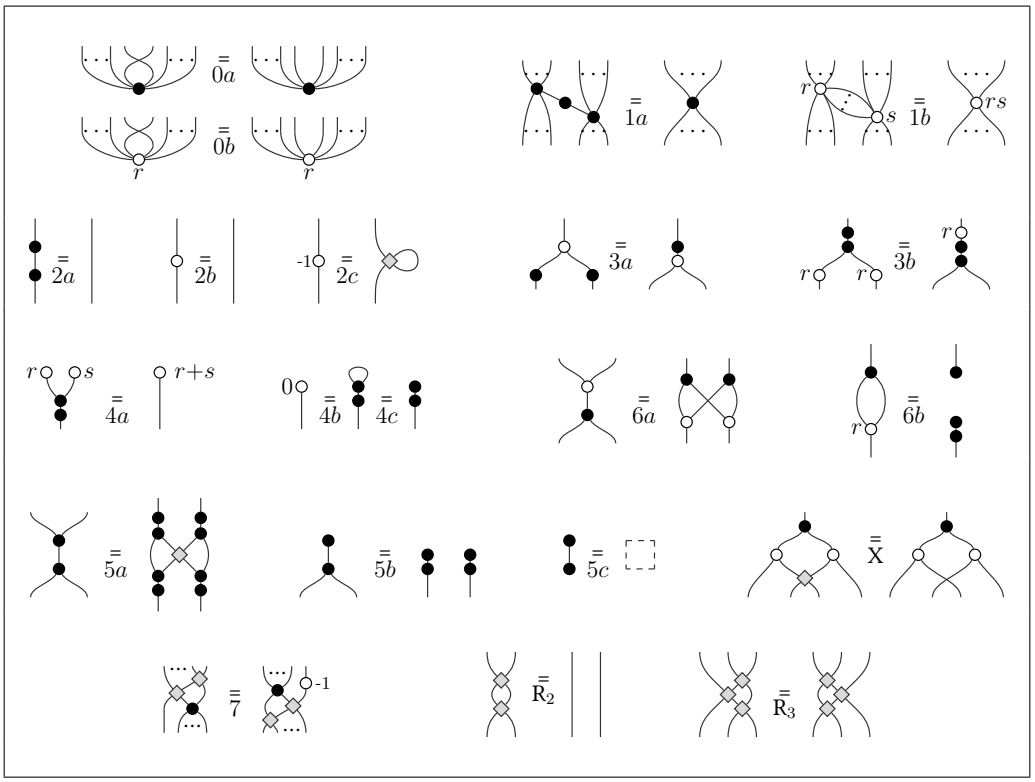


Figure 2.3: Set of rules ZW_R for the ZW-Calculus over the ring R. $r, s \in R$.

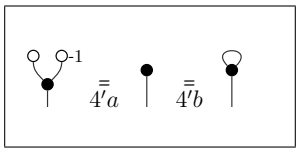
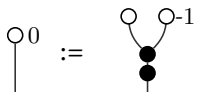
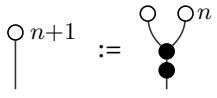


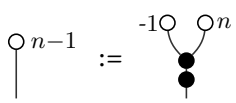
Figure 2.4: Rule $4'$. The resulting axiomatisation is denoted ZW.

Theorem 2.8.4 ([Had15]). *The restriction* $\mathbf{ZW}/\mathrm{ZW}$ *is complete, i.e.* $[\![.]\!] : \mathbf{ZW}/\mathrm{ZW} \to \mathbf{Qubit}$ *is faithful.*

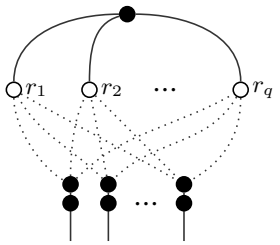
Sketch of Proof ▷ The proof for both theorems rely on normal forms. First of all, if the parameters are only in $\{-1, 1\}$ let us inductively give syntactic sugar such as to recover a ring, the smallest containing -1 and 1, that is $\mathbb{Z}$:

- -1 and 1 are already defined
- 

- If $n \geq 2$: 

- If $n \leq -2$: 

Now that we have an arbitrary ring R in any case, let us give the normal form. Again, we use the map/state duality, so that the normal form can be given only for states. A state $|\psi\rangle$ on n quits can always be written as $|\psi\rangle = \sum r_i \left| b_1^{(i)} \cdots b_n^{(i)} \right\rangle$. The normal form of the state $|\psi\rangle$ is then:



where the node with parameter r_i is connected to the j^{th} output iff $b_j^{(i)} = 1$. The proof then amounts to showing that all the generators can be put in normal form, and that the two compositions of diagrams in normal form can be put in normal form. Some of the axioms, such as rule X, have purposely been chosen so that this can be done. ◁

The ZW-Calculi are hence complete, but they are not universal, unless $R = \mathbb{C}$. However, $\mathbf{ZW}[R]$ exactly represents a sub-PROP of $\mathbf{Qubit}$.

Proposition 2.8.5. *The functor* $[\![.]\!] : \mathbf{ZW}[R]/\operatorname{ZW}_R \to \mathbf{Qubit}_R$ *is full and faithful.*

Hence, if R is dense in $\mathbb{C}$, then $\mathbf{ZW}[R]$ represents an approximately universal fragment of $\mathbf{Qubit}$.

Part II

ZX-Calculus

Chapter 3

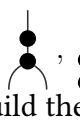
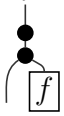
Clifford+T

We have seen that the set of axioms $\mathrm{ZX}_{\pi/2}$ is not complete for the unrestricted ZX-Calculus $\mathbf{ZX}$, but that a simple patch can be done to achieve completeness for one-qubit unitaries of, arguably, the simplest approximately universal fragment of quantum mechanics: Clifford+T. In this chapter, we provide a complete axiomatisation for the many-qubit ZX-diagrams of Clifford+T $\mathbf{ZX}[\frac{\pi}{4}]$, and we prove the completeness thanks to the language $\mathbf{ZW}$/ ZW which is complete. To do so, we first need to alter the latter language to fit our needs while preserving the completeness. We define an intermediary language, $\Delta\mathbf{ZX}$, for which we provide an axiomatisation. We then prove it to be complete for a fragment (the π-fragment), thanks to a back and forth system of interpretations between $\Delta\mathbf{ZX}$ and $\mathbf{ZW}$, that appears to have the same expressive power. Finally, by showing that all the generators of $\Delta\mathbf{ZX}$ can be expressed in $\mathbf{ZX}[\frac{\pi}{4}]$, we derive a new set of axioms, that we prove to be complete for Clifford+T, again using a back-and-forth system of interpretations between $\Delta\mathbf{ZX}[\pi]$ and $\mathbf{ZX}[\frac{\pi}{4}]$. This time, since the latter is more expressive than the former, one of the interpretations will need an encoding of what $\mathbf{ZX}[\frac{\pi}{4}]$ can express into what $\Delta\mathbf{ZX}[\pi]$ can express.

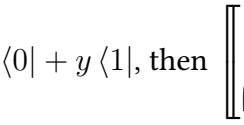
3.1 The Triangle

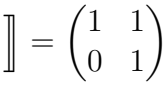
A key point in the proof of completeness for $\mathbf{ZX}[\frac{\pi}{4}]$ is the link (the two interpretations) between the two languages. The ZX-diagrams can easily represent the GHZ state, as well as any 3-qubit state that is SLOCC-equivalent to the GHZ state. The difficulty is to represent the W state with a ZX-diagram. Diagrammatically, the white spider of the ZW-Calculus is easily represented in the ZX-Calculus (recall that in $\mathbf{ZW}$ the parameters are only -1 and 1). The black spider is the troublesome one.

From a Morphism of Monoids in ZW

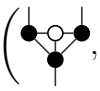
Recall that $\left(\right.$  $\left. \right)$ forms a comonoid in the ZW-Calculus. A first approach could be to try and build the (co)diagonal morphisms for this comonoid. By the proof of Proposition 2.5.6, these diagonal morphisms are exactly of the form 

. If $f : 1 \to 0$ is

generic, i.e. $[\![f]\!] = x\,\langle 0| + y\,\langle 1|$, then  $= \begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$.

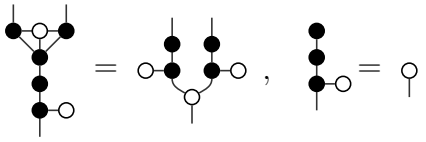
When either x or y is null, then the map is colinear to either the identity or $|0\rangle\langle 1|$, both of which are easily expressible in the ZX-Calculus, up to a global scalar. In the general case, however, things get trickier, and the map cannot be expressed as a Clifford map times a scalar. For instance, let us consider the case $x = y = 1$. Let t denote the map  $= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Interestingly, it has been noted that  is not only a diagonal morphism w.r.t.  , but also a morphism of monoids [vdW]. Consider the following diagram in $\mathbf{ZW}/\,\mathrm{ZW}$:

One can check that its interpretation is $|1\rangle\langle 11| + |0\rangle\,(\langle 00| + \langle 01| + \langle 10|)$. In other words, it acts as an And gate for the canonical basis. By completeness, the pair $\left($  $\right)$ forms a monoid. Then:

Proposition 3.1.1. *In* $\mathbf{ZW}/\,\mathrm{ZW}$*, the morphism*  *is a morphism of monoids between* $\left($  $\right)$ *and* $\left($  $\right)$.

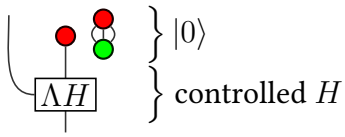
Proof ▶ One can check that all the equations of morphism of monoids are sound. By completeness of $\mathbf{ZW}/\,\mathrm{ZW}$, they are provable in the language:

$\mathrm{ZW} \vdash$ 

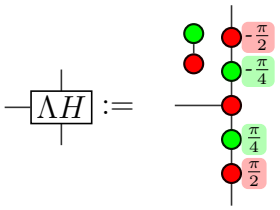
◀

Definition of the Triangle

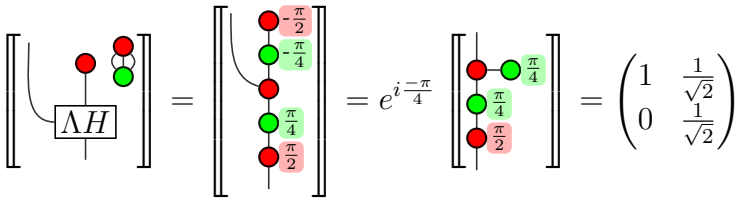
Let us see how to build in $\mathbf{ZX}$ a diagram D_t that represents t, i.e. $[\![D_t]\!] = t$. Notice that $t\,|0\rangle = |0\rangle$ and that $t\,|1\rangle = |0\rangle + |1\rangle = \sqrt{2}\,|+\rangle$. Let us ignore the factor $\sqrt{2}$ for now. t acts as if it applied the Hadamard gate on a $|0\rangle$ state depending on the value of the input. Diagrammatically, t operates as:

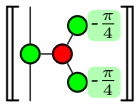
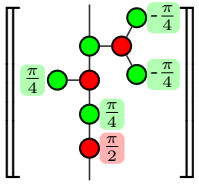


The controlled H gate ΛH can simply be expressed in $\mathbf{ZX}[\frac{\pi}{4}]$:

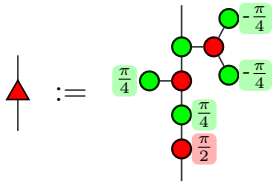


Then, using the fact that $\left[\!\left[\right.\right.$  $\left.\right]\!\right] = e^{i\frac{-\pi}{4}} \left[\!\left[\right.\right.$  $\left.\right]\!\right]$, one can show:

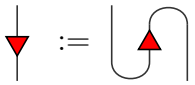


Finally, we need to "control" the scalar $\sqrt{2}$, which we can do since $\left[\!\left[\right.\right.$  $\left.\right]\!\right] = e^{i\frac{-\pi}{4}} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{pmatrix}$, so $\left[\!\left[\right.\right.$  $\left.\right]\!\right] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

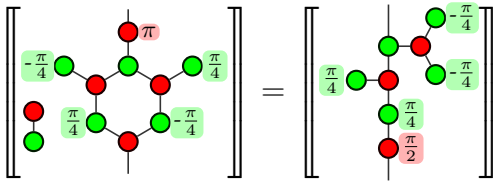
Using a diagram of $\mathbf{ZX}[\frac{\pi}{4}]$, we can now represent a non-trivial non-unitary matrix whose entries are in $\{0, 1\}$. As we will see in the following, this gives us access to the expressive power of the W SLOCC-equivalence class. In the following, this diagram will be so useful that we gave it a syntactic sugar:



Of course, being in a †-compact PROP, we can define the upside-down triangle as:

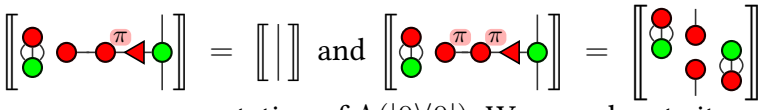


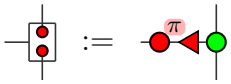
Notice that this node is oriented, i.e. the upside-down triangle is not equal to the triangle. This is due to the fact that its interpretation is not a symmetric matrix. Another diagram of $\mathbf{ZX}[\frac{\pi}{4}]$ with the same interpretation was found in [CK17]:



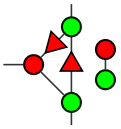
A Building Block

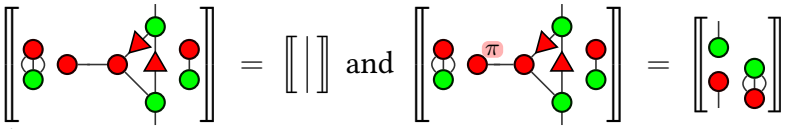
The triangle can then be used as a building block for different larger diagrams. For instance, consider the following diagram:

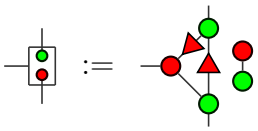
One can easily check that  Hence, this diagram can be seen as a representation of $\Lambda(|0\rangle\langle 0|)$. We may denote it:



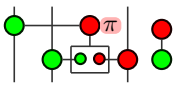
Another very interesting construction that uses the triangle is the following:



This time,  denote the diagram:



We may call this diagram *transistor*, for it acts as a switch, controlled by an additional wire. The last two diagrams can prove very useful to perform high order controlled operations. For instance, a CCNot can be represented by:



3.2 The $\mathbf{ZW}_{1/\sqrt{2}}$ Extension

We would also want to build a functor $F : \mathbf{ZX}[\frac{\pi}{4}] \to \mathbf{ZW}$ which preserves all the information. However we cannot have $[\![F(.)]\!] = [\![.]\!]$, because $[\![.]\!] : \mathbf{ZW} \to \mathbf{Qubit}_{\mathbb{Z}}$, while $[\![.]\!] : \mathbf{ZX}[\frac{\pi}{4}] \to \mathbf{Qubit}_{\mathbb{Z}\left[\frac{1}{\sqrt{2}}, e^{i\frac{\pi}{4}}\right]}$. We will need to use an encoding.

Recall that for any subring R of $\mathbb{C}$, if α is an R-algebraic integer, there exists an encoding $\psi : \mathcal{M}(R[\alpha]) \to \mathcal{M}(R)$. However, $1/\sqrt{2}$ cannot be an algebraic integer. Instead, we will define a simple extension of $\mathbf{ZW}$ that can represent morphisms of $\frac{1}{\sqrt{2}^{\mathbb{N}}}\mathbf{Qubit}_{\mathbb{Z}}$, i.e. of the form $\frac{1}{\sqrt{2}^p} f$ with $f \in \mathbf{Qubit}_{\mathbb{Z}}$, while preserving the completeness property.

Since $[\![.]\!] : \mathbf{ZW} \to \mathbf{Qubit}_{\mathbb{Z}}$ is full, all we have to do to allow the ZW-Calculus to represent any morphism of $\frac{1}{\sqrt{2}^{\mathbb{N}}}\mathbf{Qubit}_{\mathbb{Z}}$ is to add a scalar generator worth $1/\sqrt{2}$. n copies of this generator provide a representation of $1/\sqrt{2}^n$.

⌜ **Definition 3.2.1 ($\mathbf{ZW}_{1/\sqrt{2}}$ and $\mathrm{ZW}_{1/\sqrt{2}}$):** We define the graphical language $\mathbf{ZW}_{1/\sqrt{2}}$ as the language with the same generators as **ZW**, with the additional generator:

- $d : 0 \to 0 :: \scriptstyle\bigstar$

The functor $[\![.]\!]$ is extended to $\mathbf{ZW}_{1/\sqrt{2}}$ with:

- $[\![d]\!] = \frac{1}{\sqrt{2}}$

The associated axiomatisation $\mathrm{ZW}_{1/\sqrt{2}}$ is defined as:

- $\mathrm{ZW} \cup \left\{ \scriptstyle\bigstar\bigstar \bigcirc \underset{iv}{=} \boxed{}, \ \scriptstyle\bigstar \bullet \underset{z}{=} \bullet \right\}$

⌟

Proposition 3.2.2. *The functor* $[\![.]\!] : \mathbf{ZW}_{1/\sqrt{2}}/\ \mathrm{ZW}_{1/\sqrt{2}} \to \frac{1}{\sqrt{2}^{\mathbb{N}}}\mathbf{Qubit}_{\mathbb{Z}}$ *is full and faithful.*

Proof ▶ Let D_1 and D_2 be two diagrams of $\mathbf{ZW}_{1/\sqrt{2}}$ such that $[\![D_1]\!] = [\![D_2]\!]$. We can rewrite D_1 and D_2 as $D_i = d_i \otimes (\scriptstyle\bigstar)^{\otimes n_i}$ for some integers n_i and diagrams d_i of the **ZW** that do not use the $\scriptstyle\bigstar$ symbol.

We first assume $[\![D_i]\!] \neq 0$. Notice then that $n_1 = n_2 \bmod 2$. Indeed $[\![D_1]\!] = [\![D_2]\!] \implies \frac{[\![d_1]\!]}{\sqrt{2}^{n_1}} = \frac{[\![d_2]\!]}{\sqrt{2}^{n_2}}$. Since $[\![d_i]\!]$ are matrices over $\mathbb{Z}$, n_1 and n_2 are either both odd or both even.

First, assume $n_i = 0 \bmod 2$. From (iv), we get that $\mathrm{ZW}_{1/\sqrt{2}} \vdash d_i = D_i \otimes \left(\bigcirc\right)^{\otimes \frac{n_i}{2}}$. W.l.o.g. assume $n_1 \leq n_2$. Then $\left[\!\!\left[d_1 \otimes \left(\bigcirc\right)^{\otimes \frac{n_2-n_1}{2}} \right]\!\!\right] = 2^{\frac{n_2-n_1}{2}} [\![d_1]\!] = 2^{\frac{n_2}{2}} [\![D_1]\!] = [\![d_2]\!]$. Since $d_1 \otimes \left(\bigcirc\right)^{\otimes \frac{n_2-n_1}{2}}$ and d_2 are **ZW**-diagrams and have the same interpretation, thanks to the completeness of the ZW-Calculus, $\mathrm{ZW}_{1/\sqrt{2}} \vdash d_1 \otimes \left(\bigcirc\right)^{\otimes \frac{n_2-n_1}{2}} = d_2$, which implies $\mathrm{ZW}_{1/\sqrt{2}} \vdash d_1 \otimes \left(\bigcirc\right)^{\otimes \frac{n_2-n_1}{2}} \otimes (\scriptstyle\bigstar)^{\otimes n_2} = d_2 \otimes (\scriptstyle\bigstar)^{\otimes n_2}$ i.e. $\mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 = D_2$.

Now, we can easily show $\mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 \otimes \scriptstyle\bigstar = D_2 \otimes \scriptstyle\bigstar \iff \mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 = D_2$, proving the result when $n_i = 1 \bmod 2$:

$$\mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 \otimes \scriptstyle\bigstar = D_2 \otimes \scriptstyle\bigstar \implies \mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 \otimes \scriptstyle\bigstar\bigstar \bigcirc = D_2 \otimes \scriptstyle\bigstar\bigstar \bigcirc$$
$$\underset{iv}{\implies} \mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 = D_2 \implies \mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 \otimes \scriptstyle\bigstar = D_2 \otimes \scriptstyle\bigstar$$

Finally, if $[\![D_1]\!] = [\![D_2]\!] = 0$, then $[\![d_i]\!] = 0$. By completeness, $\mathrm{ZW} \vdash d_1 = d_2$ and $\mathrm{ZW} \vdash d_i \otimes \bullet = d_i$. Hence, using (iv) n_i times, $\mathrm{ZW}_{1/\sqrt{2}} \vdash d_i = d_i \otimes \bullet = d_i \otimes \bullet\ (\scriptstyle\bigstar)^{\otimes n_i} = d_i \otimes (\scriptstyle\bigstar)^{\otimes n_i} = D_i$, so $\mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 = d_1 = d_2 = D_2$. ◀

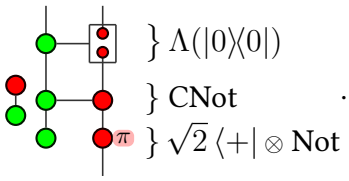
3.3 The ΔZX-Calculus

Interpreting the W-state using the Triangle

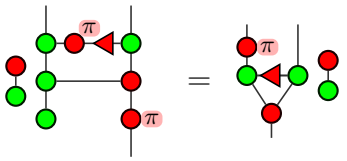
To make a link between the two languages, we first need a functor from $\mathbf{ZW}_{1/\sqrt{2}}$ to $\mathbf{ZX}[\frac{\pi}{4}]$. This should be pretty straightforward, since $\frac{1}{\sqrt{2}^{\mathbb{N}}}\mathcal{M}(\mathbb{Z}) \subset \mathcal{M}\left(\mathbb{Z}\left[\frac{1}{2}, e^{i\frac{\pi}{4}}\right]\right)$. The main difficulty is the representation in $\mathbf{ZX}[\frac{\pi}{4}]$ of the W spider. First of all, using the spider rule, we can always decompose the W spider as a composition of W nodes of arity 1, 2 and 3.

The interpretation of the three-legged W node is yet again an example of the use of the triangle. Indeed:

$$\left[\!\!\left[\right]\!\!\right] = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \left[\begin{pmatrix} 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] \circ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \circ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

These can be represented as 

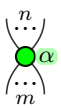
. This diagram can be simplified using $\mathrm{ZX}_{\pi/2}$:

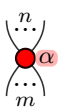


An extension of the ZX-Calculus

Hence, the functor from $\mathbf{ZW}_{1/\sqrt{2}}$ to $\mathbf{ZX}[\frac{\pi}{4}]$ would translate any white node to a 0 or π-green node, while the black nodes would be mapped to either π-red nodes or the above diagram. It turns out, the only occurrences of $\frac{\pi}{2}$ and $\frac{\pi}{4}$ would be hidden in the triangle, in the translation of the three-legged black dot. This means that using solely the triangle and ZX-generators of the π-fragment, one can express any matrix over $\mathbb{D} := \mathbb{Z}\left[\frac{1}{2}\right]$. Interestingly, this is exactly what post-selected quantum circuits generated by Toffoli and H can express. Hence, it becomes interesting to define a new intermediate language, called $\Delta\mathbf{ZX}$, where the triangle node is a generator and not mere syntactic sugar.

⌜ **Definition 3.3.1** ($\Delta\mathbf{ZX}$-Calculus)**:** The qubit $\Delta\mathbf{ZX}$-Calculus, is a †-compact graphical language, with the following set of generators and their string-diagram representation:

- $R_Z^{(n,m)}(\alpha) : n \to m ::$ 

- $R_X^{(n,m)}(\alpha) : n \to m ::$ 

- $H : 1 \to 1 ::$ 
- $\Delta : 1 \to 1 ::$ 

The PROP structure is provided by $\sigma : 2 \to 2 ::$  ; and the compact structure by $\epsilon : 2 \to 0 ::$  and $\eta : 0 \to 2 ::$  .

The functor † is such that:

- $\left(R_Z^{(n,m)}(\alpha)\right)^\dagger = R_Z^{(m,n)}(-\alpha)$
- $\left(R_X^{(n,m)}(\alpha)\right)^\dagger = R_X^{(m,n)}(-\alpha)$
- $H^\dagger = H$
- $\Delta^\dagger = (\epsilon \otimes id) \circ (id \otimes \Delta \otimes id) \circ (id \otimes \eta)$

The language comes with a PROP-functor $[\![.]\!] : \Delta\mathbf{ZX} \to \mathbf{Qubit}$, called the *standard interpretation*, and given by:

- $\left[\!\left[R_Z^{(n,m)}(\alpha)\right]\!\right] = |0^m\rangle\langle 0^n| + e^{i\alpha}\,|1^m\rangle\langle 1^n|$
- $\left[\!\left[R_X^{(n,m)}(\alpha)\right]\!\right] = |+^m\rangle\langle +^n| + e^{i\alpha}\,|-^m\rangle\langle -^n|$
- $[\![H]\!] = |+\rangle\langle 0| + |-\rangle\langle 1|$
- $[\![\Delta]\!] = |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 1|$
- $[\![\sigma]\!] = \sum_{i,j\in\{0,1\}} |ji\rangle\langle ij|$
- $[\![\eta]\!] = |00\rangle + |11\rangle$
- $[\![\epsilon]\!] = \langle 00| + \langle 11|$

Whatever the axiomatisation chosen for the $\Delta\mathbf{ZX}$-Calculus, we always consider that whenever two Δ-free diagrams are isomorphic as graphs, then they are equal. Alternatively, when keeping in mind that Δ is an oriented node, any graph isomorphism preserves the semantics. ⌟

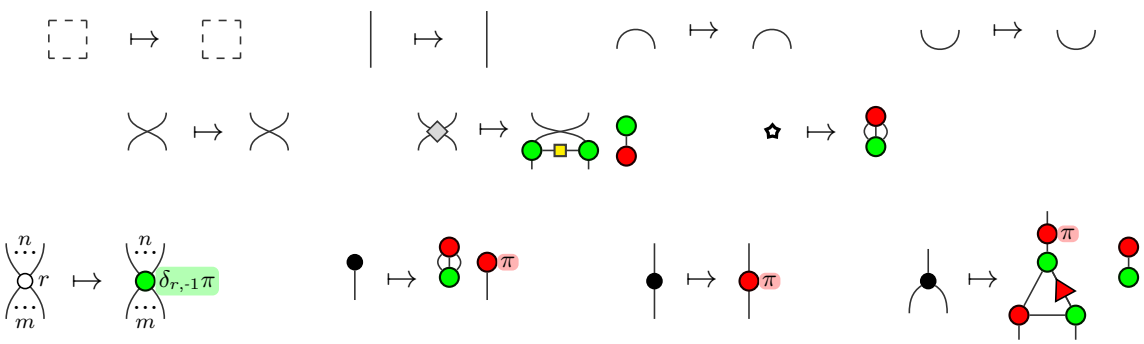
As for the ZX-Calculus, we denote by $\Delta\mathbf{ZX}[F]$ the fragment F of $\Delta\mathbf{ZX}$. $\Delta\mathbf{ZX}$ can be seen as an extension of $\mathbf{ZX}$, so axiomatisations of the ZX-Calculus can be applied to it.

3.4 From $\Delta\mathbf{ZX}[\pi]$ to $\mathbf{ZW}_{1/\sqrt{2}}$ and Back

$\mathbf{ZW}_{1/\sqrt{2}} \to \Delta\mathbf{ZX}[\pi]$

Our goal now is to provide a complete axiomatisation for $\Delta\mathbf{ZX}[\pi]$. To do so, we need functors from $\Delta\mathbf{ZX}[\pi]$ to $\mathbf{ZW}_{1/\sqrt{2}}$ and back. The one going back was roughly depicted in the previous section. We denote this functor by $[.]_X$. We can now give it a proper inductive definition:

$[.]_X$

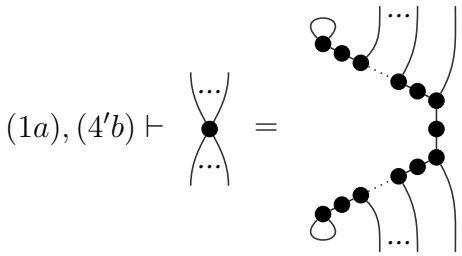


$$D_1 \circ D_2 \mapsto [D_1]_X \circ [D_2]_X \qquad D_1 \otimes D_2 \mapsto [D_1]_X \otimes [D_2]_X$$

where δ is the Kronecker symbol: $\delta_{x,y} = \begin{cases} 0 \text{ if } x \neq y \\ 1 \text{ if } x = y \end{cases}$

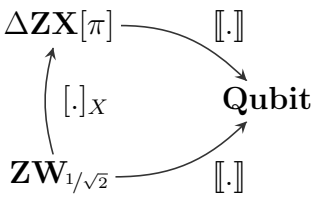
Notice that we did not give an interpretation of arbitrary black nodes $W^{(n,m)}$. By Rules $(1b)$ and $(4'b)$, one can decompose $W^{(n,m)}$ using only $W^{(1,1)}$, $W^{(1,2)}$ and $W^{(2,1)}$, in a spider-like style:

Lemma 3.4.1.



This interpretation preserves the semantics:

Proposition 3.4.2. *The following diagram commutes:*

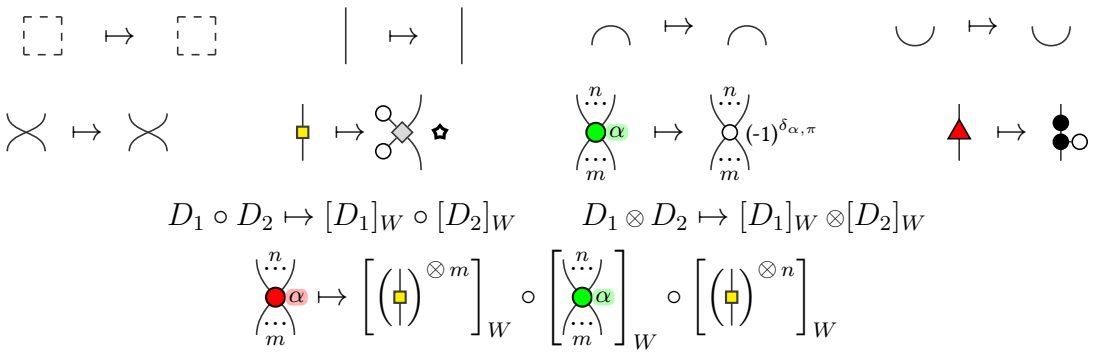


Proof ▶ This is routine. ◀

$\Delta\mathbf{ZX}[\pi] \to \mathbf{ZW}_{1/\sqrt{2}}$

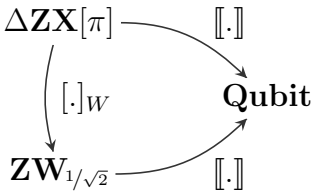
The other functor, from $\Delta\mathbf{ZX}[\pi]$ to $\mathbf{ZW}_{1/\sqrt{2}}$, will be denoted $[.]_W$. It can be easily defined as:

$[.]_W$



This interpretation also preserves the semantics:

Proposition 3.4.3. *The following diagram commutes:*



Proof ► This is routine. ◄

By introducing this intermediary language, our goal has shifted from:

- transporting the completeness of $\mathbf{ZW}_{1/\sqrt{2}}/\,\mathrm{ZW}_{1/\sqrt{2}}$ to $\mathbf{ZW}[\frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}$

to

- transporting the completeness of $\mathbf{ZW}_{1/\sqrt{2}}/\,\mathrm{ZW}_{1/\sqrt{2}}$ to $\Delta\mathbf{ZX}[\pi]/R$ for a set of axioms R
- then transporting the completeness of $\Delta\mathbf{ZX}[\pi]/R$ to $\mathbf{ZW}[\frac{\pi}{4}]$

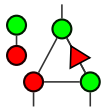
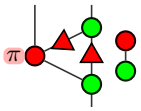
This method hence requires we provide a complete axiomatisation for the π-fragment of the new language $\Delta\mathbf{ZX}[\pi]/\,\Delta_\pi$.

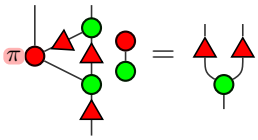
3.5 Axiomatisation for $\Delta\mathbf{ZX}[\pi]$

From interpretation $[.]_X$ we can get a set of equations that a complete axiomatisation of $\Delta\mathbf{ZX}[\pi]$ would need to verify: the interpretation of the axioms of $\mathrm{ZW}_{1/\sqrt{2}}$. We can try and reduce them using the usual axioms of the ZX-Calculus. We eventually get to the axiomatisation Δ_π given in Figure 3.1. In this section and the next two, we are going to show that it is complete:

Theorem 3.5.1 (Completeness of $\Delta\mathbf{ZX}[\pi]/\,\Delta_\pi$)**.** $[\![.]\!] : \Delta\mathbf{ZX}[\pi]/\,\Delta_\pi \to \frac{1}{\sqrt{2}^{\mathbb{N}}}\mathbf{Qubit}_{\mathbb{Z}}$ *is full and faithful. In particular, the language* $\Delta\mathbf{ZX}[\pi]/\,\Delta_\pi$ *is complete.*

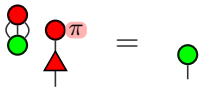
On the rules of Δ_π

Before diving into the proof, let us comment on the set of rules Δ_π. Notice that it uses most of the axioms of ZX_π, together with new rules using  . We can try and give an interpretation for these last equations. First, we have the fact that  is a diagonal morphism for the comultiplication  . This directly gives (TW). (HT) can be seen as the decomposition of Hadamard using triangles. Also, remember that  is a morphism of monoids between (AND, $|1\rangle$) and ($|0\rangle\langle 00| + |1\rangle\langle 11|$, $\sqrt{2}\,|+\rangle$). Noticing that  represents the AND gate, this gives us:



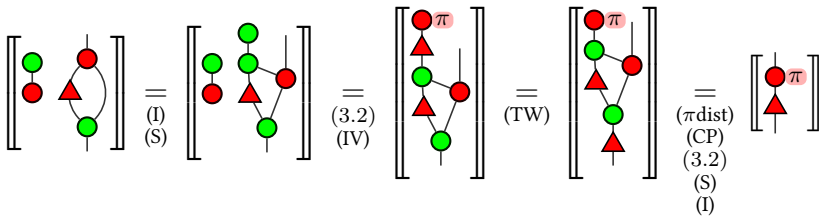
(3.1)

and



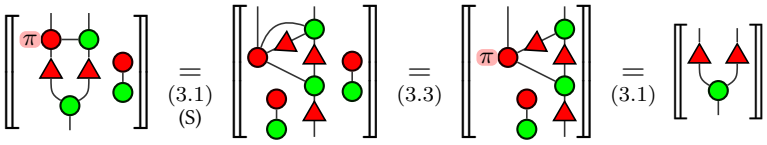
(3.2)

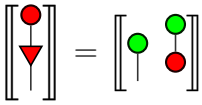
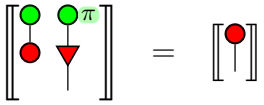
We can then recover an equation that is very close to (TCX) if we assume we can operate the π-distribution (πdist). First:

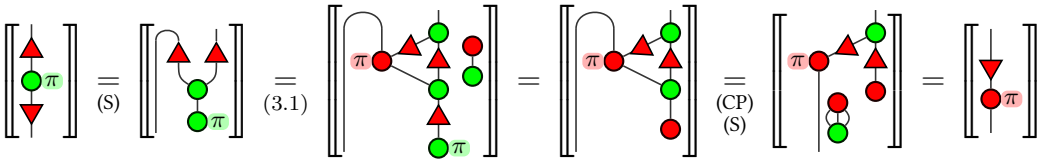


(3.3)

Then:



We can also recover (BΔ), if we assume  and  :



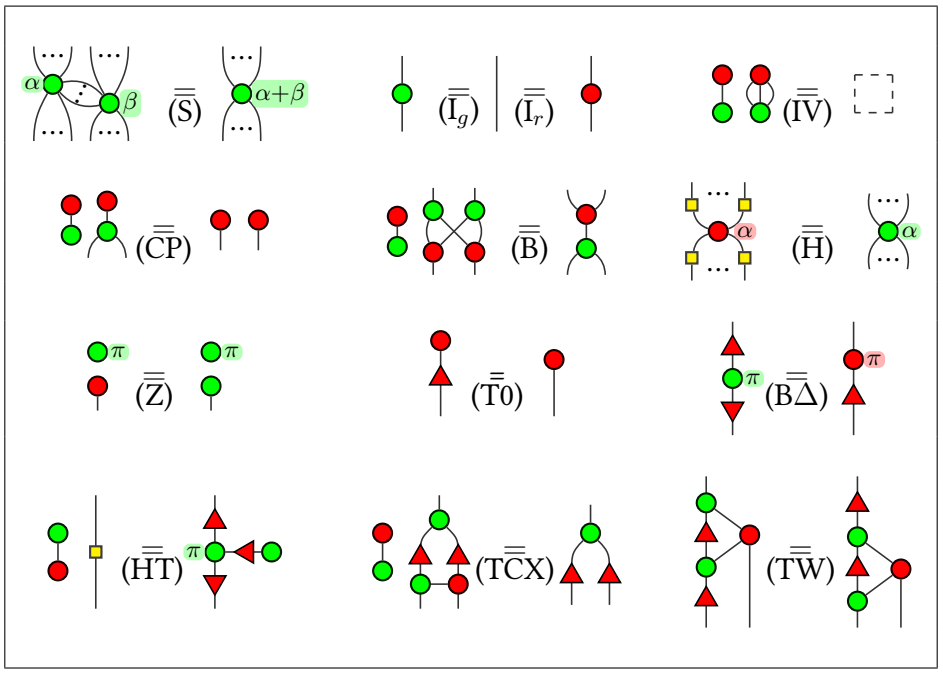


Figure 3.1: Set of rules Δ_π for the ZX-Calculus with triangles. The right-hand side of (IV) is an empty diagram. (...) denotes zero or more wires, while (.˙.) denotes one or more wires. $\alpha, \beta \in \mathbb{R}$.

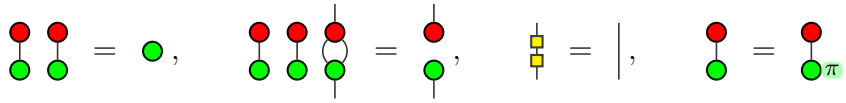
$\Delta\mathbf{ZX}[\pi]/\Delta_\pi$ is Complete for the Real Stabiliser

As announced, we want to prove that this axiomatisation is complete. First of all let us show that we can recover ZX_π:

Proposition 3.5.2. $\Delta_\pi \vdash \mathrm{ZX}_\pi$

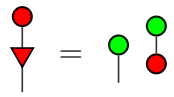
This means that any Δ-free equality between $\Delta\mathbf{ZX}[\pi]$-diagrams is derivable.

To prove this, we have to "bootstrap" the language $\Delta\mathbf{ZX}[\pi]/\Delta_\pi$. Notice that since we have most of the rules of ZX_π in Δ_π, thanks to Proposition 2.7.16, we already have access to some usual lemmas, such as:

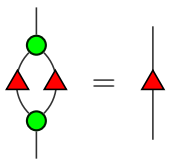
$\Delta_\pi \vdash$ 

These will be useful in the derivation of other $\Delta\mathbf{ZX}$-specific lemmas:

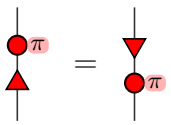
Lemma 3.5.3.



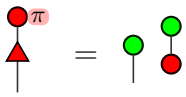
Lemma 3.5.4.



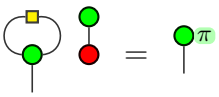
Lemma 3.5.5.



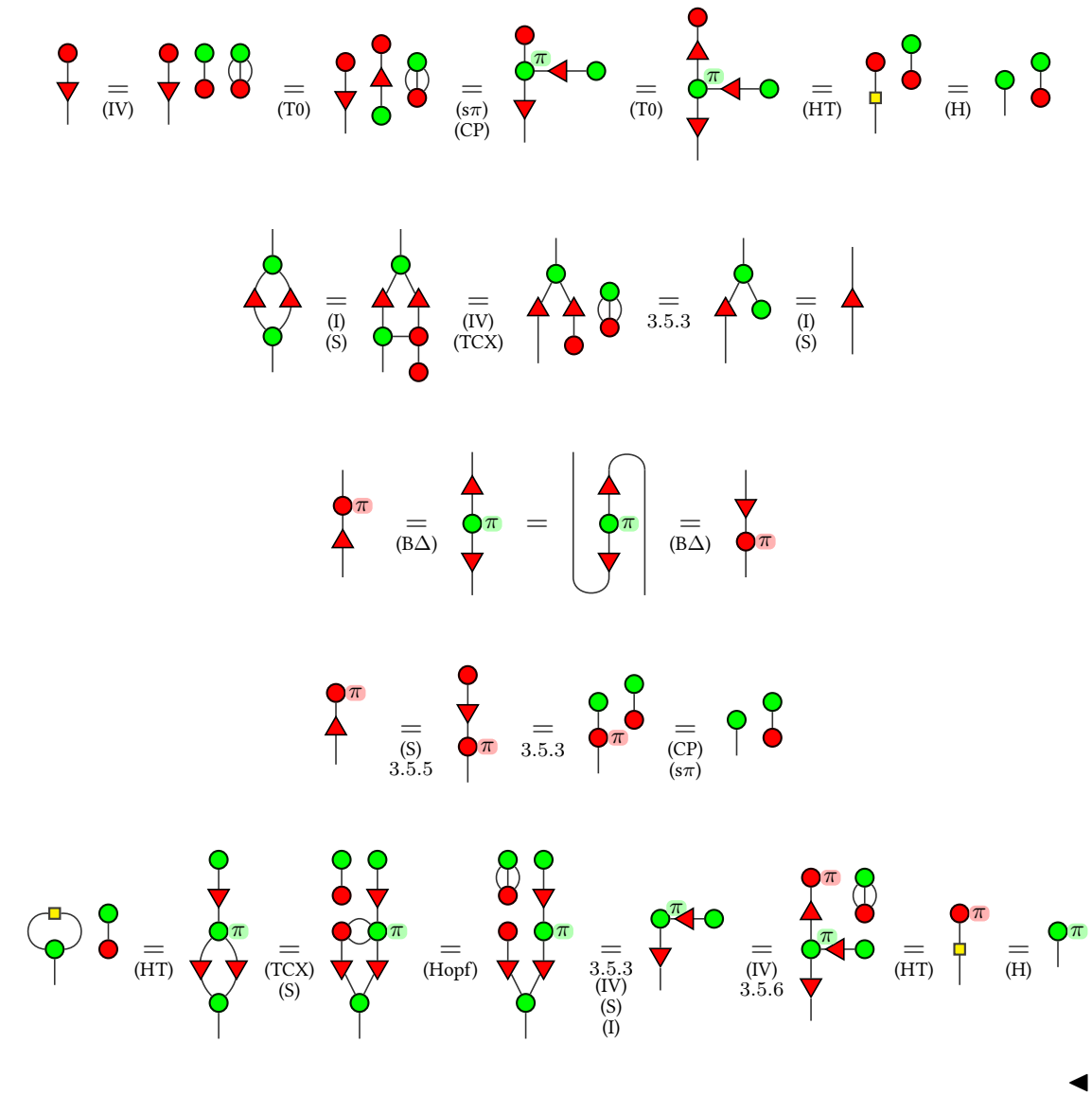
Lemma 3.5.6.



Lemma 3.5.7.



Proof ▶



◀

Proof *of Prop. 3.5.2* ▶ The only axiom of ZX_π that is not in Δ_π is (HL), which is derivable according to Lemma 3.5.7. ◀

3.6 $\mathrm{ZW}_{1/\sqrt{2}}$ derives from Δ_π

We can now state the most important proposition for the completeness.

Proposition 3.6.1. *For any two diagrams D_1 and D_2 of* $\mathbf{ZW}_{1/\sqrt{2}}$*:*

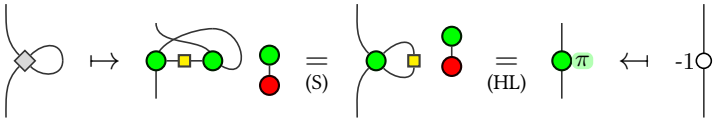
$$\mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 = D_2 \implies \Delta_\pi \vdash [D_1]_X = [D_2]_X$$

Proof *of Prop. 3.6.1* ▶ If $\mathrm{ZW}_{1/\sqrt{2}} \vdash D_1 = D_2$, then there exists a series of $\mathbf{ZW}_{1/\sqrt{2}}$-diagrams $d_1, \cdots, d_n$ such that there is exactly one axiom application between d_i and d_{i+1}, between D_1 and d_1 and between d_n and D_2. Hence, since $[.]_X$ is a PROP-functor,

it suffices to prove that every axiom of $\mathrm{ZW}_{1/\sqrt{2}}$ can be derived from Δ_π after application of $[.]_X$.

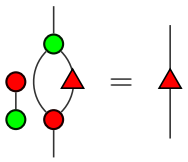
The rest of this proof is technical: every axiom of $\mathrm{ZW}_{1/\sqrt{2}}$ is translated in $\Delta\mathbf{ZX}[\pi]$ and proved using Δ_π. It will alternate between lemmas in $\Delta\mathbf{ZX}[\pi]/\,\Delta_\pi$ and axiom derivations. For the reader's convenience, this proof ends at page 99. ◀

***Proof** of Prop. 3.6.1 (ctd.)* ▶ $0b$ comes directly from the semantics-preserving graph isomorphisms.
$1b$, $2a$ and $2b$ come directly from the spider rules (S) and (I).
$2c$:

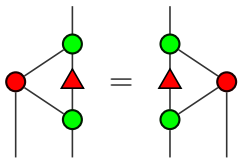


◀

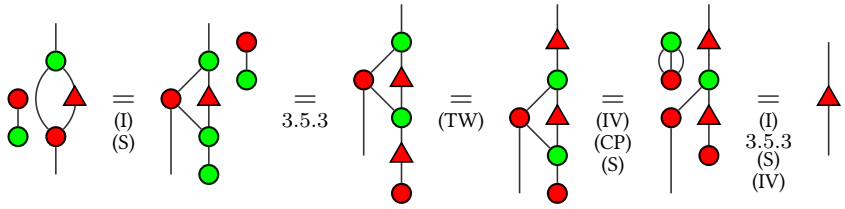
Lemma 3.6.2.

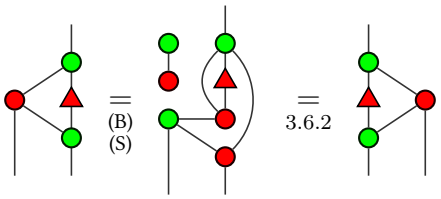


Lemma 3.6.3.

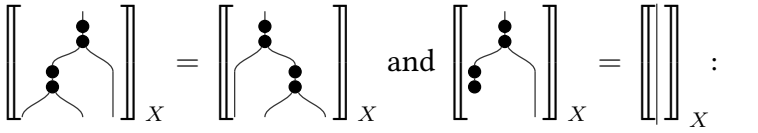


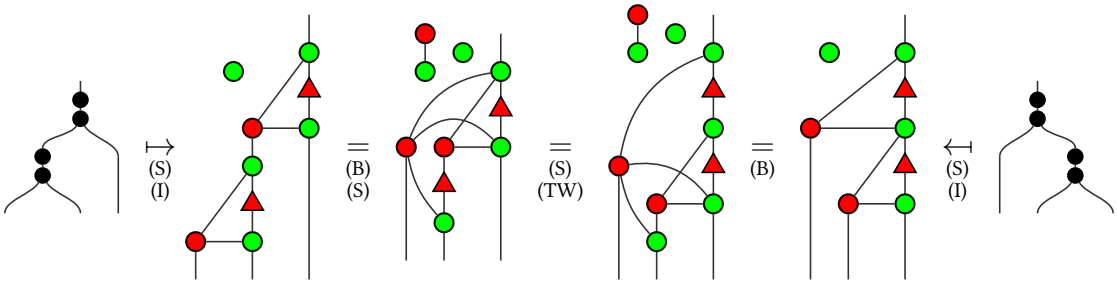
Proof ▶

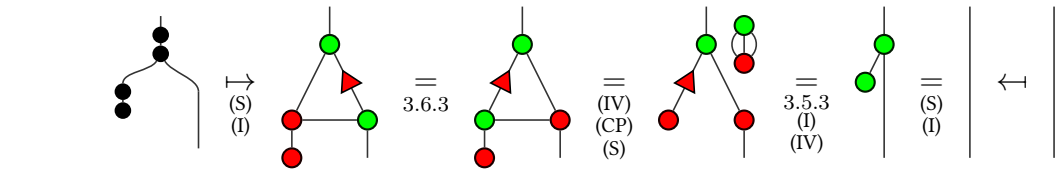




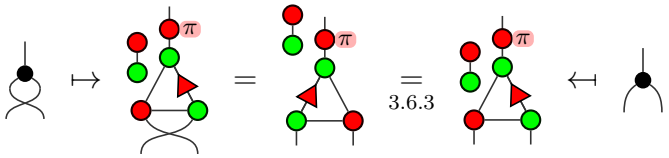
◀

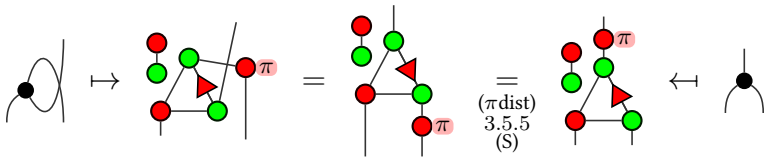
***Proof** of Prop. 3.6.1 (ctd.)* ▶ $1a$: Thanks to Lemma 3.4.1 and rule $(4b')$, the rule can be reduced to showing that  :



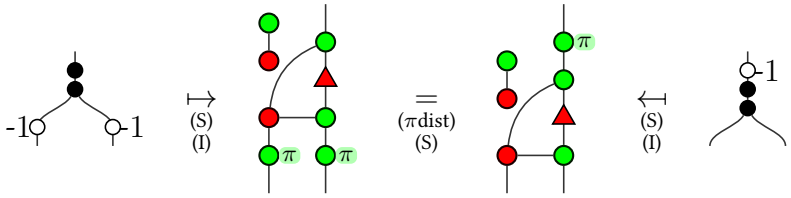


$0a$: Thanks to Lemma 3.4.1 and the previous equations, it suffices to prove the result for 2 and 3-legged W nodes. The first is obvious. For the 3-legged W nodes:

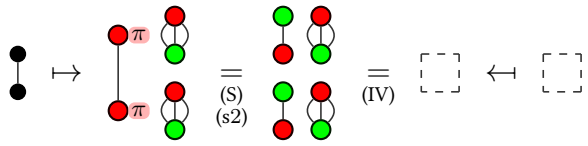




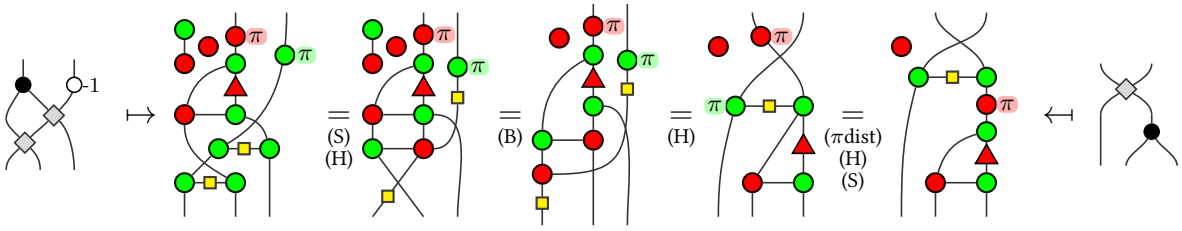
The last case in then derivable from the other two.
$3a$ is the expression of (πdist).
$3b$:



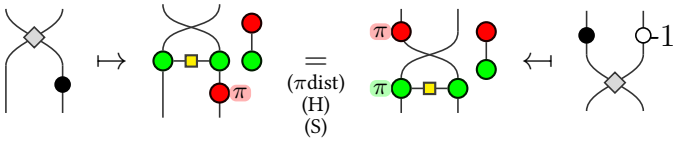
$5c$:



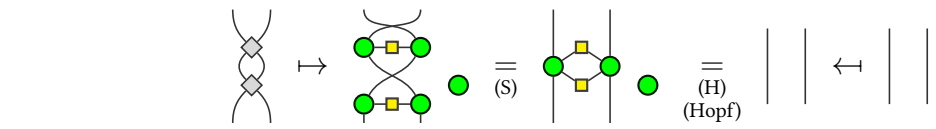
7: Again, thanks to Lemma 3.4.1, it suffices to prove the result when W has arity 2 or 3:



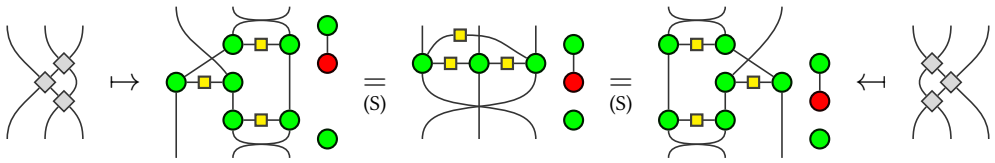
and:



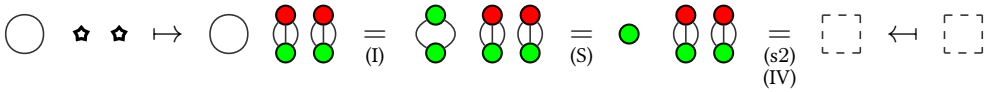
R_2:



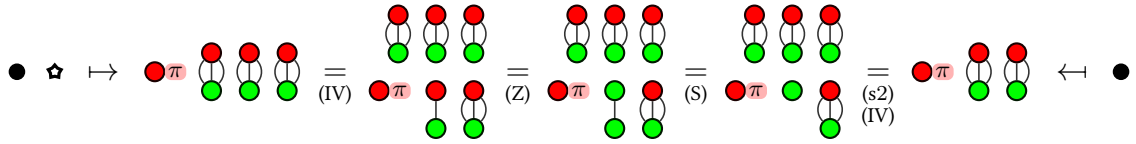
R_3:



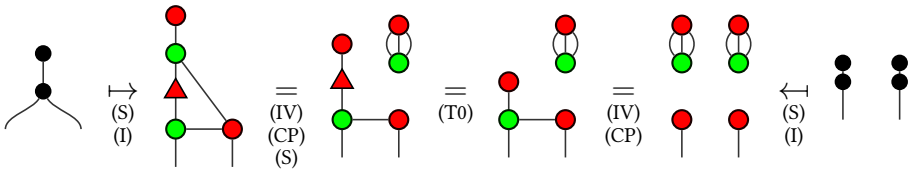
iv:



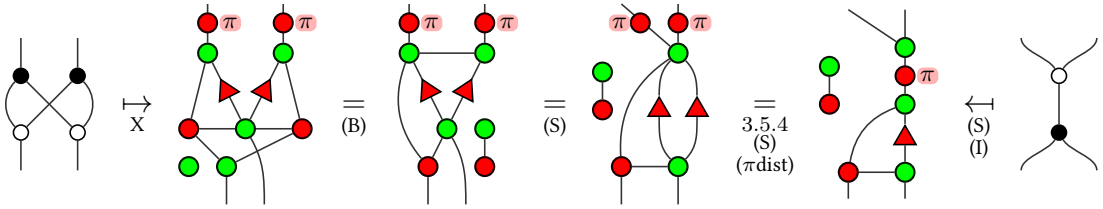
z:



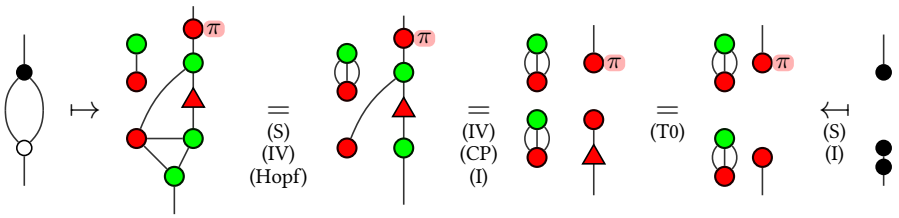
$5b$:



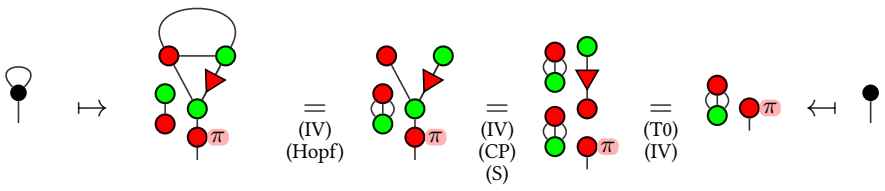
$6a$:



$6b$:

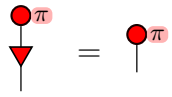


$4'b$:

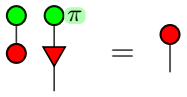


◀

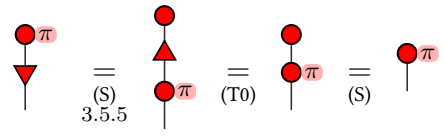
Lemma 3.6.4.

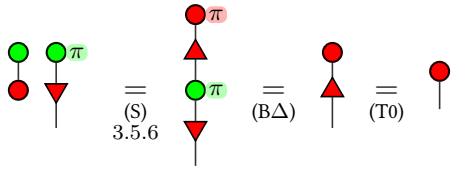


Lemma 3.6.5.



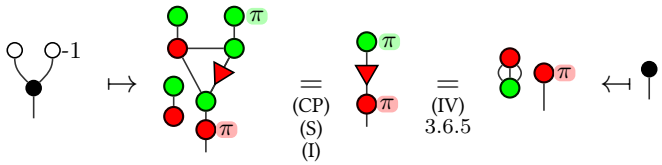
Proof ▶





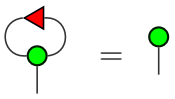
◀

Proof *of Prop. 3.6.1 (ctd.)* ▶ $4'a$:

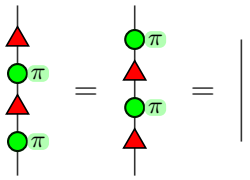


◀

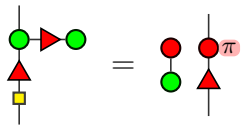
Lemma 3.6.6.



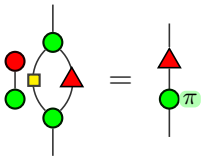
Lemma 3.6.7.



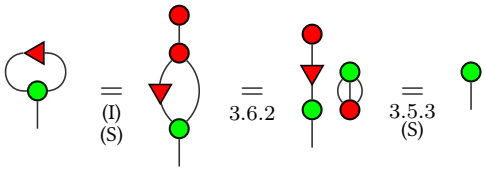
Lemma 3.6.8.

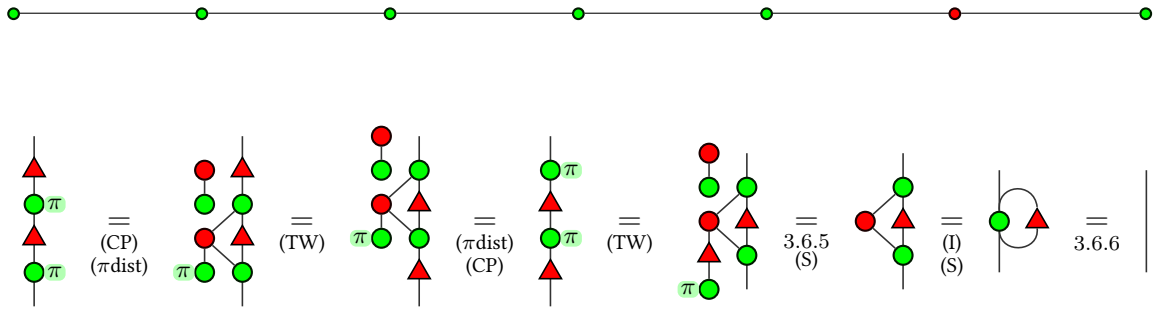


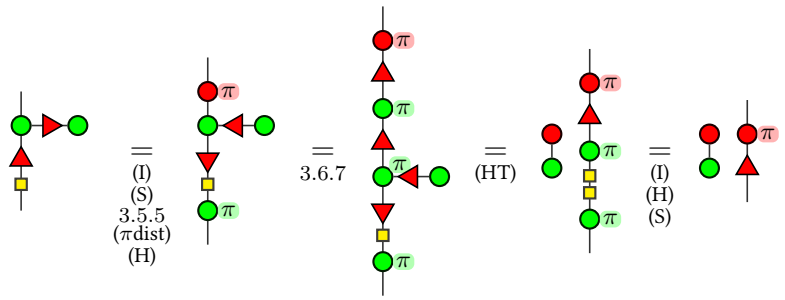
Lemma 3.6.9.

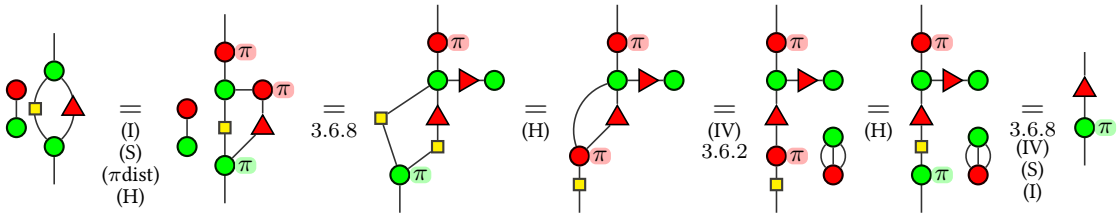


Proof ▶



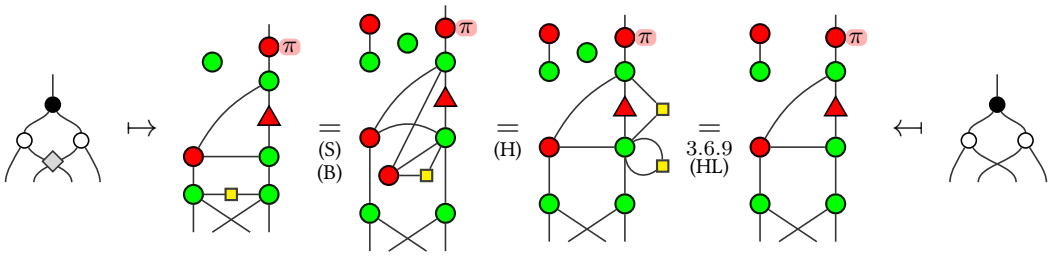






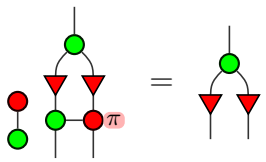
◀

***Proof** of Prop. 3.6.1 (ctd.)* ▶ X:

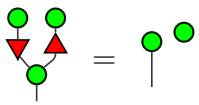


◀

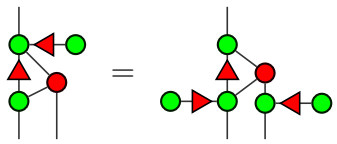
Lemma 3.6.10.



Lemma 3.6.11.

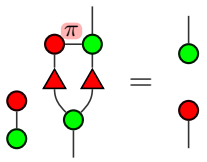


Lemma 3.6.12.

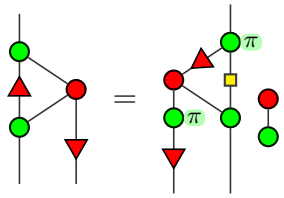


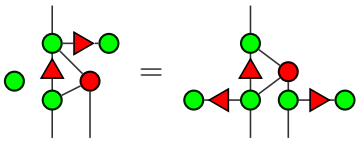
and

Lemma 3.6.13.

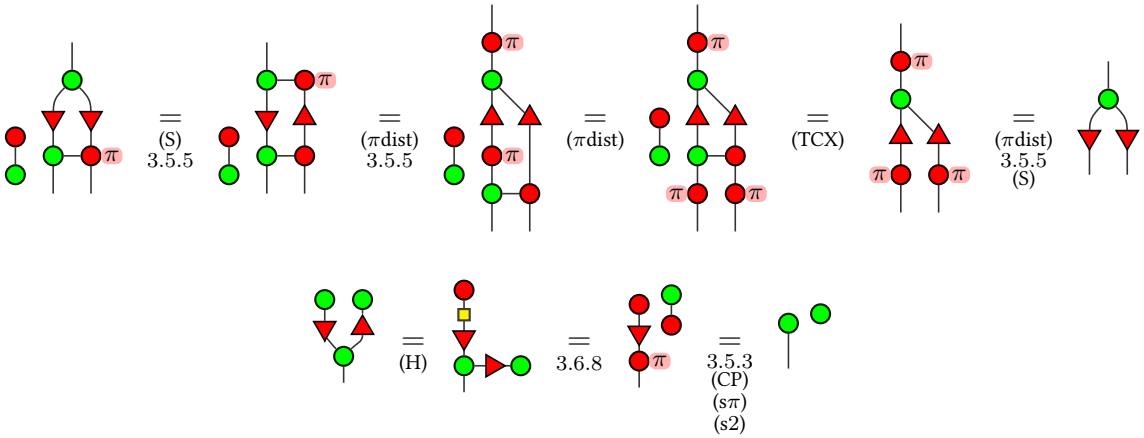


Lemma 3.6.14.

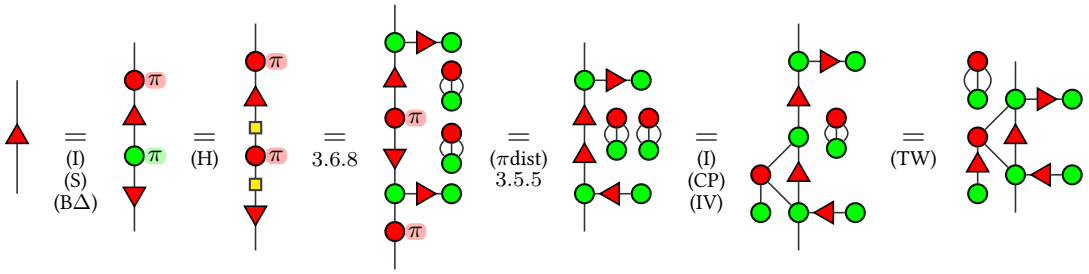




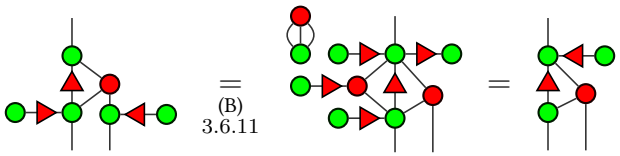
Proof ▶



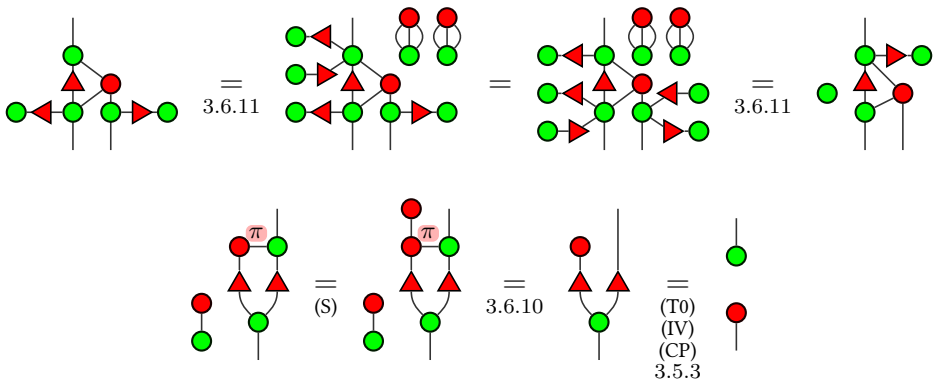
For Lemma 3.6.12, first:



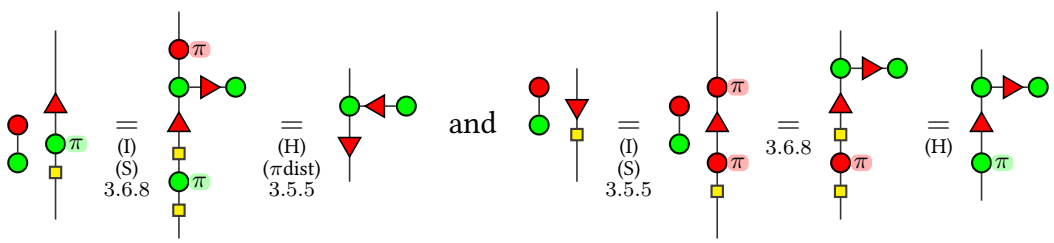
Then



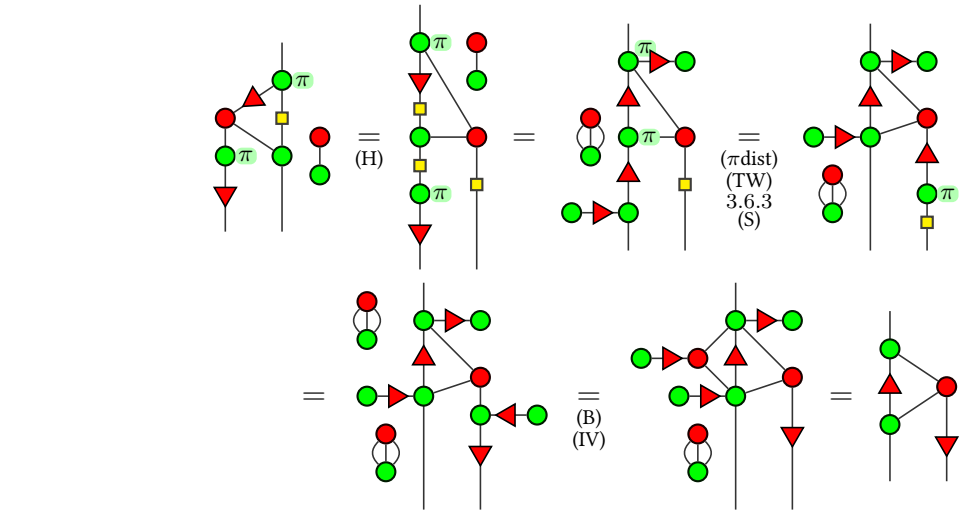
Finally



For Lemma 3.6.14, first:

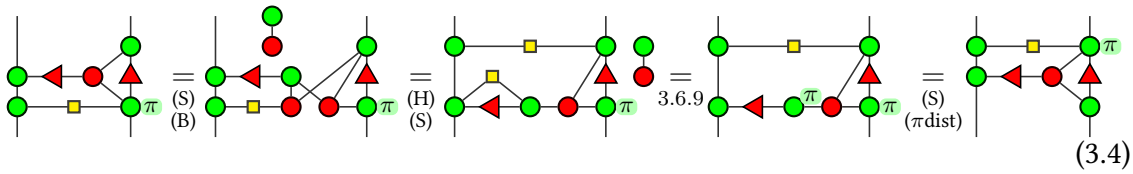


Finally:

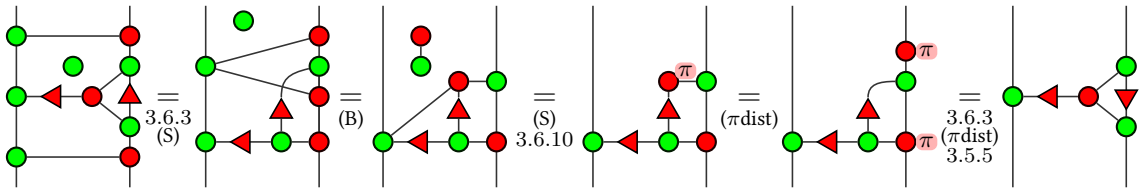


◀

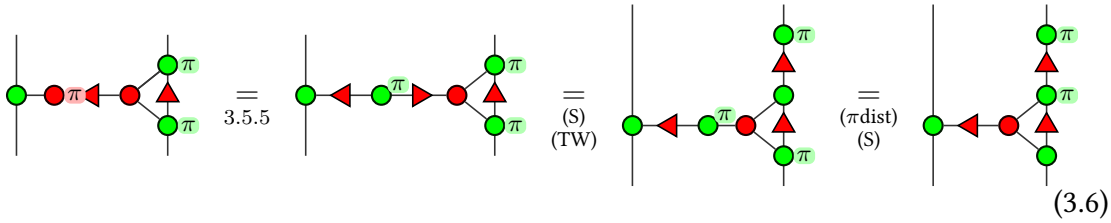
Proof *of Prop. 3.6.1 (ctd.)* ▶ $5a$: We will need a few steps to prove this equality.



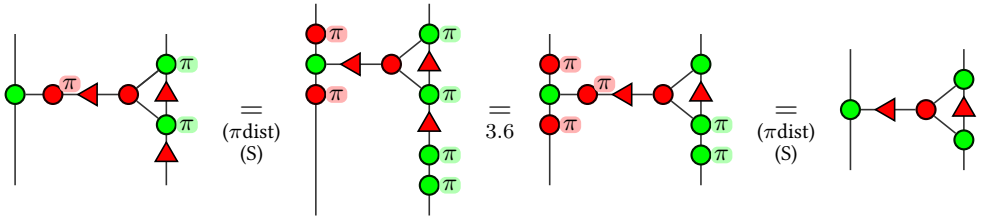
(3.4)



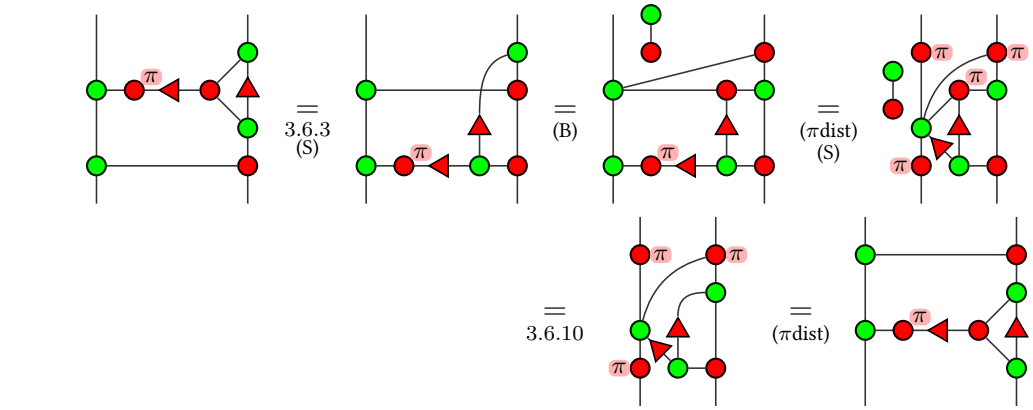
(3.5)



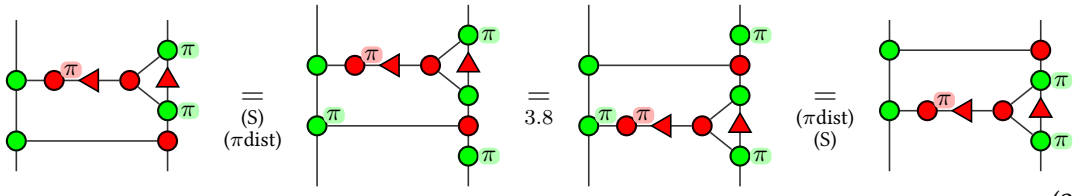
(3.6)



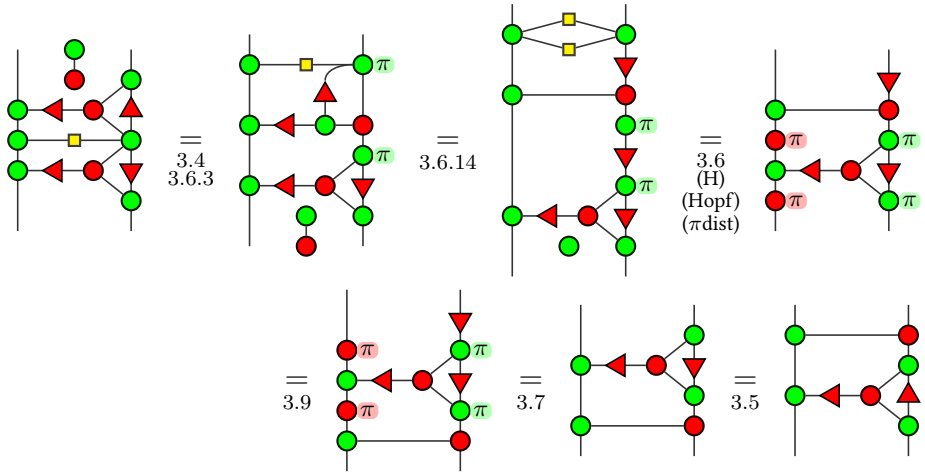
(3.7)



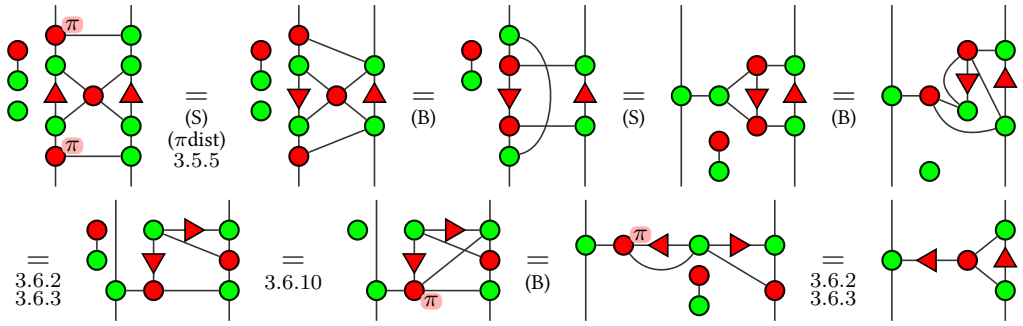
(3.8)



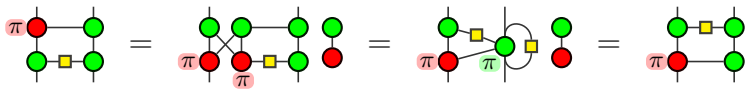
(3.9)



(3.10)

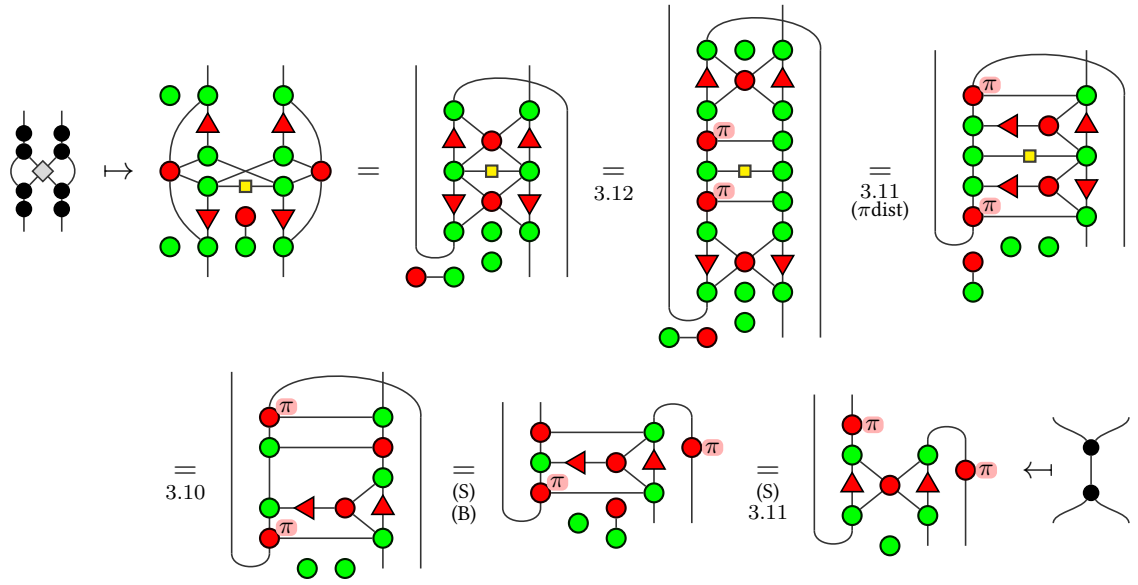


(3.11)



(3.12)

Finally,



This was the last equality of $\mathrm{ZW}_{1/\sqrt{2}}$ to derive. We hence have proven the result. ◀

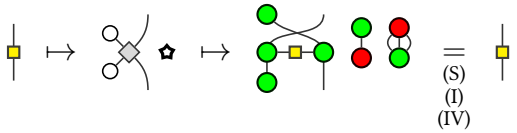
3.7 Completeness of $\Delta\mathbf{ZX}[\pi]/\,\Delta_\pi$

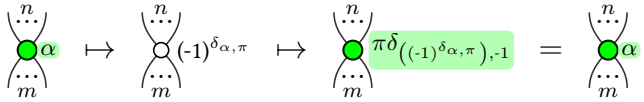
To finish the proof of completeness, we still need the property that after the application of the composite interpretation $[[.]_W]_X$ we can always recover the initial diagrams, i.e. we need to show: that $[[.]_W]_X = id$.

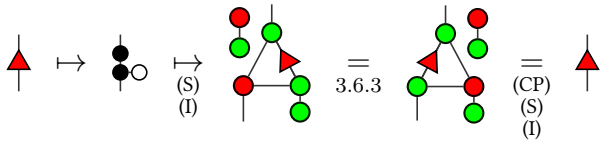
Proposition 3.7.1. *For any $\Delta\mathbf{ZX}[\pi]$-diagram D, we have:*

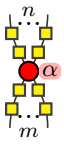
$$\Delta_\pi \vdash [[D]_W]_X = D$$

Proof ▶ This is done by induction on the diagram D:

- $[[D_1 \otimes D_2]_W]_X = [[D_1]_W]_X \otimes [[D_2]_W]_X$
- $[[D_1 \circ D_2]_W]_X = [[D_1]_W]_X \circ [[D_2]_W]_X$
- 

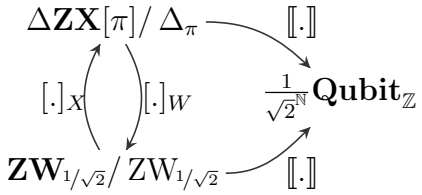
- 

- 

- $\Big[\Big[\Big[$  $\Big]_W\Big]_X$ gives  $\underset{\text{(H)}}{=}$  .

◀

***Proof** of Theorem 3.5.1* ▶ There are two results here: fullness and faithfulness. Consider the following diagram:



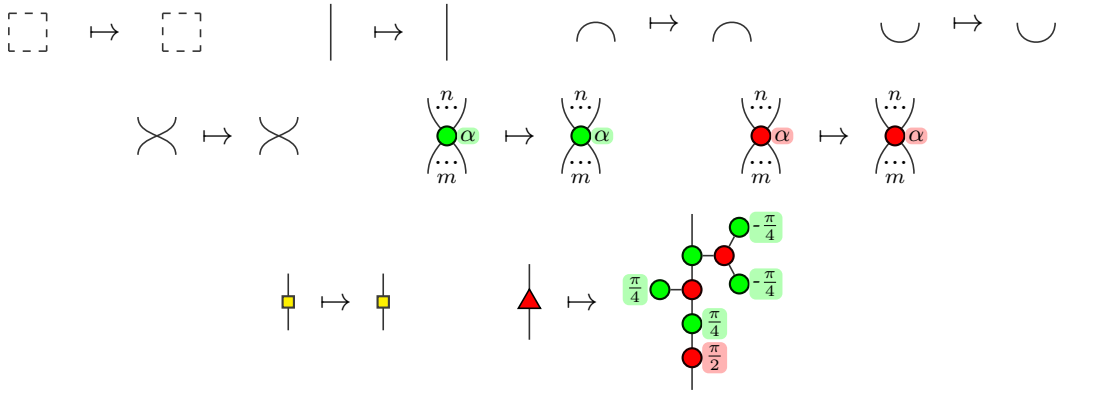
- $[.]_W$ **is faithful**: let $D_1, D_2 : n \to m \in \Delta\mathbf{ZX}[\pi]$ such that $\mathrm{ZW}_{1/\sqrt{2}} \vdash [D_1]_W = [D_2]_W$. By Proposition 3.6.1, $\Delta_\pi \vdash [[D_1]_W]_X = [[D_2]_W]_X$, so by Proposition 3.7.1, $\Delta_\pi \vdash D_1 = D_2$.
- $[.]_W$ **is full**: Let $D \in \mathbf{ZW}_{1/\sqrt{2}}$. We define $D_X := [D]_X$. By Propositions 3.4.3 and 3.4.2, $[\![[.]_X]_W]\!] = [\![.]\!]$, hence, by completeness of $\mathbf{ZW}_{1/\sqrt{2}}/\,\mathrm{ZW}_{1/\sqrt{2}}$, $\mathrm{ZW}_{1/\sqrt{2}} \vdash [[D]_X]_W = D$, i.e. $\mathrm{ZW}_{1/\sqrt{2}} \vdash [D_X]_W = D$.

By composition, $[\![[.]_W]\!]$ is full and faithful, so $\Delta\mathbf{ZX}[\pi]/\,\Delta_\pi \xrightarrow{[\![.]\!]} \frac{1}{\sqrt{2}^{\mathbb{N}}}\mathbf{Qubit}_{\mathbb{Z}}$ is full and faithful. ◀

3.8 From $\Delta\mathbf{ZX}[\pi]$ to $\mathbf{ZX}[\frac{\pi}{4}]$

We now want to do essentially the same job to find a complete axiomatisation of $\mathbf{ZX}[\frac{\pi}{4}]$, and using the newfound completeness of $\Delta\mathbf{ZX}[\pi]$. First of all, we need to translate $\Delta\mathbf{ZX}[\pi]$ into $\mathbf{ZX}[\frac{\pi}{4}]$. The two languages are very close, the only generator of the former that is not in the latter is Δ. However, we already know how to represent it (Section 3.1):

$[.]_T$



$D_1 \circ D_2 \mapsto [D_1]_T \circ [D_2]_T \qquad D_1 \otimes D_2 \mapsto [D_1]_T \otimes [D_2]_T$

Again, we can translate all the axioms of Δ_π in $\mathbf{ZX}[\frac{\pi}{4}]$. It gives a set of equations that the language is supposed to be able to derive, and reducing it leads an a potential axiomatisation for Clifford+T ZX-Calculus. We propose the set of rules given in Figure 3.2. It consists of the rules $\mathrm{ZX}_{\pi/2}$ with the additional (K) that we have already seen in Proposition 2.7.13, (E)– introduced in [JPVW17] –, (SUP)– proven necessary in [PW16] –, (C) and (BW), replacing (IV) and (Z).

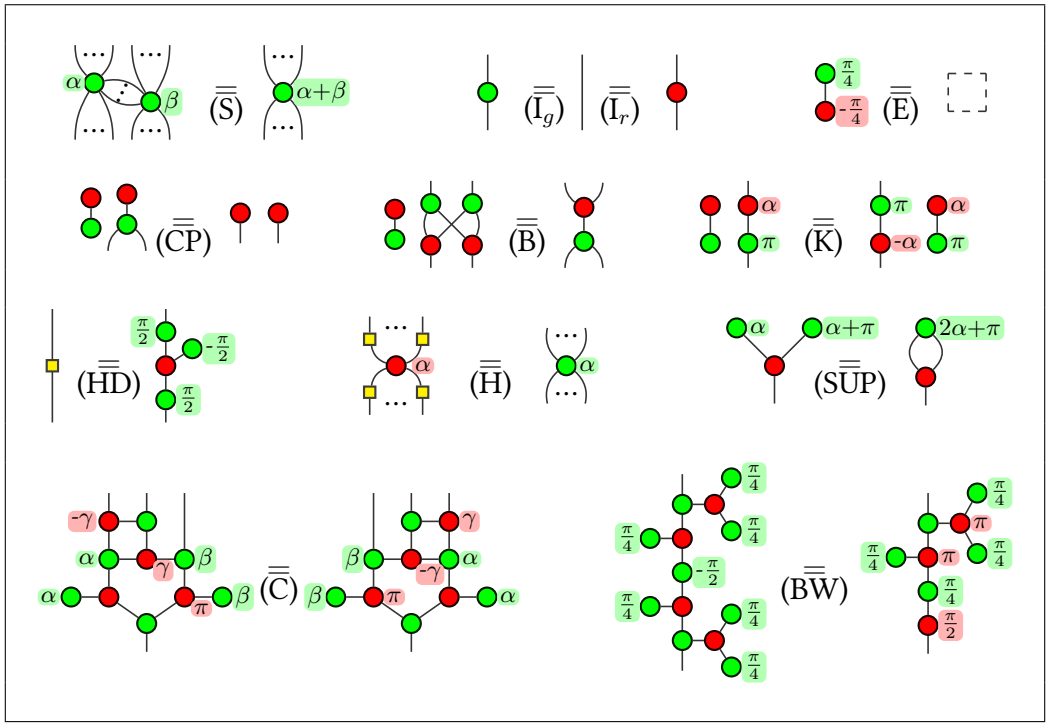
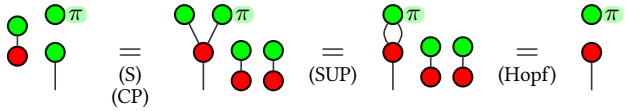


Figure 3.2: Set of rules $\mathrm{ZX}_{\pi/4}$ for the Clifford+T fragment of the ZX-Calculus.

Since this axiomatisation is pretty close to containing $\mathrm{ZX}_{\pi/2}$, a first useful result is that we can recover it.

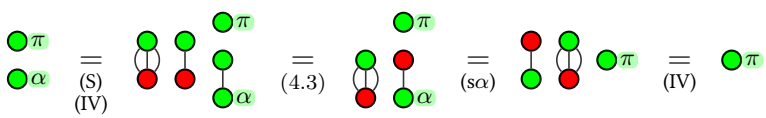
Proposition 3.8.1. $\mathrm{ZX}_{\pi/4} \vdash \mathrm{ZX}_{\pi/2}$

Proof ▶ The only axioms that need to be proven are (IV) and (Z). From Figure 2.2, we directly get the Hopf law (Hopf), as well as (IV). Still from Proposition 2.7.16 we also get (sα). Now only (Z) remains to be proven. First:



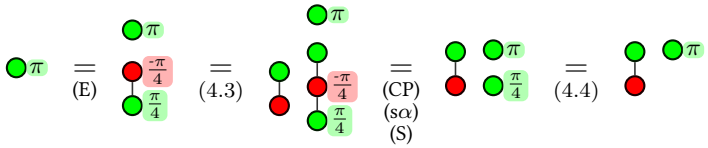
(3.13)

Then:



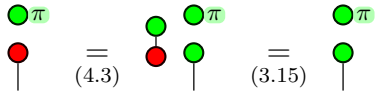
(3.14)

Then:



(3.15)

Finally:



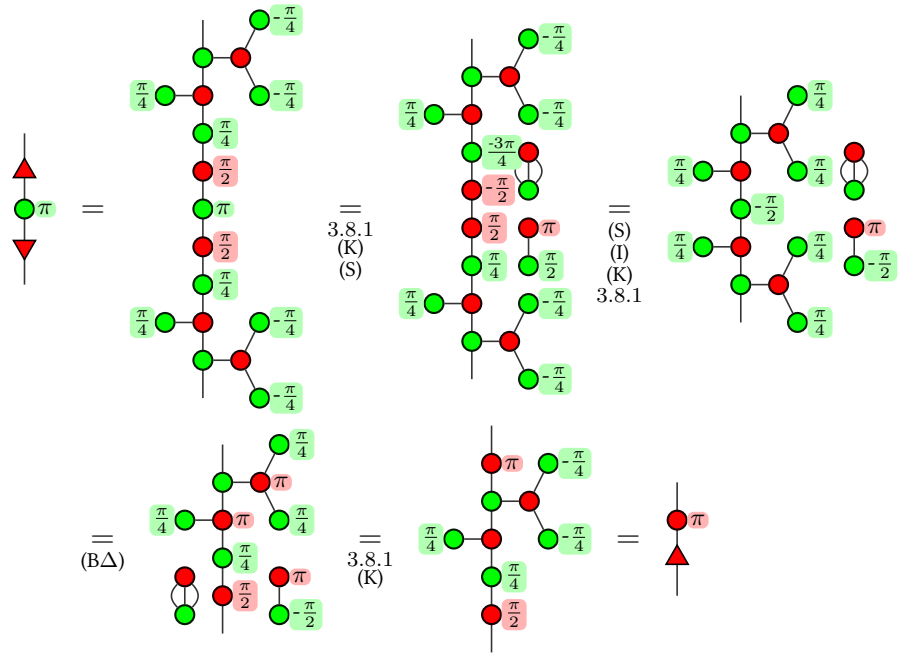
◀

This set of rules proves any equality of $\Delta\mathbf{ZX}[\pi]/\Delta_\pi$.

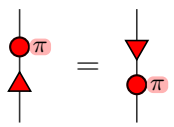
Proposition 3.8.2. *For any $\Delta\mathbf{ZX}[\pi]$-diagrams D_1 and D_2,*

$$\Delta_\pi \vdash D_1 = D_2 \implies \mathrm{ZX}_{\pi/4} \vdash [D_1]_T = [D_2]_T$$

Proof ▶ We already know that $\mathrm{ZX}_{\pi/4} \vdash \mathrm{ZX}_{\pi/2}$. The remaining axioms of Δ_π to prove are (T0), (HT), (TW), (TCX) and (BΔ).
(BΔ):



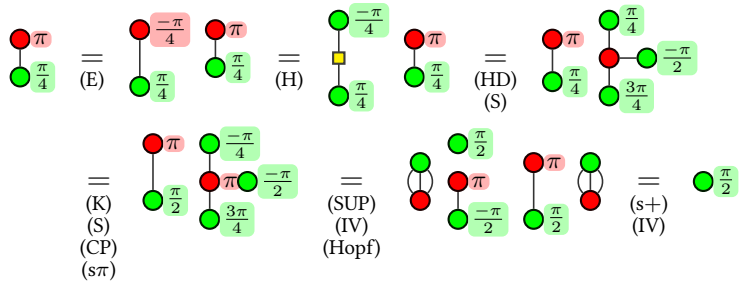
From this rule (BΔ) we instantaneously get that:



which will be used extensively in the following. The result is akin to Lemma 3.5.5, but this time expressed with syntactic sugar. Again, the rest of the proof will alternate between lemmas and proofs of the remaining rules. The proof ends at page 108. ◀

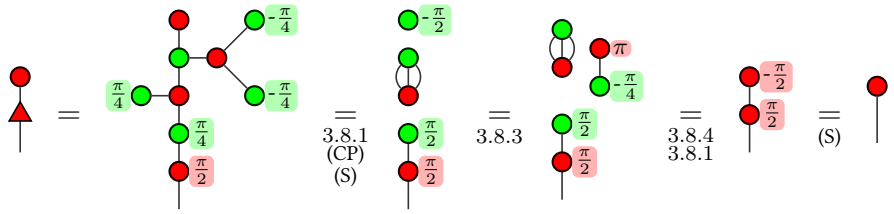
Lemma 3.8.3.

Proof ▶



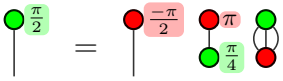
◀

Proof *of Prop. 3.8.2 (ctd.)* ▶

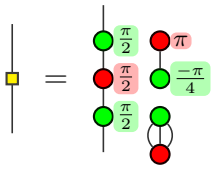


◀

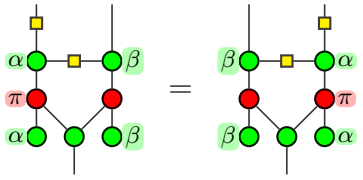
Lemma 3.8.4.



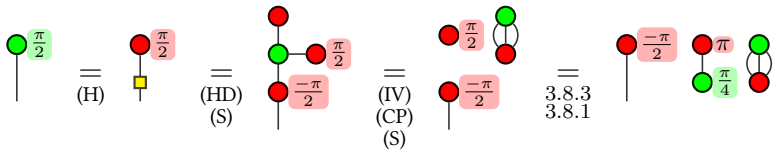
Lemma 3.8.5.

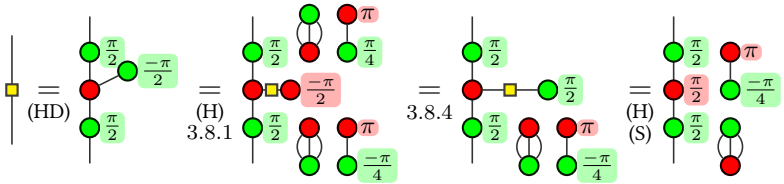


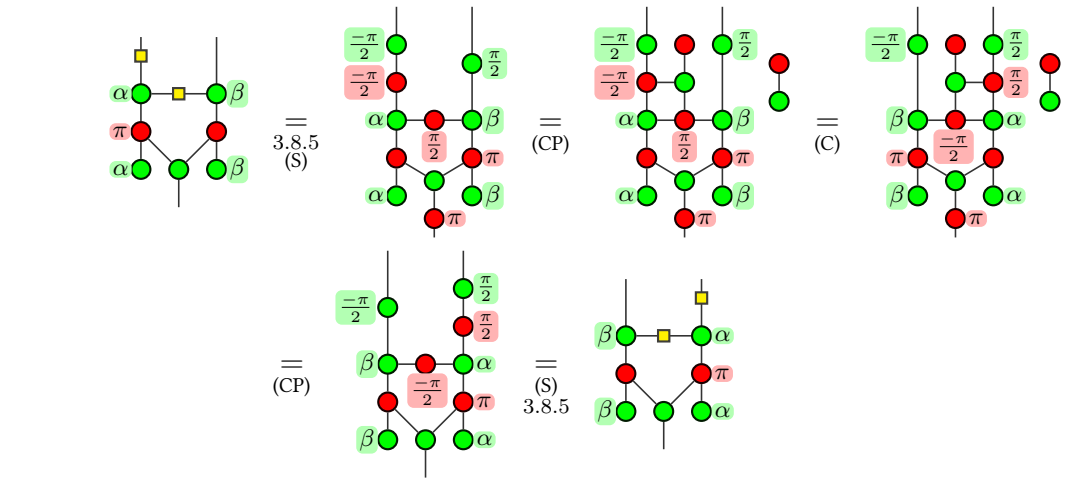
Lemma 3.8.6.



Proof ▶

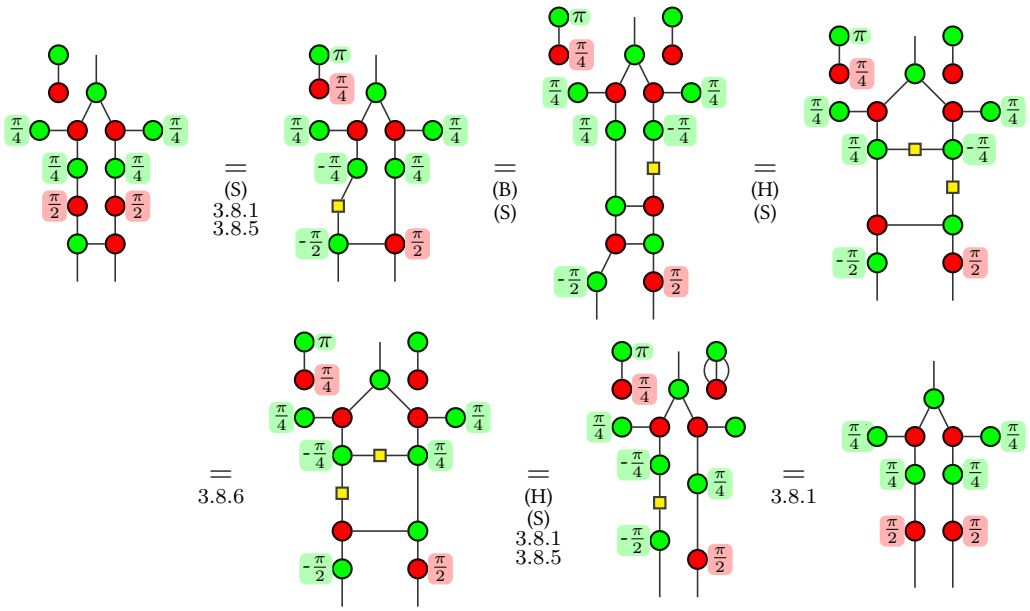






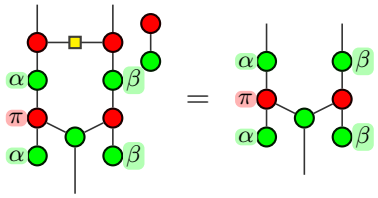
◀

Proof *of Prop. 3.8.2 (ctd.)* ▶ (TCX):

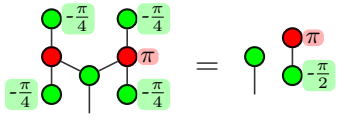


◀

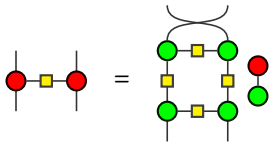
Lemma 3.8.7.



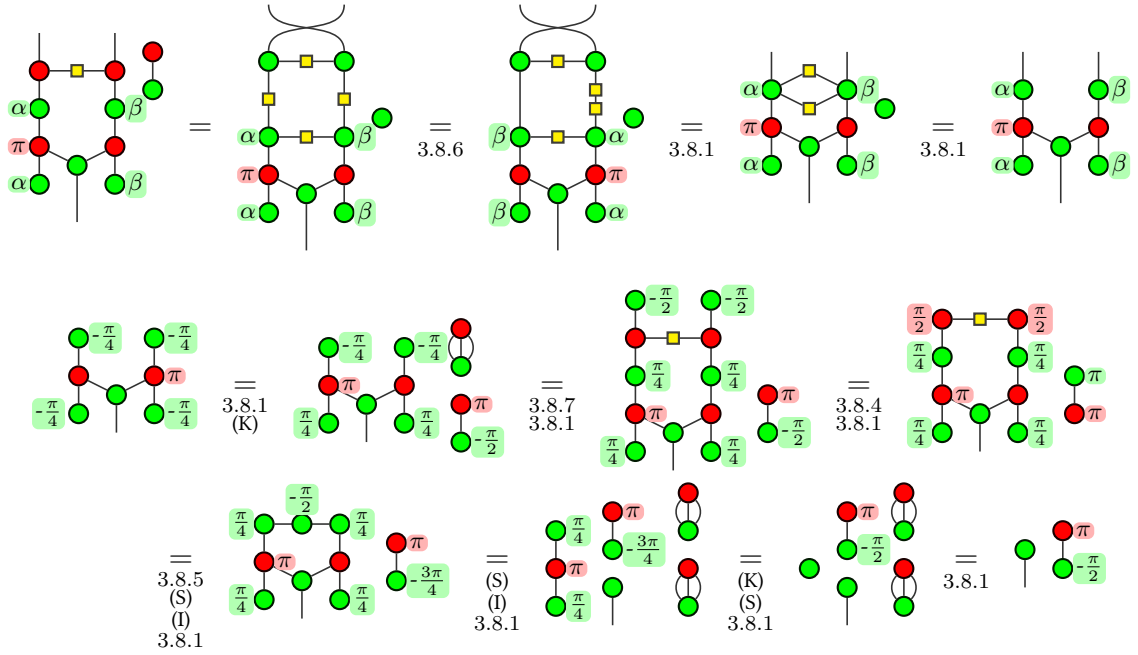
Lemma 3.8.8.



Proof ▶ By completeness of the $\frac{\pi}{2}$-fragment:

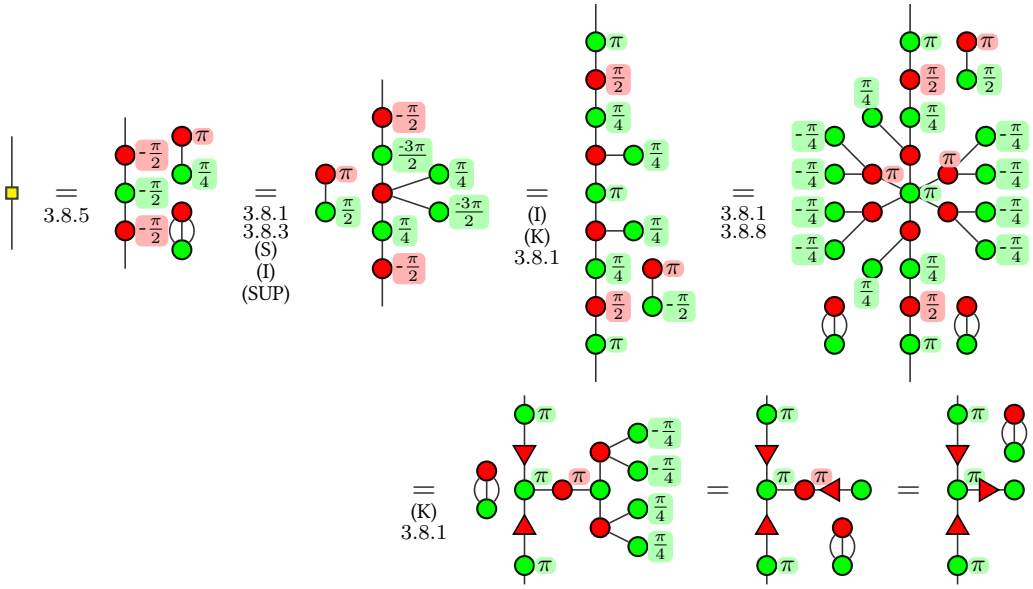


Then:

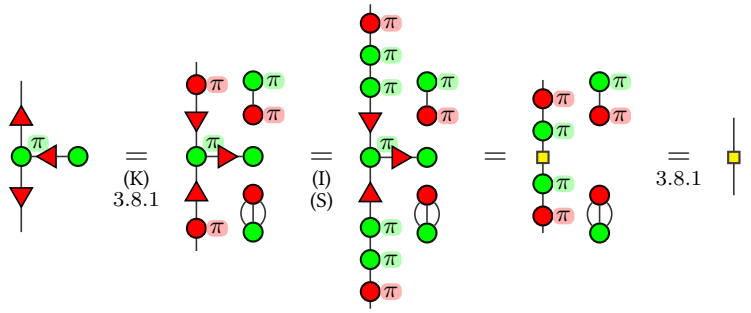


◀

***Proof** of Prop. 3.8.2 (ctd.)* ▶ (HT): First:

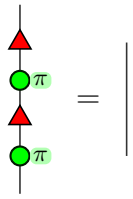


Hence:

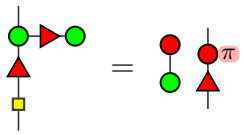


◀

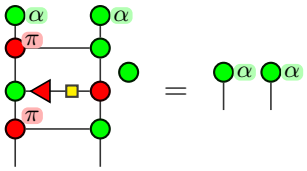
Lemma 3.8.9.



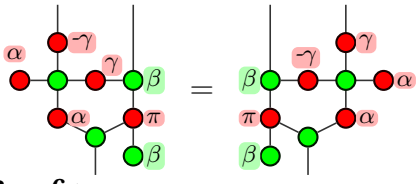
Lemma 3.8.10.



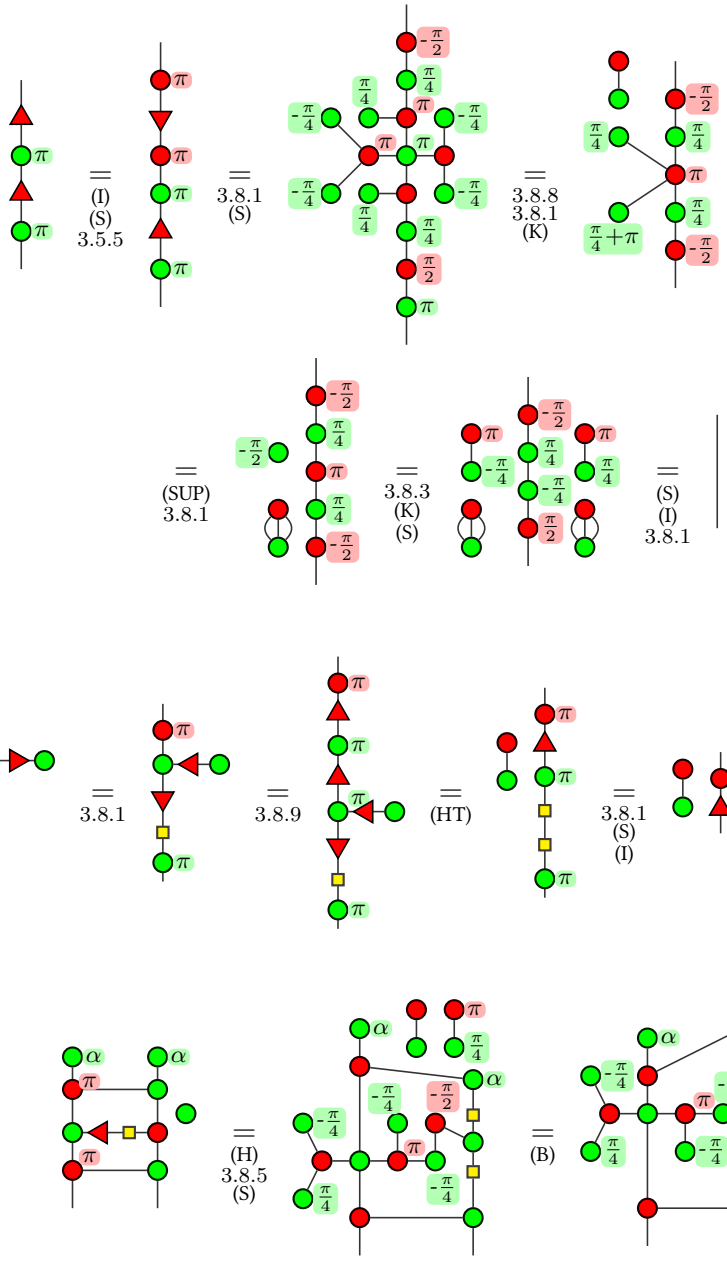
Lemma 3.8.11.

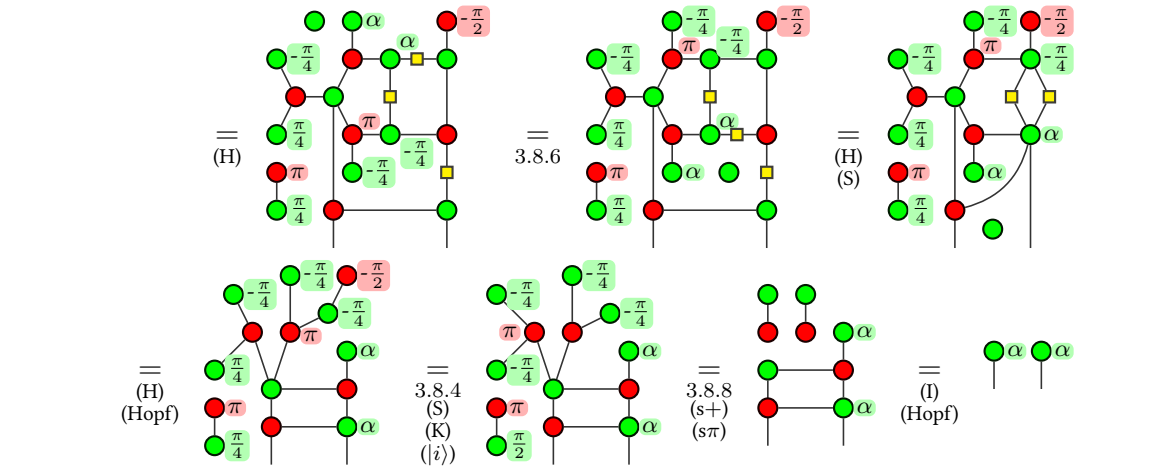


Lemma 3.8.12.

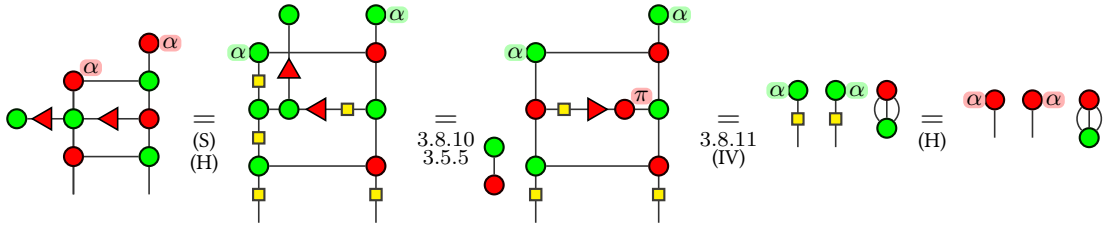


Proof ▶

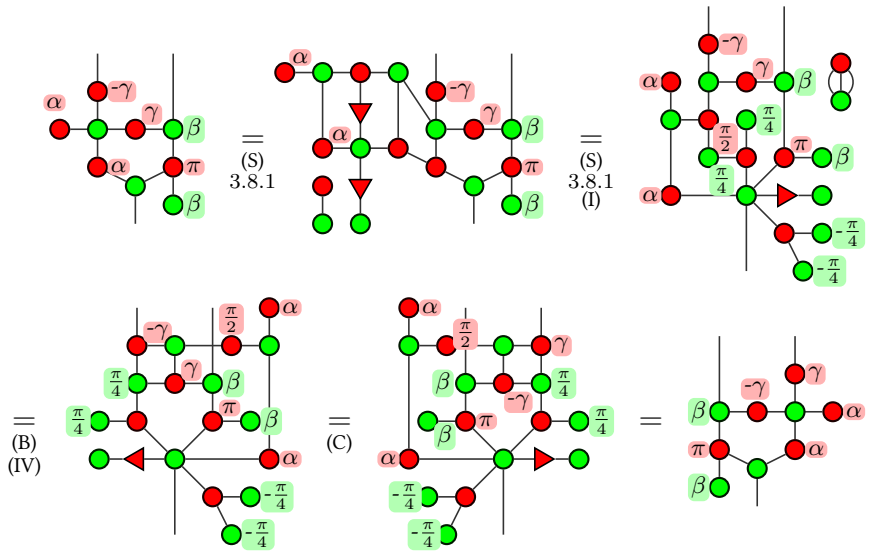




First:

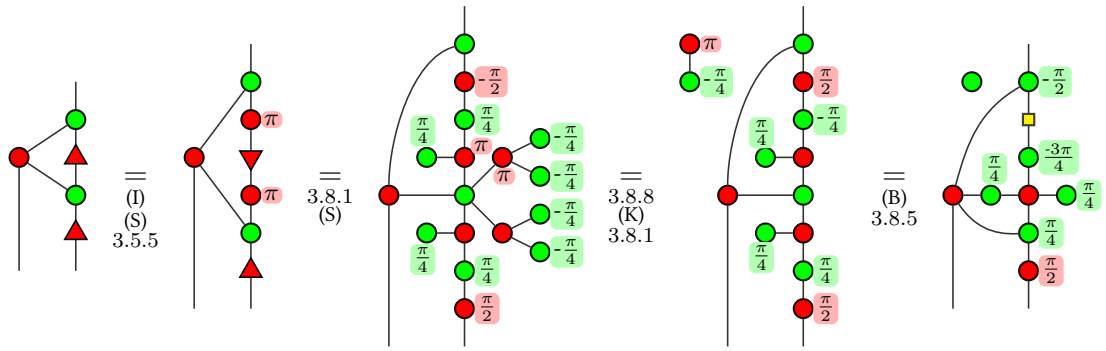


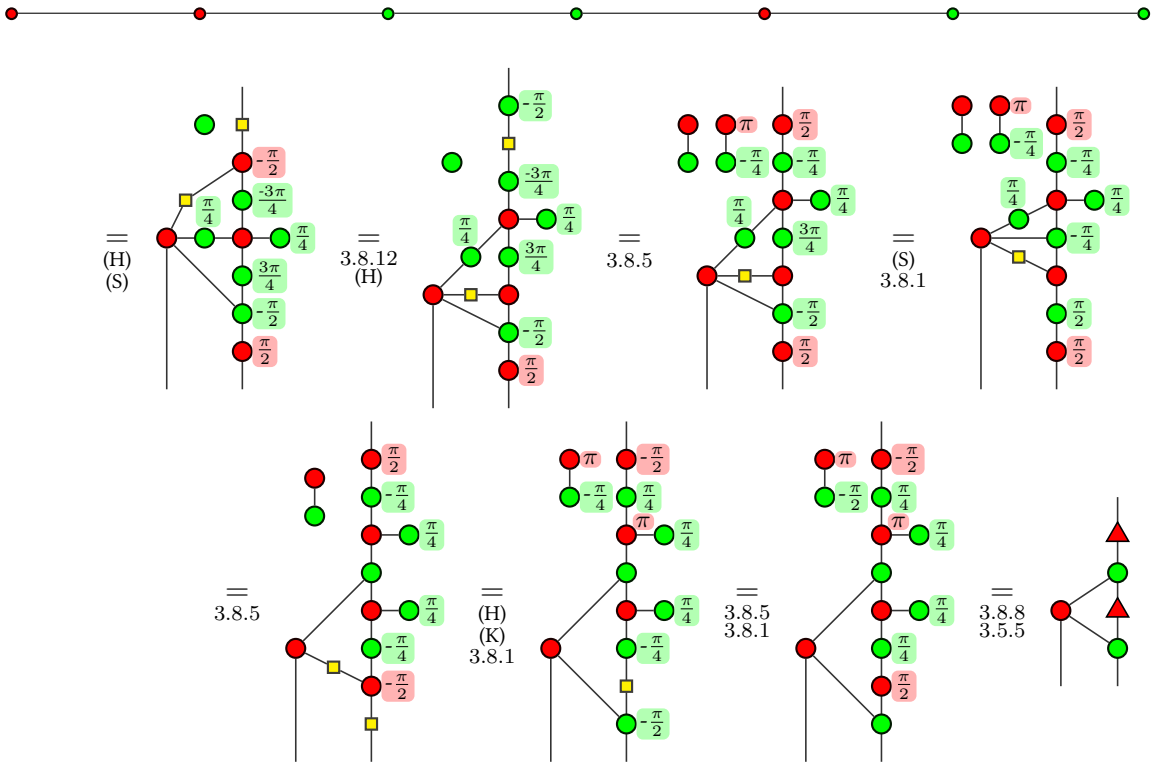
then:



◀

Proof *of Prop. 3.8.2 (ctd.)* ▶ (TW):





We have now proved that all the axioms of Δ_π are derivable with $\mathrm{ZX}_{\pi/4}$. ◀

3.9 From $\mathbf{ZX}[\frac{\pi}{4}]$ to $\Delta\mathbf{ZX}[\pi]$

We now want to define an interpretation from $\mathbf{ZX}[\frac{\pi}{4}]$, which represents morphisms of $\mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2},e^{i\frac{\pi}{4}}]}$, to $\Delta\mathbf{ZX}[\pi]$, which represents morphisms of $\frac{1}{\sqrt{2}^{\mathbb{N}}}\mathbf{Qubit}_{\mathbb{Z}}$. To do so, we will need this interpretation to perform an encoding.

The monic and irreducible polynomial of $\mathbb{Z}[X]$ of which $e^{i\frac{\pi}{4}}$ is a root is X^4+1. Any matrix over $\mathbb{Z}[\frac{1}{2},e^{i\frac{\pi}{4}}]$ can be written as $A+e^{i\frac{\pi}{4}}B+e^{i\frac{2\pi}{4}}C+e^{i\frac{3\pi}{4}}D$ with $A,B,C,D\in\mathcal{M}(\mathbb{Z}[\frac{\not{4}}{\not{2}}])$. ψ is hence defined as:

$$\psi : A+e^{i\frac{\pi}{4}}B+e^{i\frac{2\pi}{4}}C+e^{i\frac{3\pi}{4}}D \mapsto A+B\otimes M+C\otimes M^2+D\otimes M^3$$

where $M := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix}$.

The left inverse of ψ is: $\Theta : X \mapsto (I\otimes e_0^T)\circ X\circ(I\otimes\theta)$ where $\theta := \begin{pmatrix} 1 \\ e^{i\frac{\pi}{4}} \\ e^{i\frac{2\pi}{4}} \\ e^{i\frac{3\pi}{4}} \end{pmatrix}$.

We want to give an interpretation $[.]_\Delta : \mathbf{ZX}[\frac{\pi}{4}] \to \Delta\mathbf{ZX}[\pi]$ such that $[\![[.]_\Delta]\!] = \psi([\![.]\!])$, i.e., the interpretation $[.]_\Delta$ should map a diagram of $\mathbf{ZX}[\frac{\pi}{4}]$ to a $\Delta\mathbf{ZX}[\pi]$-diagram, while at the same time performing the encoding ψ for their standard interpretation.

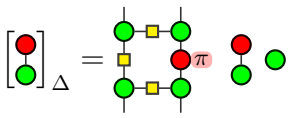
First of all, we want to represent the encoding of the scalar $\sqrt{2}$:

$$\psi(\sqrt{2}) = \psi(e^{i\frac{\pi}{4}} - e^{i\frac{3\pi}{4}}) = M - M^3 = \begin{pmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \end{pmatrix}$$

It can be decomposed with usual gates:

$$\psi(\sqrt{2}) = \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}}^{\text{CZ}} \overbrace{\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}}^{\sqrt{2}H \otimes \text{Not}} \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}}^{\text{CZ}}$$

All these gates are easily represented in $\Delta\mathbf{ZX}$:

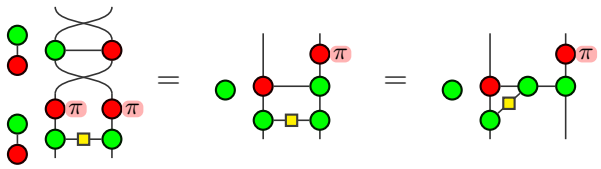


Then, H can simply be decomposed as $H = \frac{1}{2} \times \sqrt{2} \times (\sqrt{2}H)$.

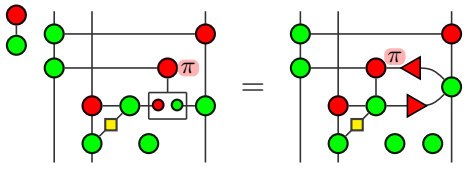
Then, we need to find a way to express the matrix M, using usual quantum operators. Notice that the matrix is CZ up to permutations.

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix} = \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}}^{\text{CZ}} \overbrace{\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}}^{\text{Not} \otimes \text{Not}} \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}^{\text{Swap}} \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}}^{\text{CNot}} \overbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}^{\text{Swap}}$$

We propose to first represent the matrices with ZX-diagrams, which hopefully will have a direct preimage by $[.]_T$. Using the usual rules of the ZX-Calculus, one can build:

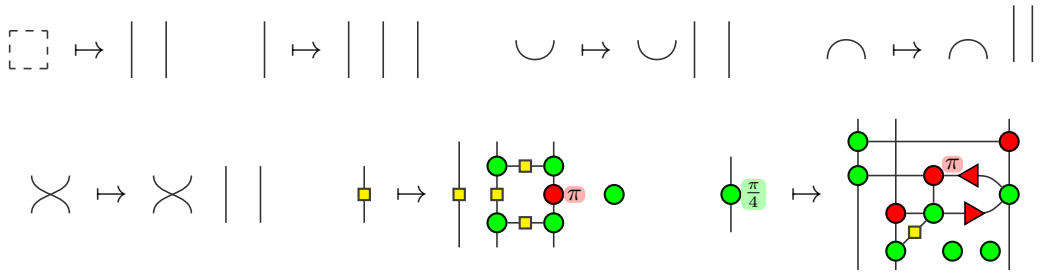


which represents M. Then, we want to represent $\psi\left(\left[\!\left[\right.\right.\right.$  $\left.\left.\left.\right]\!\right]\right) = \begin{pmatrix} I_4 & \\ & M \end{pmatrix}$. It can be seen as ΛM i.e., to represent it, we need to control the previous diagram. This can be performed using the transistor:



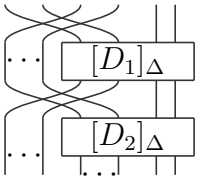
Eventually, we get to a formal and inductive definition of $[.]_\Delta$:

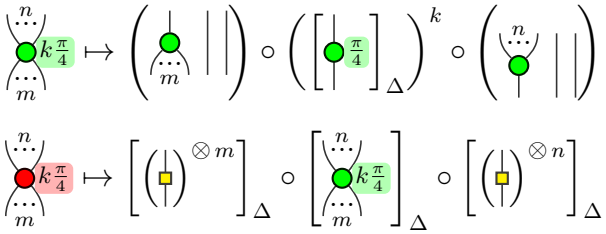
$[.]_\Delta$



$\forall D_1 : n \to n',\ \forall D_2 : m \to m' :$

$D_1 \circ D_2 \mapsto [D_1]_\Delta \circ [D_2]_\Delta \qquad (\text{if } m' = n) \qquad D_1 \otimes D_2 \mapsto$





This interpretation performs the encoding ψ.

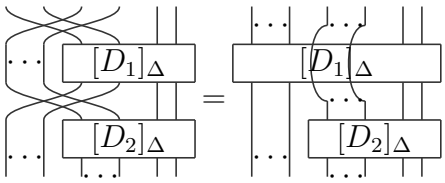
Proposition 3.9.1. *The following diagram commutes:*

$$\begin{array}{ccc} \mathbf{ZX}[\frac{\pi}{4}] & \xrightarrow{[\![.]\!]} & \mathbf{Qubit} \\ \downarrow{\scriptstyle [.]_\Delta} & & \downarrow{\scriptstyle \psi} \\ \Delta\mathbf{ZX}[\pi] & \xrightarrow{[\![.]\!]} & \mathbf{Qubit} \end{array}$$

Proof ► Again, this is routine. ◄

Remark 3.9.2. This interpretation, contrarily to $[.]_T$, is not a PROP-functor, but merely a functor. Indeed, $[. \otimes .]_\Delta \neq [.]_\Delta \otimes [.]_\Delta$. The two compositions are defined so that all the diagrams share the last two wires, which we will call "control-wire". We actually have:

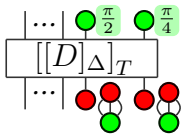
$D_1 \otimes D_2 \mapsto$



3.10 Completeness of $\mathbf{ZX}[\frac{\pi}{4}]/\mathrm{ZX}_{\pi/4}$

Recall that our goal is to prove that $\mathrm{ZX}_{\pi/4}$ make $\mathbf{ZX}[\frac{\pi}{4}]$ complete. It remains to show that one can recover any $\mathbf{ZX}[\frac{\pi}{4}]$-diagram D from $[[D]_\Delta]_T$ thanks to the decoding Θ.

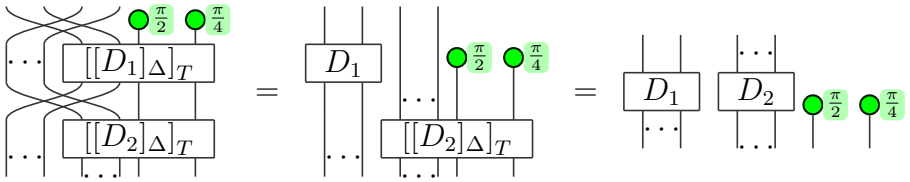
Proposition 3.10.1. *For any* $\mathbf{ZX}[\frac{\pi}{4}]$*-diagram* D*:*

$\mathrm{ZX}_{\pi/4} \vdash D =$ 

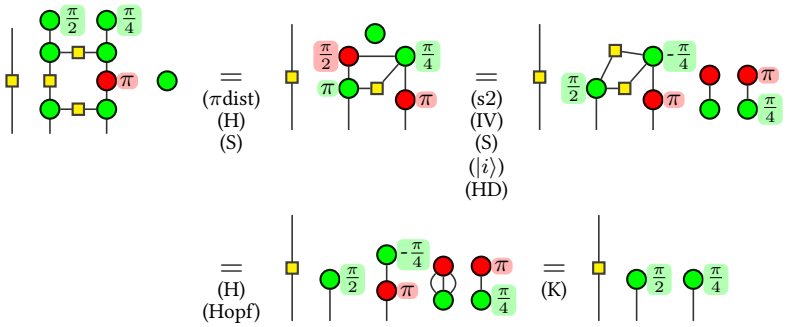
Proof ▶ We are going to prove inductively that:

$$\mathrm{ZX}_{\pi/4} \vdash [[D]_\Delta]_T \circ \left(\cdots \middle| \; \tfrac{\pi}{2} \; \tfrac{\pi}{4} \right) = D \otimes \left(\tfrac{\pi}{2} \; \tfrac{\pi}{4} \right)$$

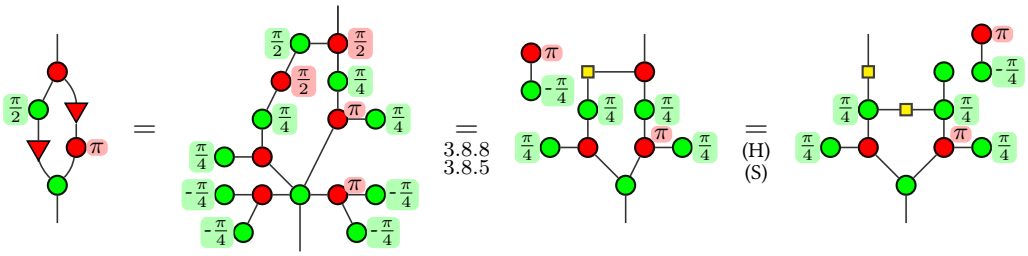
- $D_1 \circ D_2$: obvious because $[[D_1 \circ D_2]_\Delta]_T = [[D_1]_\Delta]_T \circ [[D_2]_\Delta]_T$
- $D_1 \otimes D_2$:

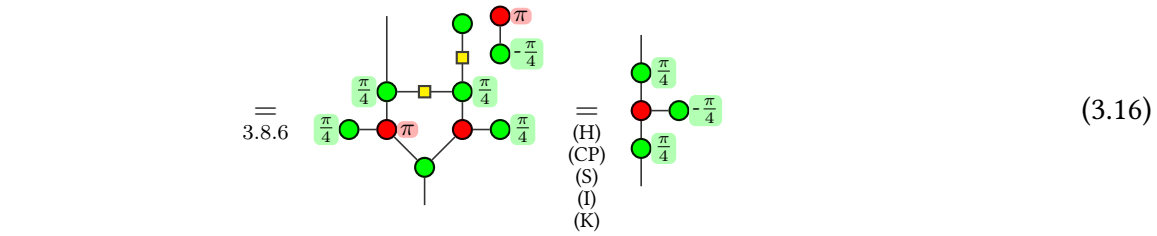


-  :



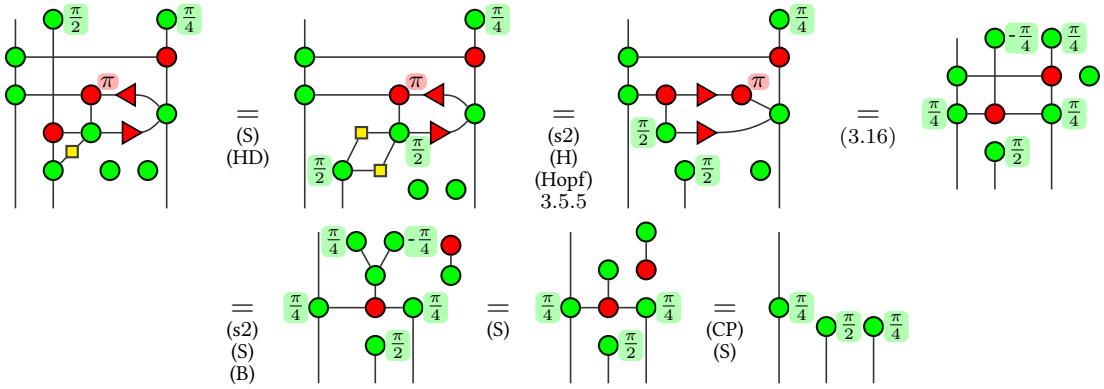
-  : First, we have:





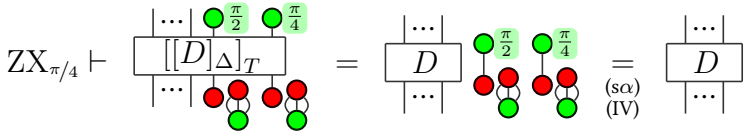
(3.16)

Then:



- The proof of the remaining cases follow from the previous ones.

Finally, we have:



◀

Theorem 3.10.2 (Completeness of $\mathbf{ZX}[\frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}$)**.** *The language* $\mathbf{ZX}[\frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}$ *is complete, and* $[\![.]\!] : \mathbf{ZX}[\frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4} \to \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{4}}]}$ *is full and faithful.*

Proof ▶ We have to show fullness and faithfulness:

- **Faithfulness:** Let D_1 and D_2 be two $\mathbf{ZX}[\frac{\pi}{4}]$-diagrams such that $[\![D_1]\!] = [\![D_2]\!]$. By Proposition 3.9.1 $[\![[D_1]_\Delta]\!] = \psi([\![D_1]\!]) = \psi([\![D_2]\!]) = [\![[D_2]_\Delta]\!]$, so by Theorem 3.5.1 $\Delta_\pi \vdash [D_1]_\Delta = [D_2]_\Delta$. By Proposition 3.8.2, $\mathrm{ZX}_{\pi/4} \vdash [[D_1]_\Delta]_T = [[D_2]_\Delta]_T$, so finally by Proposition 3.10.1, $\mathrm{ZX}_{\pi/4} \vdash D_1 = D_2$.
- **Fullness:** Let $f \in \mathbf{Qubit}_{\mathbb{D}[e^{i\frac{\pi}{4}}]}$. The morphism ψf is in $\mathbf{Qubit}_{\mathbb{D}}$. By fullness of $\Delta\mathbf{ZX}[\pi] \overset{[\![.]\!]}{\to} \mathbf{Qubit}_{\mathbb{D}}$ (Theorem 3.5.1), there exists $D_f^\Delta \in \Delta\mathbf{ZX}[\pi]$ such that $[\![D_f^\Delta]\!] = \psi f$. Finally, let $D_f := \left(\left| \cdots \right| \right) \circ [D_f^\Delta]_T \circ \left(\left| \cdots \right| \right)$. It is easy to see that $[\![D_f]\!] = f$.

◀

This allows us to prove Proposition 2.6.10, that is, that $\mathbf{Clifford{+}T} = \mathbf{Qubit}_{\mathbb{D}[e^{i\frac{\pi}{4}}]}$.

***Proof** of Proposition 2.6.10* ▶ $\mathbf{Clifford{+}T}$ has the same objects as $\mathbf{Qubit}_{\mathbb{D}[e^{i\frac{\pi}{4}}]}$, and by construction, is a sub-PROP. It remains to show that any morphism of the latter can be expressed as a morphism of the former. Let $f \in \mathbf{Qubit}_{\mathbb{D}[e^{i\frac{\pi}{4}}]}$. By fullness of $\mathbf{ZX}[\frac{\pi}{4}] \xrightarrow{[\![.]\!]} \mathbf{Qubit}_{\mathbb{D}[e^{i\frac{\pi}{4}}]}$ there exists $D_f \in \mathbf{ZX}[\frac{\pi}{4}]$ such that $[\![D_f]\!] = f$. ◀

Chapter 4

General ZX-Calculus

The aim of the present chapter is to obtain a complete axiomatisation, this time for the unrestricted ZX-Calculus, i.e. the ZX-Calculus with no restriction on the parameters, denoted **ZX**. A first useful result will be to extend the completeness of Clifford+T to the so-called linear diagrams with constants in Clifford+T.

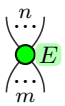
4.1 Linear Diagrams

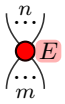
Variables and Constants

It is customary to view some angles in the **ZX**-diagrams as variables, in order to prove families of equalities. For instance, the rule (S) displays two variables α and β, and potentially gives an infinite number of equalities. Notice that in the axioms for Clifford+T ZX-calculus $\mathrm{ZX}_{\pi/4}$, the variables are used in a linear way, that is, we only perform sums of angles, hence reflecting the phase group structure.

We are going to formally define what a linear diagram is. We are going to define them for the larger $\Delta\mathbf{ZX}$. Since **ZX** can be seen as a sub-PROP of $\Delta\mathbf{ZX}$, the definition of linear **ZX**-diagrams will be a special case of that of linear $\Delta\mathbf{ZX}$-diagrams.

⌜ **Definition 4.1.1** (Linear Diagrams)**:** Let $\vec{\alpha} := \alpha_1, \ldots, \alpha_k$ be a collection of variables, and F a fragment (an additive subgroup of $\mathbb{R}$). We define $\Delta\mathbf{ZX}[\vec{\alpha}, F]$ as the †-compact PROP with the following set of generators and their string-diagram representation:

- $R_Z^{(n,m)}(E) : n \to m ::$ 

- $R_X^{(n,m)}(E) : n \to m ::$ 

- $H : 1 \to 1 ::$ 
- $\Delta : 1 \to 1 ::$ 

where E is an affine combination of α_i with coefficients in $\mathbb{Z}$ and constants in F, i.e. of the form $\sum_i n_i\alpha_i + c$, with $n_i \in \mathbb{Z}$ and $c \in F$.

The PROP structure is provided by $\sigma : 2 \to 2 :: \times$; and the compact structure by $\epsilon : 2 \to 0 :: \cup$ and $\eta : 0 \to 2 :: \cap$.

The functor $\dagger$ is such that:

- $\left(R_Z^{(n,m)}(E)\right)^\dagger = R_Z^{(m,n)}(-E)$
- $\left(R_X^{(n,m)}(E)\right)^\dagger = R_X^{(m,n)}(-E)$
- $H^\dagger = H$
- $\Delta^\dagger = (\epsilon \otimes id) \circ (id \otimes \Delta \otimes id) \circ (id \otimes \eta)$

For any $i \in \{1, \dots, k\}$ and $x \in \mathbb{R}$, there exists a PROP-functor $(.)[\alpha_i \leftarrow x] : \mathbf{\Delta ZX}[\vec{\alpha}, F] \to \mathbf{\Delta ZX}[\vec{\alpha} \setminus \{\alpha_i\}, \widehat{F \cup \{x\}}]$ (where $\widehat{F \cup \{x\}}$ is the additive closure of $F \cup \{x\}$) called the *valuation* of α_i in x, and given by:

- $\left(R_Z^{(n,m)}(E)\right)[\alpha_i \leftarrow x] = R_Z^{(n,m)}(E')$
- $\left(R_X^{(n,m)}(E)\right)[\alpha_i \leftarrow x] = R_X^{(n,m)}(E')$
- $(H)[\alpha_i \leftarrow x] = H$
- $(\Delta)[\alpha_i \leftarrow x] = \Delta$
- $(\sigma)[\alpha_i \leftarrow x] = \sigma$
- $(\eta)[\alpha_i \leftarrow x] = \eta$
- $(\epsilon)[\alpha_i \leftarrow x] = \epsilon$

where $E' = \sum_{j \neq i} n_j \alpha_j + (n_i x + c)$ if $E = \sum_j n_j \alpha_j + c$. ⌟

Again, by convention, if F is generated by $\{x_i\}_i$, we can replace $\mathbf{\Delta ZX}[\vec{\alpha}, F]$ by $\mathbf{\Delta ZX}[\vec{\alpha}, \{x_i\}_i]$. Hence we can directly write $F \cup \{x\}$ instead of $\widehat{F \cup \{x\}}$.

With this definition, we may notice that for any fragment F and any variables $\vec{\alpha}$, $\mathbf{\Delta ZX}[F]$ is a sub-PROP of $\mathbf{\Delta ZX}[\vec{\alpha}, F]$. The valuations are functors: they can be composed. Also, they commute, in the sense that the following diagram commutes when $i \neq j$:

$$\begin{array}{ccc} \mathbf{\Delta ZX}[\vec{\alpha}, F] & \xrightarrow{(.)[\alpha_i \leftarrow x_i]} & \mathbf{\Delta ZX}[\vec{\alpha}\backslash\{\alpha_i\}, F \cup \{x_i\}] \\ \downarrow{\scriptstyle (.)[\alpha_j \leftarrow x_j]} & & \downarrow{\scriptstyle (.)[\alpha_j \leftarrow x_j]} \\ \mathbf{\Delta ZX}[\vec{\alpha}\backslash\{\alpha_j\}, F \cup \{x_j\}] & \xrightarrow[(.)[\alpha_i \leftarrow x_i]]{} & \mathbf{\Delta ZX}[\vec{\alpha}\backslash\{\alpha_i, \alpha_j\}, F \cup \{x_i, x_j\}] \end{array}$$

Hence, the order of the valuations is not important. The composite $((.)[\alpha_i \leftarrow x_i])[\alpha_j \leftarrow x_j]$ can be abbreviated as $(.)[(\alpha_i, \alpha_j) \leftarrow (x_i, x_j)]$, and similarly for more than two valuations.

If all the variables are evaluated, we end up in a fragment of $\Delta\mathbf{ZX}$. So, if $D \in \Delta\mathbf{ZX}[\vec{\alpha}, F]$, we write $D(\vec{x})$ the diagram of $\Delta\mathbf{ZX}[F \cup \vec{x}]$ defined as $D(\vec{x}) := D[\vec{\alpha} \leftarrow \vec{x}]$. This allows us to define the standard interpretation of the PROP of linear diagrams:

$$\forall D \in \Delta\mathbf{ZX}[\vec{\alpha}, F], \quad [\![D]\!] := \vec{x} \mapsto [\![D(\vec{x})]\!]$$

The standard interpretation maps any linear diagram to a multivariate function whose codomain is $\mathbf{Qubit}$. It may be interesting to fine-grain the target of the standard interpretation, for we want to take into account the fragment of the source PROP.

⌜ **Definition 4.1.2:** Let F be a fragment of the language. We define the PROP $\mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2},e^{iF}]}$ as:

$$\mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2},e^{iF}]} := \left\{ \vec{\alpha} \mapsto P(e^{i\alpha_1}, \ldots, e^{i\alpha_k}) \;\middle|\; P : n \to m \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2},e^{iF}]}[X_1, \ldots, X_k] \right\}$$

where $P : n \to m$ is a multivariate polynomial with coefficients in $\mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2},e^{iF}]}[n, m]$. ⌟

Hence, if $\vec{\alpha} = \alpha_1, \ldots, \alpha_k$, then $[\![.]\!]$ is a functor from $\Delta\mathbf{ZX}[\vec{\alpha}, F]$ to $\mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2},e^{iF}]}$.

From variables to inputs

We now show that, given an equation involving diagrams linear in some variable α, the variables can be *extracted*, splitting the diagrams into two parts: a collection of points (nodes with parameter α) and a constant diagram independent of the variables.

First we define the multiplicity of a variable in an equation:

⌜ **Definition 4.1.3** (Multiplicity)**:** For any two diagrams $D_1, D_2 : n \to m$ of $\Delta\mathbf{ZX}[\vec{\alpha}, F]$, the multiplicity of α_1 in the equation $D_1 = D_2$ is defined as:

$$\mu_{\alpha_1} = \max_{i\in\{1,2\}} \left(\mu^+_{\alpha_1}(D_i)\right) + \max_{i\in\{1,2\}} \left(\mu^-_{\alpha_1}(D_i)\right)$$

where $\mu^+_{\alpha_1}(D)$ (resp. $\mu^-_{\alpha_1}(D)$) is the number of occurrences of α_1 (resp. $-\alpha_1$) in D, inductively defined as

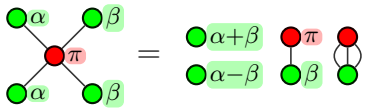
$$\mu^+_{\alpha_1}(R^{(n,m)}_Z(\ell\alpha_1 + E(\alpha_2 \cdots \alpha_n))) = \mu^+_{\alpha_1}(R^{(n,m)}_X(\ell\alpha_1 + E(\alpha_2 \cdots \alpha_n))) = \begin{cases} \ell & \text{if } \ell > 0 \\ 0 & \text{otherwise} \end{cases}$$

$$\mu^-_{\alpha_1}(R^{(n,m)}_Z(\ell\alpha_1 + E(\alpha_2 \cdots \alpha_n))) = \mu^-_{\alpha_1}(R^{(n,m)}_X(\ell\alpha_1 + E(\alpha_2 \cdots \alpha_n))) = \begin{cases} -\ell & \text{if } \ell < 0 \\ 0 & \text{otherwise} \end{cases}$$

$$\mu^\pm_{\alpha_1}(D \otimes D') = \mu^\pm_{\alpha_1}(D \circ D') = \mu^\pm_{\alpha_1}(D) + \mu^\pm_{\alpha_1}(D')$$

$$\mu^\pm_{\alpha_1}(H) = \mu^\pm_{\alpha_1}(e) = \mu^\pm_{\alpha_1}(\mathbb{I}) = \mu^\pm_{\alpha_1}(\sigma) = \mu^\pm_{\alpha_1}(\epsilon) = \mu^\pm_{\alpha_1}(\eta) = 0$$ ⌟

Example 4.1.4. Consider the following equation:

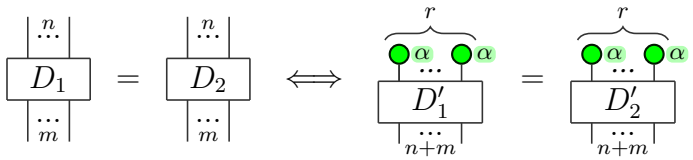


The multiplicity of α is $\mu_\alpha = 2$ and β's is $\mu_\beta = 3$.

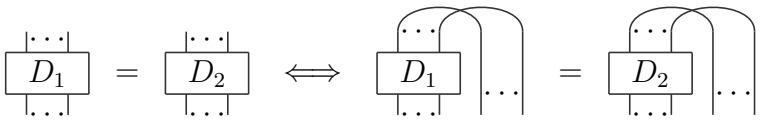
Proposition 4.1.5. *For any two diagrams $D_1, D_2 : n \to m$ of $\Delta\mathbf{ZX}[\alpha, F]$, there exist $D'_1, D'_2 : r \to n+m$ two $\Delta\mathbf{ZX}[F]$-diagrams such that the equivalence*

$$D_1 = D_2 \iff D'_1 \circ \theta_r = D'_2 \circ \theta_r$$

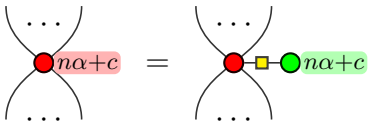
is provable using the axioms of ZX_π +(K)*, where r is the multiplicity of α in $D_1 = D_2$, and* $\theta_r := \left(R_Z^{(0,1)}(\alpha)\right)^{\otimes r}$.
Pictorially:



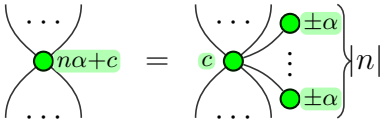
Proof ▶ The proof consists in transforming the equation $D_1 = D_2$ into the equivalent equation $D'_1 \circ \theta_r = D'_1 \circ \theta_r$ using axioms of ZX_π +(K). This transformation involves 6 steps:
– *Turn inputs into outputs.* First, each input can be bent to an output using η:

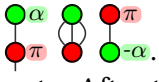
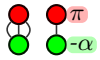


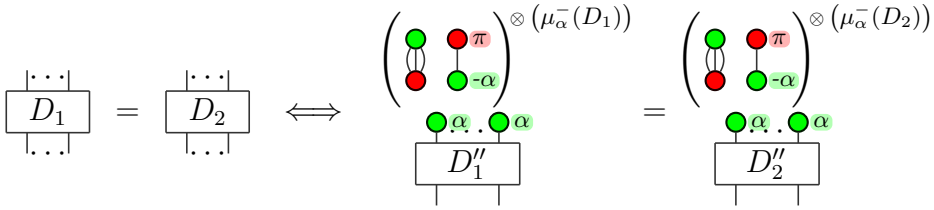
– *Make the red spiders green.* All red spiders $R_X^{(k,l)}(n\alpha + c)$ are transformed into green spiders using the axioms (S) and (H):



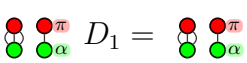
– *Expanding spiders.* All spiders $R_Z(n\alpha + c)$ are expanded using (S) so that all the occurrences of α are either  or  :



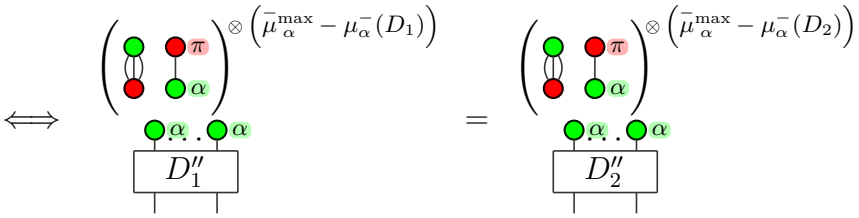
– *Changing the sign.* Using (K) all occurrences of  are replaced as follows:  ↦  . Notice that this rule is not applied recursively, which would not terminate. After this step all the original $-\alpha$ have been replaced by an α and as many scalars  have been created. So far, we have shown:

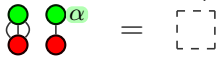


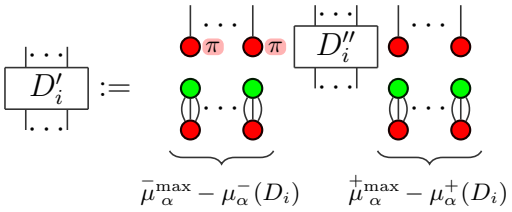
– *(Re)moving scalars.* The scalar  has an inverse for $\otimes$, which is  (by (s+) and (IV)). This has as consequence:

- $\mathrm{ZX}_{\pi/4} \vdash$  $D_1 = D_2 \iff \mathrm{ZX}_{\pi/4} \vdash D_1 =$  D_2
- $\mathrm{ZX}_{\pi/4} \vdash$  $D_1 =$ $D_2 \iff \mathrm{ZX}_{\pi/4} \vdash D_1 = D_2$

The scalars  are eliminated by adding $\bar{\mu}_\alpha^{\max} := \max\left(\mu_\alpha^-(D_1), \mu_\alpha^-(D_2)\right)$ times the scalar  on both sides, then simplifying when we have a scalar and its inverse.



– *Balancing the variables.* At this step the number of occurrences of α might be different on both sides of the equation. Indeed, one can check that the side of D_i has $\mu_\alpha^+(D_i) + \bar{\mu}_\alpha^{\max}$ occurrences of α. One can then use the simple equation  (by (sα) and (IV)) $\overset{+}{\mu}{}_\alpha^{\max} - \mu_\alpha^+(D_i)$ times on the side of D_i, where $\overset{+}{\mu}{}_\alpha^{\max} := \max\left(\mu_\alpha^+(D_1), \mu_\alpha^+(D_2)\right)$. We hence end up with $\mu_\alpha = \overset{+}{\mu}{}_\alpha^{\max} + \bar{\mu}_\alpha^{\max}$ occurrences of α on both sides. Formally, D_i' is defined as:



◀

Proposition 4.1.5 implies in particular that if the equation $D_1' \circ \theta_r = D_2' \circ \theta_r$ is provable using the axioms of the ZX-calculus, then so is $D_1 = D_2$. Proposition 4.1.5 also implies that if $[\![D_1]\!] = [\![D_2]\!]$, then $[\![D_1' \circ \theta_r]\!] = [\![D_2' \circ \theta_r]\!]$, thanks to the soundness of the ZX-calculus.

4.2 ΔZX Beyond Toffoli-Hadamard

We give a new axiomatisation Δ_π^+ for $\Delta\mathbf{ZX}$ in Figure 4.1 (augmented from the one in Figure 3.1 and want to show that it makes the fragment of linear diagrams with constants in $\pi\mathbb{Z}$ complete, i.e., we want to show that $\Delta\mathbf{ZX}[\vec{\alpha}, \pi]/\Delta_\pi^+$ is complete. We can actually show something more powerful:

Theorem 4.2.1. *Let F be a fragment, and R and axiomatisation such that $\Delta\mathbf{ZX}[F]/R$ is complete and such that $R \vdash \Delta_\pi^+$. Then $\Delta\mathbf{ZX}[\vec{\alpha}, F]/R$ is complete.*

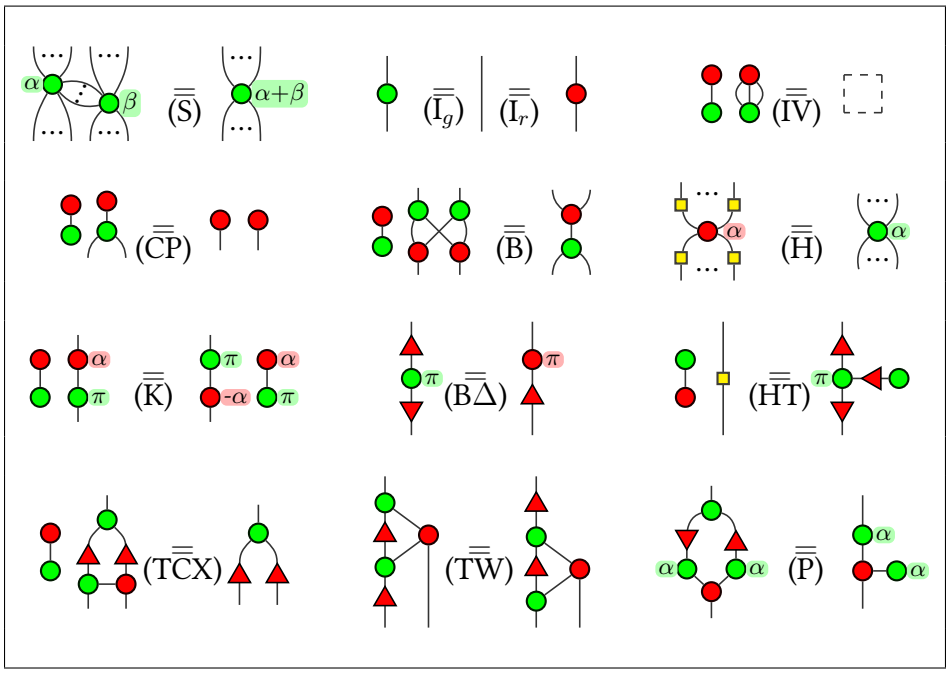


Figure 4.1: Set of rules Δ_π^+. The right-hand side of (IV) is an empty diagram. (...) denote zero or more wires, while (.˙.˙.) denote one or more wires.

The rest of this section is committed to proving this theorem. Notice however that from it we can directly obtain:

Corollary 4.2.2. *The language* $\Delta\mathbf{ZX}[\vec{\alpha}, \pi]/\,\Delta_\pi^+$ *is complete, i.e. the functor:*

$$\Delta\mathbf{ZX}[\vec{\alpha}, \pi]/\,\Delta_\pi^+ \xrightarrow{[\![\cdot]\!]} \frac{1}{\sqrt{2}^{\mathbb{N}}}\mathbf{Qubit}_{\mathbb{Z}}^{\mathbb{R}^k}$$

is faithful.

Proof ► $\Delta\mathbf{ZX}[\pi]/\,\Delta_\pi$ is complete, and since $\Delta_\pi^+ \vdash \Delta_\pi$, so is $\Delta\mathbf{ZX}[\pi]/\,\Delta_\pi^+$. Of course, $\Delta_\pi^+ \vdash \Delta_\pi^+$, so by Theorem 4.2.1, $\Delta\mathbf{ZX}[\vec{\alpha}, \pi]/\,\Delta_\pi^+$ is complete. ◄

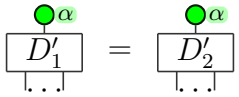
We can actually also show that it is full, but this will require particular constructions that will be found in Chapter 5.

One Variable

The idea of the proof of Theorem 4.2.1 is, given a pair of linear diagrams of which we want to check the equality, to separate the variables from the rest of the diagrams, that are in $\Delta\mathbf{ZX}[F]$, and show that the initial diagrams are equal iff some pair of variable-free diagrams are equal. It will then be easy to conclude, using the completeness of $\Delta\mathbf{ZX}[F]/R$.

Let us begin with a single occurrence of a single variable. Given two diagrams D_1 and D_2 of $\Delta\mathbf{ZX}[\alpha, F]$, if α has multiplicity 1 in $D_1 = D_2$, then according to Proposition 4.1.5, the equation can be transformed into the following equivalent equation involving

a single occurrence of α:

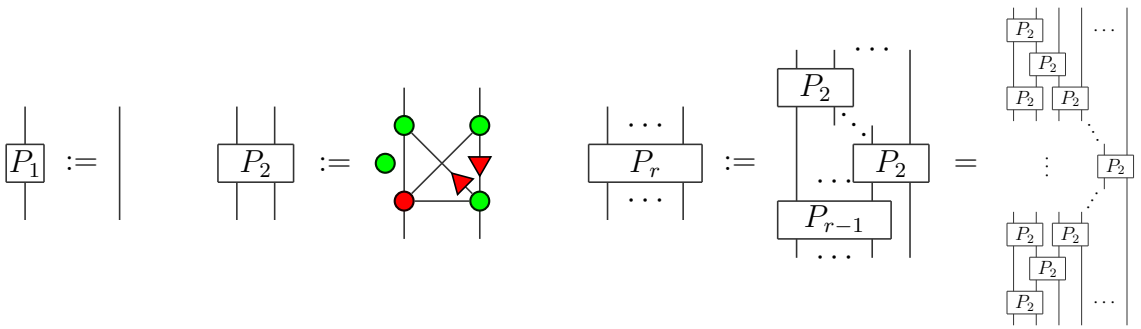


(4.1)

where D'_1 and D'_2 are in the fragment F. Notice that equation (4.1) holds if and only if $[\![D'_1]\!] = [\![D'_2]\!]$, since $\left(\text{Z}_0, \text{Z}_\pi\right)$ forms a basis of the input space. Thus, a variable of multiplicity 1 can easily be removed, leading to an equivalent equation in the fragment F of the ZX-calculus. If moreover this fragment is complete and proves ZX_π+(K), the equation $D'_1 = D'_2$ is derivable, which makes the equation (4.1) derivable with the same axiomatisation.

When a variable has a multiplicity $r > 1$ in an equation, the variable cannot be removed similarly as $\left(\text{Z}_\alpha\right)^{\otimes r}$ does not generate a basis of the 2^r dimensional space when $r > 1$. However these dots can be replaced by an appropriate projector on the subspace generated by these dots, as described in the following.

Consider the following family of diagrams $(P_r)_{r\geq 1}$:



For the reader convenience, here are the interpretations of P_2 and P_3:

$$[\![P_2]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad [\![P_3]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We can characterise the interpretation of P_r for any r.

Proposition 4.2.3. *For any word $\vec{x} \in \{0,1\}^r$, $[\![P_r]\!]^t |\vec{x}\rangle = \left|1^{|\vec{x}|_1} 0^{r-|\vec{x}|_1}\right\rangle$ where $|\vec{x}|_1$ is the Hamming weight of x i.e. the number of symbol 1 in the word $\vec{x}$.*

Informally, $[\![P_r]\!]^t$ sends all the words of the same Hamming weight to the word of the same weight where all the 1s are on the left.

Proof ► First of all, notice that the result is true for P_2:

$$[\![P_2]\!]^t |00\rangle = |00\rangle\,, \qquad [\![P_2]\!]^t |01\rangle = [\![P_2]\!]^t |10\rangle = |10\rangle\,, \qquad [\![P_2]\!]^t |11\rangle = |11\rangle$$

Let us denote $\mathrm{Op}^{[i_1,\cdots,i_k]}$ the application of the k-qubit operator Op on the wires $i_1,\ldots,i_k$. With this notation, $[\![P_r]\!]^t = [\![P_2]\!]^{t[1,2]} \circ [\![P_2]\!]^{t[2,3]} \circ \cdots \circ [\![P_2]\!]^{t[r-1,r]} \circ [\![P_{r-1}]\!]^{t[1,\cdots,r-1]}$. We then prove the result by induction on r. Let $\vec{x} \in \{0,1\}^r$ be a word. Then:

$$\begin{aligned}
[\![P_{r+1}]\!] \left|\vec{x}0\right\rangle &= [\![P_2]\!]^{t[1,2]} \circ [\![P_2]\!]^{t[2,3]} \circ \cdots \circ [\![P_2]\!]^{t[r,r+1]} \circ [\![P_r]\!]^{t[1,\cdots,r]} \left|\vec{x}0\right\rangle \\
&= [\![P_2]\!]^{t[1,2]} \circ \cdots \circ [\![P_2]\!]^{t[r,r+1]} \left|1^{|\vec{x}|_1}0^{r-|\vec{x}|_1}0\right\rangle \\
&= \cdots \\
&= \left|1^{|\vec{x}|_1}0^{r+1-|\vec{x}|_1}\right\rangle
\end{aligned}$$

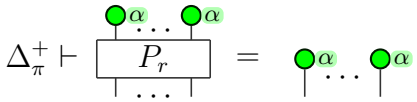
and

$$\begin{aligned}
[\![P_{r+1}]\!] \left|\vec{x}1\right\rangle &= [\![P_2]\!]^{t[1,2]} \circ [\![P_2]\!]^{t[2,3]} \circ \cdots \circ [\![P_2]\!]^{t[r,r+1]} \circ [\![P_r]\!]^{t[1,\cdots,r]} \left|\vec{x}1\right\rangle \\
&= [\![P_2]\!]^{t[1,2]} \circ \cdots \circ [\![P_2]\!]^{t[r,r+1]} \left|1^{|\vec{x}|_1}0^{r-|\vec{x}|_1}1\right\rangle \\
&= [\![P_2]\!]^{t[1,2]} \circ \cdots \circ \left|1^{|\vec{x}|_1}0^{r-1-|\vec{x}|_1}10\right\rangle \\
&= \cdots \\
&= [\![P_2]\!]^{t[1,2]} \circ \cdots \circ [\![P_2]\!]^{t[|\vec{x}|_1,|\vec{x}|_1+1]} \circ \left|1^{|\vec{x}|_1}10^{r-|\vec{x}|_1}\right\rangle \\
&= \cdots \\
&= \left|1^{|\vec{x}|_1+1}0^{r-|\vec{x}|_1}\right\rangle
\end{aligned}$$

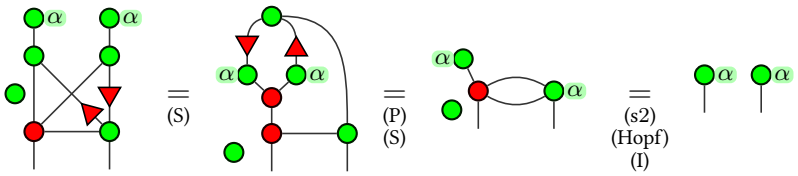
◀

Corollary 4.2.4. *The rank of* $[\![P_r]\!]$ *is exactly* $r+1$.

Lemma 4.2.5. *For any* $r \geq 1$, $\Delta_\pi^+ \vdash P_r \circ \theta_r = \theta_r$ *i.e.,*

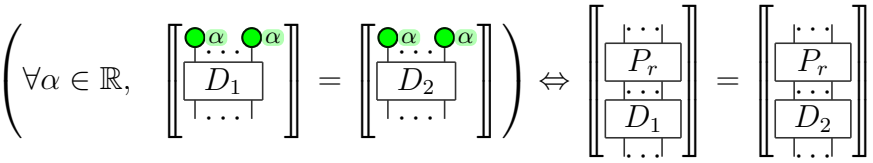


Proof ▶ The case for P_1 is obvious. Also, if the result is shown for P_2, then by an easy induction, it is true for P_r. P_2 is essentially an occurrence of rule (P):



◀

Lemma 4.2.6. *For any* $r \geq 2$ *and any* $D_1, D_2 : r \to n$ *two* $\Delta\mathbf{ZX}[F]$*-diagrams,* $([\![D_1 \circ \theta_r]\!] = [\![D_2 \circ \theta_r]\!]) \Leftrightarrow [\![D_1 \circ P_r]\!] = [\![D_2 \circ P_r]\!]$ *i.e.,*



Proof ▶ The proof consists in showing that $[\![P_r]\!]$ is a projector onto

$$S_r = \text{span}\{[\![\theta_r(\alpha)]\!] \mid \alpha \in \mathbb{R}\}$$

According to Lemma 4.2.5, $[\![P_r]\!]$ is the identity on S_r, and $[\![P_r]\!]$ is of rank at most $r+1$ according to Corollary 4.2.4, thus to finish the proof, it is sufficient to prove that the $r+1$ vectors $(\theta_r(\alpha^{(j)}))_{j=0\ldots r}$ are linearly independent, where $\alpha^{(j)} = j\pi/r$.

Let $\lambda_0, \ldots, \lambda_r$ be scalars such that $\sum_j \lambda_j \theta_r(\alpha^{(j)}) = 0$. Notice that the 2^p-th row (when rows are labeled from 1 to 2^r) of $\theta_r(\alpha^{(j)})$ is exactly $e^{ip\alpha^{(j)}}$. Therefore, if we look at all 2^p-th rows of the equations, we obtain

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ e^{i\alpha^{(0)}} & e^{i\alpha^{(1)}} & \cdots & e^{i\alpha^{(r)}} \\ \vdots & \vdots & \ddots & \vdots \\ e^{ir\alpha^{(0)}} & e^{ir\alpha^{(1)}} & \cdots & e^{ir\alpha^{(r)}} \end{pmatrix} \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_r \end{pmatrix} = 0$$

However, the first matrix is a Vandermonde matrix, with $e^{i\alpha^{(j)}} = e^{i\alpha^{(l)}}$ iff $j = l$, which is enough to state that this matrix is invertible. Therefore all λ_j are equal to 0 and the vectors $\theta_r(\alpha^{(j)})$ are linearly independent. ◀

We are now ready to prove the main theorem in the particular case of a single variable:

Proposition 4.2.7. *For any complete language $\Delta\mathbf{ZX}[F]/R$ such that $R \vdash \Delta_\pi^+$ and any two $\Delta\mathbf{ZX}[\alpha, F]$-diagrams D_1, D_2,*

$$[\![D_1]\!] = [\![D_2]\!] \iff \Delta_\pi^+ \vdash D_1 = D_2$$

Proof ▶ [⇐] is a direct consequence of the soundness of the $\Delta\mathbf{ZX}$-calculus.
[⇒] Assume $[\![D_1]\!] = [\![D_2]\!]$, i.e. $\forall \alpha \in \mathbb{R}, [\![D_1(\alpha)]\!] = [\![D_2(\alpha)]\!]$. According to Proposition 4.1.5, $[\![D_1' \circ \theta_r]\!] = [\![D_2' \circ \theta_r]\!]$ where D_i' are in $\Delta\mathbf{ZX}[F]$. It implies, according to Lemma 4.2.6, that $[\![D_1' \circ P_r]\!] = [\![D_2' \circ P_r]\!]$. Thanks to the completeness of $\Delta\mathbf{ZX}[F]/R$, $R \vdash D_1' \circ P_r = D_2' \circ P_r$, so $R \vdash D_1' \circ P_r \circ \theta_r = D_2' \circ P_r \circ \theta_r$. Thus, by Lemma 4.2.5, $R \vdash D_1' \circ \theta_r = D_2' \circ \theta_r$, which is equivalent to $R \vdash D_1 = D_2$ according to Proposition 4.1.5. ◀

Several Variables

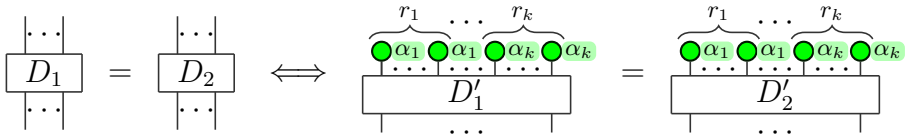
Proposition 4.1.5 can be straightforwardly extended to multiple variables:

Proposition 4.2.8. *For any $D_1, D_2 : n \to m$ two $\Delta\mathbf{ZX}[\vec{\alpha}, F]$-diagrams, there exist $D_1', D_2' : (\sum_{i=1}^k r_i) \to n+m$ two $\Delta\mathbf{ZX}[F]$-diagrams such that,*

$$D_1 = D_2 \quad \Leftrightarrow \quad D_1' \circ \theta_{\vec{r}} = D_2' \circ \theta_{\vec{r}}$$

is provable using ZX_π +(K), where r_i is the multiplicity of α_i in $D_1 = D_2$, $\vec{r} := r_1, \ldots, r_k$, and $\theta_{\vec{r}} := \left(\alpha_1\right)^{\otimes r_1} \otimes \ldots \otimes \left(\alpha_k\right)^{\otimes r_k}$.

Pictorially:



Similarly Lemma 4.2.6 can also be extended to multiple variables:

Lemma 4.2.9. *For any $k \geq 0$, any $\vec{r} = r_1, \ldots, r_k \in \mathbb{N}^k$ and any $D_1, D_2 : (\sum_i r_i) \to n$ two $\Delta\mathbf{ZX}[F]$-diagrams,*

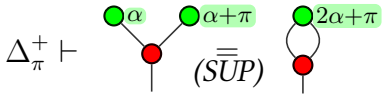
$$[\![D_1 \circ \theta_{\vec{r}}]\!] = [\![D_2 \circ \theta_{\vec{r}}]\!] \Leftrightarrow [\![D_1 \circ P_{\vec{r}}]\!] = [\![D_2 \circ P_{\vec{r}}]\!]$$

where $P_{\vec{r}} = P_{r_1} \otimes \ldots \otimes P_{r_k}$.

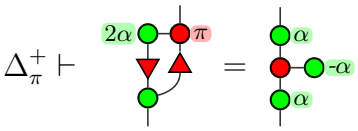
Using Proposition 4.2.8 and Lemma 4.2.9 (whose proofs are similar to those of 4.1.5 and 4.2.6), the proof of Theorem 4.2.1 is similar to the single variable case (Proposition 4.2.7) by induction.

Notice that Theorem 4.2.1 implies that if $\forall \vec{\alpha} \in \mathbb{R}^k, [\![D_1(\vec{\alpha})]\!] = [\![D_2(\vec{\alpha})]\!]$ then $D_1(\vec{\alpha}) = D_2(\vec{\alpha})$ has a *uniform* proof in the ZX-calculus in the sense that the structure of the proof is the same for all the values of $\vec{\alpha} \in \mathbb{R}^k$. Indeed, following the proof of Theorem 4.2.1, the sequence of axioms which leads to a proof of $D_1(\vec{\alpha}) = D_2(\vec{\alpha})$ is independent of the particular values of $\vec{\alpha}$. This gives us some equalities for free, that will be used in the following.

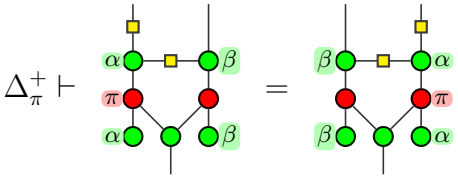
Corollary 4.2.10.



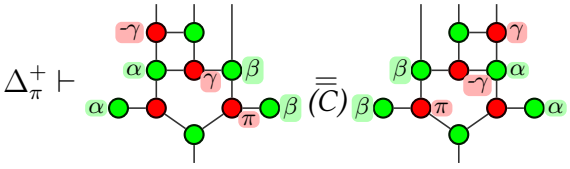
Corollary 4.2.11.



Corollary 4.2.12.



Corollary 4.2.13.



4.3 $\Delta_{\pi/4}$ for $\Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$

The aim of linear diagrams is to get a completeness result for $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}$. Theorem 4.2.1 was given for fragments of $\Delta\mathbf{ZX}$. Hence, the next step is logically to apply the theorem to such a fragment that is as expressive as $\mathbf{ZX}[\frac{\pi}{4}]$. We already know that Δ_π^+ is a complete axiomatisation for $\Delta\mathbf{ZX}[\vec{\alpha}, \pi]$. Through very few changes, we can give a complete axiomatisation $\Delta_{\pi/4}$ for $\Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$. This set of rules is given in Figure 4.2.

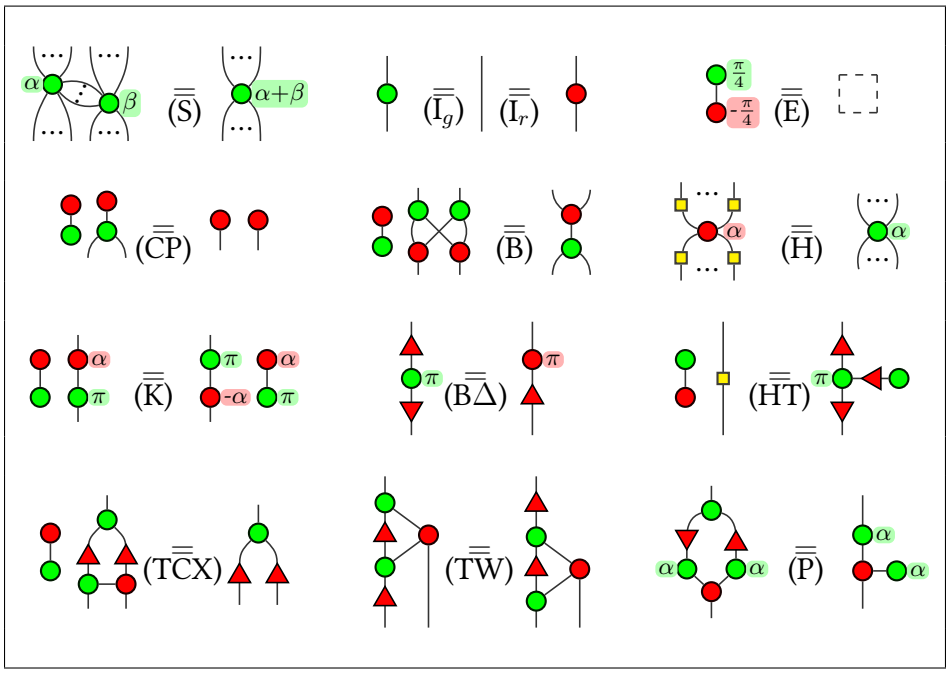


Figure 4.2: Set of rules $\Delta_{\pi/4}$. The right-hand side of (E) is an empty diagram. (...) denote zero or more wires, while ($\vdots$) denote one or more wires.

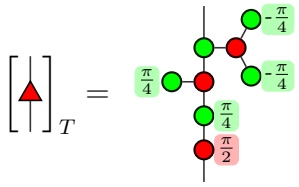
Theorem 4.3.1. *The language* $\Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\Delta_{\pi/4}$ *is complete, i.e. the functor:*

$$\Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\Delta_{\pi/4} \xrightarrow{[\![.]\!]} \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{4}}]}$$

is faithful.

Proof ▶ We are going to use the completeness of $\mathbf{ZX}[\frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}$ to first prove that $\Delta\mathbf{ZX}[\frac{\pi}{4}]/\,\Delta_{\pi/4}$ is complete. We will then be able to use Theorem 4.2.1 to extend the completeness to linear diagrams since $\Delta_{\pi/4} \vdash \Delta^+_\pi$ (only (IV) is missing, but it it is derivable thanks to Proposition 2.7.16).

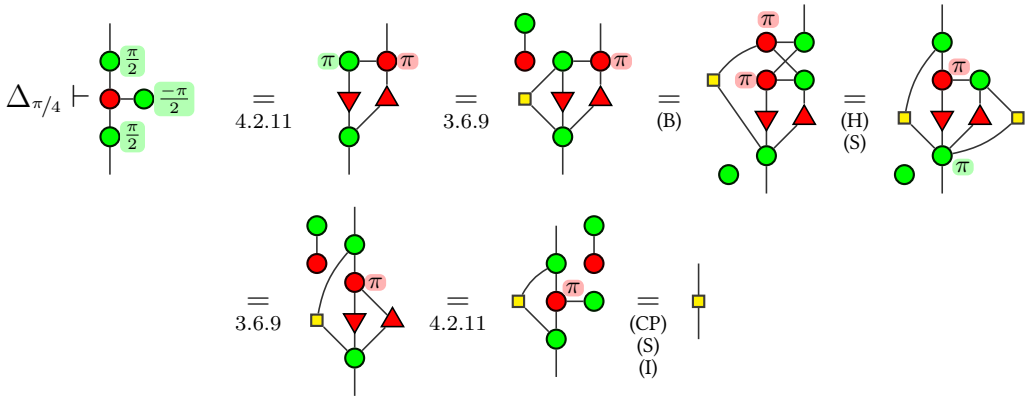
Remember that we have a functor $\Delta\mathbf{ZX}[\pi] \xrightarrow{[.]_T} \mathbf{ZX}[\frac{\pi}{4}]$. It can easily be extended to $\Delta\mathbf{ZX}[\frac{\pi}{4}] \xrightarrow{[.]_T} \mathbf{ZX}[\frac{\pi}{4}]$, it is the identity on every generator except for which

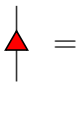
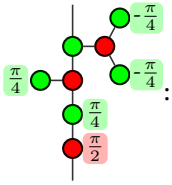


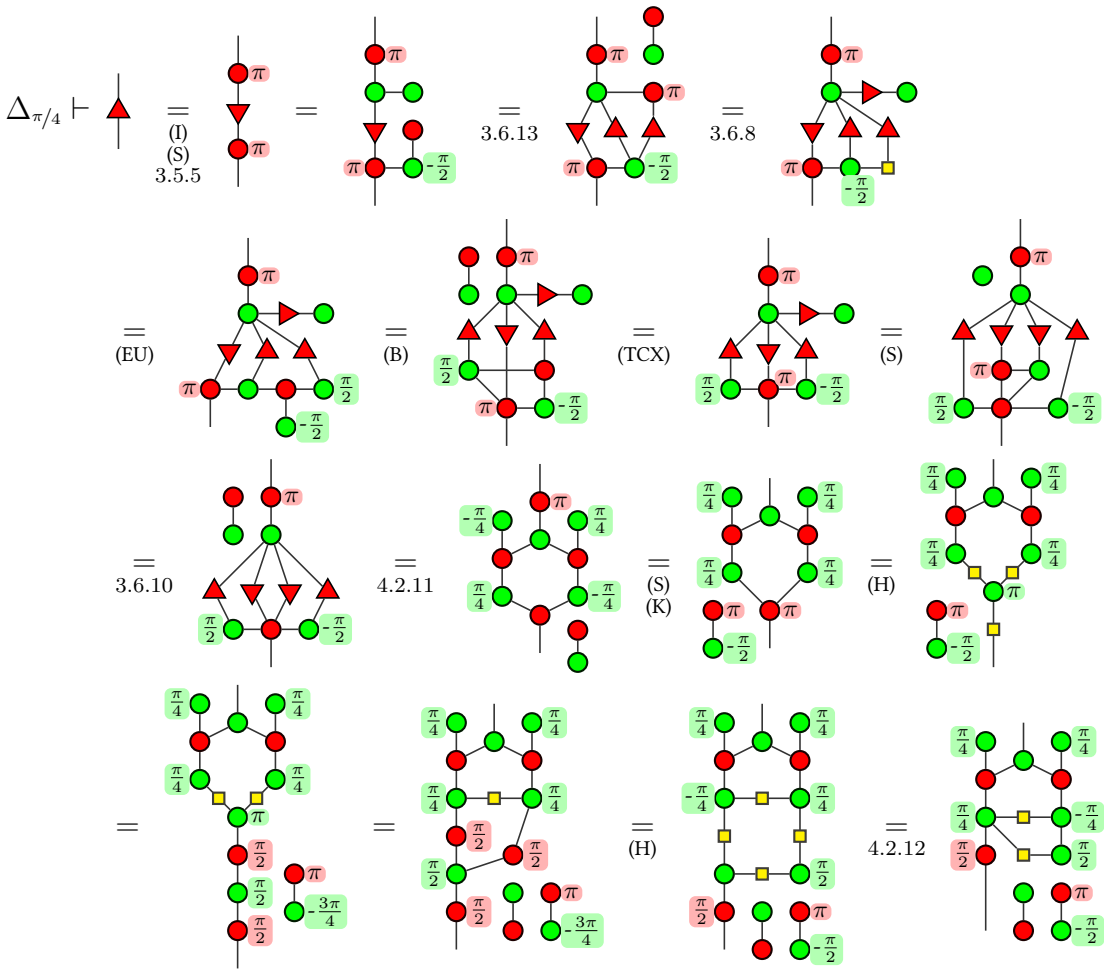
We can now use the inclusion functor $\mathbf{ZX}[\frac{\pi}{4}] \xrightarrow{\iota} \Delta\mathbf{ZX}[\frac{\pi}{4}]$.

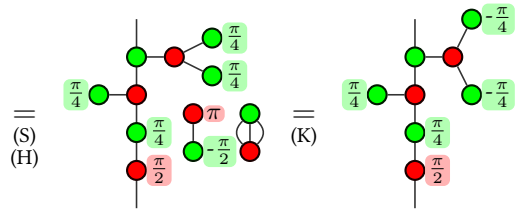
Both these functors are PROP-functors, and one can check that $[\![[.]_T]\!]_{\mathbf{ZX}} = [\![.]\!]_{\Delta\mathbf{ZX}}$. We are now going to prove that for any $\mathbf{ZX}[\frac{\pi}{4}]$-diagrams D_1 and D_2, $\mathrm{ZX}_{\pi/4} \vdash D_1 = D_2 \implies \Delta_{\pi/4} \vdash \iota(D_1) = \iota(D_2)$. We do so by deriving all the axioms of $\mathrm{ZX}_{\pi/4}$ with $\Delta_{\pi/4}$. A lot of them are found in $\Delta_{\pi/4}$, so they don't need to be proven. Also, (C) is provable

thanks to Corollary 4.2.13. We can prove (HD):



Also, we can prove $\Delta_{\pi/4} \vdash$  $=$  :





The rule (BW) of $\mathrm{ZX}_{\pi/4}$ is now easily derivable from the decomposition of the triangle and the rule (BΔ) of $\Delta_{\pi/4}$.

Now, let $D_1, D_2 \in \Delta\mathbf{ZX}[\frac{\pi}{4}]$ such that $[\![D_1]\!] = [\![D_2]\!]$. Since $[\![[.]_T]\!]_{\mathbf{ZX}} = [\![.]\!]_{\Delta\mathbf{ZX}}$, by completeness of $\mathbf{ZX}[\frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}$, $\mathrm{ZX}_{\pi/4} \vdash [D_1]_T = [D_2]_T$, so $\Delta_{\pi/4} \vdash \iota([D_1]_T) = \iota([D_2]_T)$. We have $\Delta_{\pi/4} \vdash \iota([D_i]_T) = D_i$, because $\iota([.]_T)$ is the identity for all generators except , and in this case we just proved $\iota\left([\,]_T\right) =$. As a consequence $\Delta_{\pi/4} \vdash D_1 = D_2$, so $\Delta\mathbf{ZX}[\frac{\pi}{4}]/\,\Delta_{\pi/4}$ is complete. By Theorem 4.2.1, $\Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\Delta_{\pi/4}$ is complete. ◀

4.4 ZX Beyond Clifford+T

Now that we have proven the completeness result for $\Delta\mathbf{ZX}$ beyond Toffoli-Hadamard, we can derive a similar one for the $\mathbf{ZX}$-Calculus.

Theorem 4.4.1. *The language* $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}$ *is complete, i.e. the functor*

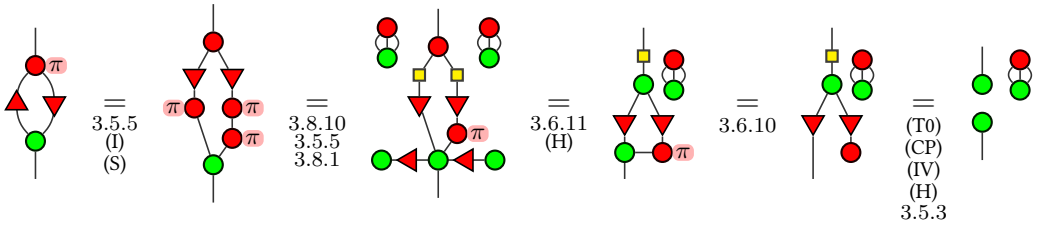
$$\mathbf{ZX}\left[\vec{\alpha}, \frac{\pi}{4}\right] / \,\mathrm{ZX}_{\pi/4} \xrightarrow{[\![.]\!]} \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{4}}]}$$

is faithful.

Again, this functor is also full, but the proof needs constructions introduced in Chapter 5.

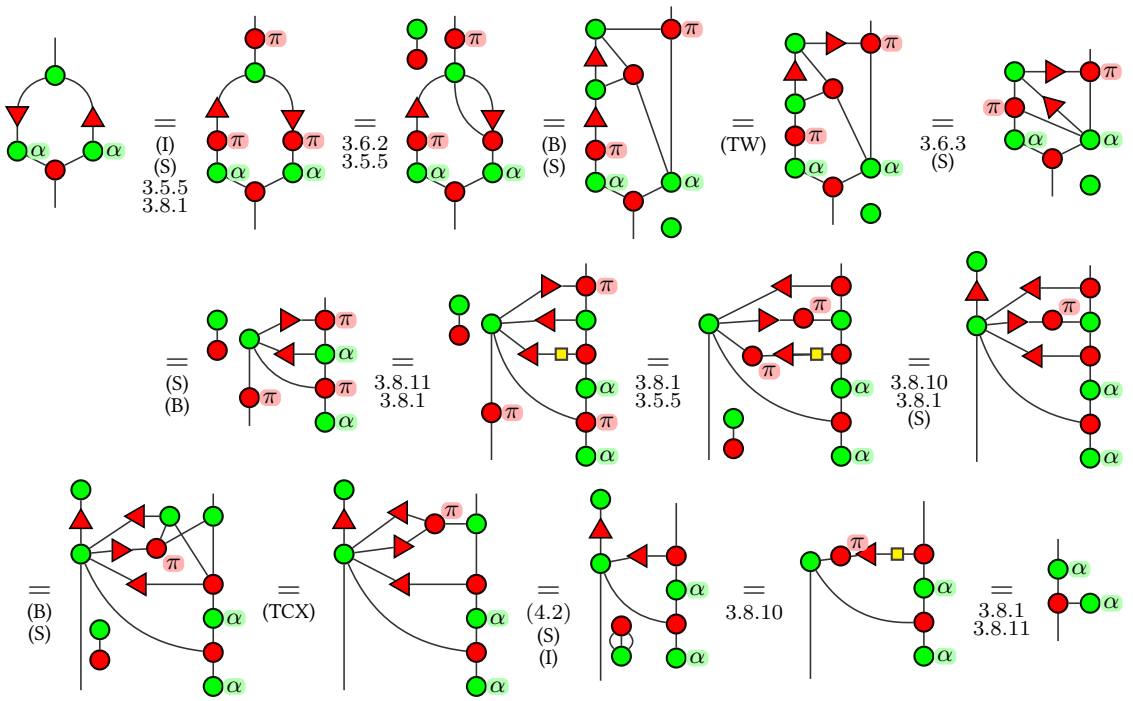
Proof ▶ To prove this result, we are going to use the previously proven result for linear diagrams of $\Delta\mathbf{ZX}[\frac{\pi}{4}]$ (Theorem 4.3.1). As usual, we need a pair of functors that translate one one language into the other. We can easily extend the functor $[.]_T$ but this time for linear diagrams $\Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}] \xrightarrow{[.]_T} \mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$. Again, it is the identity on all generators except . And again, we have the inclusion functor $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}] \xrightarrow{\iota} \Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$.

We first prove that $\Delta_{\pi/4} \vdash D_1 = D_2 \implies \mathrm{ZX}_{\pi/4} \vdash [D_1]_T = [D_2]_T$. We do so by proving all the axioms of $\Delta_{\pi/4}$ with $\mathrm{ZX}_{\pi/4}$, most of which have already been done. It remains to prove (P). First:



(4.2)

Then:



Now, suppose we have $D_1, D_2 \in \mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$ such that $[\![D_1]\!] = [\![D_2]\!]$. By completeness of $\Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\Delta_{\pi/4}$, $\Delta_{\pi/4} \vdash \iota(D_1) = \iota(D_2)$, so $\mathrm{ZX}_{\pi/4} \vdash [\iota(D_1)]_T = [\iota(D_2)]_T$. Finally, it is obvious that $[\iota(D)]_T = D$, so $\mathrm{ZX}_{\pi/4} \vdash D_1 = D_2$. Hence $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}$ is complete. ◀

We just showed that $\mathrm{ZX}_{\pi/4} \vdash \Delta_{\pi/4}$. In the previous section, we showed the converse, that $\Delta_{\pi/4} \vdash \mathrm{ZX}_{\pi/4}$. The result is that:

Proposition 4.4.2. $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4} \simeq \Delta\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\Delta_{\pi/4}$.

4.5 Applications of Linear Diagrams

In order to prove that $\mathrm{ZX}_{\pi/4} \vdash D_1 = D_2$ using Theorem 4.4.1, one has to double check the semantic condition $[\![D_1(\vec{\alpha})]\!] = [\![D_2(\vec{\alpha})]\!]$ for all $\vec{\alpha} \in \mathbb{R}^k$, which might not be easy in practice. We show in the following alternative ways to prove $\mathrm{ZX}_{\pi/4} \vdash D_1 = D_2$, the two first based on a finite case-based reasoning in the ZX-calculus, and the last one by diagram substitution. The following techniques will be proven for $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}$ but can be easily stated out for $\Delta\mathbf{ZX}[\vec{\alpha}, \pi]/\,\Delta_{\pi}^{+}$.

Considering a basis

Theorem 4.5.1. *For any* $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$*-diagrams* $D_1, D_2 : 1 \to m$*, if*

$$\forall j \in \{0,1\},\ \mathrm{ZX}_{\pi/4} \vdash \boxed{D_1}^{\,j\pi} = \boxed{D_2}^{\,j\pi}$$

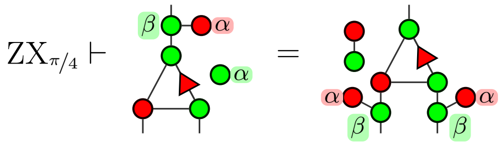
then

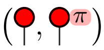
$$\mathrm{ZX}_{\pi/4} \vdash D_1 = D_2$$

Proof ▶ The argument was already mentioned at page 121, up to a change of basis. We give it again here for the sake of consistency.
Assume $\mathrm{ZX}_{\pi/4} \vdash D_1 \circ R_X(j\pi) = D_2 \circ R_X(j\pi)$ for any $j \in \{0, 1\}$. It implies that for $x \in \left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$, $[\![D_1]\!]\, x = [\![D_2]\!]\, x$, so $[\![D_1]\!] = [\![D_2]\!]$, which implies according to Theorem 4.4.1 $\mathrm{ZX}_{\pi/4} \vdash D_1 = D_2$. ◀

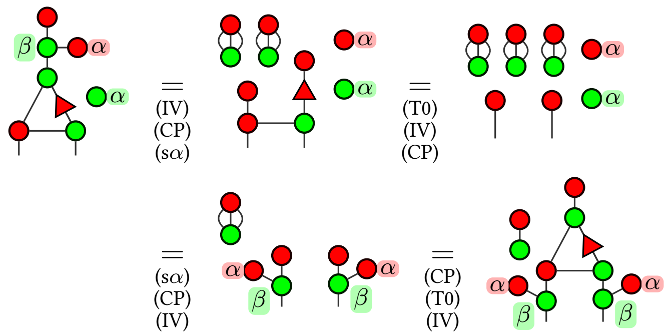
Notice that Theorem 4.5.1 can be applied recursively: in order to prove the equality between two diagrams with n inputs, m outputs, and constants in $\frac{\pi}{4}\mathbb{Z}$, one can consider the 2^{n+m} ways to fix these inputs/outputs in a standard basis states. It reduces the existence of a proof between two diagrams with constants in $\frac{\pi}{4}\mathbb{Z}$ to the existence of proofs on scalar diagrams (diagrams with no input and no output).

Corollary 4.5.2.

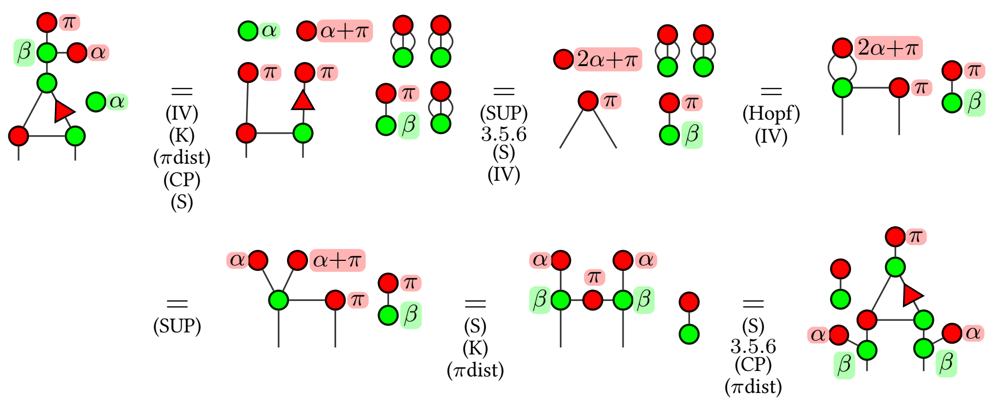


Proof ▶ We can prove that this equality is derivable by plugging our basis () on the input.

-  :



-  :



◀

Considering a finite set of angles

Theorem 4.5.3. *For any* $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$*-diagrams* $D_1, D_2 : n \to m$*, if*

$$\forall \vec{\alpha} \in T_1 \times \ldots \times T_k, \mathrm{ZX}_{\pi/4} \vdash D_1(\vec{\alpha}) = D_2(\vec{\alpha})$$

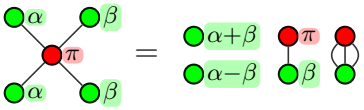
then

$$\mathrm{ZX}_{\pi/4} \vdash D_1 = D_2$$

with T_i *a set of* μ_i+1 *distinct angles in* $\mathbb{R}/2\pi\mathbb{Z}$ *where* μ_i *is the multiplicity of* α_i *in* $D_1 = D_2$*.*

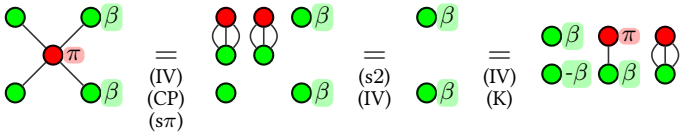
Proof ▶ In the proof of Lemma 4.2.6, we actually only used $\mu_\alpha + 1$ values of α that constitute a basis of S_{μ_α}. This extends naturally to several variables: the dimension of $S_{\mu_{\alpha_1}} \times \cdots \times S_{\mu_{\alpha_k}}$ is $(\mu_{\alpha_1} + 1) \times \cdots \times (\mu_{\alpha_k} + 1)$, and taking $\vec{\alpha} \in T_1 \times \ldots \times T_k$ gives as many linearly independent vectors in (hence a basis of) $S_{\mu_{\alpha_1}} \times \cdots \times S_{\mu_{\alpha_k}}$. ◀

Corollary 4.5.4.

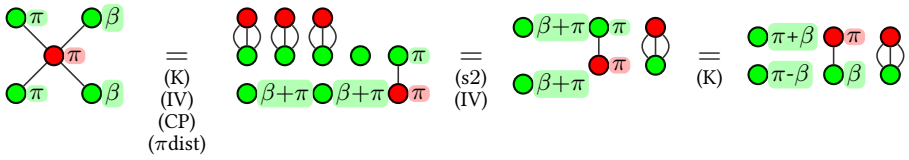


Proof ▶ Notice that $\mu_\alpha = 2$ and $\mu_\beta = 3$ in this equation. Hence we need to evaluate it for 12 values of (α, β), for instance for $\alpha, \beta \in \{0, \pi, \frac{\pi}{2}\} \times \{0, \pi, \frac{\pi}{2}, -\frac{\pi}{2}\}$. We can actually simplify the proof, by showing that whatever the value of $\beta \in \mathbb{R}$, the equation is derivable for $\alpha \in \{0, \pi, \frac{\pi}{2}\}$. This means the equation is derivable for all $\alpha, \beta \in \{0, \pi, \frac{\pi}{2}\} \times \mathbb{R}$, and a fortiori for all $\alpha, \beta \in \{0, \pi, \frac{\pi}{2}\} \times \{0, \pi, \frac{\pi}{2}, -\frac{\pi}{2}\}$ which would be a direct application of the theorem.

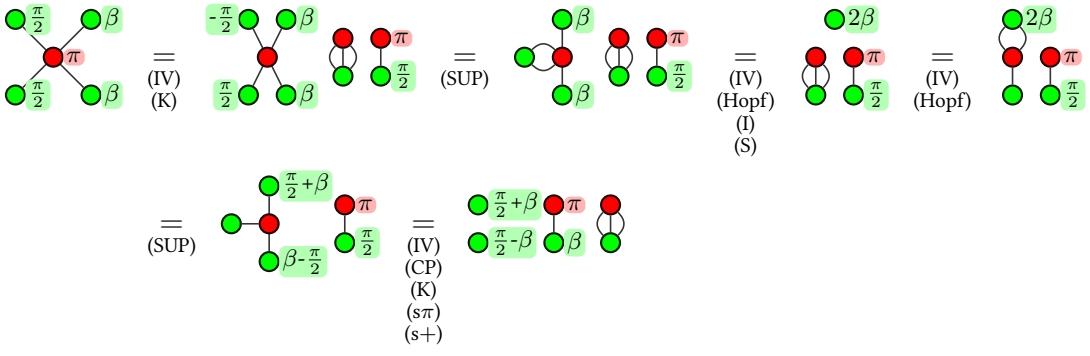
- $\alpha = 0$:



- $\alpha = \pi$:



- $\alpha = \frac{\pi}{2}$:



The results are the same for three different values of α. This is enough to get the equation in Corollary 4.5.4, according to Theorem 4.5.3. ◀

Remark 4.5.5. The number of occurrences of a variable is not to be mistaken for its multiplicity. For instance consider the following equation:

This equation is obviously wrong in general, but not for 0 and π. If we tried to apply Theorem 4.5.3 with the number of occurrences (which seems to be 1), then we might end up with the wrong conclusion. The multiplicity (here $\mu_\alpha = 2$) prevents this.

Diagram substitution

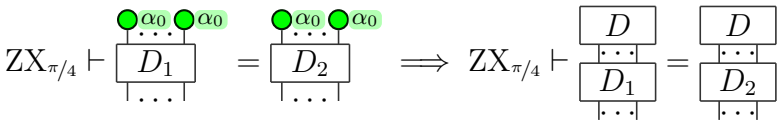
⌜ **Definition 4.5.6** (Symmetric Diagram)**:** A diagram $D : 0 \to n$ is symmetric if for any permutation τ on $\{1, \dots n\}$,

$$Q_\tau([\![D]\!]) = [\![D]\!]$$

where $Q_\tau : \mathbb{C}^{2^r} \to \mathbb{C}^{2^r}$ is the unique morphism such that:
$\forall \varphi_1, \dots, \varphi_r \in \mathbb{C}^2, Q_\tau(\varphi_1 \otimes \dots \otimes \varphi_r) = \varphi_{\tau(1)} \otimes \dots \otimes \varphi_{\tau(r)}$. ⌟

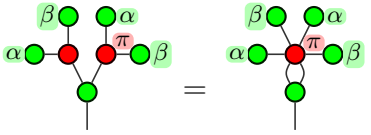
In particular for any diagram $D_0 : 0 \to 1$, $D_0 \otimes \dots \otimes D_0$ is a symmetric diagram.

Theorem 4.5.7. *For any* $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$*-diagrams* $D_1, D_2 : r \to n$ *and symmetric* $\mathbf{ZX}[\vec{\beta}, \frac{\pi}{4}]$*-diagram* $D : 0 \to r$*, if* $\mathrm{ZX}_{\pi/4} \vdash D_1 \circ \theta_{r_0} = D_2 \circ \theta_{r_0}$ *then* $\mathrm{ZX}_{\pi/4} \vdash D_1 \circ D = D_2 \circ D$ *i.e., pictorially:*

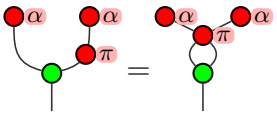


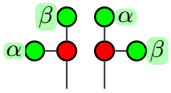
Proof ▶ If $\mathrm{ZX}_{\pi/4} \vdash D_1 \circ \theta_{r_0} = D_2 \circ \theta_{r_0}$ then $[\![D_1 \circ \theta_{r_0}]\!] = [\![D_2 \circ \theta_{r_0}]\!]$, so according to Lemma 4.2.6, $[\![D_1 \circ P_{r_0}]\!] = [\![D_2 \circ P_{r_0}]\!]$. It implies that $\mathrm{ZX}_{\pi/4} \vdash D_1 \circ P_{r_0} = D_2 \circ P_{r_0}$, so $\mathrm{ZX}_{\pi/4} \vdash D_1 \circ P_{r_0} \circ D = D_2 \circ P_{r_0} \circ D$. To complete the proof, it is enough to show that $\mathrm{ZX}_{\pi/4} \vdash P_{r_0} \circ D = D$.
Let $\mathcal{S} = \{[\![D]\!] \mid D : 0 \to n \text{ symmetric}\}$. First we show that $\mathcal{S}$ is of dimension at most $r + 1$. Indeed, notice that if $\varphi \in \mathcal{S}$, then $\forall i, j \in \{0, \dots, 2^r - 1\}$ s.t. $|i|_1 = |j|_1$, $\varphi_i = \varphi_j$, where $|x|_1$ is the Hamming weight of the binary representation of x. As a consequence, for any $\varphi \in \mathcal{S}$, $\exists a_0, \dots, a_r \in \mathbb{C}$ s.t. $\varphi = \sum_{h=0}^{n} a_h \varphi^{(h)}$ where $\varphi^{(h)} \in \mathbb{C}^{2^r}$ is defined as $\varphi_i^{(h)} = \begin{cases} 1 & \text{if } |i|_1 = h \\ 0 & \text{otherwise} \end{cases}$. Thus $\mathcal{S}$ is of dimension at most $r + 1$. Moreover, for any $\alpha \in \mathbb{R}$, $[\![\theta_{r_0}(\alpha)]\!] \in \mathcal{S}$, so $\mathcal{S} \subseteq \mathcal{S}_{r_0} := \mathrm{span}\{[\![\theta_{r_0}(\alpha)]\!] \mid \alpha \in \mathbb{R}\}$. Since $\mathcal{S}_r$ is of dimension $r+1$ (see proof of Lemma 4.2.6), $\mathcal{S} = \mathcal{S}_r$. As a consequence $\forall \vec{\beta}, \left[\!\!\left[D(\vec{\beta})\right]\!\!\right] \in \mathcal{S}_r$, so $[\![P_{r_0}]\!] \circ [\![D]\!] = [\![D]\!]$, since, according to Lemma 4.2.5 $[\![P_r \circ \theta_{r_0}]\!] = [\![\theta_{r_0}]\!]$. Thus, $\mathrm{ZX}_{\pi/4} \vdash P_{r_0} \circ D$ thanks to Theorem 4.4.1. ◀

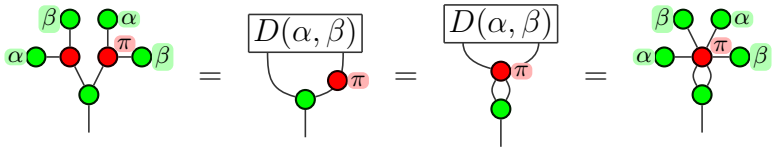
Corollary 4.5.8.

$\mathrm{ZX}_{\pi/4} \vdash$  $=$

Proof ▶ Indeed, simply by decomposing the colour-swapped version of (SUP) using (S), we can derive:

$\mathrm{ZX}_{\pi/4} \vdash$ 

Now we just need to apply Theorem 4.5.7 with $\boxed{D} := $  which is clearly symmetric:



◀

4.6 Axiomatisation for ZX

We are now well equipped to give an axiomatisation for the unrestricted ZX-Calculus ($\mathbf{ZX}[\mathbb{R}] = \mathbf{ZX}$), and prove that it is complete. The axiomatisation is given in Figure 4.3.

Theorem 4.6.1. *The language* $\mathbf{ZX}/\mathrm{ZX}$ *is complete: the functor* $\mathbf{ZX}/\mathrm{ZX} \xrightarrow{[\![.]\!]} \mathbf{Qubit}$ *is full and faithful.*

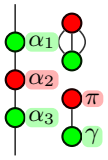
But first, let us consider the set of rules ZX. Notice that this axiomatisation basically consists of $\mathrm{ZX}_{\pi/2}$ with two additional rules (that replace the scalar axioms): (E), which is already in $\mathrm{ZX}_{\pi/4}$, and (EU).

The rule (EU) is really all about 1-qubit unitaries. Indeed, we have the following result:

Proposition 4.6.2. *Any one-qubit unitary can be decomposed as:*

$$e^{i\gamma} R_Z(\alpha_3) R_X(\alpha_2) R_Z(\alpha_1)$$

which can be represented in ZX as:



If the unitary is not diagonal or anti-diagonal (i.e. if $\alpha_2 \neq 0 \bmod \pi$*), then this decomposition can be made unique if we impose* $\alpha_1 \in [0, \pi)$

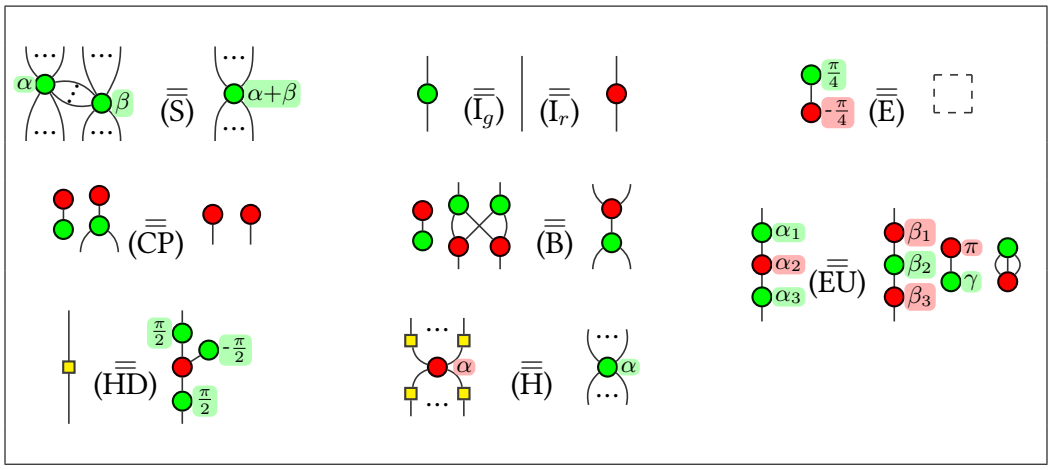


Figure 4.3: Set of rules ZX for the ZX-Calculus with scalars. The right-hand side of (E) is an empty diagram. (...) denote zero or more wires, while ($\therefore$) denote one or more wires. In rule (EU), $\beta_1, \beta_2, \beta_3$ and γ can be determined as follows: $x^+ := \frac{\alpha_1+\alpha_3}{2}$, $x^- := x^+ - \alpha_3$, $z := \cos\left(\frac{\alpha_2}{2}\right)\cos\left(x^+\right) + i\sin\left(\frac{\alpha_2}{2}\right)\cos\left(x^-\right)$ and $z' := \cos\left(\frac{\alpha_2}{2}\right)\sin\left(x^+\right) - i\sin\left(\frac{\alpha_2}{2}\right)\sin\left(x^-\right)$, then $\beta_1 = \arg z + \arg z', \beta_2 = 2\arg\left(i + \left|\frac{z}{z'}\right|\right), \beta_3 = \arg z - \arg z', \gamma = x^+ - \arg(z) + \frac{\alpha_2-\beta_2}{2}$

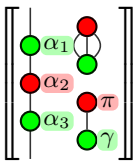
Proof ►

• Existence:

Any element of $U(2)$ can be decomposed as:

$$e^{i\varphi/2}\begin{pmatrix} e^{i\psi_0} & 0 \\ 0 & e^{-i\psi_0}\end{pmatrix}\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta)\end{pmatrix}\begin{pmatrix} e^{i\psi_1} & 0 \\ 0 & e^{-i\psi_1}\end{pmatrix}$$

Hence, the existence is given by:

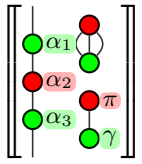
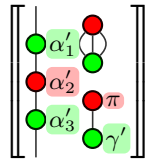


$$= e^{i(\gamma+\frac{\alpha_2}{2})}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha_3}\end{pmatrix}\begin{pmatrix} \cos\left(\frac{\alpha_2}{2}\right) & -i\sin\left(\frac{\alpha_2}{2}\right) \\ -i\sin\left(\frac{\alpha_2}{2}\right) & \cos\left(\frac{\alpha_2}{2}\right)\end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha_1}\end{pmatrix}$$

$$= e^{i(\gamma+\frac{\alpha_2}{2})}\begin{pmatrix} 1 & 0 \\ 0 & e^{i(\alpha_3+\frac{\pi}{2})}\end{pmatrix}\begin{pmatrix} \cos\left(\frac{\alpha_2}{2}\right) & \sin\left(\frac{\alpha_2}{2}\right) \\ -\sin\left(\frac{\alpha_2}{2}\right) & \cos\left(\frac{\alpha_2}{2}\right)\end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i(\alpha_1-\frac{\pi}{2})}\end{pmatrix}$$

$$= e^{i(\gamma+\frac{\alpha_1+\alpha_2+\alpha_3}{2})}\begin{pmatrix} e^{-i(\frac{\alpha_3}{2}+\frac{\pi}{4})} & 0 \\ 0 & e^{i(\frac{\alpha_3}{2}+\frac{\pi}{4})}\end{pmatrix}\begin{pmatrix} \cos\left(\frac{\alpha_2}{2}\right) & \sin\left(\frac{\alpha_2}{2}\right) \\ -\sin\left(\frac{\alpha_2}{2}\right) & \cos\left(\frac{\alpha_2}{2}\right)\end{pmatrix}\begin{pmatrix} e^{-i(\frac{\alpha_1}{2}-\frac{\pi}{4})} & 0 \\ 0 & e^{i(\frac{\alpha_1}{2}-\frac{\pi}{4})}\end{pmatrix}$$

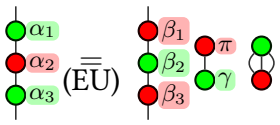
• Uniqueness:

Suppose  =  . The first diagram yields:

$$e^{i(\gamma+\frac{\alpha_2}{2})}\begin{pmatrix} \cos\left(\frac{\alpha_2}{2}\right) & -ie^{i\alpha_1}\sin\left(\frac{\alpha_2}{2}\right) \\ -ie^{i\alpha_3}\sin\left(\frac{\alpha_2}{2}\right) & e^{i(\alpha_1+\alpha_3)}\cos\left(\frac{\alpha_2}{2}\right)\end{pmatrix}$$

and similarly for the second one. If $\alpha_2 \neq 0 \bmod \pi$, then neither $\cos\left(\frac{\alpha_2}{2}\right)$ nor $\sin\left(\frac{\alpha_2}{2}\right)$ is null. Hence, dividing element (1,1) by element (0,0) on both sides gives $e^{i(\alpha_1+\alpha_3)} = e^{i(\alpha'_1+\alpha'_3)}$ and dividing element (0,1) by element (1,0) on both sides gives $e^{i(\alpha_1-\alpha_3)} = e^{i(\alpha'_1-\alpha'_3)}$. In other words, $\alpha_1 + \alpha_3 = \alpha'_1 + \alpha'_3 \bmod 2\pi$ and $\alpha_1 - \alpha_3 = \alpha'_1 - \alpha'_3 \bmod 2\pi$, so $2\alpha_1 = 2\alpha'_1 \bmod 2\pi$ i.e. $\alpha_1 = \alpha'_1 \bmod \pi$. Since we required $\alpha_1, \alpha'_1 \in [0, \pi)$, we get $\alpha_1 = \alpha'_1$. It then follows easily that $\alpha_3 = \alpha'_3$, $\alpha_2 = \alpha'_2$ and $\gamma = \gamma'$. ◀

In 1775, Euler proved what is now called Euler's rotation theorem [Eul76], stating that there are several ways to decompose a rotation into several rotations around elementary axes. In quantum mechanics, a consequence is that any unitary operator on one qubit can be seen as either a composition of rotations around Z, X, Z; or around X, Z, X. On the one hand, the rule (HD) says – in a distorted, ZX-style way – that the Hadamard gate can be decomposed as a series of rotations, while on the other hand, the rule (EU) gives the equality between two different decompositions of the same unitary:



where

$$\begin{cases} x^+ := \frac{\alpha_1+\alpha_3}{2} \qquad x^- := x^+ - \alpha_3 \\ z := \cos\left(\frac{\alpha_2}{2}\right)\cos\left(x^+\right) + i\sin\left(\frac{\alpha_2}{2}\right)\cos\left(x^-\right) \\ z' := \cos\left(\frac{\alpha_2}{2}\right)\sin\left(x^+\right) - i\sin\left(\frac{\alpha_2}{2}\right)\sin\left(x^-\right) \\ \beta_1 = \arg z + \arg z \\ \beta_2 = 2\arg\left(i + \left|\frac{z}{z'}\right|\right) \\ \beta_3 = \arg z - \arg z' \\ \gamma = x^+ - \arg(z) + \frac{\alpha_2-\beta_2}{2} \end{cases}$$

This rule is meant to be read from left to right, this is why the angles β_i and γ are expressed in terms of the angles α_i. However, up to the scalar, which only represents a global phase, and hence is invertible, applying the rule from right to left can be performed by using the colour-swapped version of the rule from left to right.

There are several sets of angles for β_i and γ that make the rule sound. However, we only gave one, but the others can be found from it and the other rules of ZX. We will not need to prove this claim directly, it is an implication of the upcoming theorem.

The angles β_i and γ seem to not always be defined. Indeed, $\arg$ is not defined at 0, and β_2 is not defined when $z' = 0$. By convention, we set $\arg(0) = 0$ and $\beta_2 = 0$ when $z' = 0$.

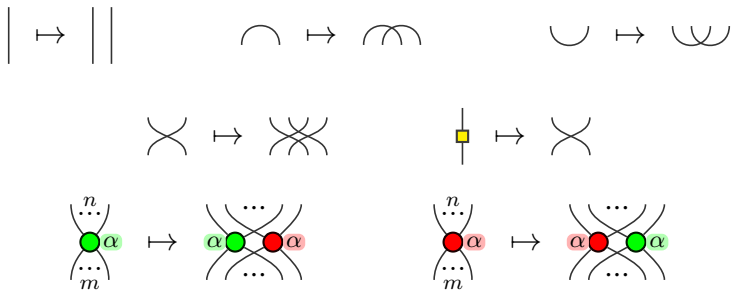
The first proof of incompleteness of the unrestricted ZX-Calculus [SdWZ14] relied on an Euler decomposition, but adding it to the set of ZX axioms has been avoided for a while because of its non-linearity. However, a non-linear axiom is necessary to get the completeness for the general ZX-Calculus [JPV18b]. And so, it has been used in [CW18] to prove the completeness of the 2-qubit $\frac{\pi}{4}$-fragment of the ZX-Calculus. The rule (EU) is actually much more powerful than this, for, as we already announced, it makes the language complete.

On Minimality

We call an axiomatisation minimal when there is no redundancy in the axioms. Particularly, we want a proof that none of the axioms are derivable from the others. We conjecture that all the axioms in Figure 4.3 are necessary. Indeed, in [BPW17b], nearly all the rules for Clifford – i.e. all of the axioms in Figure 4.3 except (E) and (EU)– are proven to be necessary. We reproduce the arguments here:

- (S): It is the only axiom that can transform a node of degree four or higher into a diagram containing lower-degree nodes.
- (I_g) or (I_r): These are the only two axioms that can transform a diagram with nodes connected to a boundary to a node-free diagram.
- (CP): It is the only axiom that can transform a diagram with two connected outputs into one with two disconnected outputs.
- (HD) and (H): To prove their necessity, we define two non-standard interpretation.

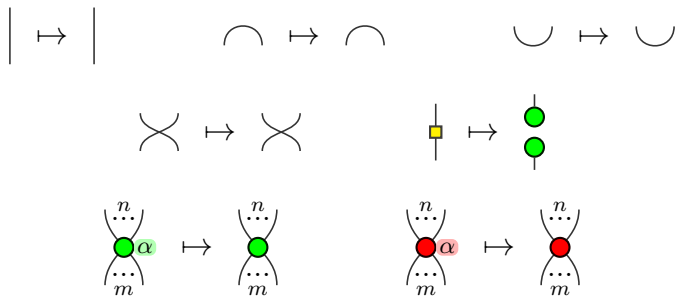
Proof *of Necessity of Rules* (HD) *and* (H) ▶ First, to prove the necessity of (HD), we define the non-standard interpretation $[\![.]\!]^\natural$ as follows:



$$D_1 \circ D_2 \mapsto [\![D_1]\!]^\natural \circ [\![D_2]\!]^\natural \qquad D_1 \otimes D_2 \mapsto [\![D_1]\!]^\natural \otimes [\![D_2]\!]^\natural$$

It is then easy to see that all the rules but (HD) hold under this interpretation, hence proving that (HD) could not be derived from the other rules.

Then, to prove the necessity of (H), we define the non-standard interpretation $[\![.]\!]^\natural$ as follows:



$$D_1 \circ D_2 \mapsto [\![D_1]\!]^\natural \circ [\![D_2]\!]^\natural \qquad D_1 \otimes D_2 \mapsto [\![D_1]\!]^\natural \otimes [\![D_2]\!]^\natural$$

and consider equality in the codomain up to a scalar, i.e. we consider colinearity. One can check that all the rules preserve colinearity except (H). ◀

In this new axiomatisation, (E) and (EU) can also be proven to be necessary:

- (E): It is the only axiom that can transform a non-empty diagram into an empty one.
- (EU): It is the only non-linear axiom.

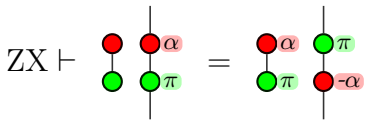
In summary, all the axioms are proven to be necessary, except (B) and one of the (I).

ZX proves $\mathrm{ZX}_{\pi/2}$

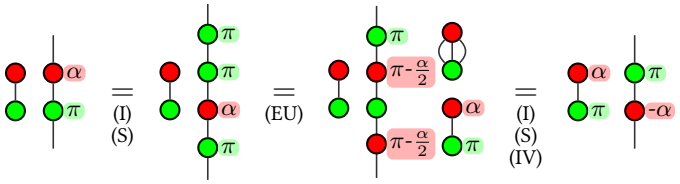
A first and easy step towards overall completeness is to show that we can recover the axiomatisation $\mathrm{ZX}_{\pi/2}$ that we know complete for Clifford. We already have most of these rules, we only lack two: (Z) and (IV). However, we can see from Figure 2.2 that (IV) is derivable.

To prove the rule (Z), we will first derive (K).

Lemma 4.6.3. *The π-commutation* (K) *is derivable:*



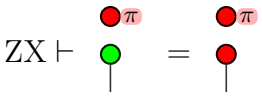
Proof ▶



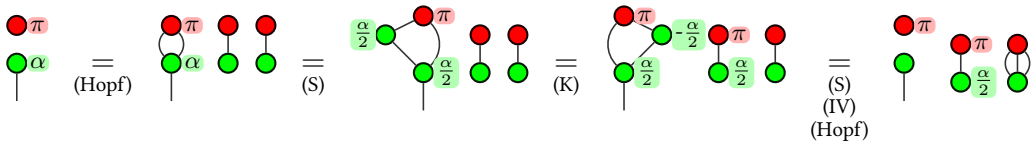
◀

Remark 4.6.4. This is one of the few applications of (EU) that still preserves linearity.

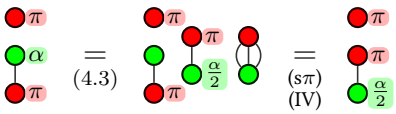
Lemma 4.6.5. *The zero rule is derivable:*



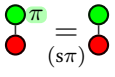
Proof ▶

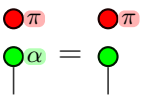


(4.3)



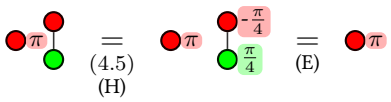
(4.4)

Now, if $\alpha \in \mathbb{D}\pi$ (where $\mathbb{D} := \mathbb{Z}\left[\frac{1}{2}\right]$), then there exists n such that $2^n\alpha = 0 \bmod 2\pi$. Hence, in this case the scalar on the right hand side of (4.3) can be removed by applying (4.4) from right to left $n+1$ times then using  and (IV) to remove it. Hence:



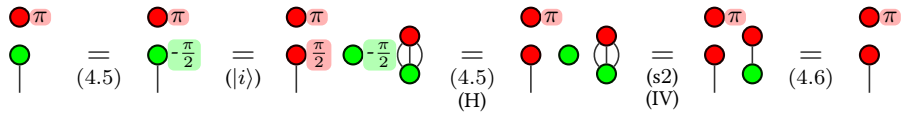
(4.5)

So:



(4.6)

And finally:



◀

As a result:

Proposition 4.6.6. *For any diagrams D_1, D_2 of* $\mathbf{ZX}[\frac{\pi}{2}]$*:*

$$[\![D_1]\!] = [\![D_2]\!] \iff \mathrm{ZX} \vdash D_1 = D_2$$

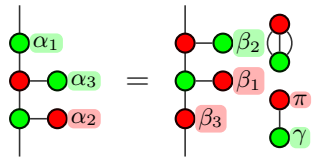
4.7 Singular-Value Decomposition

The next step is logically to get the completeness for Clifford+T quantum mechanics, i.e. for $\mathbf{ZX}[\frac{\pi}{4}]$. Now that we are seeking to prove equations that are out of Clifford, we will begin to use (EU) to its full potential. However, we would like, as much as possible, to avoid computing the angles, because, since we work on the problem of completeness, we need to *formally* prove the equality between two diagrams, and hence to formally write what the angles resulting from (EU) are, which becomes tedious after a few applications of the rule.

To simplify this task, instead of showing directly that two diagrams can be turned into one another, we will define a normal form for them, show that it is unique, and show that there is an algorithm to turn them into this normal form.

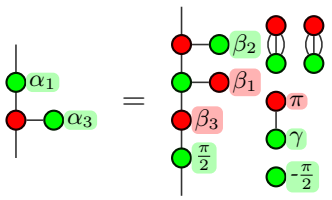
To do so, we prove a few useful lemmas:

Lemma 4.7.1.



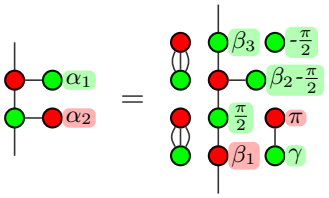
where $\beta_1, \beta_2, \beta_3, \gamma$ can be determined as in rule (EU)*.*

Corollary 4.7.2.



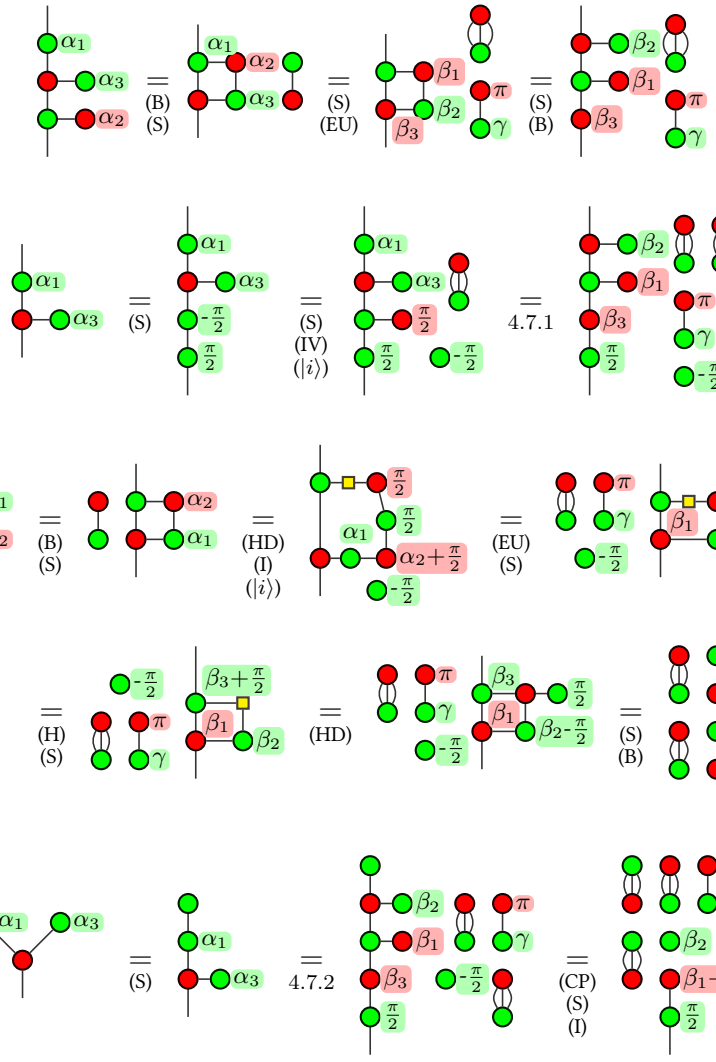
where $\beta_1, \beta_2, \beta_3, \gamma$ can be determined as in rule (EU) *with* $\alpha_2 \leftarrow \frac{\pi}{2}$*.*

Lemma 4.7.3.



where $\beta_1, \beta_2, \beta_3, \gamma$ can be determined as in rule (EU) *applied with the angles:* $\alpha_2 \leftarrow \alpha_2 + \frac{\pi}{2}$ *and* $\alpha_3 \leftarrow \frac{\pi}{2}$.

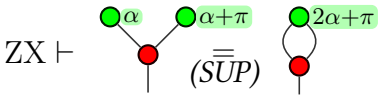
Proof ▶



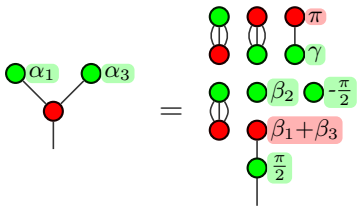
◀

Now, by specialising the angles to α and $\alpha + \pi$, we shall recover (SUP):

Proposition 4.7.5. *The supplementarity is derivable:*

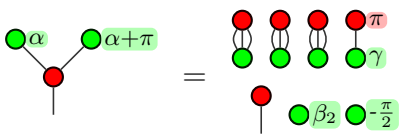


Lemma 4.7.4.



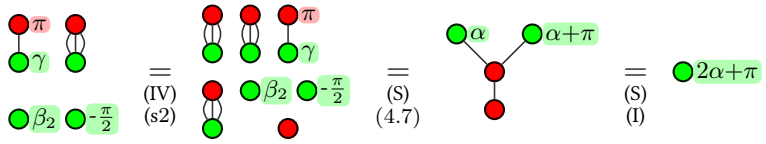
where $\beta_1, \beta_2, \beta_3, \gamma$ can be determined as in rule (EU) *with* $\alpha_2 \leftarrow \frac{\pi}{2}$.

Proof ▶ We first use Lemma 4.7.4, where $\alpha_3 = \alpha_1 + \pi$. In this case, it can be computed that $\beta_1 + \beta_3 = 0$, so we end up with:



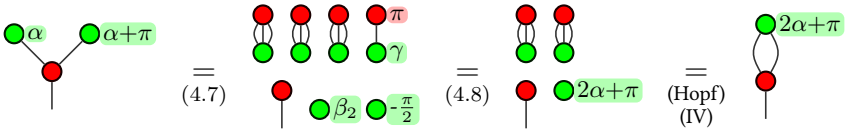
(4.7)

From this, we can easily specify the scalar on the right part:



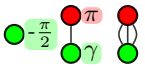
(4.8)

So finally:



◀

Remark 4.7.6. The supplementarity allows us to prove:

which implies that  can be replaced by  in Corollary 4.7.2 and Lemmas 4.7.3 and 4.7.4.

So far, we have proven all the rules of $\mathrm{ZX}_{\pi/4}$ except (C) and (BW). For the rest, we present the singular-value decomposition of a matrix, and introduce it to ZX-diagrams.

⌜ **Definition 4.7.7** (Singular Value Decomposition)**:** A *singular value decomposition* (SVD) of a matrix is a decomposition of the form

$$M = U\Sigma V^\dagger$$

where U and V are unitary, and Σ is diagonal. The diagonal entries of Σ are referred to as the *singular values*. Notice that M needs not be square (in this case Σ has the same dimensions as M). ⌟

To justify the use of SVDs, we give some of their interesting properties [HJ85]:

Proposition 4.7.8. *The SVD $M = U\Sigma V^\dagger$ of a matrix M has the following properties:*

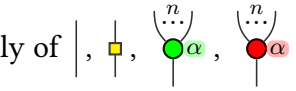
- *It exists for all M*
- *Σ can be made unique if we impose that its diagonal entries are decreasing non-negative real numbers*
- *U and V are not unique in general, though:*

- *If M is square with distinct and non-zero singular values, then U and V are essentially unique:*

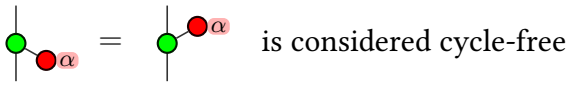
$$U\Sigma V^\dagger = U'\Sigma V'^\dagger \iff (\exists d, (U' = Ud) \wedge (V' = Vd))$$

where d is diagonal with diagonal entries some roots of unity.

Even though the singular-value decomposition is relevant for any diagram, we are only going to give its derivation for a particular family of diagrams:

⌜ **Definition 4.7.9** (Cycle-Free Diagram)**:** A *cycle-free* diagram is a diagram composed only of  , where $n \in \mathbb{N}$ and $\alpha \in \mathbb{R}$. ⌟

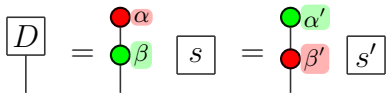
Remark 4.7.10. Some diagrams that do not strictly follow the conditions of the previous definition will still be considered cycle-free if they are equal to a cycle-free diagram by mere application of the "only connectivity matters" paradigm, i.e. if they are isomorphic to a cycle-free diagram. E.g.:



One-Qubit States

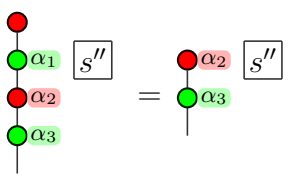
We can now easily give a normal form for one-qubit states, using the SVD of the underlying matrix.

Proposition 4.7.11 (SVD of a One-Qubit State)**.** *Any cycle-free state $D : 0 \to 1$ can be put in the following forms using* ZX*:*



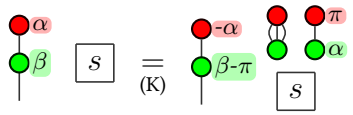
where $\beta, \beta' \in [0, \pi)$, and where s and s' are $0 \to 0$ diagrams, i.e. scalars. We call these two forms respectively SVD_g and SVD_r.

To understand where it comes from, notice that if $M \in \mathbb{C}^2 \times \mathbb{C}$, with $U\Sigma V^\dagger$ its SVD, then U is a 2×2 unitary, and $V^\dagger$ is a 1×1 unitary. A 2×2 unitary can be expressed as in Proposition 4.6.2, while a 1×1 unitary is merely a global phase i.e. a root of unity. Σ is of the form $\begin{pmatrix} s \\ 0 \end{pmatrix} = s' \begin{pmatrix} \sqrt{2} \\ 0 \end{pmatrix}$ (where $s = 0$ if $M = 0$). Hence one of its representations is:

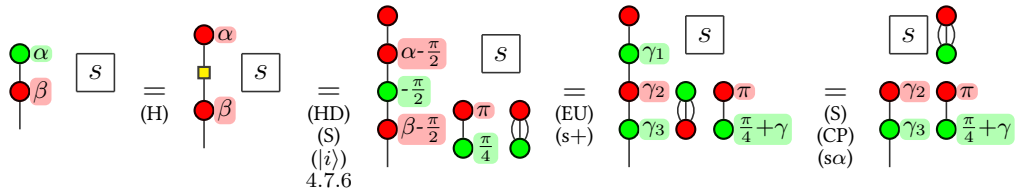


thanks to some rules of ZX, and where s'' is the aggregation of the scalars produced by U, Σ and $V^\dagger$.

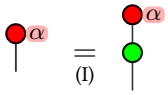
Proof ▶ First, notice that a state in the previous form of SVD_g, but with the bas constraints on angles, can easily be transformed into an SVD. Indeed, if $\beta \in [\pi, 2\pi)$:



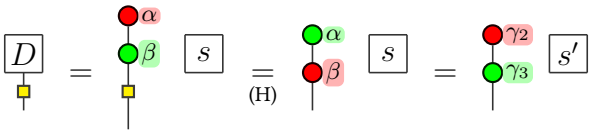
and similarly for the SVD_r. We can show that we can transform an SVD_r into an SVD_g and vice-versa: :



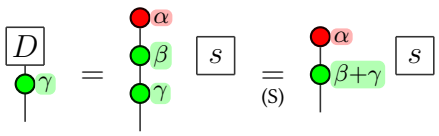
Then, we prove the result by induction.

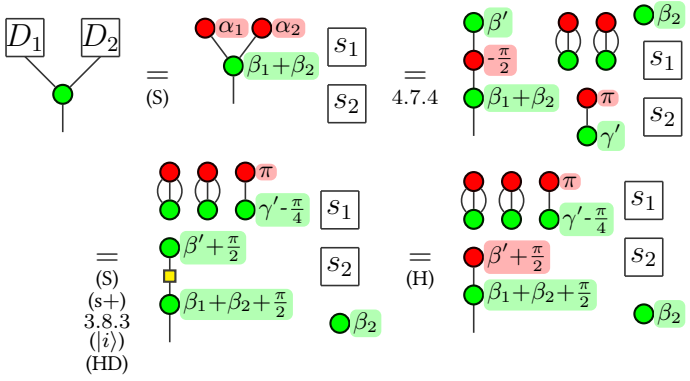


Then :



Notice that the generator $R_Z^{(0,1)}(\alpha)$ can be obtained as a combination of the last two. Then :





Finally, the generator $R_Z^{(n,1)}(\alpha)$ can be obtained by composition of $R_Z(\alpha)$ and $R_Z^{(2,1)}(\alpha)$; and $R_X^{(n,1)}(\alpha)$ can be obtained by composition of $R_Z^{(n,1)}(\alpha)$ and H. ◀

Proposition 4.7.12 (SVDs of states are essentially unique). *If* $D_1 =$  *and* $D_2 =$  *are in SVD, and if* $[\![D_1]\!] = [\![D_2]\!] \neq 0$*, then either:*

- $\alpha_1 = \alpha_2 \bmod 2\pi$ *and* $\alpha_i = 0 \bmod \pi$
- $\alpha_1 = \alpha_2 \bmod 2\pi$ *and* $\beta_1 = \beta_2$

Proof ▶ The equality reads $s_1 \begin{pmatrix} 1 + e^{i\alpha_1} \\ e^{i\beta_1}(1 - e^{i\alpha_1}) \end{pmatrix} = s_2 \begin{pmatrix} 1 + e^{i\alpha_2} \\ e^{i\beta_2}(1 - e^{i\alpha_2}) \end{pmatrix}$. If $\alpha_1 = \pi \bmod 2\pi$, then it is easy to see that $\alpha_2 = \pi \bmod 2\pi$ and $s_1 e^{i\beta_1} = s_2 e^{i\beta_2}$. If $\alpha_i \neq \pi \bmod 2\pi$, then the upper coefficient is non-null, hence we can divide the lower coefficient by the upper one, which yields:

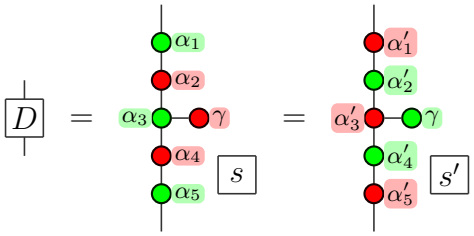
$$e^{i\beta_1} \frac{1 - e^{i\alpha_1}}{1 + e^{i\alpha_1}} = e^{i\beta_2} \frac{1 - e^{i\alpha_2}}{1 + e^{i\alpha_2}} \qquad \Longleftrightarrow \qquad e^{i\beta_1} \tan\left(\frac{\alpha_1}{2}\right) = e^{i\beta_2} \tan\left(\frac{\alpha_2}{2}\right)$$

If $\alpha_1 = 0 \bmod 2\pi$ then $\alpha_2 = 0 \bmod 2\pi$. Otherwise, since $\beta_1, \beta_2 \in [0, \pi)$, $\beta_1 = \beta_2$ and $\alpha_1 = \alpha_2 \bmod 2\pi$. ◀

$1 \to 1$ Operators

Applying the singular-value decomposition on $1 \to 1$ operators gives them a particular form, again with properties of essential uniqueness:

Proposition 4.7.13 (SVD of a $1 \to 1$ diagram). *Any cycle-free diagram* $D : 1 \to 1$ *can be written in the forms:*

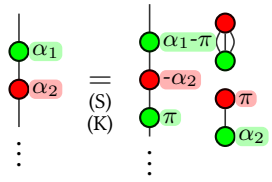


where $\gamma \in [0, \frac{\pi}{2}]$*, and* $\alpha_1, \alpha_5, \alpha'_1, \alpha'_5 \in [0, \pi)$*, using* ZX*. We denote the two forms respectively* SVD_g *and* SVD_r*.*

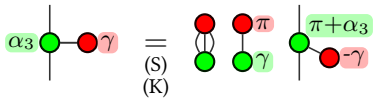
The intuition is that  has interpretation (up to a scalar) $\begin{pmatrix} 1 & 0 \\ 0 & \tan\left(\frac{\gamma}{2}\right) \end{pmatrix}$, and hence can be used to represent Σ in the SVD of $[\![D]\!]$. U and $V^\dagger$ here are 2×2 unitaries, and so can be represented as in Proposition 4.6.2. Using (S) to merge the green nodes gives the above form.

Proof ▶ First, if D is in the form SVD_g, but where the constraints on the angles are not met, we can transform it into an actual SVD_g:

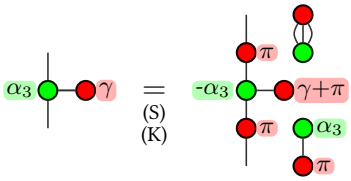
- If $\alpha_1 \in [\pi, 2\pi)$ (and similarly for α_5):



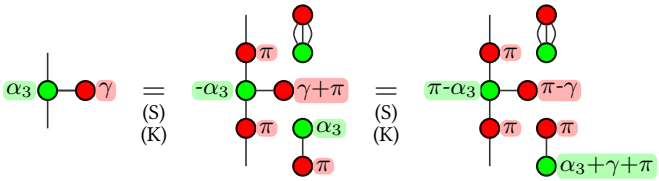
- If $\gamma \in [-\frac{\pi}{2}, 0)$:



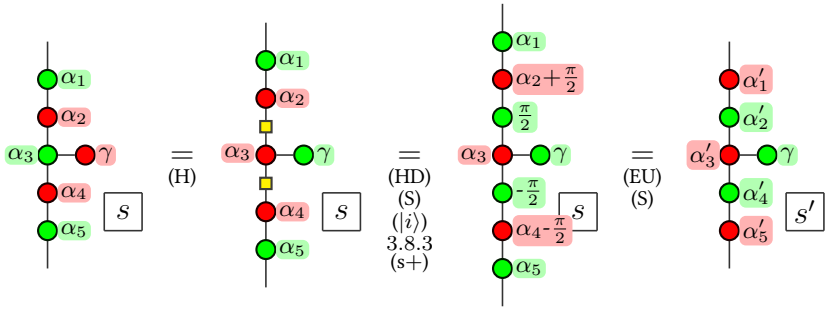
- If $\gamma \in [-\pi, -\frac{\pi}{2})$:



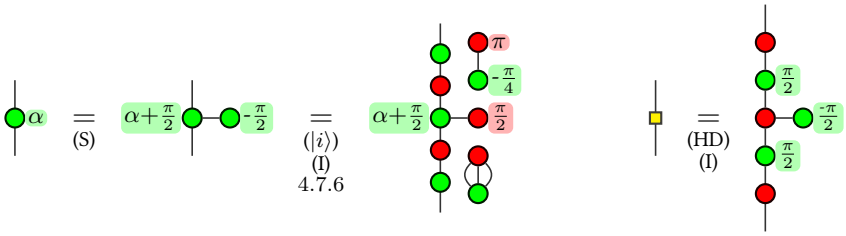
- If $\gamma \in [\frac{\pi}{2}, \pi)$:



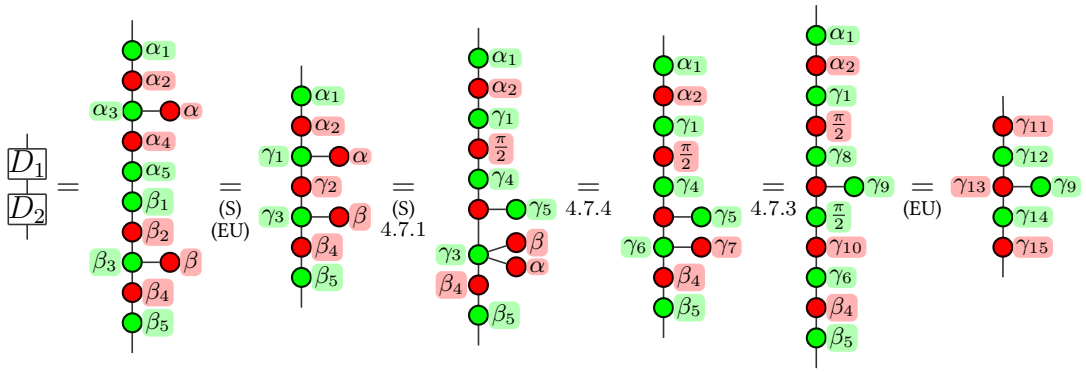
Then, we show that the two decompositions are equivalent:



We are going then to prove the result by induction on the structure of cycle-free diagrams given in Definition 4.7.9. The two $1 \to 1$ generators $R_Z^{(1,1)}(\alpha)$ and H can be put in SVD:

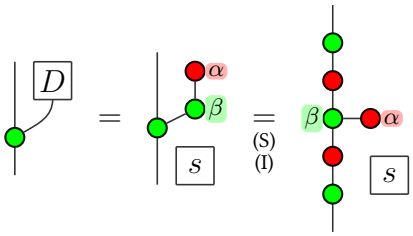


The composition of two SVDs can be put in SVD (here, ignoring the scalars):



Notice that, by composition, the $1 \to 1$ generator $R_X^{(1,1)}(\alpha)$ can be put in SVD.

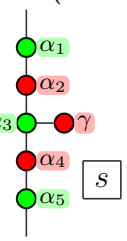
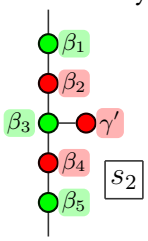
If the $1 \to 1$ diagram has no cycle, there can still be branching. Hence, there can be a state $D : 0 \to 1$ in tree-like form attached to the "main wire" by a node, say green, as follows:



A branching made by a red node $R_X^{(2,1)}$ can be deduced by composing the green one and Hadamard nodes. ◀

Remark 4.7.14. We gave two conventions for the SVDs of $0 \to 1$ and $1 \to 1$ diagrams. These two depend on the basis in which we consider the decomposition. SVD_g corresponds to the computational basis, while SVG_r corresponds to the diagonal basis. If $M = U\Sigma V^\dagger$ with Σ diagonal in the computational basis, $M = (UH) \cdot H\Sigma H \cdot (VH)^\dagger$.

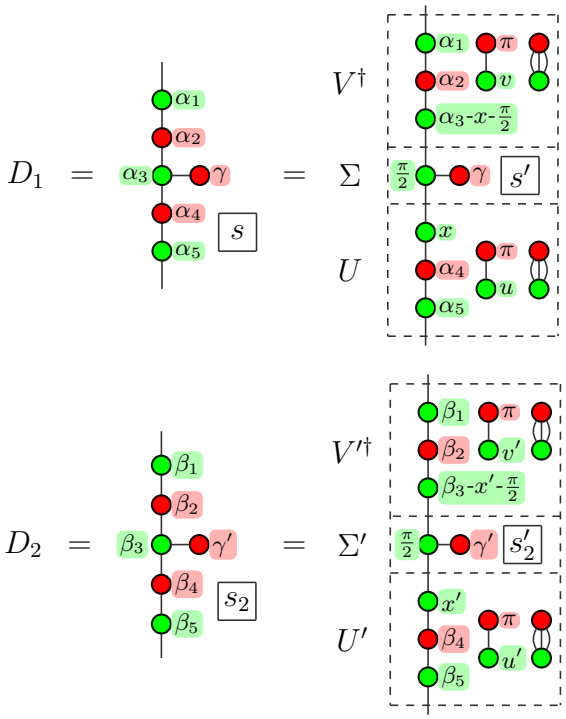
Proposition 4.7.15 ($1 \to 1$ SVDs are essentially unique)**.**

Suppose $D_1 =$  *and* $D_2 =$  *are in SVD, and that* $[\![D_1]\!] = [\![D_2]\!] \neq 0$.

Then, either:

- $\gamma = \gamma' = 0$
- $\gamma = \gamma' = \frac{\pi}{2}$
- $\alpha_i = \beta_i \bmod 2\pi$ *and* $\gamma = \gamma'$

Proof ▶ First we decompose D_1 and D_2 as:

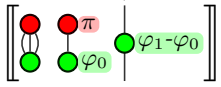
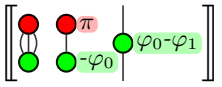


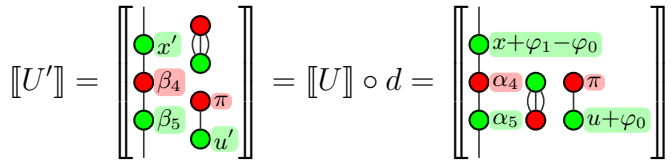
where u, v, u' and v' have been chosen so that $[\![\Sigma]\!]$ and $[\![\Sigma']\!]$ are real matrices, and where x and x' are arbitrary angles. Notice that $[\![U]\!]$, $[\![V^\dagger]\!]$, $[\![U']\!]$, $[\![V'^\dagger]\!]$ are unitaries. We have two SVDs that represent the same matrix:

$$[\![U]\!] \circ [\![\Sigma]\!] \circ [\![V^\dagger]\!] = [\![D_1]\!] = [\![D_2]\!] = [\![U']\!] \circ [\![\Sigma']\!] \circ [\![V'^\dagger]\!]$$

First off, let us show that Σ and Σ' are essentially the same. One could compute $[\![\Sigma]\!] = [\![s']\!]\,(1+e^{i\gamma}) \begin{pmatrix} 1 & 0 \\ 0 & \tan\left(\frac{\gamma}{2}\right) \end{pmatrix}$ and $[\![\Sigma']\!] = [\![s'_2]\!]\,(1+e^{i\gamma'}) \begin{pmatrix} 1 & 0 \\ 0 & \tan\left(\frac{\gamma'}{2}\right) \end{pmatrix}$. Since $\gamma, \gamma' \in [0, \frac{\pi}{2}]$, $\tan\left(\frac{\gamma}{2}\right)$ and $\tan\left(\frac{\gamma'}{2}\right)$ are smaller than 1, and since the diagrams are non-null, we get $[\![\Sigma]\!] = [\![\Sigma']\!]$ by Proposition 4.7.8, which implies $\gamma = \gamma'$.

If $\gamma = \gamma' \neq 0$, then $[\![\Sigma]\!]$ and $[\![\Sigma']\!]$ have full rank. Moreover, if $\gamma = \gamma' \neq \frac{\pi}{2}$, then $[\![\Sigma]\!]$ and $[\![\Sigma']\!]$ are not colinear to the identity. Hence, if $\gamma = \gamma' \in (0, \frac{\pi}{2})$, then we can apply Proposition 4.7.8.

By Proposition 4.7.8, there exists $d = \begin{pmatrix} e^{i\varphi_0} & 0 \\ 0 & e^{i\varphi_1} \end{pmatrix}$ such that $[\![U']\!] = [\![U]\!] \circ d$ and $[\![V'^\dagger]\!] = d^\dagger \circ [\![V^\dagger]\!]$. Notice that  $= d$ and  $= d^\dagger$. Hence:

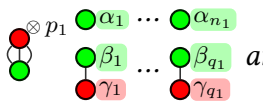
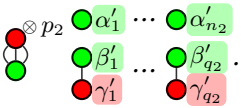


Since β_5 and α_5 are in $[0, \pi)$, the representation of the unitary is unique by Proposition 4.6.2, so $\beta_5 = \alpha_5$, $\beta_4 = \alpha_4$, and $x' = x + \varphi_1 - \varphi_0$. Similarly, the second equation yields

$\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$ and $\beta_3 - x' - \frac{\pi}{2} = \alpha_3 - x - \frac{\pi}{2} + \varphi_0 - \varphi_1$. Together, the equations on x and x' imply that $\alpha_3 = \beta_3$. ◀

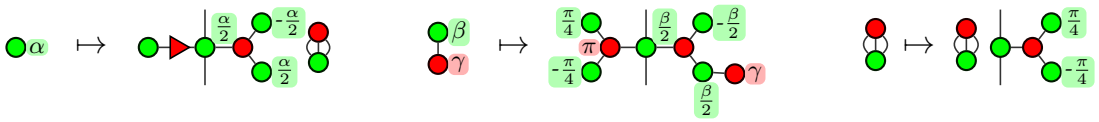
Completeness for some Scalars

Propositions 4.7.12 and 4.7.15 state that the SVD decomposition is essentially unique *in their structure*, but left out the scalars. To remedy this, we give the following result:

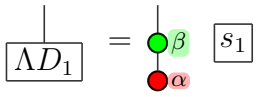
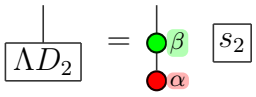
Proposition 4.7.16. *Let* $D_1 :=$  *and* $D_2 :=$  . *Then:*

$$[\![D_1]\!] = [\![D_2]\!] \iff \mathrm{ZX} \vdash D_1 = D_2$$

Proof ▶ For both diagrams, we are going to build a larger one. We define λ inductively by connected components:



and such that $\lambda(. \otimes .) = \lambda(.) \circ \lambda(.)$. Then, we define $\Lambda D_i :=$  $\circ \lambda(D_i)$ (the choice of notation Λ will be made clearer in Chapter 5). One can check that $[\![\lambda(D_i)]\!] = \begin{pmatrix} 1 & 0 \\ 0 & [\![D_i]\!] \end{pmatrix}$, so $[\![\Lambda D_i]\!] = \begin{pmatrix} 1 & [\![D_i]\!] \end{pmatrix}$. Hence, since $[\![D_1]\!] = [\![D_2]\!]$, we have $[\![\Lambda D_1]\!] = [\![\Lambda D_1]\!]$. By Propositions 4.7.11 and 4.7.12, both reduce to the same SVD form, with potentially different scalars, i.e.:

$\mathrm{ZX} \vdash$  and $\mathrm{ZX} \vdash$ 

It is fairly easy to prove that $\mathrm{ZX} \vdash \lambda(.) \circ$  $=$  , so $\mathrm{ZX} \vdash \Lambda D_i \circ$  $=$  . It helps us prove that the two scalars  and  are equal under ZX:

Hence, we have:

$$\mathrm{ZX} \vdash \Lambda D_1 = \Lambda D_2$$

It is also fairly easy to show that $\mathrm{ZX} \vdash \lambda(.) \circ$  $= . \otimes$  , so $\mathrm{ZX} \vdash \Lambda D_i \circ$  $= D_i$. Finally:

$$\mathrm{ZX} \vdash D_1 = \Lambda D_1 \circ \left(\pi \right) = \Lambda D_2 \circ \left(\pi \right) = D_2$$

◀

Remark 4.7.17. This gives a result of completeness only on a particular class of scalars. However, one can check that all the scalars produced by the two SVD algorithms (Propositions 4.7.11 and 4.7.13) are of this form.

From this we can directly get some equalities on scalars that will prove useful in the following.

Corollary 4.7.18.

$$\mathrm{ZX} \vdash \quad \overset{\frac{\pi}{3}}{\underset{-\frac{\pi}{3}}{\bullet}} \quad = \quad \bullet\!\!\bullet$$

Corollary 4.7.19.

$$\mathrm{ZX} \vdash \quad \overset{\arccos\left(\frac{1}{4}\right)}{\underset{-\arccos\left(\frac{1}{4}\right)}{\bullet}} \quad = \quad \bullet\!\!\bullet\!\!\bullet$$

Corollary 4.7.20. *If* $\alpha \neq \pi \bmod 2\pi$*:*

$$\mathrm{ZX} \vdash \quad \alpha \quad \overset{\otimes n}{\underset{-\alpha}{\bullet}} \quad \overset{\gamma}{\underset{-\gamma}{\bullet}} \quad = \quad \boxed{}$$

with:
$n := \max\left(0, \lceil -\log_2(1+\cos(\alpha))\rceil - 2\right)$
$\gamma := \arccos\left(\frac{1}{2^{n+1}(1+\cos(\alpha))}\right)$.

Corollary 4.7.21.

$$\mathrm{ZX} \vdash \quad \overset{\pi}{\underset{\frac{\pi}{2}}{\bullet}} \quad \overset{\alpha+\pi}{\underset{-\alpha}{\bullet}} \quad \overset{\gamma}{\underset{-\gamma}{\bullet}} \quad = \quad \boxed{}$$

with $\alpha := 2\arctan\left(\frac{1}{\sqrt{2}}\right)$
and $\gamma := \arccos\left(\frac{3}{8}\right)$.

4.8 Completeness of ZX/ ZX

Recovering $\mathrm{ZX}_{\pi/4}$

The point now is to exploit the SVD of ZX-diagrams and their uniqueness, first to recover $\mathrm{ZX}_{\pi/4}$, and then to prove the completeness for unrestricted ZX-Calculus. A rule that can directly use these results is (BW), because the diagrams on both sides of the equation are cycle-free:

Corollary 4.8.1.

$$\mathrm{ZX} \vdash \quad \overset{\frac{\pi}{4}}{\underset{\frac{\pi}{4}}{\bullet}}\!\!\overset{\frac{\pi}{4}}{\underset{-\frac{\pi}{2}}{\bullet}}\!\!\overset{\frac{\pi}{4}}{\underset{\frac{\pi}{4}}{\bullet}} \quad \overset{(BW)}{=} \quad \overset{\frac{\pi}{4}}{\underset{\frac{\pi}{4}}{\bullet}}\!\!\overset{\pi}{\underset{\pi}{\bullet}}\!\!\overset{\frac{\pi}{4}}{\underset{\frac{\pi}{2}}{\bullet}}$$

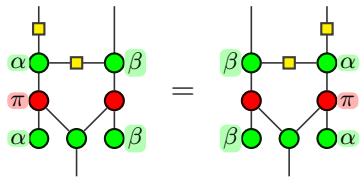
***Proof** of Cor. 4.8.1* ▶ Using Proposition 4.7.13, we can put both sides of the equation in SVD form, and thanks to Proposition 4.7.15, the two forms have the same structural angles. We can even compute:

$$\overset{\frac{\pi}{4}}{\underset{\frac{\pi}{4}}{\bullet}}\!\!\overset{\frac{\pi}{4}}{\underset{\frac{-\pi}{2}}{\bullet}}\!\!\overset{\frac{\pi}{4}}{\underset{\frac{\pi}{4}}{\bullet}} \quad = \quad \gamma \quad \overset{\frac{\pi}{2}}{\underset{\frac{\pi}{2}}{\bullet}} \quad \boxed{s_1} \quad \overset{\beta_1}{\underset{\beta_1}{\bullet}} \qquad \text{and} \qquad \overset{\frac{\pi}{4}}{\underset{\frac{\pi}{4}}{\bullet}}\!\!\overset{\pi}{\underset{\pi}{\bullet}}\!\!\overset{\frac{\pi}{4}}{\underset{\frac{\pi}{2}}{\bullet}} \quad = \quad \gamma \quad \overset{\frac{\pi}{2}}{\underset{\frac{\pi}{2}}{\bullet}} \quad \boxed{s_2} \quad \overset{\beta_1}{\underset{\beta_1}{\bullet}}$$

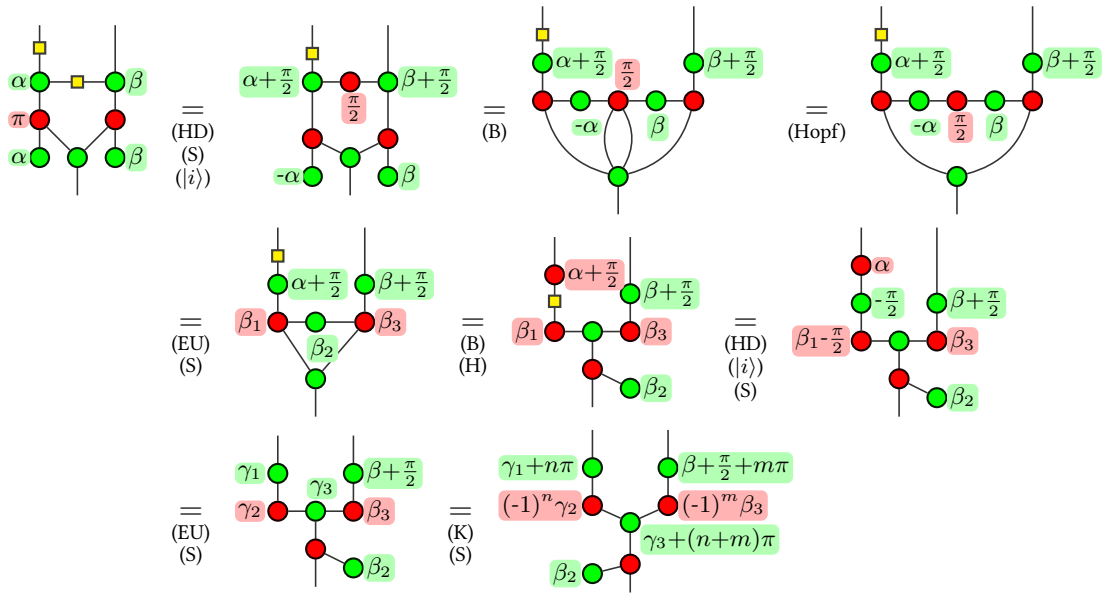
with $\gamma = \frac{\pi}{2} - 2\arctan\left(\frac{1}{\sqrt{5}}\right)$ and $\beta_1 = \arctan(2)$.
Also, combining Remark 4.7.17 and Proposition 4.7.16, we directly get that the two scalars are provably equal, which concludes this proof. ◀

The results on SVDs cannot be directly used to prove the equation (C) though, for its diagrams have 4 inputs/outputs, and have cycles. However, the SVDs can be used to prove a first intermediary result:

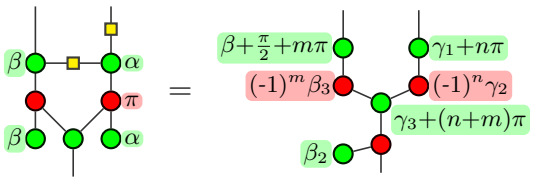
Lemma 4.8.2.

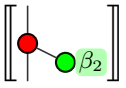


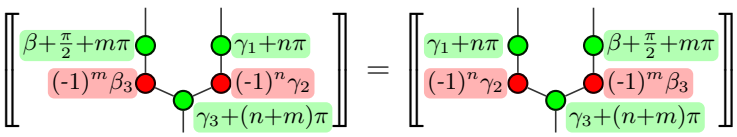
Proof ▶ We prove the equality by simplifying both sides of the equation. The left hand side yields, when ignoring the scalars:



where n and m are chosen in $\{0, 1\}$ so that $\gamma_1 + n\pi$ and $\beta + \frac{\pi}{2} + m\pi$ are in $[0, \pi)$. By symmetry, the right hand side yields:

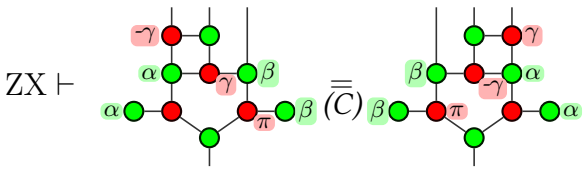


Notice that, due to the symmetry of the two diagrams, the resulting scalars (that we ignored) are equal (and non null). If $\beta_2 = 0 \bmod \pi$, then we can compute that both α and β are multiples of π, and in this case the equation is trivially derivable. Else, notice that $\left[\!\left[\right.\right.$  $\left.\right]\!\right]$ is invertible, $\left(\text{its inverse is } \frac{1}{1-e^{2i\beta_2}} \begin{pmatrix} 1 & -e^{i\beta_2} \\ -e^{i\beta_2} & 1 \end{pmatrix}\right)$. Hence, we get:

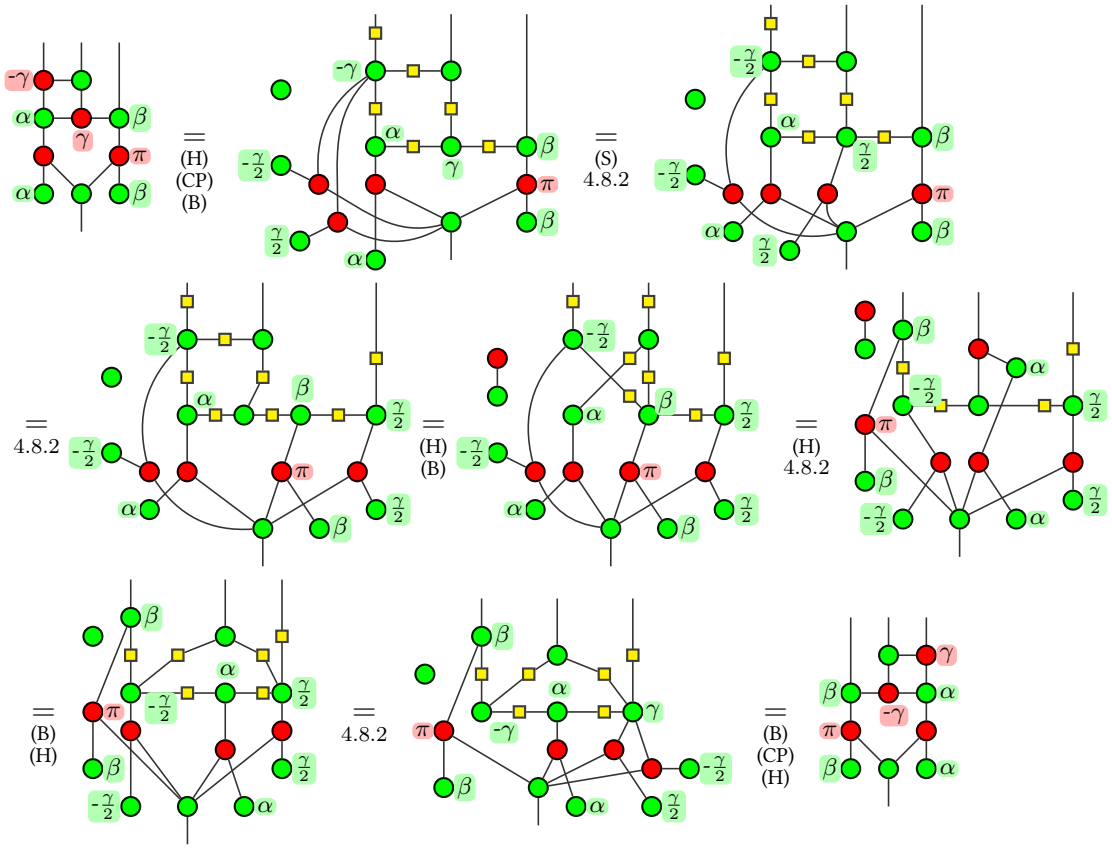


We can then plug any red dot with angle $\in (0, \frac{\pi}{2})$, say $\frac{\pi}{4}$, on the lower branch. We can now use Proposition 4.7.15, match the angles $\gamma_1 + n\pi = \beta + \frac{\pi}{2} + m\pi$ and $(-1)^n\gamma_2 = (-1)^m\beta_3$, so the two initial diagrams are equal. ◀

Proposition 4.8.3.



***Proof** of Prop. 4.8.3* ▶



◀

Remark 4.8.4. The proof of Proposition 4.8.3 shows that (C) can be derived using only Lemma 4.8.2 and the Clifford rules $\mathrm{ZX}_{\pi/2}$. However, the provided proof requires using half angles (for γ). Hence, whenever the considered fragment contains all its half angles, the equation in Lemma 4.8.2 should be preferred to (C).

We have derived all the rules necessary for the completeness of the Clifford+T fragment of the ZX-Calculus (Lemma 4.6.3, Propositions 4.7.5 and 4.8.3, and Corollary 4.8.1), which means:

Proposition 4.8.5. *For any diagrams D_1, D_2 of* $\mathbf{ZX}[\frac{\pi}{4}]$*:*

$$[\![D_1]\!] = [\![D_2]\!] \iff \mathrm{ZX} \vdash D_1 = D_2$$

In other words, $\mathrm{ZX} \vdash \mathrm{ZX}_{\pi/4}$. Hence, by Theorem 4.4.1, we can also derive any sound linear equation with constants in $\frac{\pi}{4}\mathbb{Z}$.

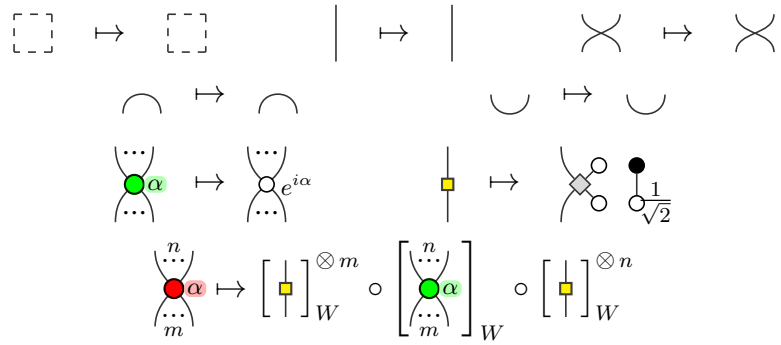
Corollary 4.8.6. *For any* $\mathbf{ZX}[\vec{\alpha}, \frac{\pi}{4}]$*-diagrams* D_1 *and* D_2*:*

$$[\![D_1]\!] = [\![D_2]\!] \iff \mathrm{ZX} \vdash D_1 = D_2$$

Completeness from $\mathrm{ZW}_{\mathbb{C}}$

We are now going to prove Theorem 4.6.1 using the completeness of $\mathbf{ZW}[\mathbb{C}]/\mathrm{ZW}_{\mathbb{C}}$, again through a system of back and forth translation between the two languages. The interpretation $[.]_W$ from **ZX** to $\mathbf{ZW}[\mathbb{C}]$ is pretty obvious:

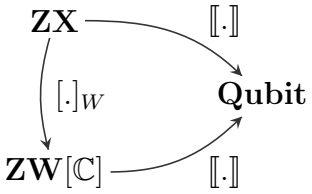
$[.]_W$

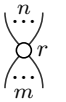
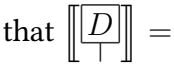
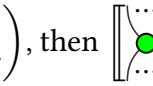
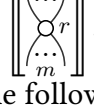


$$D_1 \circ D_2 \mapsto [D_1]_W \circ [D_2]_W \qquad D_1 \otimes D_2 \mapsto [D_1]_W \otimes [D_2]_W$$

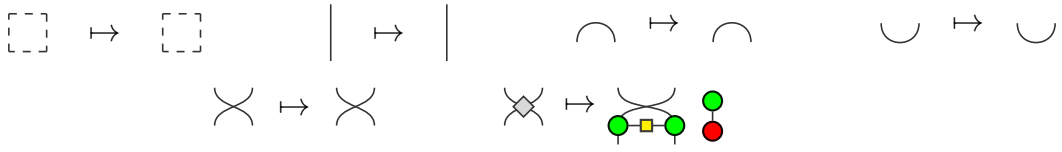
It preserves the semantics:

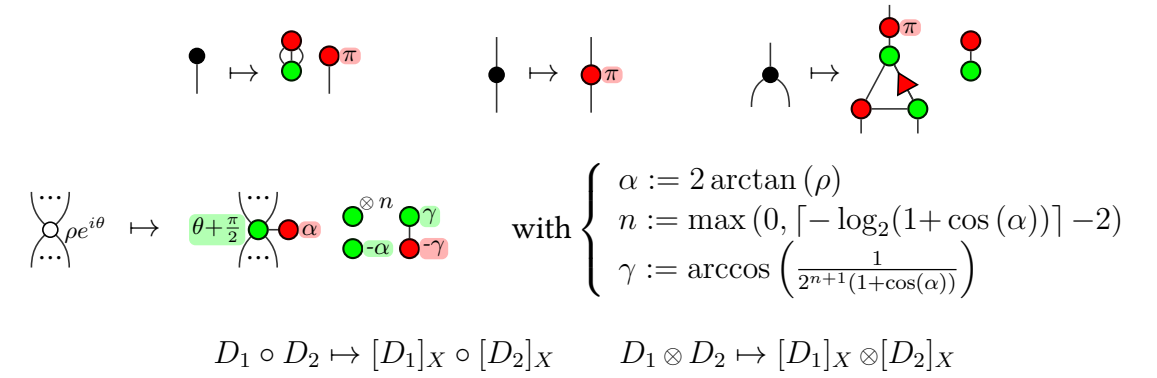
Lemma 4.8.7. *The following diagram commutes:*



The other way round is slightly less straightforward, because of the ring structure of the ZW-Calculus: how to represent  in **ZX**? First of all, notice that if we find a 1-qubit state D such that  $= \begin{pmatrix} 1 \\ r \end{pmatrix}$, then  $=$  . However, we can use the SVD form of a 1-qubit state to determine D. We get the following interpretation:

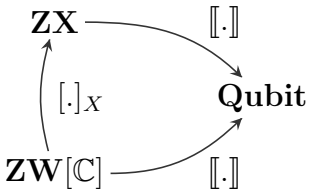
$[.]_X$





As you can see, some side calculation is buried in the scalars. Particularly, the scalars in the interpretation of the GHZ node basically amount to the inverse of α, as evidenced by Corollary 4.7.20. Here again, the interpretation preserves the semantics:

Lemma 4.8.8. *The following diagram commutes:*

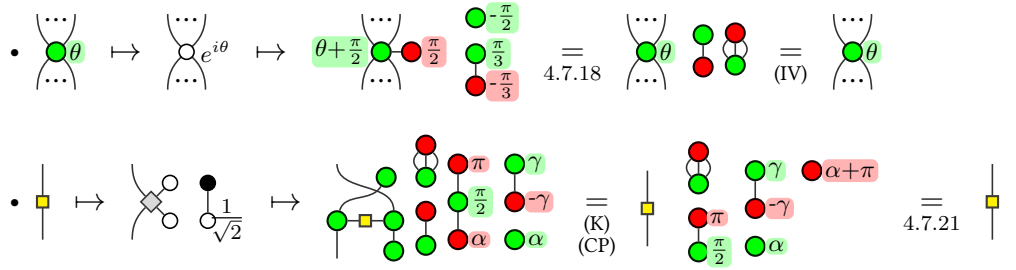


A first part of the proof of completeness is to show that any diagram can be recovered from its back and forth interpretation:

Proposition 4.8.9. *For any* **ZX***-diagram:*

$$\mathrm{ZX} \vdash [[D]_W]_X = D$$

Proof ▶ We prove the result by induction. Since both interpretations are PROP-functors, we only need to prove the result for the generators. The result for wire generators is obvious.



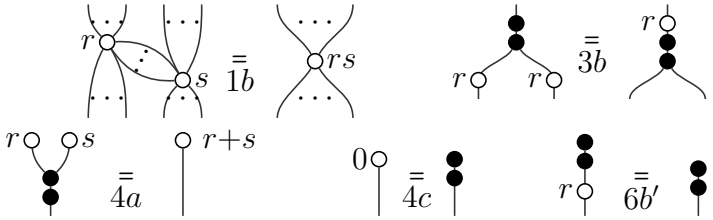
Finally, R_X is a composition of R_Z and H. ◀

Then, we can show that ZX proves any equality of $\mathbf{ZW}[\mathbb{C}]/\,\mathrm{ZW}_{\mathbb{C}}$ through $[.]_X$.

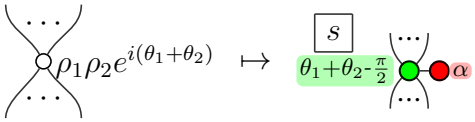
Proposition 4.8.10. *Let D_1 and D_2 be two* $\mathbf{ZW}[\mathbb{C}]$*-diagrams.*

$$\mathrm{ZW}_{\mathbb{C}} \vdash D_1 = D_2 \implies \mathrm{ZX} \vdash [D_1]_X = [D_2]_X$$

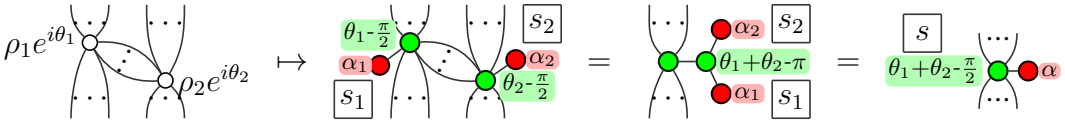
Proof ▶ As before, we are going to show that all the axioms in $\mathrm{ZW}_{\mathbb{C}}$ are derivable using ZX. Most of them are already proven by $\mathrm{ZX}_{\pi/4}$, so a fortiori by ZX, thanks to Proposition 4.8.5. Only 5 remain:



- $1b$: On the one hand:

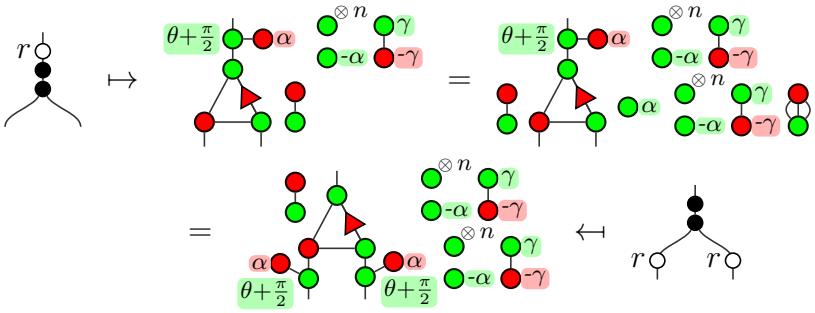


and on the other:

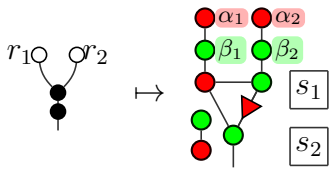


Using SVD decomposition and its uniqueness (Props. 4.7.13 and 4.7.15) on the dangling branch, together with Proposition 4.7.16 and Remark 4.7.17 for the scalar equality.

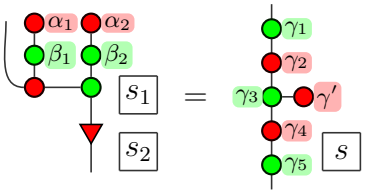
- $3b$:



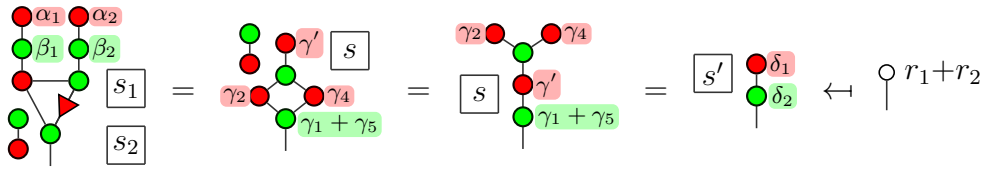
- $4a$: The right hand side can be directly put in SVD form. However, the left hand side yields:



and it contains a cycle. This can be remedied since by Proposition 4.7.13:

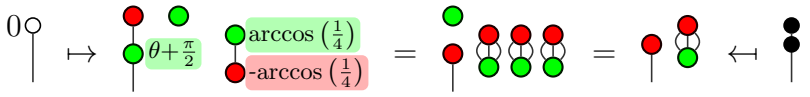


Hence:

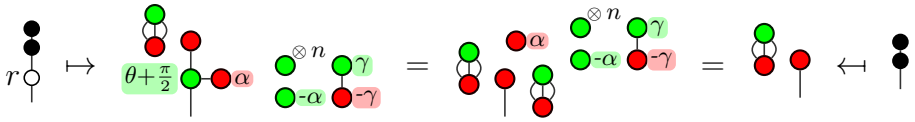


by uniqueness of the SVD-decomposition (Prop. 4.7.12), and using Proposition 4.7.16 and Remark 4.7.17 to deal with the scalars.

- $4c$:

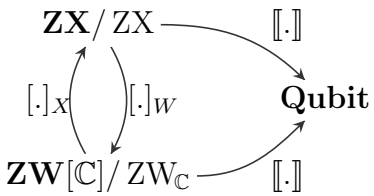


- $6b'$:



◀

***Proof** of Theorem 4.6.1* ▶ We have the following diagram:



Let's prove that $[.]_W$ is full and faithful.

- $[.]_W$ **is faithful:** Let D_1, D_2 be two **ZX**-diagrams such that $\mathrm{ZW}_\mathbb{C} \vdash [D_1]_W = [D_2]_W$. By Proposition 4.8.10, we have $\mathrm{ZX} \vdash [[D_1]_W]_X = [[D_2]_W]_X$, and by Proposition 4.8.9, $\mathrm{ZX} \vdash D_1 = [[D_1]_W]_X = [[D_2]_W]_X = D_2$.
- $[.]_X$ **is full:** Let D be a **ZW**$[\mathbb{C}]$-diagram. We define $D_X := [D]_X$. By Lemmas 4.8.7 and 4.8.8, $[\![[.]_X]_W]\!] = [\![.]\!]$, hence, by completeness of **ZW**$[\mathbb{C}]$/ $\mathrm{ZW}_\mathbb{C}$, $\mathrm{ZW}_\mathbb{C} \vdash [[D]_X]_W = D$, i.e. $\mathrm{ZW}_\mathbb{C} \vdash [D_X]_W = D$.

Then, by composition, since **ZW**$[\mathbb{C}]$/ $\mathrm{ZW}_\mathbb{C} \xrightarrow{[\![.]\!]}$ **Qubit** is full and faithful, the functor **ZX**/ ZX $\xrightarrow{[\![.]\!]}$ **Qubit** $= [\![[.]_W]\!]$ is full and faithful. ◀

4.9 Another Axiomatisation for Universal ZX-Calculus

In the axiomatisation ZX, there are two rules that deal with one-qubit unitaries: the Euler angles (EU), and the Hadamard decomposition (HD). We explore the possibility of merging the two rules, and give an axiomatisation ZX′ in Figure 4.4.

This axiomatisation is as powerful as ZX.

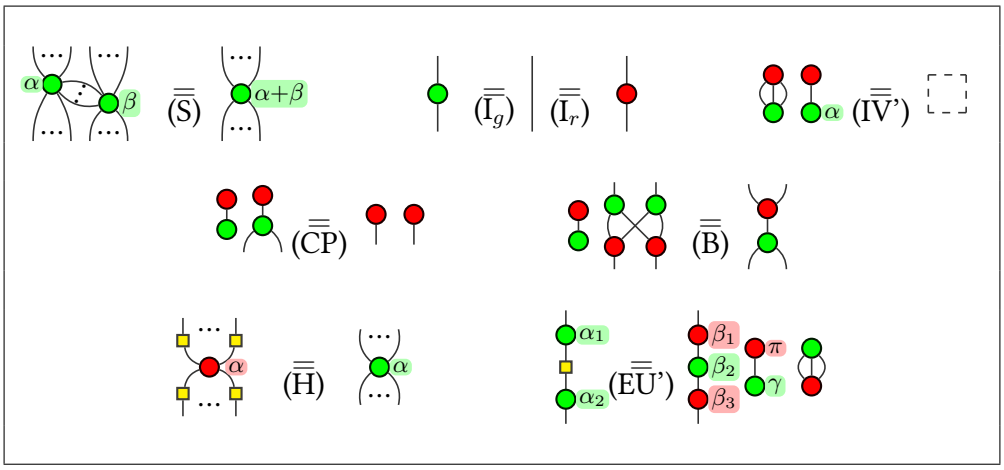
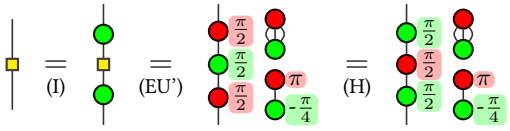


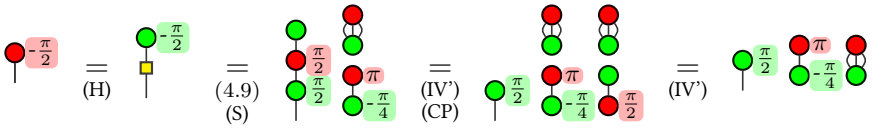
Figure 4.4: Set of rules ZX′ for the ZX-Calculus with scalars. The right-hand side of (IV') is an empty diagram. (...) denote zero or more wires, while (⋰) denote one or more wires. In rule (EU'), $\beta_1, \beta_2, \beta_3$ and γ can be determined as follows: $x^+ := \frac{\alpha_1+\alpha_2}{2}$, $x^- := x^+ - \alpha_2$, $z := -\sin(x^+) + i\cos(x^-)$ and $z' := \cos(x^+) - i\sin(x^-)$, then $\beta_1 = \arg z + \arg z', \beta_2 = 2\arg\left(i + \left|\frac{z}{z'}\right|\right), \beta_3 = \arg z - \arg z', \gamma = x^+ - \arg(z) + \frac{\pi-\beta_2}{2}$ where by convention $\arg(0) := 0$ and $z' = 0 \implies \beta_2 = 0$.

Theorem 4.9.1. *The language* $\mathbf{ZX}/\mathrm{ZX}'$ *is complete. The functor* $\mathbf{ZX}/\mathrm{ZX}' \xrightarrow{[\![\cdot]\!]} \mathbf{Qubit}$ *is full and faithful.*

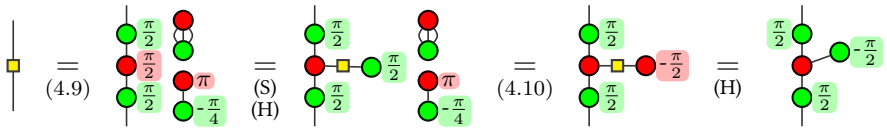
Proof ▶ The functor is obviously full, since the diagrams are the same in $\mathbf{ZX}/\mathrm{ZX}'$ as in $\mathbf{ZX}/\mathrm{ZX}$. To prove the faithfulness, we are going to show $\mathrm{ZX}' \vdash \mathrm{ZX}$. First, let us recover the Hadamard decomposition (HD):



(4.9)

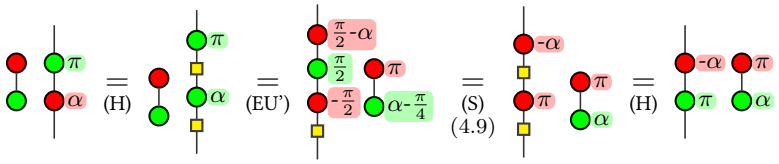


(4.10)

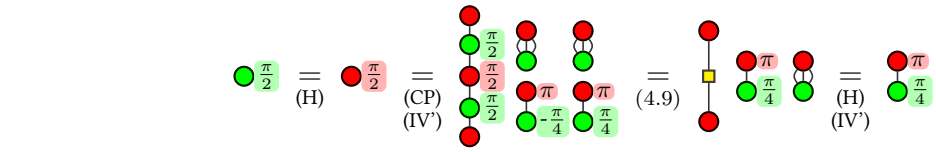


(4.11)

The next step is to prove that the equation (E) is derivable. To do so, we will first derive (K) and (SUP).

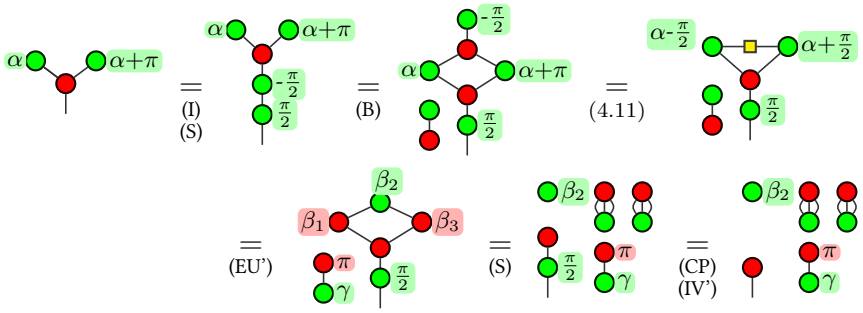


(4.12)

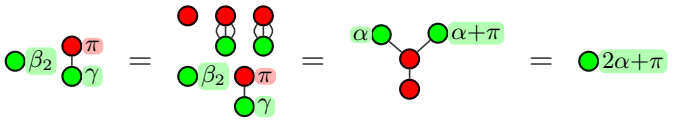


(4.13)

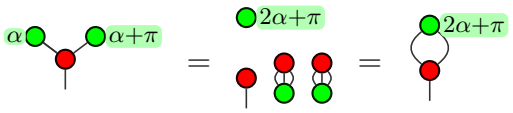
First, for proving (SUP):



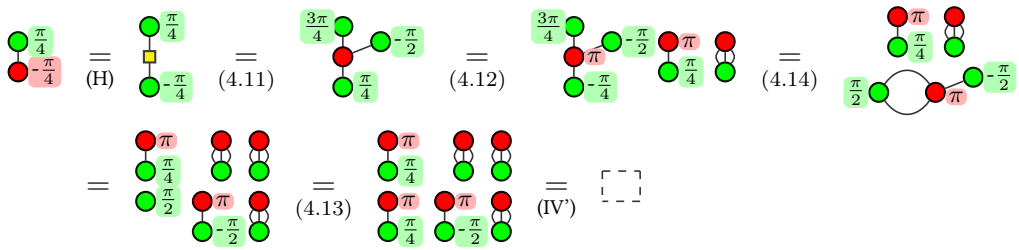
Hence:



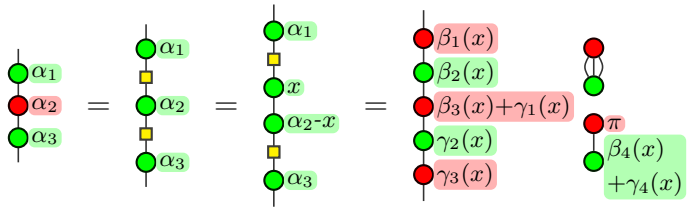
so finally:



(4.14)



It now remains to prove the rule (EU) can be derived. We decompose the left hand side diagram as such:



where x is considered as a variable, and hence, all the computed angles depend on it, while the angles α_i are fixed. We want to find x_0 such that $\beta_3(x_0) + \gamma_1(x_0) = 0 \bmod \pi$. Let the functions f and g be defined as:

$$f : x \mapsto \arctan\left(\frac{\tan(\alpha_1)\cos(x) + \tan(\alpha_3)\cos(\alpha_2 - x)}{1 - \tan(\alpha_1)\cos(x)\tan(\alpha_3)\cos(\alpha_2 - x)}\right)$$

$$g : x \mapsto \tan(\alpha_1)\cos(x) + \tan(\alpha_3)\cos(\alpha_2 - x)$$

Notice that

$$g\left(-\frac{\pi}{2}\right) = \tan(\alpha_3)\cos\left(\alpha_2 + \frac{\pi}{2}\right)$$

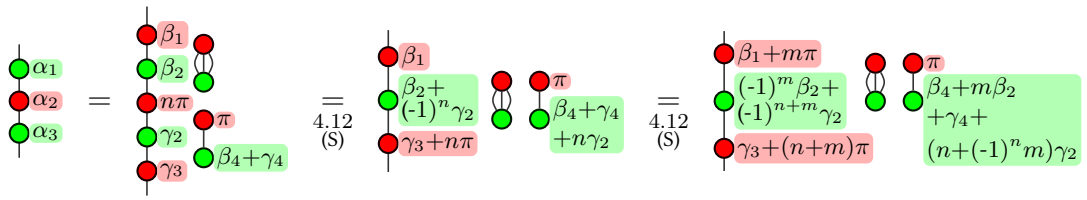
and

$$g\left(\frac{\pi}{2}\right) = \tan(\alpha_3)\cos\left(\alpha_2 - \frac{\pi}{2}\right)$$

Hence, $g\left(-\frac{\pi}{2}\right) g\left(\frac{\pi}{2}\right) \leq 0$. Since g is continuous, by the intermediate value theorem, there exists $x_0 \in [\frac{-\pi}{2}, \frac{\pi}{2}]$ such that $g(x_0) = 0$. Notice now that

$$f(x_0) = \arctan\left(\frac{0}{1 + \tan(\alpha_1)^2 \cos(\alpha_2 - x_0)^2}\right) = 0$$

Also, it can be computed that $f = \beta_3 + \gamma_1 \bmod \pi$. Hence, $\beta_3(x_0) + \gamma_1(x_0) = 0 \bmod \pi$ i.e. $\beta_3(x_0) + \gamma_1(x_0) = n\pi$. Hence, denoting $\beta_i \leftarrow \beta_i(x_0)$ and $\gamma_i \leftarrow \gamma_i(x_0)$:



Since, thank to Proposition 4.6.2, the unitary representation is unique if $\beta_1 + m\pi \in [0, \pi)$ (m has been chosen for this purpose), then the previous diagram is provably equivalent to the one resulting directly from (EU). ◀

On the one hand, this new axiomatisation is one axiom shorter, and (EU') and (IV') can be considered simpler than (EU) and (E). On the other hand, the axiomatisation in Figure 4.3 has the nice property that it suffices to remove (EU) and (E) to get a complete axiomatisation for the scalar-free Clifford fragment. Moreover, (EU) is arguably more natural, and has already been given for instance in [CW18].

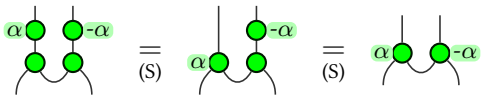
Again, we conjecture that all the rules in ZX′ are necessary, i.e. none of the rules are derivable from the others. Indeed, the arguments given for the minimality of ZX can easily be adapted here, and we are left with the same observation: only (B) and (I_r) are not proven to be necessary.

4.10 ZX-Calculus for Completely Positive Maps

As pointed out in Section 1.5, there exists a formalism for expressing quantum evolutions in a non-isolated system. They are represented as density matrices, and the trace operator is used to represent the interaction of the system to its environment. In [Sel07], it is pointed out that any †-compact monoidal category for pure quantum mechanics could be turned into a category for CPMs thanks to the so-called CPM-construction. For the simplified case of PROPs, it becomes:

⌜ **Definition 4.10.1** (CPM-construction)**:** Given a †-compact PROP $\mathbf{C}$, let $\mathrm{CPM}(\mathbf{C})$ be the †-compact PROP such that its arrows are $\left\{ \left. \right| \; n, m \in \mathbb{N},\ f : n \to m \right\}$, where $:=$. ⌟

Notice that if we have a PROP $\mathbf{L}$ quotiented by R, R can also quotient $\mathrm{CPM}(\mathbf{L})$. However, this is ill defined, for a term of $\mathrm{CPM}(\mathbf{L})$ after application of an equality of R may not be in $\mathrm{CPM}(\mathbf{L})$ but in the larger PROP $\mathbf{L}$. For instance, consider the following derivation in $\mathbf{ZX}/\,\mathrm{ZX}$:



The first and the third diagram are both in $\mathrm{CPM}(\mathbf{ZX})$, but the second one is not. In other words, in order to prove that two diagrams of $\mathrm{CPM}(\mathbf{L})$ are equal, one would need to derive the equality in $\mathbf{L}$.

Notice also that the representation of a CPM in the CPM-construction requires a "doubling" of the diagram: one needs f and its adjoint f^*.

Another approach to relate pure quantum mechanics to the general one is the notion of environment structure [Coe08, CH16, CP12]. The notion of *purification* is central in the definition of environment structure. Intuitively, it means that (1) there is a discard morphism; (2) any morphism can be purified, i.e. decomposed into a pure morphism followed by a discarding map, and (3) this purification is essentially unique. More formally:

⌜ **Definition 4.10.2** (Environment Structure)**:** An environment structure for a †-compact PROP $\mathbf{C}$ is an compact closed PROP $\overline{\mathbf{C}}$ with an i.o.o. PROP-functor $\iota : \mathbf{C} \to \overline{\mathbf{C}}$ and a morphism $\frac{\perp}{=} : 1 \to 0$ such that:

(1) For all $f : n \to m \in \overline{\mathbf{C}}$, there exists $f' : n \to m + k \in \mathbf{C}$ such that: f $=$ $\iota^{\frac{\perp}{=}}(f')$

(2) For any $f : n \to m + k_1$ and $g : n \to m + k_2$ in $\mathbf{C}$: $f \sim_{\mathrm{cp}} g \iff$ $\iota(f)$ $=$ $\iota(g)$

where the relation $\sim_{\mathrm{cp}}$ is defined as: $f \sim_{\mathrm{cp}} g \iff$ f $f^\dagger$ $=$ g $g^\dagger$ ⌟

Notice that $\sim_{\mathrm{cp}}$ is technically not a relation on morphisms but on tuples (n, m, k, f) with $f : n \to m + k \in \mathbf{C}$: $(n, m, k, f) \sim_{\mathrm{cp}} (n', m', k', g)$ if $n = n'$, $m = m'$ and f and g satisfy the graphical condition represented above. As an abuse of notation, we write $f \sim_{\mathrm{cp}} g$, as the other components of the tuple will be usually obvious from context. We will do the same for our relation $\sim_{\mathrm{iso}}$ below.

$\mathrm{CPM}(\mathbf{FdHilb})$ is actually an environment structure for the category $\mathbf{FdHilb}$, and more generally for any †-compact PROP $\mathbf{C}$, $\mathrm{CPM}(\mathbf{C})$ is an environment structure for $\mathbf{C}$ and conversely any environment structure for $\mathbf{C}$ is equivalent to $\mathrm{CPM}(\mathbf{C})$ [CH16].

The Discard Construction

First we need to define for any †-PROP its subcategory of isometries.

⌜ **Definition 4.10.3:** Let $\mathbf{C}$ be a †-PROP. We define $\mathbf{C}_{\text{iso}}$ as the subcategory of $\mathbf{C}$ such that its arrows are $\left\{ f : n \to m \;\middle|\; f^\dagger \circ f = id_n \right\}$. ⌟

Notice that $\mathbf{C}_{\text{iso}}$ is usually not a †-PROP. Any †-PROP-functor $F : \mathbf{C} \to \mathbf{D}$ between two †-PROPs can be restricted to their subcategories of isometries leading to a PROP-functor $F_{\text{iso}} : \mathbf{C}_{\text{iso}} \to \mathbf{D}_{\text{iso}}$. Thus there is a restriction functor $\text{iso} : \text{†-PROP} \to \text{PROP}$. Remark that this functor preserves fullness and faithfulness. One always has a faithful inclusion PROP-functor: $\iota_{\text{iso}} : \mathbf{C} \to \mathbf{C}_{\text{iso}}$.

In quantum mechanics, isometries are causal evolutions, i.e. applying an isometry and then discarding all outputs is equivalent to discarding the inputs straight away. As pointed out in [HS19], adding discard maps to the category of isometries would make 0 a terminal object. We define this category, called affine completion:

⌜ **Definition 4.10.4:** Given an PROP $\mathbf{C}$, we define $\mathbf{C}^!$ as $\mathbf{C}$ with an additional morphism $! : 1 \to 0$, such that, for all $f : n \to m \in \mathbf{C}$, $!^{\otimes m} \circ f = !^{\otimes n}$. By convention, we have $!^{\otimes 0} = id_0$. This makes 0 a terminal object in $\mathbf{C}^!$, and hence makes $\mathbf{C}^!$ the affine completion of $\mathbf{C}$. ⌟

Remark 4.10.5. Formally, a morphism $!_n$ should be defined for every object n of the PROP, such that for any $f : n \to m$, $!_m \circ f = !_n$, and such that $!_0 = id_0$. However, we have that $!_n \otimes !_m = id_0 \circ (!_n \otimes !_m) = !_0 \circ (!_n \otimes !_m) = !_{n+m}$. This means that $!_n = !_1^{\otimes n}$.

Again given a PROP-functor $F : \mathbf{C} \to \mathbf{D}$, one can define a functor $F^! : \mathbf{C}^! \to \mathbf{D}^!$ by $F^!(!) = !$ and $F^!(f) = \iota^!(F(f))$ for the other morphisms. In [HS19], Huot and Staton show that $\mathbf{CPTP}$, the category of completely positive trace preserving maps, is equivalent to $\mathbf{FdHilb}^!_{\text{iso}}$, thus giving a characterisation of it via a universal property. We extend this idea to non-trace preserving maps by proceeding to a local affine completion of the subcategory of isometries.

We define the category $\mathbf{C}^{\doteqdot}$ as the pushout of $\mathbf{C}$ and $\mathbf{C}^!_{\text{iso}}$:

⌜ **Definition 4.10.6** (Discard Construction)**:** Given a †-PROP $\mathbf{C}$, $\mathbf{C}^{\doteqdot}$ is defined as the pushout:

$$\begin{array}{ccc} \mathbf{C}_{\text{iso}} & \xhookrightarrow{\iota_{\text{iso}}} & \mathbf{C} \\ {\scriptstyle \iota^!}\downarrow & \ulcorner & \downarrow{\scriptstyle \iota^{\doteqdot}} \\ \mathbf{C}^!_{\text{iso}} & \xhookrightarrow[\iota^!_{\text{iso}}]{} & \mathbf{C}^{\doteqdot} \end{array}$$

⌟

The pushout of two PROPs always exist [Zan15]. We can also describe it simply combinatorially. The morphisms of $\mathbf{C}^{\doteqdot}$ are equivalence classes generated by formal composition and tensoring of morphisms in $\mathbf{C}^!_{\text{iso}}$ and $\mathbf{C}$. The equivalence relation is generated by the equations of both categories augmented with equations $\iota^!(f) = \iota_{\text{iso}}(f)$ for all f in $\mathbf{C}_{\text{iso}}$. The functors $\iota^{\doteqdot}$ and $\iota^!_{\text{iso}}$ are the natural ways to embed $\mathbf{C}$ and $\mathbf{C}^!_{\text{iso}}$.

Since the only morphisms in $\mathbf{C}_{\text{iso}}$ which are not identified with the morphisms of $\mathbf{C}$ are those that contain $!$, we can see $\mathbf{C}^{\doteqdot}$ as $\mathbf{C}$ augmented with discard maps which delete isometries.

⌜ **Definition 4.10.7** (Discard)**:** The discard map for the object 1 is defined in $\mathbf{C}^{\perp\!\!\!\perp}$ by

$$\perp := \iota^{!}_{\text{iso}}(!)$$

Since $\iota^{!}_{\text{iso}}$ is a PROP-functor, we have that the discard map for the object n is

$$\iota^{!}_{\text{iso}}(!^{\otimes n}) = \iota^{!}_{\text{iso}}(!)^{\otimes n} = \perp^{\otimes n}$$ ⌟

Notice, that for any isometry $f : n \to m$ in $\mathbf{C}^{\perp\!\!\!\perp}$, $\boxed{f}$ $=$, thus any isometry is causal.

When seeing the initial category as quotiented by a set of rules $\mathbf{C}/R$, we end up technically with $(\mathbf{C}/R)^{\perp\!\!\!\perp}$ which can be expressed as:

$$(\mathbf{C}/R)^{\perp\!\!\!\perp} = (\mathbf{C} + \{\perp\!\!\!\perp\})/\left(R \cup \left\{ \boxed{\iota^{!}_{\text{iso}}(\iota^{!}(f))} = \;\middle|\; f : n \to m \in \mathbf{C}_{\text{iso}} \right\}\right)$$

where $\mathbf{C} + \{\perp\!\!\!\perp\}$ is the smallest PROP that contains $\mathbf{C}$ and the generator $\perp\!\!\!\perp : 1 \to 0$.

It is natural to compare this new construction to the CPM one and the environment structure defined above. To do so, we need to study in details the purification process in $\mathbf{C}^{\perp\!\!\!\perp}$. First notice that any morphism of $\mathbf{C}^{\perp\!\!\!\perp}$ admits a purification:

Lemma 4.10.8. *Let $\mathbf{C}$ be a †-PROP. For all $f : n \to m \in \mathbf{C}^{\perp\!\!\!\perp}$, there exist $k \in \mathbb{N}$ and $f' : n \to m + k \in \mathbf{C}$ such that* $\boxed{f}$ $=$.

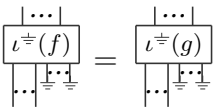
Proof ▶ Let us reason diagrammatically. Using the axioms of PROP f is equivalent to a diagram of $\mathbf{C}^{\perp\!\!\!\perp}$ where all the discards have been pushed to the bottom right: . There are no discards among the components of the part f'' of this diagram. So it represents a morphism in the range of $\iota^{\perp\!\!\!\perp}$ and then there is an $f' : n \to m + k \in \mathbf{C}$ such that $\boxed{f}$ $=$. In other words, f' is a purification of f. ◀

The purification needs not be unique, however it satisfies an essential uniqueness condition. To state it we define the relation $\sim_{\text{iso}}$.

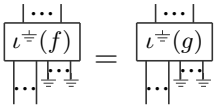
⌜ **Definition 4.10.9** ($\sim_{\text{iso}}$)**:** Let $\mathbf{C}$ be a †-PROP, and two morphisms $f : n \to m + k_1$, $g : n \to m + k_2$, $f \sim_{\text{iso}} g$ if there are two isometries $u : k_1 \to k_3$ and $v : k_2 \to k_3$, such that $\boxed{f}$ $\boxed{u}$ $=$ $\boxed{g}$ $\boxed{v}$. ⌟

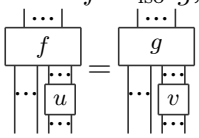
Notice that the relation $\sim_{\text{iso}}$ is not transitive, thus we consider $\sim^{+}_{\text{iso}}$ its transitive closure to make it an equivalence relation. It is easy to show that if $f \sim^{+}_{\text{iso}} g$ then f and g purify the same morphism of $\mathbf{C}^{\perp\!\!\!\perp}$. The converse is also true:

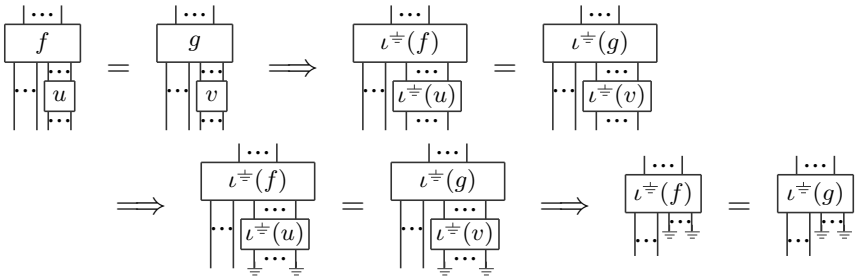
Lemma 4.10.10. *For all $f : n \to m + k_1$ and $g : n \to m + k_2$:*

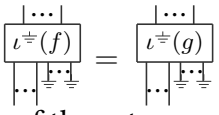
$$f \sim^{+}_{\text{iso}} g \iff$$ 

Proof ►

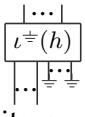
($\Rightarrow$) It is enough to show $f \sim_{\text{iso}} g \implies$  since equality is transitive.

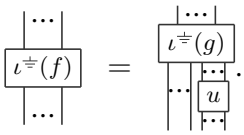
Since $f \sim_{\text{iso}} g$, there are two isometries $u : k_1 \to k_3$ and $v : k_2 \to k_3$ such that  and then:

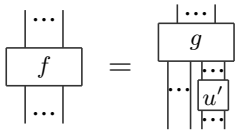


($\Leftarrow$) We have  in $\mathbf{C}^{\doteq}$. To do the proof, we will have to go back to the definition of the category $\mathbf{C}^{\doteq}$ as a pushout. Recall that two terms are equal if one can rewrite one into the other using the equations defining $\mathbf{C}^{\doteq}$.

We can assume that, among those steps, the only one involving discards are isometry deletion/creation. Diagramatically this amounts to say that the discards are never moved, in fact one can always moves the other morphisms to make them interact with the discards.

Doing this, we ensure that all intermediary diagrams in the chain of equations are of the form  for some h. Therefore, to prove the result for a chain of equations of arbitrary size, it is enough to do it just for one step of rewriting.

Consider then this step of rewriting. There are two cases. Either we have used an equation which, by identification, can be seen as an equation of $\mathbf{C}$, that is which involves no discards. Then by functoriality of $\iota^{\doteq}$ we recover that $f = g$ and therefore $f \sim_{\text{iso}} g$. Or the equation involves a discard which has deleted an isometry u. Then one of the upper part, let's say $\iota^{\doteq}(f)$, can be written  . But

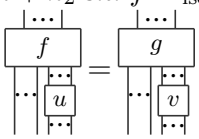
u being an isometry, there exists u' in $\mathbf{C}$ such that $\iota^{\fallingdotseq}(u') = u$. Hence, we have  in $\mathbf{C}$. It follows that $f \sim_{\text{iso}} g$.

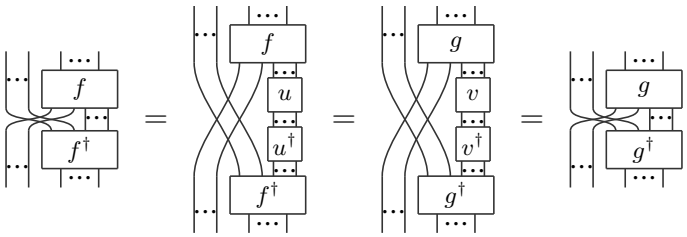
◀

So the purification is unique up to $\sim^{+}_{\text{iso}}$. Lemma 4.10.10 also gives an alternative definition of $\mathbf{C}^{\fallingdotseq}$ which relates more easily to the CPM construction. It is the same construction as CPM with $\sim_{\text{cp}}$ replaced by $\sim^{+}_{\text{iso}}$.

As we have introduced a new discard construction, a natural question is whether $\mathbf{C}^{\fallingdotseq}$ is an environment structure for $\mathbf{C}$. To be an environment structure, three conditions are required. The first two are satisfied: $\mathbf{C}^{\fallingdotseq}$ has a discard morphism for every object, and every morphism can be purified. The third one is the uniqueness of the purification: according to the definition of the environment structures, f and g purify the same morphism if and only if $f \sim_{\text{cp}} g$ whereas according to Lemma 4.10.10, f and g purify the same morphism if and only if $f \sim^{+}_{\text{iso}} g$. As a consequence $\mathbf{C}^{\fallingdotseq}$ is an environment structure for $\mathbf{C}$ if and only if $\sim_{\text{cp}} = \sim^{+}_{\text{iso}}$. It turns out that one of the inclusions is always true:

Lemma 4.10.11. *For any †-PROP $\mathbf{C}$, we have $\sim^{+}_{\text{iso}} \subseteq \sim_{\text{cp}}$.*

Proof ▶ Since $\sim_{\text{cp}}$ is transitive it is enough to show that $\sim_{\text{iso}} \subseteq \sim_{\text{cp}}$. Let $f : n \to m + k_1$ and $g : n \to m + k_2$ s.t. $f \sim_{\text{iso}} g$. Then there are two isometries $u : k_1 \to k_3$ and $v : k_2 \to k_3$ such that  and then:



So $f \sim_{\text{cp}} g$. ◀

As a consequence, if $\sim_{\text{cp}} \neq \sim^{+}_{\text{iso}}$, it means that there are some morphisms f, g that are equal in $\sim_{\text{cp}}$ but cannot be proved equal in $\sim^{+}_{\text{iso}}$. Intuitively it means the category has not enough isometries to prove those terms equal, which leads to the following definition:

⌜ **Definition 4.10.12** (Enough Isometries)**:** A †-PROP $\mathbf{C}$ has *enough isometries* if the equivalences relations $\sim_{\text{cp}}$ and $\sim^{+}_{\text{iso}}$ of $\mathbf{C}$ are equal. ⌟

Lemma 4.10.13. *Given a †-PROP $\mathbf{C}$, the following properties are equivalent:*

1. *$\mathbf{C}$ has enough isometries*
2. *$\mathbf{C}^{\fallingdotseq}$ is an environment structure for $\mathbf{C}$*
3. *$\mathbf{C}^{\fallingdotseq} \simeq \mathrm{CPM}(\mathbf{C})$*

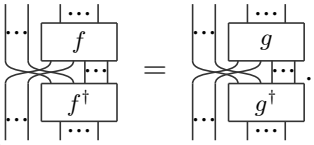
Proof ▶ $[(i) \Leftrightarrow (ii)]$ First $\iota : \mathbf{C} \to \overline{\mathbf{C}}$ is an i.o.o. PROP-functor. We need to check the three conditions hold:

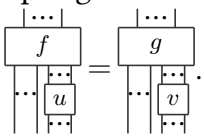
- Since $\iota^!_{\text{iso}}$ is strict monoidal one has:
$$\ni^{\otimes 0} = \iota^!_{\text{iso}}(!^{\otimes 0}) = \iota^!_{\text{iso}}(id_0) = id_0$$
$$\ni^{\otimes n} \otimes \ni^{\otimes m} = \ni^{\otimes n+m}$$
So the first condition is satisfied.
- The second condition is Lemma 4.10.8.
- According to Lemma 4.10.11, $\sim^+_{\text{iso}} \subseteq \sim_{\text{cp}}$, thus the third condition is satisfied if and only if $\sim_{\text{cp}} \subseteq \sim^+_{\text{iso}}$.

$[(ii) \Leftrightarrow (iii)]$ Direct consequence of the fact that $\mathbf{D}$ is an environment structure for $\mathbf{C}$ iff $\mathbf{D}$ is equivalent to $\mathrm{CPM}(\mathbf{C})$ [CH16]. ◀

We want eventually to apply these results to the ZX-Calculus. A first step is to show that **Qubit** has enough isometries. We can actually be stronger than this and show it for **Qudit**.

Proposition 4.10.14.
$\mathbf{Qudit}^{\ni}$ *is an environment structure for* **Qudit**. *Furthermore* $\sim^+_{\text{iso}} = \sim_{\text{iso}}$.

Proof ▶ Let $f : n \to m + k_1$ and $g : n \to m + k_2$ be two linear maps such that $f \sim_{\text{cp}} g$. By definition: 

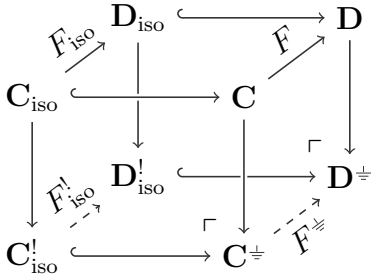
. It follows that the two superoperators $\rho \mapsto \mathrm{tr}_{[m+1,m+k_1]}(f^\dagger \rho f)$ and $\rho \mapsto \mathrm{tr}_{[m+1,m+k_2]}(g^\dagger \rho g)$ are equal and then by the Stinespring dilation theorem (see for example [HS19]), there are isometries u and v such that 

. In other words $f \sim_{\text{iso}} g$. This shows that $\sim_{\text{cp}} \subseteq \sim_{\text{iso}}$ which is even stronger than the necessary condition. From Lemma 4.10.11 it follows that $\sim_{\text{iso}} \subseteq \sim^+_{\text{iso}}$. ◀

Corollary 4.10.15. $\mathbf{Qubit}^{\ni} \simeq \mathrm{CPM}(\mathbf{Qubit})$.

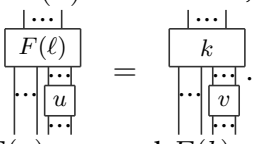
Application to ZX

We now focus on the behaviour of interpretation functors with respect to the discard construction. The discard construction defines a functor $(\_)^{\ni} : \dagger\text{-}\mathbf{PROP} \to \mathbf{PROP}$. Indeed, given a †-PROP functor F, F_{iso} and $F^!_{\text{iso}}$ uniquely define a functor $F^{\ni}$ by pushout.

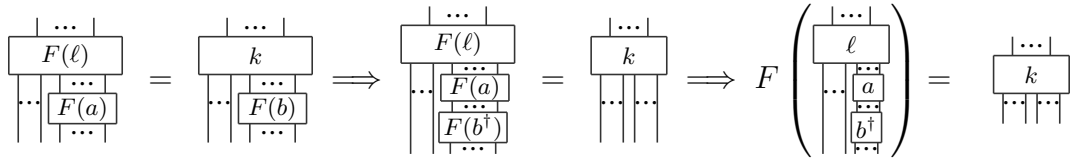


The following lemma and theorem are the main tools to apply the discard construction to the ZX-Calculus:

Lemma 4.10.16. *If F is faithful and if $F_{\text{iso}} : \mathbf{C}_{\text{iso}} \to \mathbf{D}_{\text{iso}}$ is surjective, then $F(f) \sim^{+}_{\text{iso}} F(g) \implies f \sim^{+}_{\text{iso}} g$.*

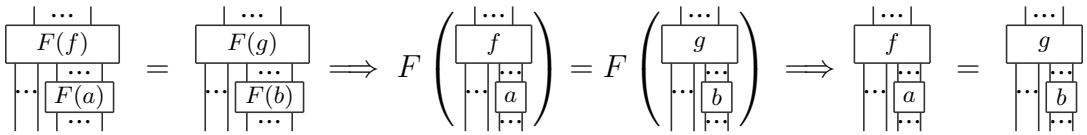
Proof ▶ First, remark that if $F(\ell) \operatorname{iso} k$, then there exists h s.t. $F(h) = k$. Indeed, under the hypothesis, there are two isometries u and v such that: 

. Since F_{iso} is surjective, there are two isometries a and b such that $F(a) = u$ and $F(b) = v$.



The first implication uses the fact that $F(b)$ is an isometry. So k is in the image of F.

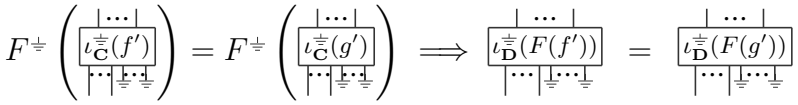
By the first remark, it is therefore sufficient to prove the result if $F(f) \sim_{\text{iso}}= F(g)$. Since F_{iso} is surjective, there are two isometries a and b such that $F(a) = u$ and $f(b) = v$. Therefore:

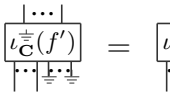


The second implication holds because F is faithful. The last equation is the definition of $f \sim_{\text{iso}} g$. ◀

Theorem 4.10.17. *Let $\mathbf{C}$ and $\mathbf{D}$ be two †-PROPs and $F : \mathbf{C} \to \mathbf{D}$ a †-PROP-functor. If F is faithful and if $F_{\text{iso}} : \mathbf{C}_{\text{iso}} \to \mathbf{D}_{\text{iso}}$ is surjective, then $F^{\fallingdotseq} : \mathbf{C}^{\fallingdotseq} \to \mathbf{D}^{\fallingdotseq}$ is faithful. If furthermore F is surjective then $F^{\fallingdotseq}$ is surjective and faithful.*

Proof ▶ Let f and g be two morphisms such that $F^{\fallingdotseq}(f) = F^{\fallingdotseq}(g)$. By Lemma 4.10.8, f and g can be purified, respectively by f' and g'. Then:



The implication follows from the right hand face of the commutative cube. By Lemma 4.10.10 we have $F(f') \sim^{+}_{\text{iso}} F(g')$. By Lemma 4.10.16, $f' \sim^{+}_{\text{iso}} g'$. Then Lemma 4.10.10 gives 

that is $f = g$, so F is faithful. ◀

A direct application of this theorem is:

Corollary 4.10.18. *$(\mathbf{ZX}/\,\mathrm{ZX})^{\fallingdotseq}$ is a universal complete language for $\mathrm{CPM}(\mathbf{Qubit})$. Particularly, the functor $(\mathbf{ZX}/\,\mathrm{ZX})^{\fallingdotseq} \xrightarrow{[\![.]\!]^{\fallingdotseq}} \mathrm{CPM}(\mathbf{Qubit})$ is full and faithful.*

This is because $\mathbf{ZX}/\mathrm{ZX} \xrightarrow{[\![.]\!]} \mathbf{Qubit}$ is surjective and faithful by Theorem 4.6.1 (the theorem actually says that $[\![.]\!]$ is full and not surjective. However, the standard interpretation is i.o.o., which makes the two properties equivalent).

$(\mathbf{ZX}/\mathrm{ZX})^{\fatslash}$ is naively presented as $\mathbf{ZX}$ augmented with $\fatslash$, and ZX augmented with $\fatslash^{\otimes m} \circ f = \fatslash^{\otimes n}$ for any isometry $f : n \to m$. This implies adding an infinite number of rules to ZX. However, we can drastically reduce them if we are provided with a spanning set of isometries.

Theorem 4.10.19 ([NC10]). *The set* $(e^{i\alpha}, |0\rangle, H, R_Z(\alpha), CNot)$ *spans* $\mathbf{Qubit}_{\mathrm{iso}}$.

Using this result, we provide an axiomatisation $\mathrm{ZX}^{\fatslash}$ for CPMs. It is given in Figure 4.5.

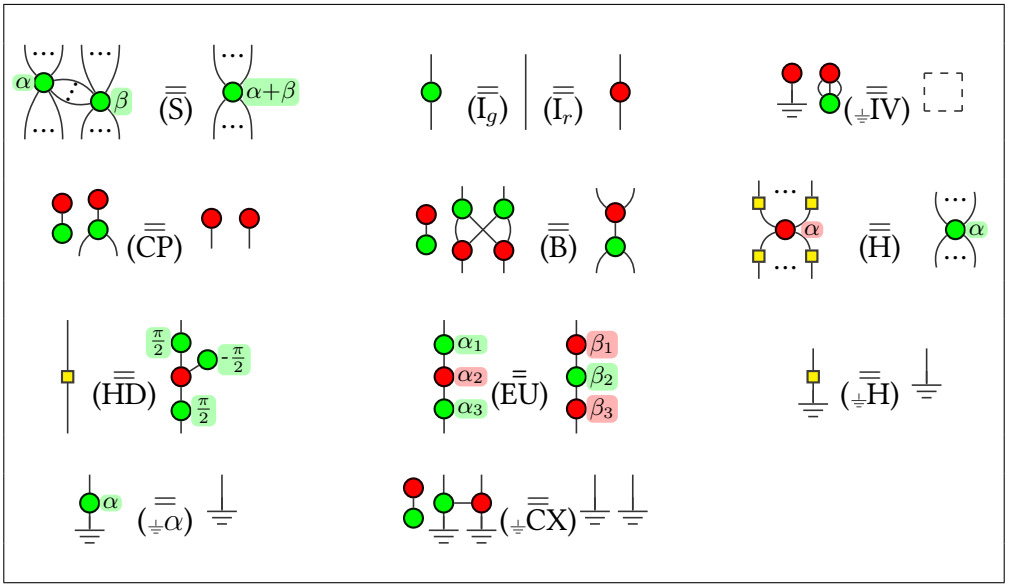


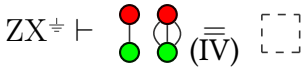
Figure 4.5: Set of rules $\mathrm{ZX}^{\fatslash}$ for the ZX-Calculus for CPMs. The right-hand side of (⏚IV) is an empty diagram. (...) denote zero or more wires, while (⋰) denote one or more wires. In rule (EU), $\beta_1, \beta_2, \beta_3$ and γ can be determined as follows: $x^+ := \frac{\alpha_1+\alpha_3}{2}$, $x^- := x^+ - \alpha_3$, $z := \cos\left(\frac{\alpha_2}{2}\right)\cos\left(x^+\right) + i\sin\left(\frac{\alpha_2}{2}\right)\cos\left(x^-\right)$ and $z' := \cos\left(\frac{\alpha_2}{2}\right)\sin\left(x^+\right) - i\sin\left(\frac{\alpha_2}{2}\right)\sin\left(x^-\right)$, then $\beta_1 = \arg z + \arg z'$, $\beta_2 = 2\arg\left(i + \left|\frac{z}{z'}\right|\right)$, $\beta_3 = \arg z - \arg z'$

This axiomatisation is designed to be complete.

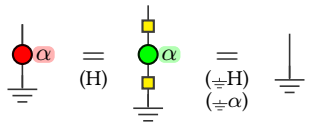
Theorem 4.10.20. $\mathbf{ZX}^{\fatslash}/\mathrm{ZX}^{\fatslash}$ *is complete. The functor* $\mathbf{ZX}^{\fatslash}/\mathrm{ZX}^{\fatslash} \xrightarrow{[\![.]\!]^{\fatslash}} \mathrm{CPM}(\mathbf{Qubit})$ *is full and faithful.*

Proof ▶ We will prove that $\mathbf{ZX}^{\fatslash}/\mathrm{ZX}^{\fatslash} \simeq (\mathbf{ZX}/\mathrm{ZX})^{\fatslash}$. First, notice that all the morphisms are the same in both categories.

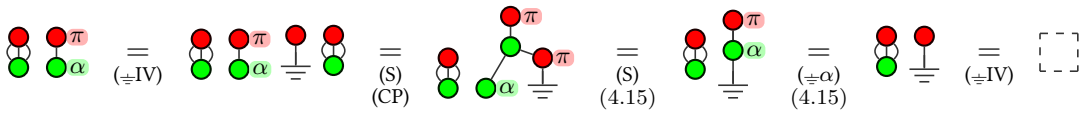
We can see that our axiomatisation $\mathrm{ZX}^{\fatslash}$ is very close to capture ZX, which is complete for pure quantum mechanics. The only two differences are that (EU) dropped the scalars, and that (E) was replaced by (⏚IV). First of all, thanks to Figure 2.2, we have:



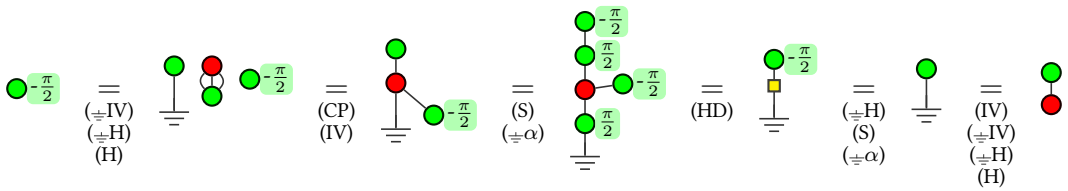
We use this then to prove:



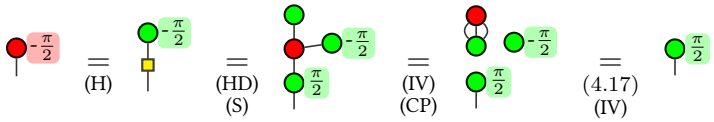
(4.15)



(4.16)

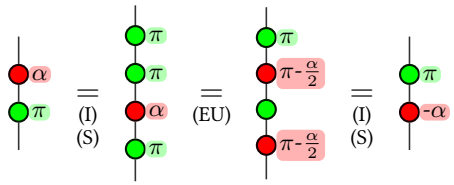


(4.17)



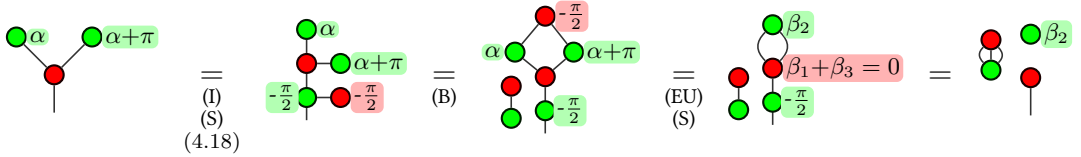
(4.18)

We can recover (K):

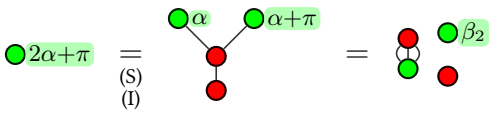


(4.19)

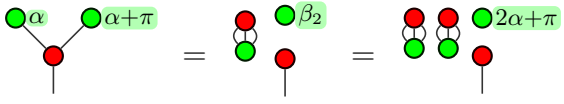
We can recover (SUP). First:



So:

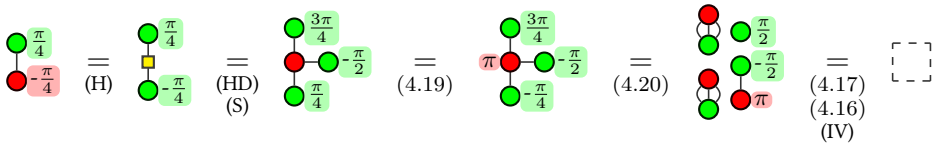


Wrapping things up:



(4.20)

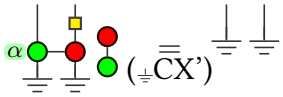
We finally recover (E), and hence ZX:



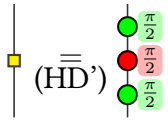
It remains to prove that for any isometry $f : n \to m$, $\mathrm{ZX}^{\fallingdotseq} \vdash \frac{\perp}{\fallingdotseq}^{\otimes m} \circ f = \frac{\perp}{\fallingdotseq}^{\otimes n}$. Since $(e^{i\alpha}, |0\rangle, \mathrm{H}, R_Z(\alpha), \mathrm{CNot})$ spans the isometries of $\mathbf{Qubit}$, and since $\mathbf{ZX}/\mathrm{ZX}$ is complete, any isometry of $\mathbf{ZX}$ can be turned into a diagram that solely uses:

Hence, it is sufficient to prove the result for these diagrams. The last four are directly given as axioms. The last one is given by equation (4.16). ◀

Remark 4.10.21. Variations on this axiomatisation can easily be made to reduce the number of rules. For instance, $\{(\fallingdotseq\mathrm{H}), (\fallingdotseq\alpha), (\fallingdotseq\mathrm{CX})\}$ can be replaced by:

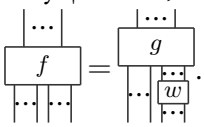


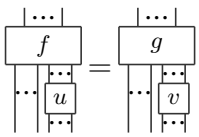
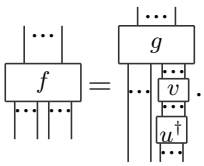
Furthermore, the Hadamard decomposition (HD) can be replace by a single-line scalar-free version:



We now have a complete axiomatisation for of $\mathbf{ZX}^{\fallingdotseq}$ for $\mathrm{CPM}(\mathbf{Qubit})$. We can naturally ask the question for fragments of the language. This is not the case in general. Some fragments may not have enough isometries. For instance:

Proposition 4.10.22. *$(\mathbf{Clifford{+}T})^{\fallingdotseq}$ is not an environment structure for $\mathbf{Clifford{+}T}$. More precisely, there exists a scalar ϕ s.t. $\phi \sim_{\mathrm{cp}} \phi^*$ but $\phi \nsim^{+}_{\mathrm{iso}} \phi^*$. One can take for example $\phi = 1 + 2i$.*

Proof ▶ First remark that, in any †-PROP, if $f \sim^{+}_{\mathrm{iso}} g$ then there is a morphism (usually not an isometry) w such that  .

This is true if $f \sim_{\mathrm{iso}} g$: From  we immediately get  .

The result then follows by a straightforward induction.

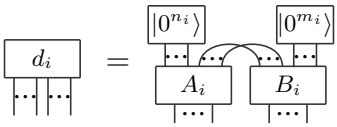
Now take $\phi = 1 + 2i$ and $\phi^* = 1 - 2i$. The scalars are in $\mathbf{Clifford{+}T}$ since their entries are in $\mathbb{Z}[i, \frac{1}{\sqrt{2}}]$, and are clearly $\sim_{\mathrm{cp}}$ equivalent. Now let's suppose $1+2i \sim^{+}_{\mathrm{iso}} 1-2i$. Then by the previous remark, there exists a morphism u such that $(1 - 2i)u = 1 + 2i$. But the only possibility for u is $\frac{4i-3}{5}$, which is not in $\mathbb{Z}[i, \frac{1}{\sqrt{2}}]$, a contradiction. ◀

This means that the discard construction is not sufficient to provide an environment structure to **Clifford+T**. A fortiori, $\left(\mathbf{ZX}[\frac{\pi}{4}]/\,\mathrm{ZX}_{\pi/4}\right)^{\frac{+}{=}}$ will not be a graphical language for an environment structure for **Clifford+T**. However:

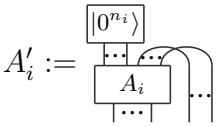
Proposition 4.10.23. $\mathbf{Stab}^{\frac{+}{=}}$ *is an environment structure for* **Stab**.

Proof ▶ First of all, since **Stab** is compact closed, using the map/state duality, proving the result for states in sufficient. Since all the non-zero scalar are invertible in **Stab** we can furthermore w.l.o.g focus on normalized states.

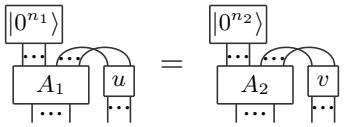
Consider two states $d_1 : n + k_1$ and $d_2 : n + k_2$ in **Stab** such that $d_1 \sim_{\mathrm{cp}} d_2$. The point of focusing on normalised states is that we can decompose them using [AP05] so that



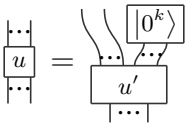
where A_i and B_i are unitaries in **Stab**. Defining:



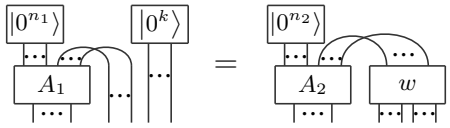
we have that $d_i \sim_{\mathrm{iso}} A'_i$ since we just have deleted isometries. So, by transitivity, to prove $d_1 \sim^{+}_{\mathrm{iso}} d_2$ we just have to show $A'_1 \sim_{\mathrm{iso}} A'_2$. But since $d_1 \sim_{\mathrm{cp}} d_2$ in **Stab** we also have $d_1 \sim_{\mathrm{cp}} d_2$ in **Qubit** and so by Lemma 4.10.14, $d_1 \sim^{+}_{\mathrm{iso}} d_2$ in **Qubit**. By transitivity $A'_1 \sim^{+}_{\mathrm{iso}} A'_2$ in **Qubit** and so by Lemma 4.10.14 $A'_1 \sim_{\mathrm{iso}} A'_1$ in **Qubit**. So there are two unitaries u and v such that



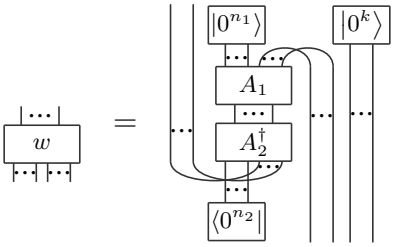
In **Qubit** any isometry can be written as a unitary with ancillae. In other words there is a unitary u' such that:



Composing by $u'^{\dagger}$ on both side and denoting $w = u'^{\dagger} \circ v$ one has:



It only remains to show that the isometry w is in **Stab** since the isometry on the left hand side is clearly in it. It is since:



Hence, $A_1' \sim_{\text{iso}} A_1'$ in $\mathbf{Stab}$, so $d_1 \sim^{+}_{\text{iso}} d_2$. ◀

Since $\mathbf{Stab}^{\doteq}$ is an environment structure for $\mathbf{Stab}$ and that $\mathbf{ZX}[\frac{\pi}{2}]/\operatorname{ZX}_{\pi/2}$ is complete pour $\mathbf{Stab}$, we can build thanks to the discard construction $\left(\mathbf{ZX}[\frac{\pi}{2}]/\operatorname{ZX}_{\pi/2}\right)^{\doteq}$ that is complete for $\operatorname{CPM}(\mathbf{Stab})$. Again, we can simplify the resulting axiomatisation, and provide a finite presentation denoted $\operatorname{ZX}^{\doteq}_{\pi/2}$ given in Figure 4.6. Notice that the axiomatisation is basically $\operatorname{ZX}^{\doteq}$ where (EU) is replaced by (Z). Notice also that the potential simplifications given in Remark 4.10.21 still stand here.

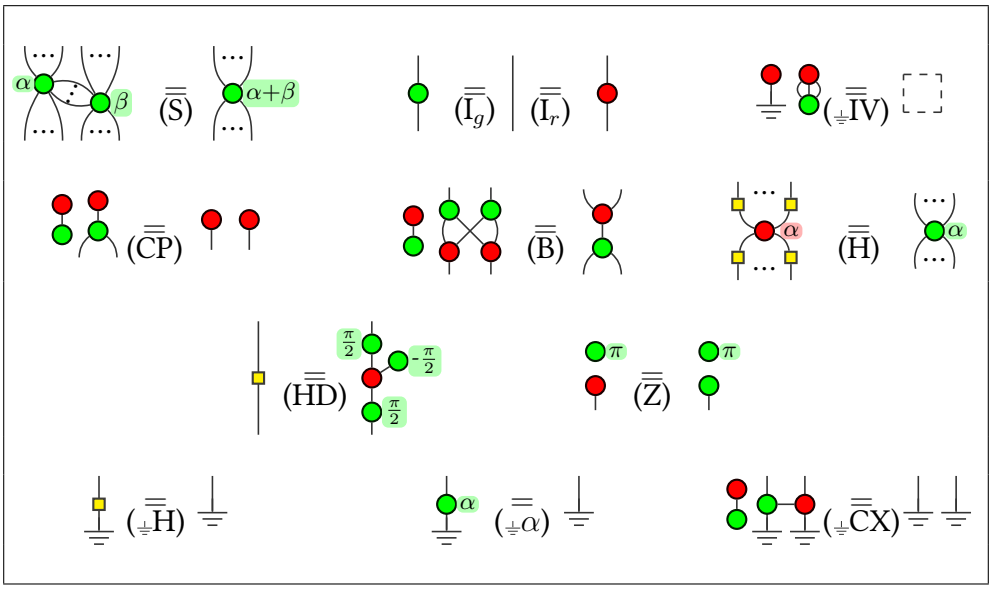


Figure 4.6: Set of rules $\operatorname{ZX}^{\doteq}_{\pi/2}$ for the Clifford fragment of the ZX-Calculus for CPMs. The right-hand side of (⏚IV) is an empty diagram. (...) denote zero or more wires, while ($\therefore$) denote one or more wires.

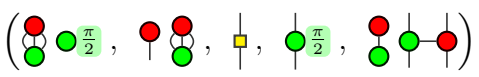
Theorem 4.10.24. $\mathbf{ZX}^{\doteq}[\frac{\pi}{2}]/\operatorname{ZX}^{\doteq}_{\pi/2}$ *is complete for* $\operatorname{CPM}(\mathbf{Stab})$. *The functor:*

$$\mathbf{ZX}^{\doteq}[\frac{\pi}{2}]/\operatorname{ZX}^{\doteq}_{\pi/2} \xrightarrow{[\![.]\!]^{\doteq}} \operatorname{CPM}(\mathbf{Stab})$$

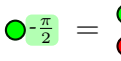
is full and faithful.

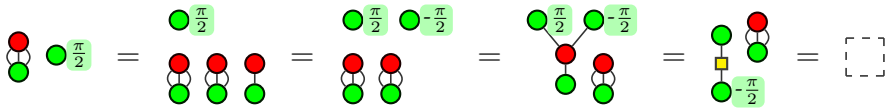
Proof ▶ We can prove that $\mathbf{ZX}^{\doteq}[\frac{\pi}{2}]/\operatorname{ZX}^{\doteq}_{\pi/2} \simeq (\mathbf{ZX}[\frac{\pi}{2}]/\operatorname{ZX}_{\pi/2})^{\doteq}$. First, we can recover $\operatorname{ZX}_{\pi/2}$: the only missing axiom is (IV) which is derivable (Figure 2.2). $\mathbf{Stab}$ is spanned by ($\sqrt{2}$, i, $|0\rangle$, $\langle 0|$, H, $R_Z(\frac{\pi}{2})$, CNot). Notice in particular that $e^{i\frac{\pi}{4}}$ is in $\mathbf{Stab}$: $e^{i\frac{\pi}{4}} = \sqrt{2}\langle 0| HR_Z(\frac{\pi}{2})H |0\rangle$. One can actually show that all the scalars $s : 0 \to 0 \in \mathbf{Stab}$ are in $\{\sqrt{2}^n e^{i\frac{m\pi}{4}} \mid n, m \in \mathbb{Z}\}$ [Bac15].

By Proposition 4.10.23, $\mathbf{Stab}$ has enough isometries, they are spanned by ($e^{i\frac{\pi}{4}}$, $|0\rangle$, H, $R_Z(\frac{\pi}{2})$, CNot). These can be represented in $\mathbf{ZX}[\frac{\pi}{2}]$ by:



By completeness of $\mathbf{ZX}[\frac{\pi}{2}]/\operatorname{ZX}_{\pi/2}$, any diagram of $\mathbf{ZX}[\frac{\pi}{2}]_{\text{iso}}$ can be turned into an equivalent diagram that only uses the above subdiagrams. They are all consumed by ⏚: the

last four thanks to the axioms (⏚IV), (⏚H), (⏚α), (⏚CX), and the first one because, first  (the proof is similar to that in Theorem 4.10.20). Then:



Hence all the isometries of $\mathbf{ZX}[\frac{\pi}{2}]$ are consumed by ⏚. ◀

Example: Quantum Pseudo-Telepathy

We propose in this section to study a quantum pseudo-telepathy protocol described in [BBT05]. The problem takes the form of a game between two parties, Alice and Bob, and uses a third-party, called referee. The game is played on a 3×3 board, where each cell can be filled with either 0 or 1. The game is inspired by the *magic square*, in which the cells of each row sum to an even number, and the cells of each column sum to an odd number. Of course, this configuration is impossible, for summing all rows would give an even number, while summing all columns would give an odd number.

In the magic square game, the referee chooses a row and a column of the board. Alice is then asked to fill the chosen row, and Bob the chosen column, while respecting the constraints of the magic square: the entries of the row sum to an even number, the ones of the column sum to an odd number, and of course, Alice and Bob have to agree on their common entry. These are the winning conditions. The trick is that the two parties cannot communicate, they cannot see what the other has played.

Obviously, classical players cannot define a strategy that wins 100% of the time. However, if they are quantum, and share entangled states at the beginning, then there exists a winning strategy. The protocol is the following, as explained in [BBT05]:

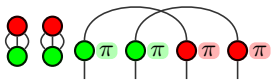
- Alice and Bob share the state $\frac{1}{2}\left(|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle\right)$ (the two left-hand qubits are owned by Alice, and the two right-hand ones by Bob).
- Alice and Bob both apply a particular quantum circuit to their pair, depending on the row/column they are given: if row i is chosen, Alice applied circuit A_i, if column j is chosen, Bob applies circuit B_j.
- Both Alice and Bob measure their qubits in the computational basis. Each hence gets two classical bits, the third one is then determined so that it satisfies the parity conditions: Alice XORs her two bits, while Bob flips the XOR of his two bits.

We are given the interpretation of each circuit:

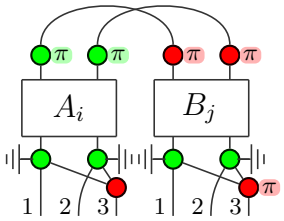
$$[\![A_1]\!] = \begin{pmatrix} i & 0 & 0 & 1 \\ 0 & -i & 1 & 0 \\ 0 & i & 1 & 0 \\ 1 & 0 & 0 & i \end{pmatrix} \qquad [\![A_2]\!] = \begin{pmatrix} i & 1 & 1 & i \\ -i & 1 & -1 & i \\ i & 1 & -1 & -i \\ -i & 1 & 1 & -i \end{pmatrix} \qquad [\![A_3]\!] = \begin{pmatrix} -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{pmatrix}$$

$$[\![B_1]\!] = \begin{pmatrix} i & -i & 1 & 1 \\ -i & -i & 1 & -1 \\ 1 & 1 & -i & i \\ -i & i & 1 & 1 \end{pmatrix} \qquad [\![B_2]\!] = \begin{pmatrix} -1 & i & 1 & i \\ 1 & i & 1 & -i \\ 1 & -i & 1 & i \\ -1 & -i & 1 & -i \end{pmatrix} \qquad [\![B_3]\!] = \begin{pmatrix} 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

First, we translate the protocol to the ZX-Calculus, and show that it can be used for simplification. First, the shared entangled state can be represented as:

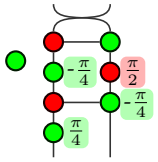
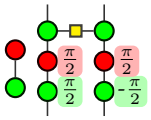
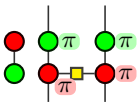


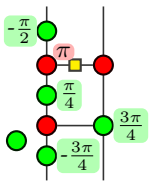
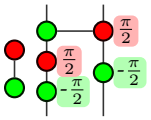
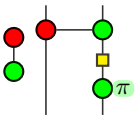
Then, since the measurement in the computational basis can be represented as  , the protocol is carried as follows, for a right choice of circuits A_i, and B_j when row i and column j are selected:



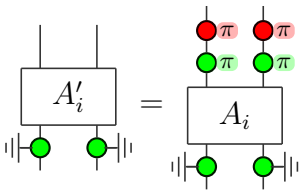
The parity conditions are necessarily satisfied since  represents the XOR operation on classical bits.

We can give a representation of each of the previous operators:

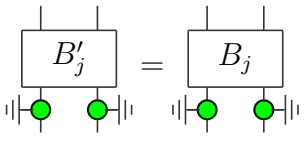
$A_1 :=$  $A_2 :=$  $A_3 :=$ 

$B_1 :=$  $B_2 :=$  $B_3 :=$ 

These are not ideal, particularly because A_1 and B_1 are in $\mathbf{ZX}[\frac{\pi}{4}]$. Also, it may feel more natural to have  as a shared entangled state instead of the one suggested by the protocol. This can be easily done by pushing the π-green and red nodes down to the circuits A for instance. Hence, we are going to search for A'_i and B'_j such that:

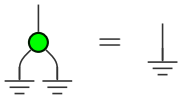


and

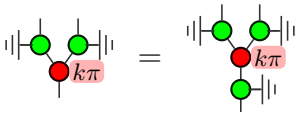


To do so, we are going to use the following lemmas.

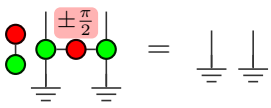
Lemma 4.10.25.



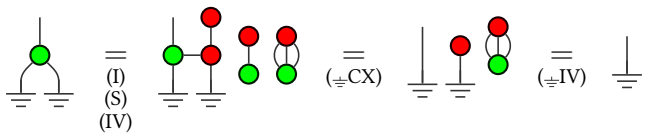
Lemma 4.10.26.

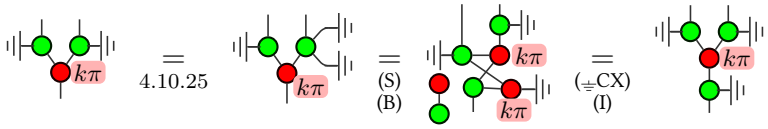


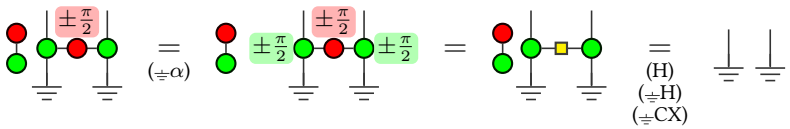
Lemma 4.10.27.



Proof ▶

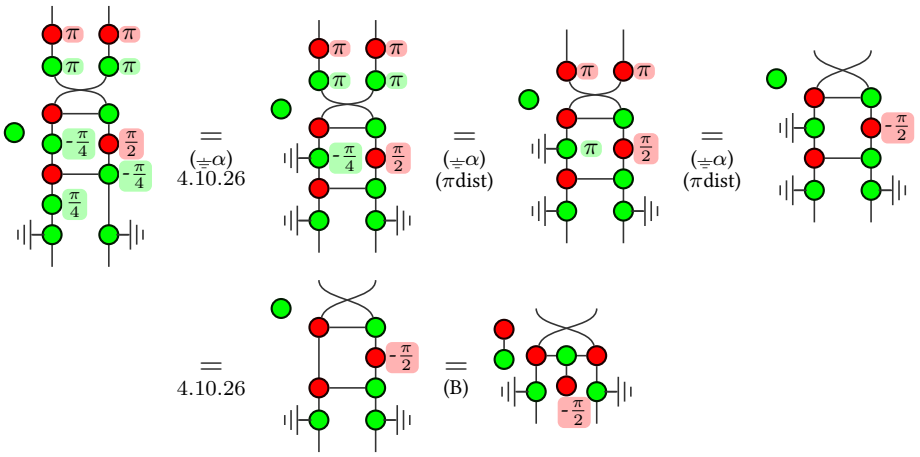


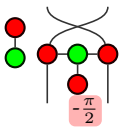




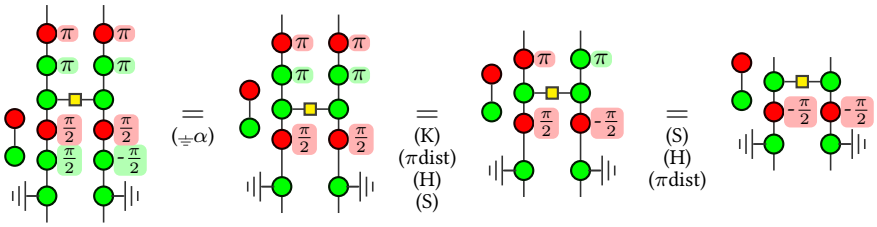
◀

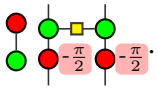
A_1' can be found as:

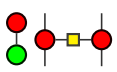


So we define $A_1' :=$ 

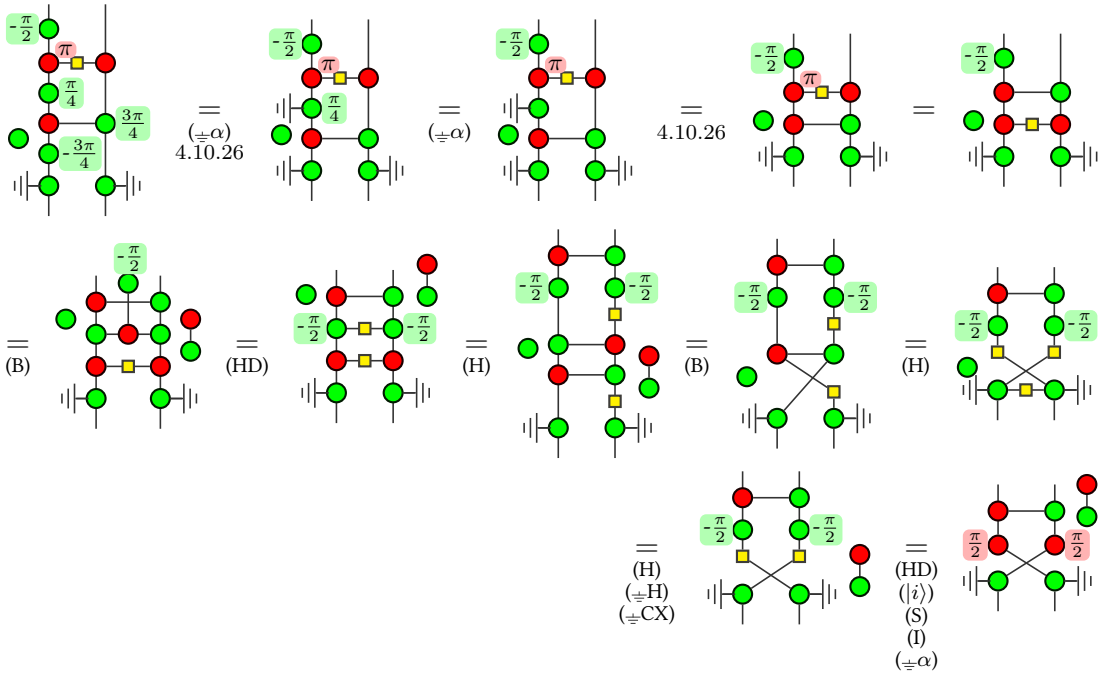
Similarly:

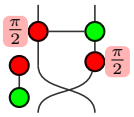


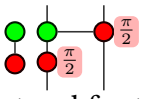
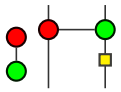
So $A_2' :=$ 

. Finally, it is easy to see that A_3' can be defined as: $A_3' :=$  .

B'_1 can be found as:



So we define $B'_1 :=$ 

Again, it is easy to see that $B'_2 :=$  and $B'_3 :=$  suffice.

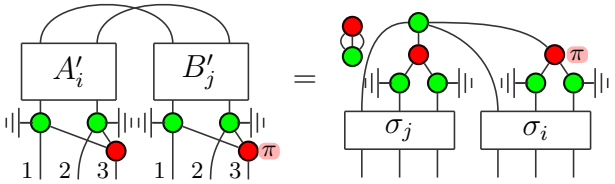
We can now give an alternative protocol for the game: Alice and Bob initially share the state $\frac{1}{2}(|0000\rangle + |1010\rangle + |0101\rangle + |1111\rangle)$, and apply A'_i (resp. B'_j) to their pair according to the row number i (resp. column number j) given by the referee; where:

$$[\![A'_1]\!] = \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & i & 1 & 0 \\ 0 & 1 & i & 0 \\ i & 0 & 0 & 1 \end{pmatrix} \qquad [\![A'_2]\!] = \begin{pmatrix} 1 & i & i & 1 \\ i & 1 & -1 & -i \\ i & -1 & 1 & -i \\ -1 & i & i & -1 \end{pmatrix} \qquad [\![A'_3]\!] = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

$$[\![B'_1]\!] = \begin{pmatrix} 1 & -1 & -i & -i \\ -i & -i & 1 & -1 \\ -i & -i & -1 & 1 \\ -1 & 1 & -i & -i \end{pmatrix} \qquad [\![B'_2]\!] = \begin{pmatrix} 1 & -i & -1 & -i \\ -i & 1 & -i & -1 \\ -i & -1 & -i & 1 \\ -1 & -i & 1 & -i \end{pmatrix} \qquad [\![B'_3]\!] = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \end{pmatrix}$$

A summary of the choices of maps for Alice and Bob is given in Figure 4.7.

We can then verify the protocol using the ZX-Calculus. With diagrams A'_i and B'_j defined above (whose interpretation correspond to the requirement of the protocol), we can show that:



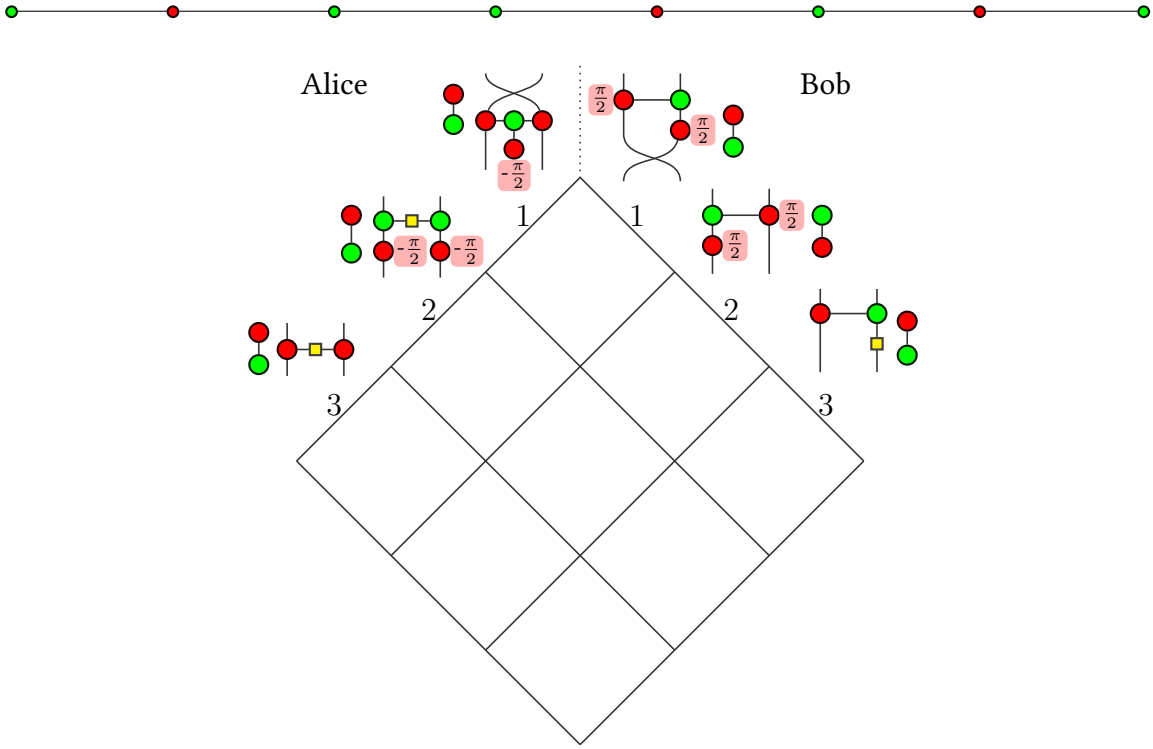
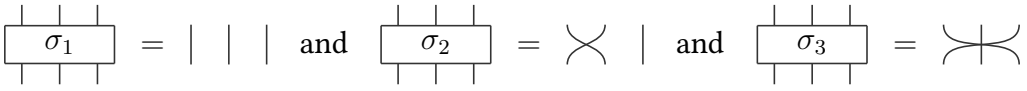
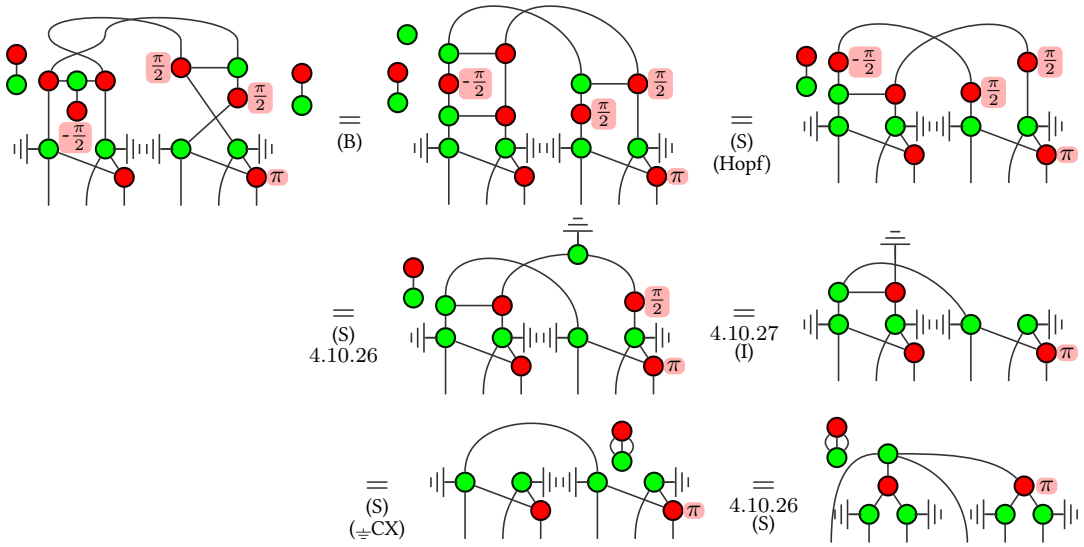


Figure 4.7: Choice of ZX-diagram in the Quantum Pseudo-Telepathy winning strategy.

for each pair $(i, j) \in \{1, 2, 3\}^2$, and where σ_i exchanges the first and ith wire:

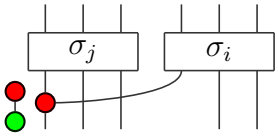


For instance, for the pair $(1, 1)$:

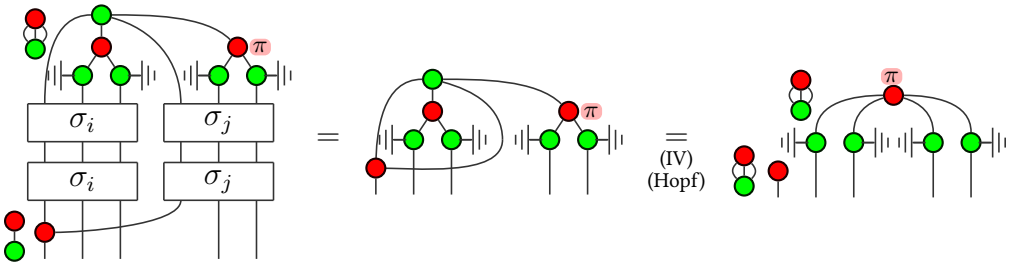


Since the parity conditions are necessarily met by construction ( representing exactly the XOR of two qubits) all we have to do is check whether Alice and Bob agree

on the bits j and i. To do so, we can XOR them, and check that it results in $|0\rangle$. To do so, we can apply:



where the σ_i are here to allow the selection of qubits i and j. Of course, since the these permutations are merely inversions, $\sigma_i^2 = \mathbb{I}^{\otimes 3}$. Hence:



where the leftmost qubit represents $|0\rangle$.

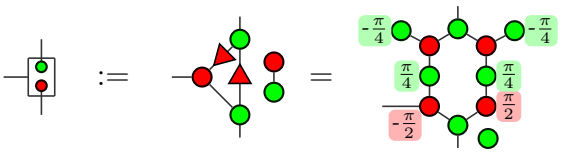
Chapter 5

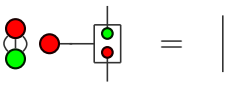
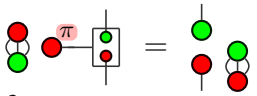
Normal Forms

One of the fundamental differences between ZX and ZW-Calculi is the fact that the latter enjoys a pleasant notion of normal form. This is why historically, completeness was first proven for ZW (using normal forms), and later on for ZX (using the completeness of the ZW-Calculus). Even though completeness has been proven for several version of the ZX-Calculus, it would be interesting to have a normal form for them. We have already seen how graph states could be used to define a normal form for diagrams of $\mathbf{ZX}[\frac{\pi}{2}]$. In this Chapter, we are going to see how to define a normal form for any diagram of $\Delta\mathbf{ZX}[F]$ where F is a fragment that contains $\frac{\pi}{4}$, or equivalently for any diagram of $\mathbf{ZX}[F]$ that contains $\frac{\pi}{4}$. This will particularly allow us to define a nice sufficient condition for completeness with these fragments. We will then apply the results for several new fragments of the ZX-Calculus.

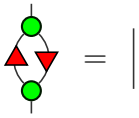
5.1 The Algebra of the Transistor

The normal forms will use some particular diagrams as building blocks. Particularly, we are going to use the *transistor*, that was introduced in Section 3.1. Recall that:

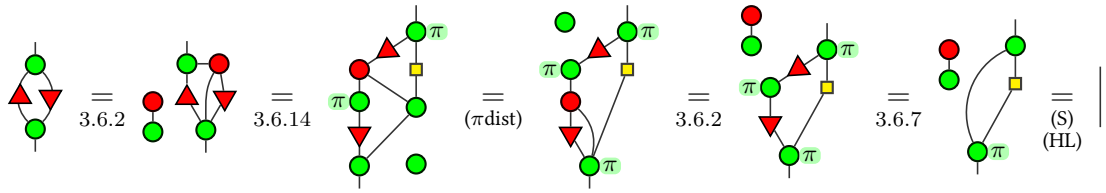


We can now diagrammatically prove the two sound equations:  and  The second one comes from Lemma 3.6.13, while the first one comes from:

Lemma 5.1.1.

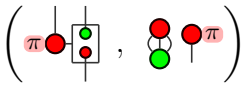


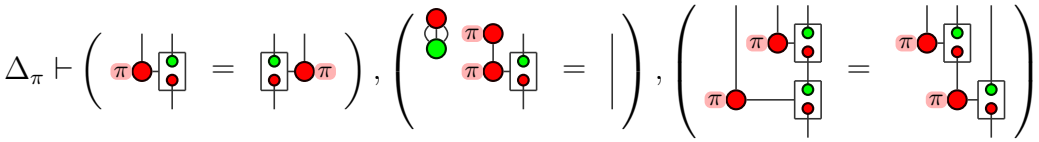
Proof ▶

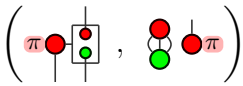
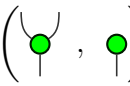


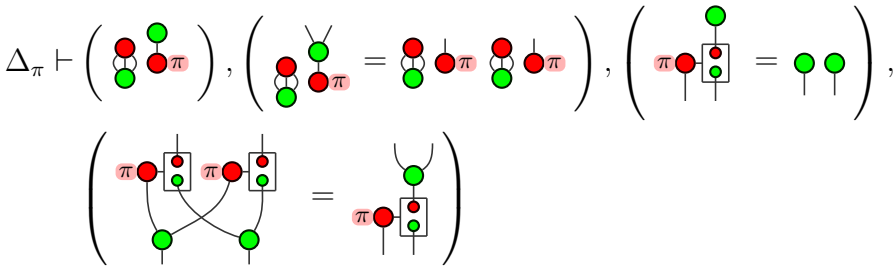
◀

The transistor with the Not gate on the control wire reacts interestingly with the generators of the ZX-Calculus:

Proposition 5.1.2.  *forms a commutative monoid:*

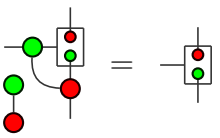


Proposition 5.1.3.  *and*  *form a bialgebra:*

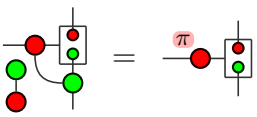


The first Proposition requires the following lemmas:

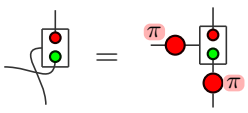
Lemma 5.1.4.



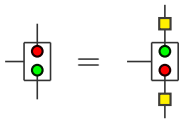
Lemma 5.1.5.



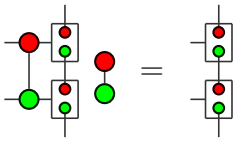
Lemma 5.1.6.



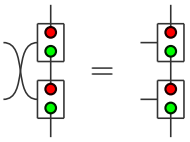
Lemma 5.1.7.



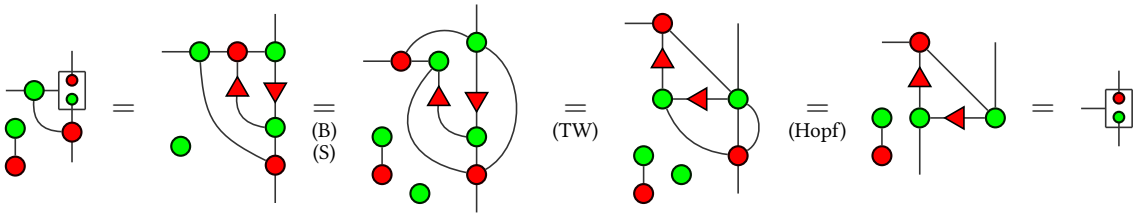
Lemma 5.1.8.

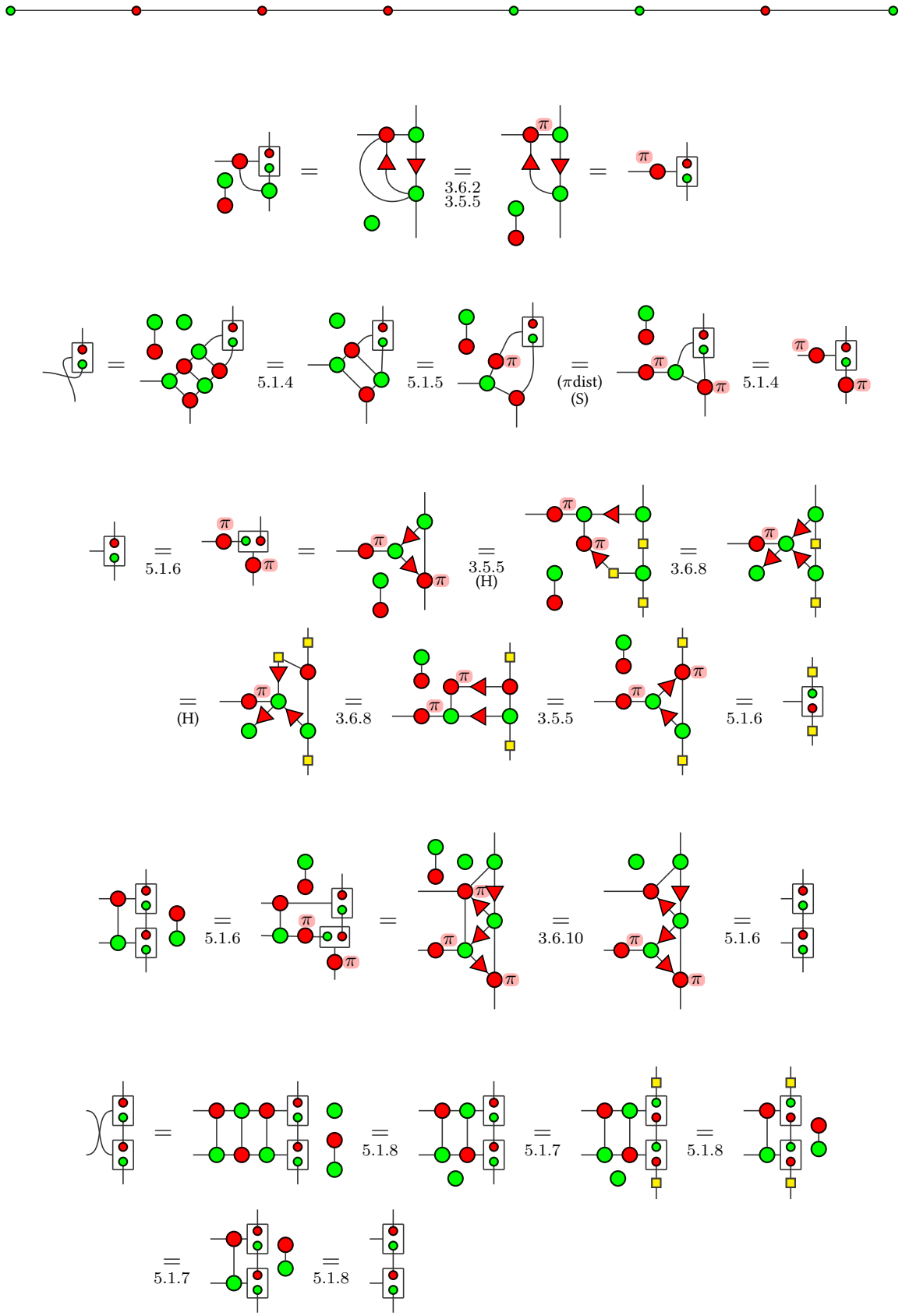


Lemma 5.1.9.



Proof ▶





◀

***Proof** of Prop. 5.1.2* ▶ The three equations can be obtained by:

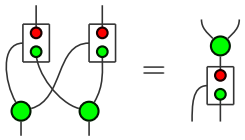
- (S) and Lemma 5.1.6

- by (S) and Lemma 5.1.1
- by Lemmas 5.1.6 and 5.1.9

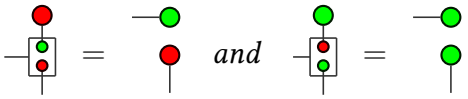
◀

The proof of the bialgebra furthermore requires:

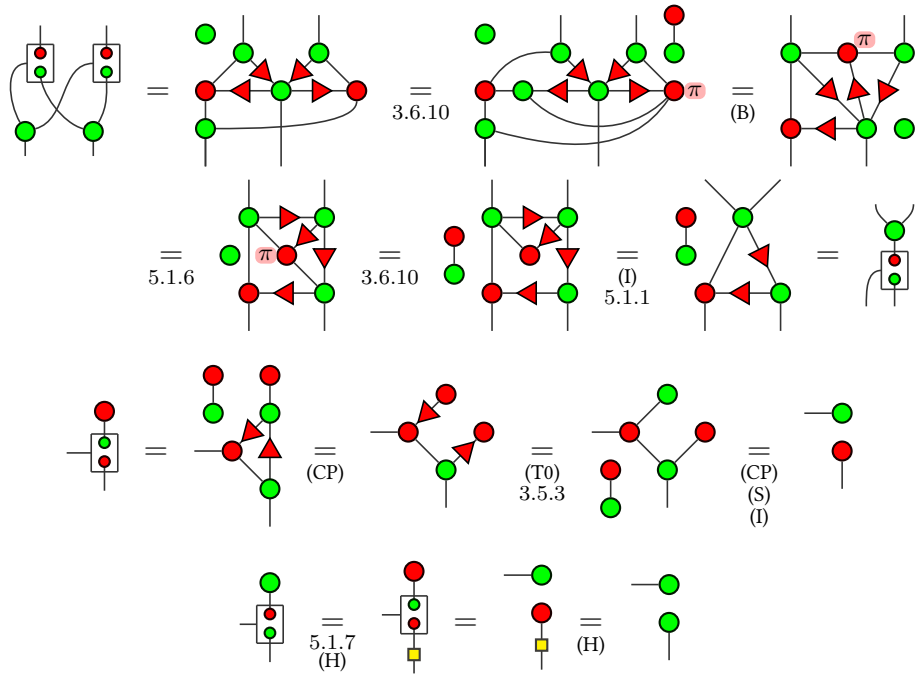
Lemma 5.1.10.



Lemma 5.1.11.



Proof ▶



◀

Proof *of Prop. 5.1.3* ▶ The four equations can be obtained by:

- (sπ) +(IV)
- (πdist) +(IV) +(CP)
- Lemma 5.1.11 and (CP) +(sπ)
- (πdist) and Lemma 5.1.10

◀

Remark 5.1.12. The diagram  can be seen as an AND gate (notice that when plugging  , the result is  , when $k, \ell \in \{0, 1\}$). As such, it has been used previously to create the Toffoli gate. The previous two propositions where observed as tensor network transformations with AND gates in [BCJ11].

5.2 Controlled States and Normal Forms

In this section, we build our way up to the definition of a normal form. We do it in such a way that its structure is the same for all fragments of $\Delta\mathbf{ZX}$ that contain π.

⌜ **Definition 5.2.1:** We denote by $\mathcal{F}$ the set of all fragments that contain $\frac{\pi}{4}$:

$$\mathcal{F} := \{F \mid F \subseteq \mathbb{R}/2\pi\mathbb{Z},\ \frac{\pi}{4} \in F\}$$ ⌟

Controlled States

The cornerstone of the normal form is the controlled state. Controlled states form a particular family of $\Delta\mathbf{ZX}$-diagrams with a single input and n outputs. Their interpretation should map $|0\rangle$ to the uniform superposition $\sum_{x\in\{0,1\}^n} |x\rangle$. Intuitively, a controlled state $D : 1 \to n$ is just an encoding for the state $[\![D]\!]\,|1\rangle$.

⌜ **Definition 5.2.2** (Controlled states)**:** A $\Delta\mathbf{ZX}$-diagram $D : 1 \to n$ is a *controlled state* if $[\![D]\!]\,|0\rangle = \sum_{x\in\{0,1\}^n} |x\rangle$. ⌟

A controlled state with no output is called a controlled scalar:

⌜ **Definition 5.2.3** (Controlled scalars)**:** A $\Delta\mathbf{ZX}$-diagram $D : 1 \to 0$ is a *controlled scalar* if $[\![D]\!]\,|0\rangle = 1$. ⌟

For instance  is a controlled scalar encoding $\frac{1}{2}$:

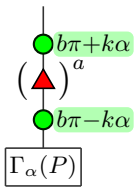
$$\left[\!\!\left[\ \right]\!\!\right]|x\rangle = \begin{cases} 1 & \text{if } x = 0 \\ \frac{1}{2} & \text{if } x = 1 \end{cases}$$

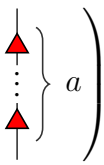
We introduce other examples of controlled scalars, parameterised by integer polynomials:

⌜ **Definition 5.2.4:** For any $F \in \mathcal{F}$ and any $\alpha \in F$, let $\Gamma_\alpha : \mathbb{Z}[X] \to \Delta\mathbf{ZX}[F]$ be the map which associates to any polynomial P a $\Delta\mathbf{ZX}$-diagram $\Gamma_\alpha(P) : 1 \to 0$, inductively defined as

$0 \mapsto$ 

and $\forall a \in \mathbb{N} \setminus \{0\}, \forall b \in \{0,1\}, \forall k \in \mathbb{N}$, and $\forall P \in \mathbb{Z}[X]$ such that $\deg(P) < k$,

$(-1)^b aX^k + P \mapsto$ 

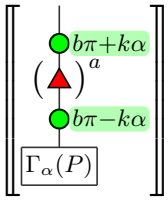
(where $\left(\ \right)^a :=$  a)

⌟

For any integer polynomial P, the corresponding diagram $\Gamma_\alpha(P)$ is a controlled scalar encoding the scalar $P(e^{i\alpha})$:

Lemma 5.2.5. *$\forall F \in \mathcal{F}, \forall \alpha \in F$, and $\forall P \in \mathbb{Z}[X]$,* $[\![\Gamma_\alpha(P)]\!]\,|x\rangle = \begin{cases} 1 & \text{if } x = 0 \\ P(e^{i\alpha}) & \text{if } x = 1 \end{cases}$.

Proof ▶ By induction. First, notice that $[\![\Gamma_\alpha(0)]\!] = \begin{pmatrix}1 & 0\end{pmatrix}$. Then:

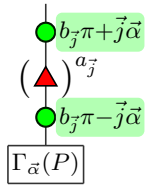


$$= \begin{pmatrix}1 & P(e^{i\alpha})\end{pmatrix} \begin{pmatrix}1 & (-1)^b a e^{ik\alpha} \\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & (-1)^b a e^{ik\alpha} + P(e^{i\alpha})\end{pmatrix}$$

◀

This definition can easily be extended to represent any multivariate polynomial in $P(e^{i\vec{\alpha}}) := P(e^{i\alpha_1}, \ldots, e^{i\alpha_k})$ with coefficients in $\mathbb{Z}$. Indeed, $P(e^{i\vec{\alpha}})$ can be written as $\sum (-1)^{b_{j_1,\ldots,j_k}} a_{j_1,\ldots,j_k} e^{i(j_1\alpha_1+\ldots+j_k\alpha_k)}$, where $a_{j_1,\ldots,j_k} \in \mathbb{N}$. We hence define inductively $\Gamma_{\vec{\alpha}}$ thanks to:

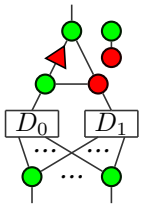
$$(-1)^{b_{\vec{j}}} a_{\vec{j}} X_1^{j_1} \ldots X_k^{j_k} + P \mapsto$$

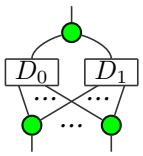


where $b_{\vec{j}}$ stands for $b_{j_1,\ldots,j_k}$, $a_{\vec{j}}$ for $a_{j_1,\ldots,j_k}$, and $\vec{j}\vec{\alpha}$ for $j_1\alpha_1 + \ldots + j_k\alpha_k$. Notice that after building this diagram, some of the variables may be evaluated to particular values. This way, given a fragment $F \in \mathcal{F}$, any multivariate polynomial with constants in $\mathbb{Z}[e^{iF}]$ can be controlled.

While it is not obvious in the ZX-Calculus to add two given diagrams (i.e. build a third diagram whose interpretation is the sum of the two firsts'), a fundamental property of controlled states is that they can be freely added and multiplied (according to the entrywise product a.k.a. the Hadamard product or Schur product) as follows:

Lemma 5.2.6 (Sum and Product)**.** *For any controlled states $D_0, D_1 : 1 \to n$,*

$D_{\text{sum}} :=$ 

$D_{\text{prod}} :=$ 

are controlled states such that:

$$[\![D_{\text{sum}}]\!]\,|1\rangle = [\![D_0]\!]\,|1\rangle + [\![D_1]\!]\,|1\rangle \quad \textit{and} \quad [\![D_{\text{prod}}]\!]\,|1\rangle = ([\![D_0]\!]\,|1\rangle) \bullet ([\![D_1]\!]\,|1\rangle)$$

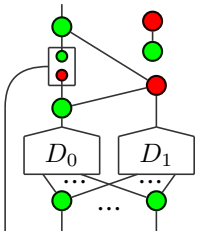
where $. \bullet .$ is the entrywise product.

Proof ▶ This is routine to show. ◀

Normal Form

Amongst the family of controlled state diagrams, we define those that are in normal form. Our definition of normal form is *generic* in the sense that it is defined with respect to a given set of controlled scalars. Intuitively the choice of these controlled scalars depends on the considered fragment of the language, as detailed in the next sections.

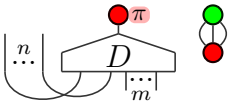
⌜ **Definition 5.2.7** (Controlled Normal Form)**:** Given a set S of controlled scalars, the diagrams in *controlled normal form* with respect to S (S-CNF) are inductively defined as follows:

- $\forall D \in S$, D is in S-CNF;
- $\forall D_0, D_1$ in S-CNF,  is in S-CNF.

A diagram D in S-CNF is depicted  . ⌟

One can double check that diagrams in controlled normal form are actually controlled states: if $D : 1 \to n$ is in S-CNF, $[\![D]\!] |0\rangle = \sum_{x \in \{0,1\}^n} |x\rangle$ (this is a consequence of Lemma 5.3.4, proven in the following).

We are now ready to give a definition of diagrams in normal form, based on the diagrams in controlled normal forms:

⌜ **Definition 5.2.8** (Normal Form)**:** Given a set S of controlled scalars, for any $n, m \in \mathbb{N}$, and any $D : 1 \to n + m$ in S-CNF,  is in *normal form* with respect to S (S-NF). ⌟

Universality

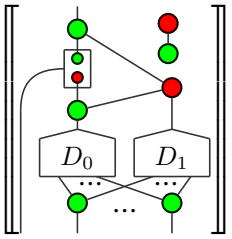
While the main application of the notion of normal form is to prove completeness results (in the next sections), our first application is to prove the universality of $\Delta\mathbf{ZX}[F]$ for any $F \in \mathcal{F}$. First notice that the universality of $\Delta\mathbf{ZX}[F]$ can be reduced to the existence of an appropriate set of controlled scalars:

Lemma 5.2.9 (Sufficient condition for universality)**.** *Given $F \in \mathcal{F}$, if $\exists S \subseteq \Delta\mathbf{ZX}[F]$ a set of controlled scalars such that the map $\eta : S \to \mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}] = D \mapsto [\![D]\!] |1\rangle$ is surjective, then $\Delta\mathbf{ZX}[F]$ is universal, i.e. the functor $\Delta\mathbf{ZX}[F] \xrightarrow{[\![\cdot]\!]} \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}$ is full.*

Proof ▶ It is easier to see this if we look at the interpretation of ZX-diagrams as matrices. η being surjective, for any $x \in \mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$, there exists $D_x \in S$ such that $[\![D_x]\!] = \begin{pmatrix} 1 & x \end{pmatrix}$.

As pointed out, any diagram in S-CNF represents a quantum evolution of the form $\begin{pmatrix} \mathbb{1} & \psi \end{pmatrix}$, where $\mathbb{1}$ is a column vector whose entries are all 1, and ψ is another column

vector. Moreover, one can show that if $[\![D_0]\!] = \begin{pmatrix} \mathbb{1} & \psi_0 \end{pmatrix}$ and $[\![D_1]\!] = \begin{pmatrix} \mathbb{1} & \psi_1 \end{pmatrix}$, then



$$= \begin{pmatrix} \mathbb{1} & \psi_0 \\ \mathbb{1} & \psi_1 \end{pmatrix}$$

Hence, by induction, for any column vector ψ over $\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$, one can perform the matrix $\begin{pmatrix} \mathbb{1} & \psi \end{pmatrix}$ as an S-CNF. Plus, $[\![$  $]\!] = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ so we can recover a diagram representing the vector ψ. Finally, using the map/state duality, any matrix over $\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$ can be represented as a ZX-state over $\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$, where some outputs wire are bent so as to become inputs (this procedure gives the S-NF form). ◀

Theorem 5.2.10. *For any $F \in \mathcal{F}$, $\Delta\mathbf{ZX}[F]$ is universal for $\mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}$:*

$$\forall M \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]},\ \exists D \in \Delta\mathbf{ZX}[F],\ [\![D]\!] = M$$

In other words, the functor $\Delta\mathbf{ZX}[F] \xrightarrow{[\![\cdot]\!]} \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}$ is full.

Proof ▶ Let $S \subseteq \Delta\mathbf{ZX}[F]$ be the set of all controlled scalars. According to Lemma 5.2.9 it suffices to show that $\eta : S \to \mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$ is onto. Let $x \in Z[\frac{1}{\sqrt{2}}, e^{iF}]$, there exist $p \in \mathbb{N}$, $\alpha_0, \ldots, \alpha_k \in F$, and $P_0 \ldots P_k \in \mathbb{Z}[X]$ such that $x = \frac{1}{2^p} \sum_{j=0}^{k} P_j(e^{i\alpha_j})$. Since $\Gamma_{\alpha_j}(P_j)$ encodes $P_j(e^{i\alpha_j})$,  encodes $\frac{1}{2}$ and they can be added and multiplied according to Lemma 5.2.6, there exists a diagram $D \in S$ such that $[\![D]\!] |1\rangle = x$. ◀

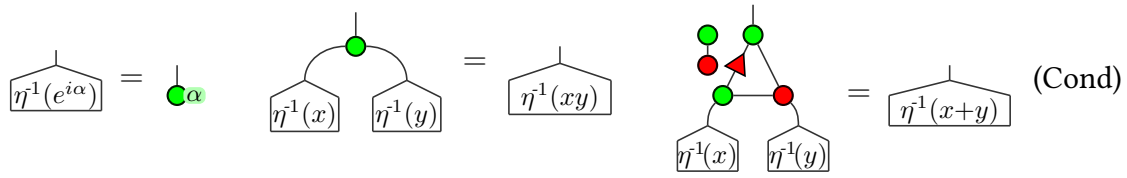
5.3 A sufficient condition for completeness

The *controlled states* give a generic internal structure for a diagram in normal form, by separating the coefficients of the process – i.e. controlled scalars intuitively accounting for the entries of the represented matrix – from the way they are combined. While the representation of the controlled scalars depends on the considered fragment, their combination is done in $\Delta\mathbf{ZX}[\pi]$.

Hence, all the sound operations on the *structure* of the normal forms should be doable using the Δ_π^+ rules. The completeness for broader fragments is then reduced to the capacity to apply elementary operations on coefficients:

Theorem 5.3.1 (Sufficient condition for completeness). *Given a fragment $F \in \mathcal{F}$ and an axiomatisation R, $\Delta\mathbf{ZX}[F]/R$ is complete if $R \vdash \Delta_{\pi/4}$ and if $\exists S \subseteq \mathbf{ZX}[F]$ a set of controlled scalars such that $\eta : S \to \mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}] = D \mapsto [\![D]\!] |1\rangle$ is bijective, and the*

following equations hold: $\forall \alpha \in F, \forall x, y \in \mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$,



(Cond)

Before proving Theorem 5.3.1, notice that all the above equations are involving diagrams with a single input and no output, thus for any fragment the completeness reduces to the completeness for diagrams with 1 input and no output, or equivalently – by bending the wires – to diagrams representing 1-qubit state preparations which have no input and a single output:

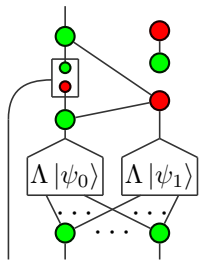
Corollary 5.3.2. *For any fragment $F \in \mathcal{F}$ and axiomatisation R, $\Delta\mathbf{ZX}[F]/R$ is complete if and only if it is complete for 1-qubit state preparations, i.e. for all diagrams with no input and a single output.*

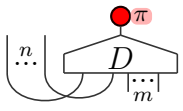
Notice that thanks to the hypothesis of Theorem 5.3.1, one can associate to any state $|\varphi\rangle : 0 \to n \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}$ a diagram $\Lambda(|\varphi\rangle)$ in S-CNF, and to any evolution $f : n \to m \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}$, a diagram $\lambda(f)$ in S-NF:

⌜ **Definition 5.3.3:** With the hypothesis of Theorem 5.3.1, let

$$\Lambda : \bigcup_{n \in \mathbb{N}} \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}[0, n] \to S\text{-CNF} \quad \text{and} \quad \lambda : \bigcup_{n,m \in \mathbb{N}} \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}[n, m] \to S\text{-NF}$$

be defined as follows:

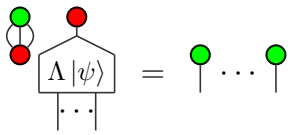
- $\Lambda(x) := \eta^{-1}(x)$ if $x \in \mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$,
- $\Lambda(|0\rangle \otimes |\psi_0\rangle + |1\rangle \otimes |\psi_1\rangle) :=$ 

- $\lambda\left(\sum_{\substack{x \in \{0,1\}^n \\ y \in \{0,1\}^m}} \alpha_{x,y} |y\rangle \langle x|\right) :=$ 

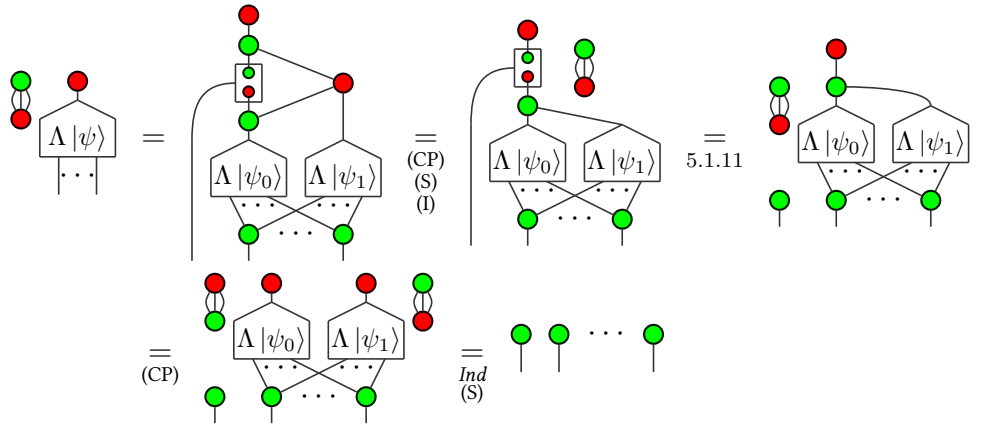
, where $D = \Lambda\left(\sum_{\substack{x \in \{0,1\}^n \\ y \in \{0,1\}^m}} \alpha_{x,y} |x\rangle |y\rangle\right)$ ⌟

Notice that if the conditions (Cond) are met, the language proves that for any $|\psi\rangle : 0 \to n$ in S-CNF, $[\![\Lambda\,|\psi\rangle]\!]\,|0\rangle = \sum_{x \in \{0,1\}^n} |x\rangle$:

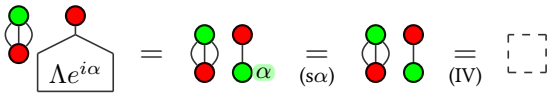
Lemma 5.3.4.

$\Delta_{\pi/4}$ +(Cond) $\vdash$ 

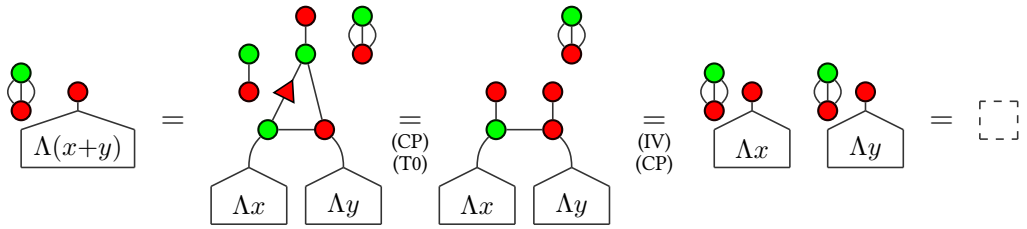
Proof ▶ First, let $|\psi_0\rangle$ and $|\psi_1\rangle : 0 \to n \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}$ such that $|\psi\rangle = |0\rangle |\psi_0\rangle + |1\rangle |\psi_1\rangle$. Then:



It then remains to prove the result for the base cases Λx. Any x can be decomposed as a sum of $e^{i\alpha}$ where αs are in the fragment. Then:



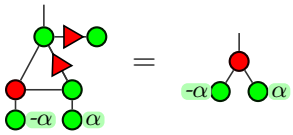
and:



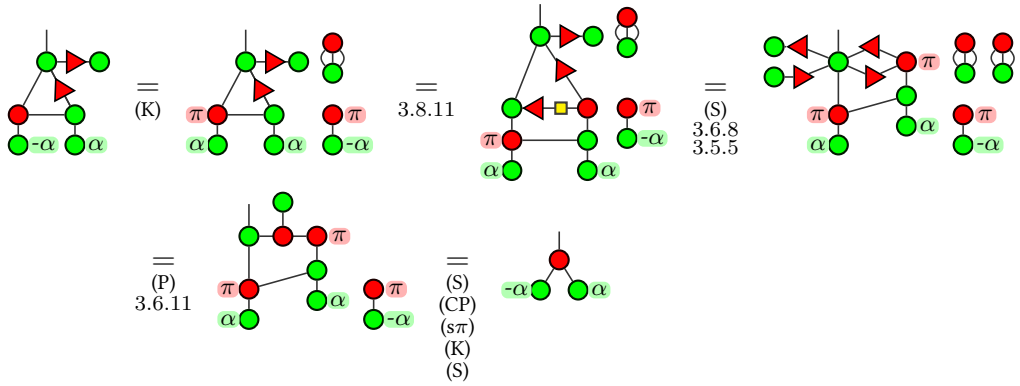
◀

Also, if the conditions (Cond) are met, then some control scalars can obviously be derived, thanks to the following lemma:

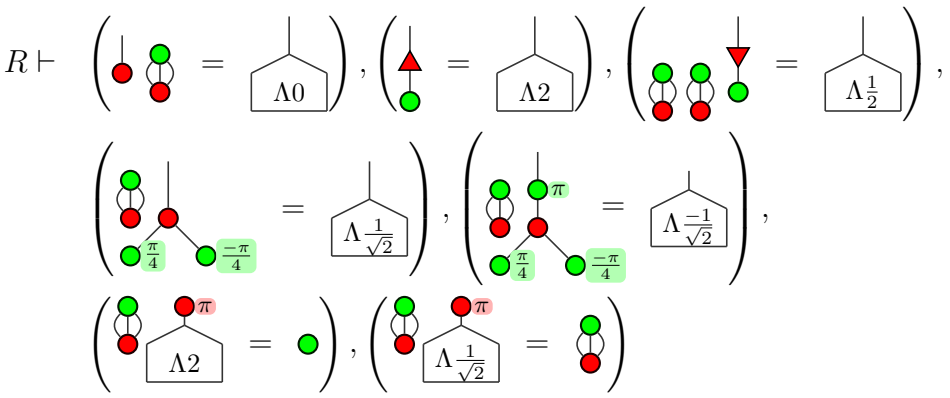
Lemma 5.3.5.



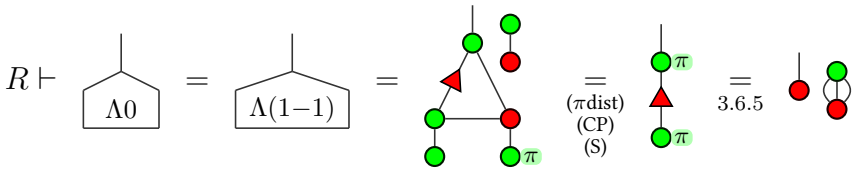
Proof ▶

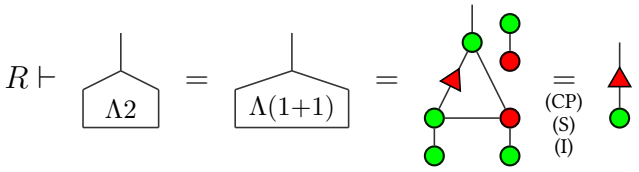


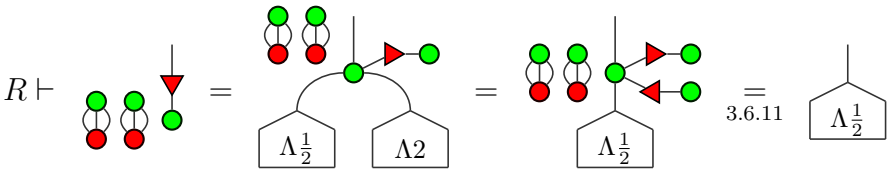
Lemma 5.3.6. *With R a set of axioms such that $R \vdash \Delta_{\pi/4}$ +(Cond):*

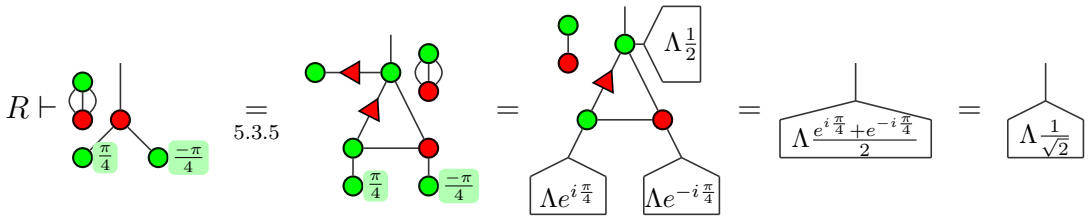


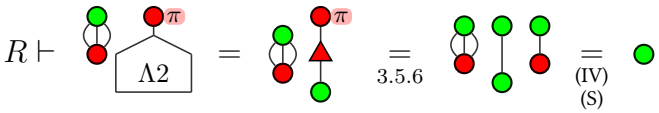
Proof ▶ Since $R \vdash \mathrm{ZX}_{\pi/4}$:

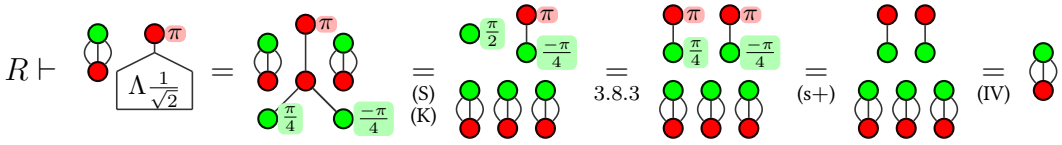












◀

The proof of Theorem 5.3.1 consists in showing that any diagram can be transformed into a diagram in S-normal form. The proof is inductive: every generator of the language can be set in S-normal form, moreover both the parallel and sequential compositions of S-normal forms can be transformed into diagrams in S-normal form.

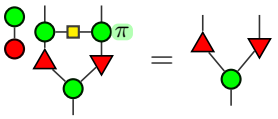
5.4 Preliminary Derivations

Proving that the compositions of two normal forms can be put in normal form will rely extensively on different lemmas that we will lay out in this section. We will explore here how the transistor interacts with the other generators of the language, with the triangle, and with other transistors. This section only produces diagrammatic derivations. For the reader convenience, it ends at page 193.

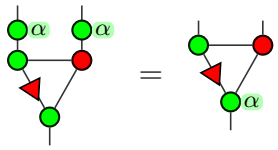
Derivations of ΔZX

First, we derive some supporting lemmas that do not use the transistor. Two of them (Lemmas 5.4.2 and 5.4.3) were proven to be derivable thanks to Corollary 4.2.2, but were not given an explicit derivation.

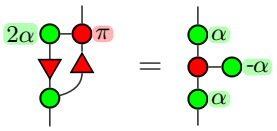
Lemma 5.4.1.



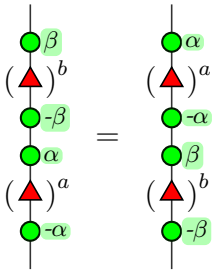
Lemma 5.4.2.



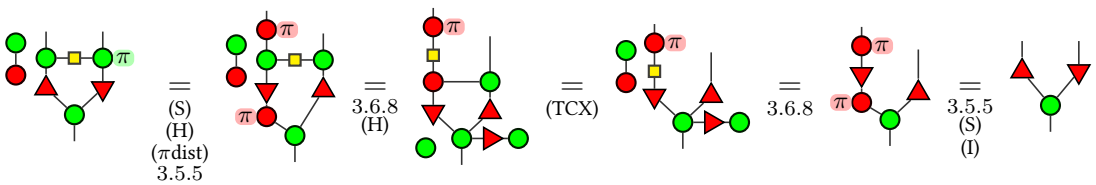
Lemma 5.4.3.



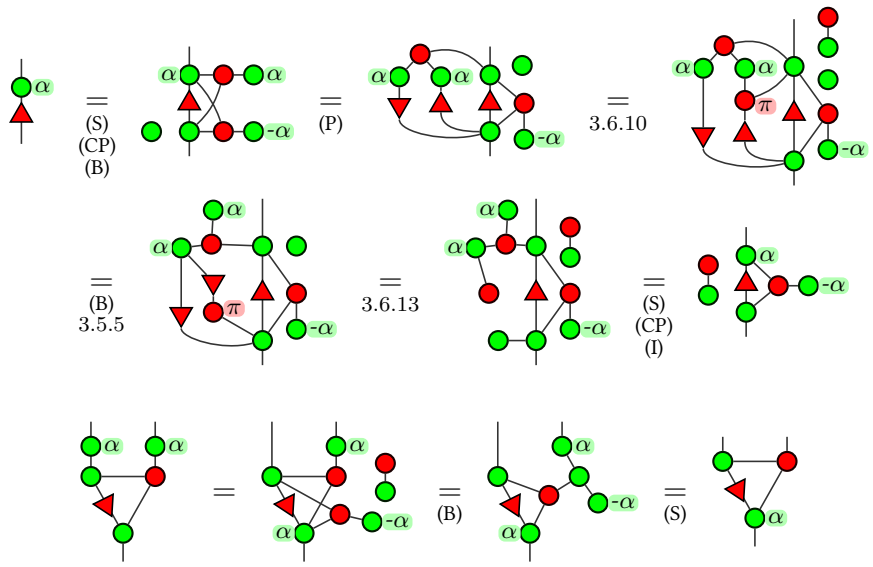
Lemma 5.4.4.



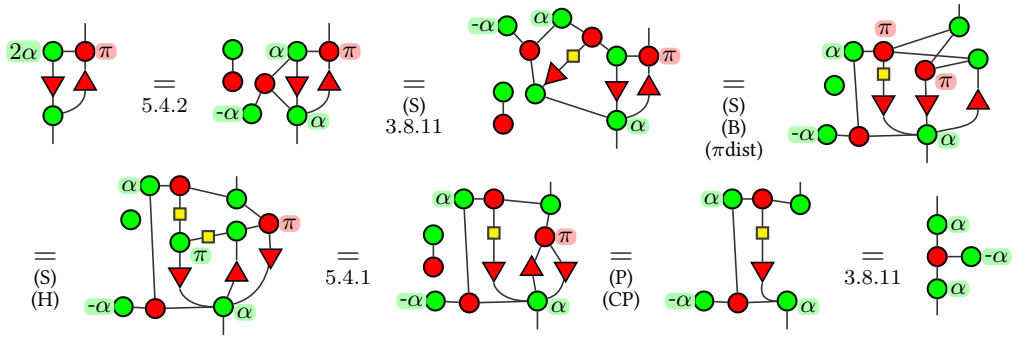
Proof ▶ ● 5.4.1:



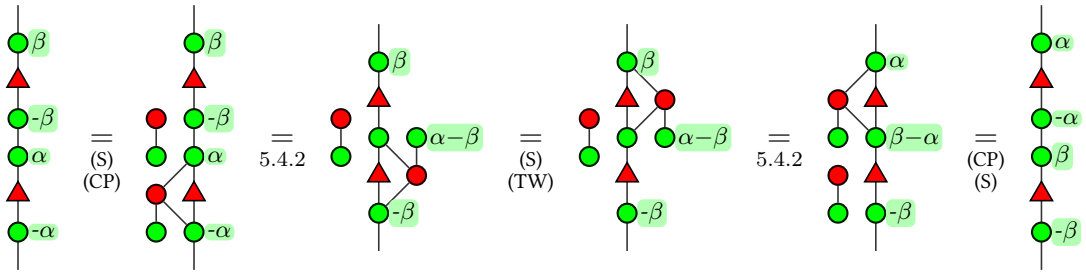
- 5.4.2:



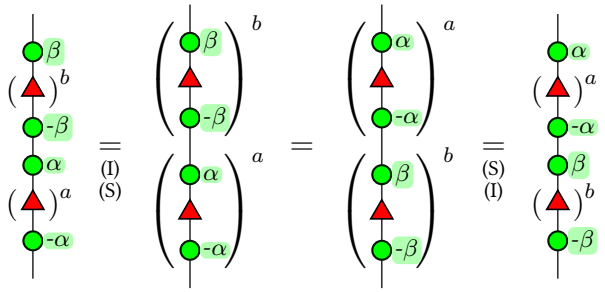
- 5.4.3:



- 5.4.4: First, if $a = 1 = b$:



Then:

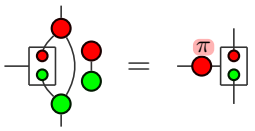


◀

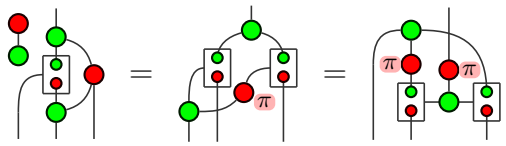
Derivations using the Transistor

We derive here some equations on the transistor that will come in handy when we try to have transistors and triangles interact in the following.

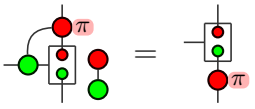
Lemma 5.4.5.



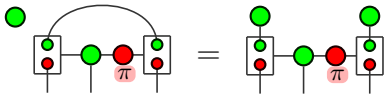
Lemma 5.4.6.



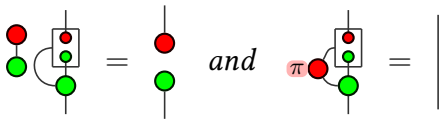
Lemma 5.4.7.



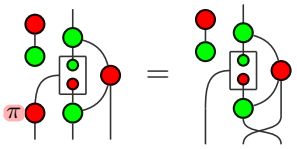
Lemma 5.4.8.



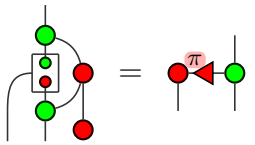
Lemma 5.4.9.



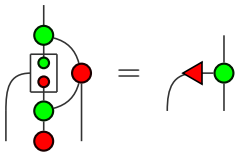
Lemma 5.4.10.



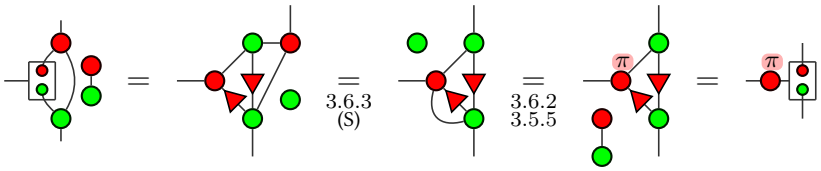
Lemma 5.4.11.



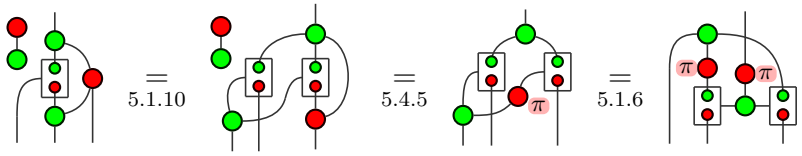
Lemma 5.4.12.



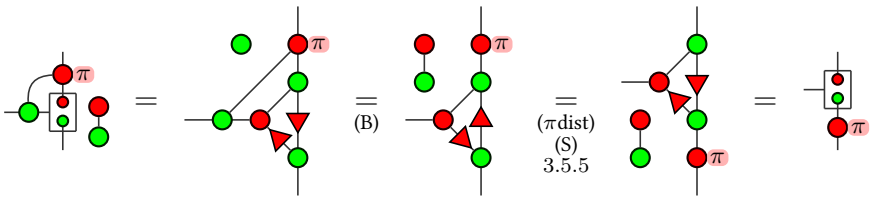
Proof ▶ • 5.4.5:



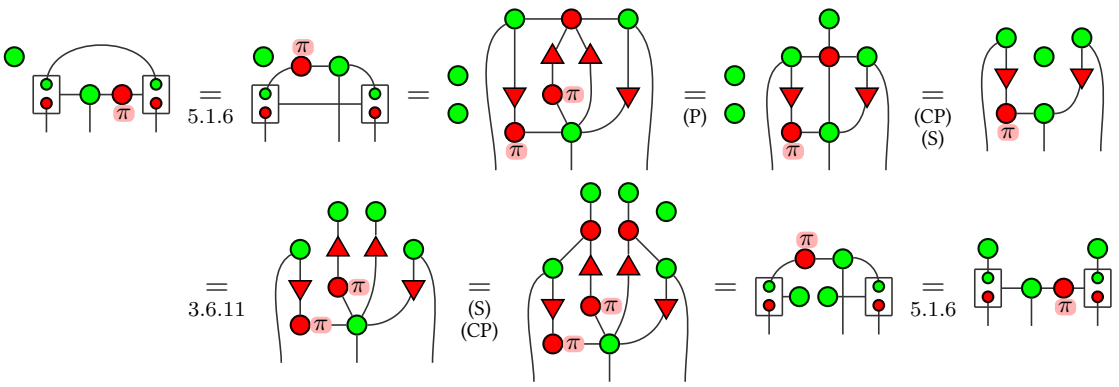
• 5.4.6:



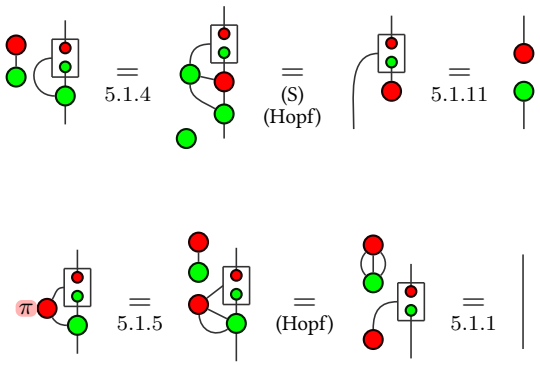
• 5.4.7:



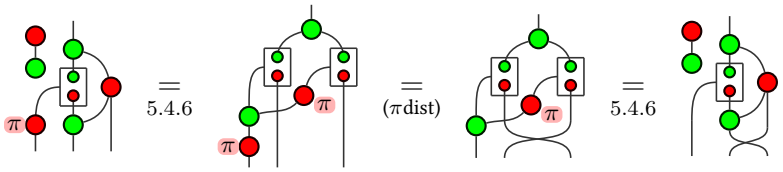
- 5.4.8:



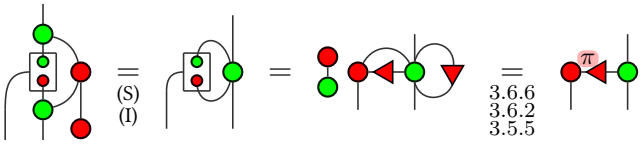
- 5.4.9:



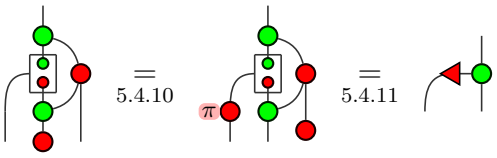
- 5.4.10:



- 5.4.11:



- 5.4.12:

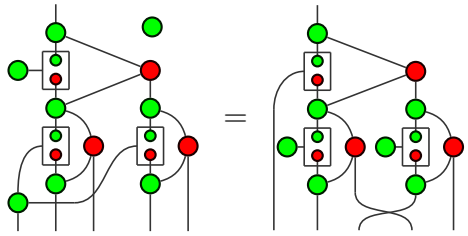


◀

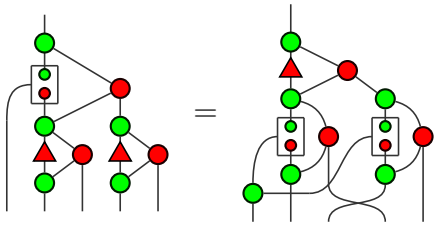
Interactions of Transistors and Δ

Finally, we show how the transistor interact with other diagrams of the language.

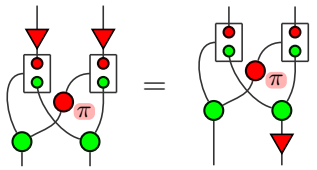
Lemma 5.4.13.



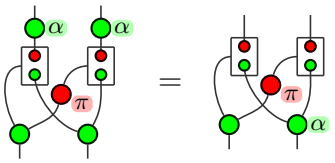
Lemma 5.4.14.



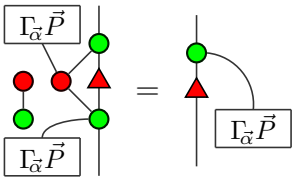
Lemma 5.4.15.



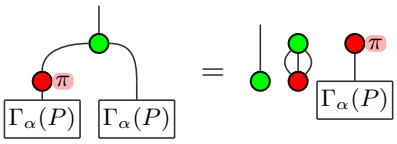
Lemma 5.4.16.



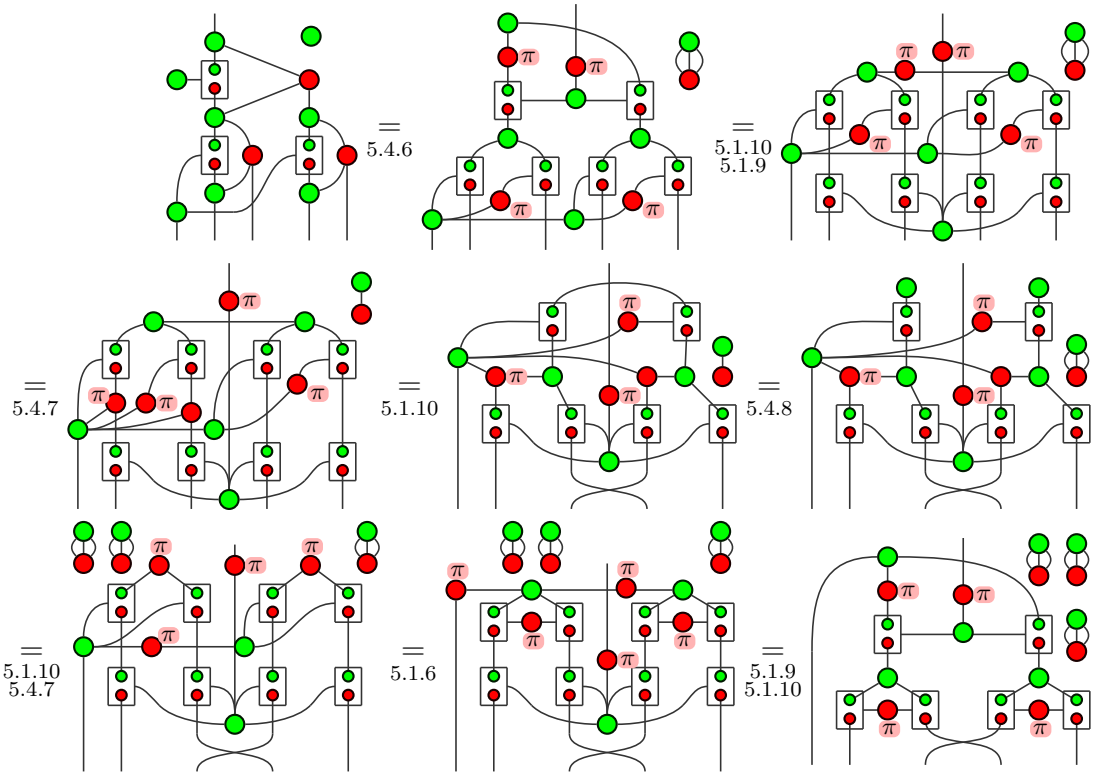
Lemma 5.4.17.



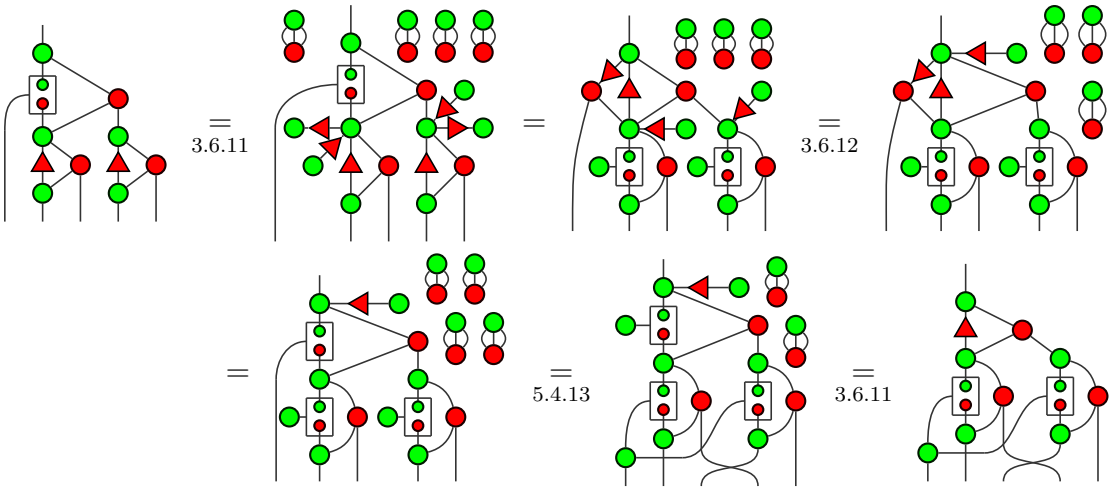
Lemma 5.4.18.



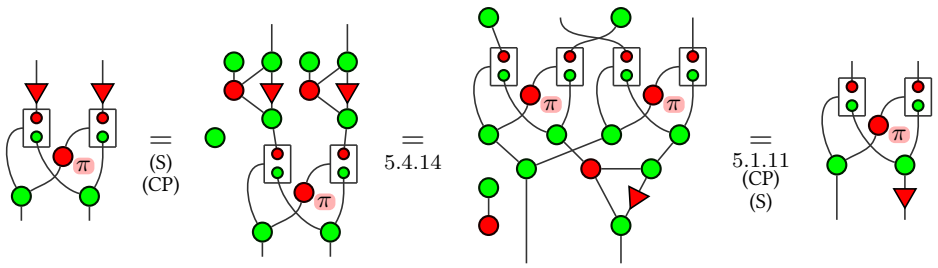
Proof ▶ ● 5.4.13:



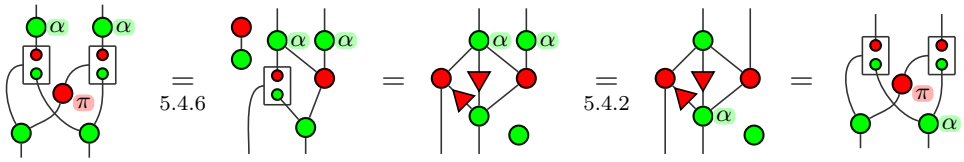
- 5.4.14:



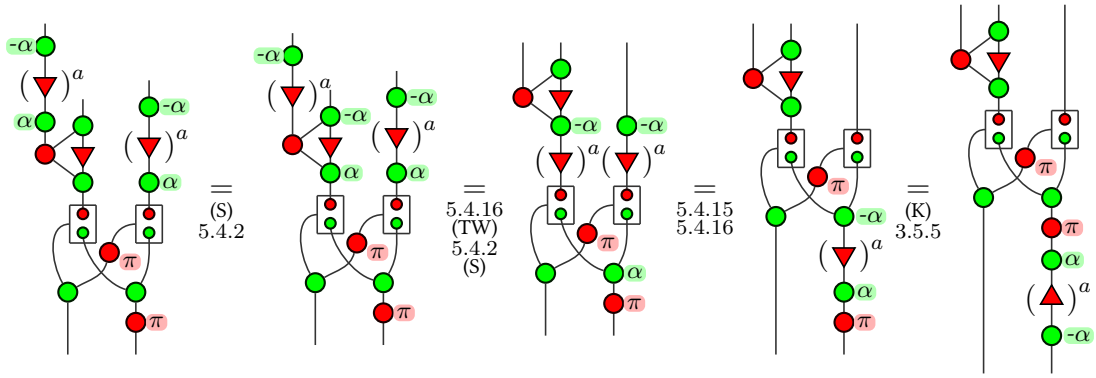
- 5.4.15:



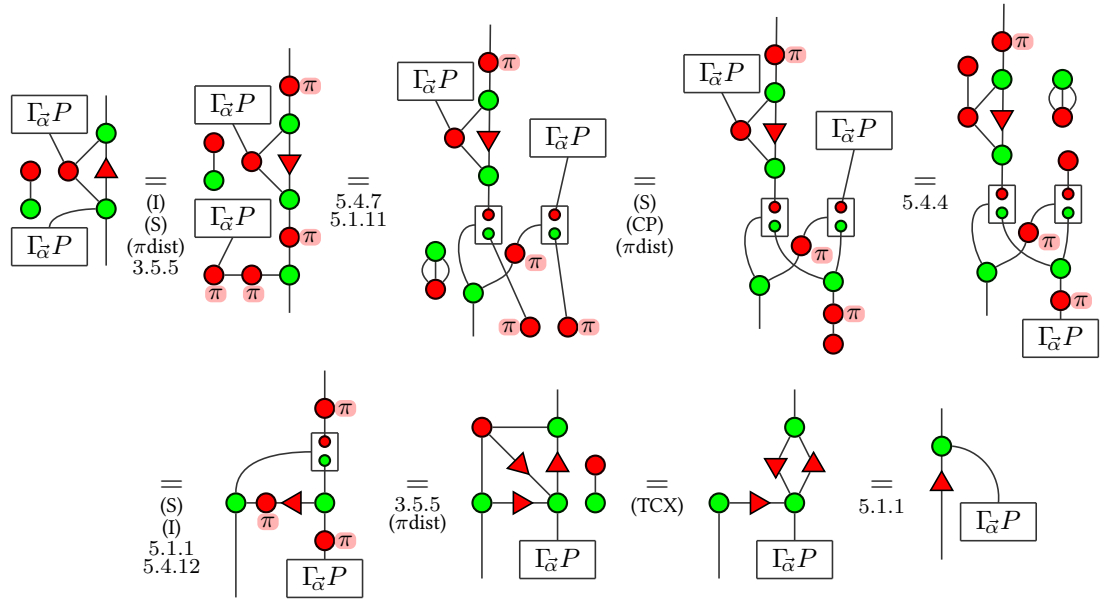
- 5.4.16:



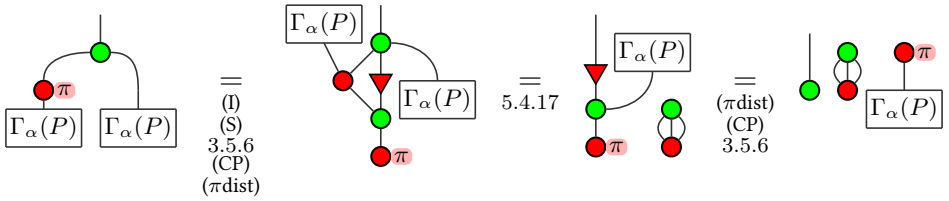
- 5.4.17: First notice that:



Then, using the previous derivation repeatedly:



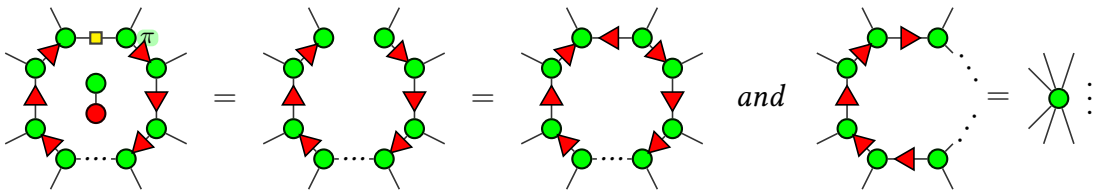
• 5.4.18:



◀

Interestingly, we can derive the whole following family of equations:

Lemma 5.4.19.

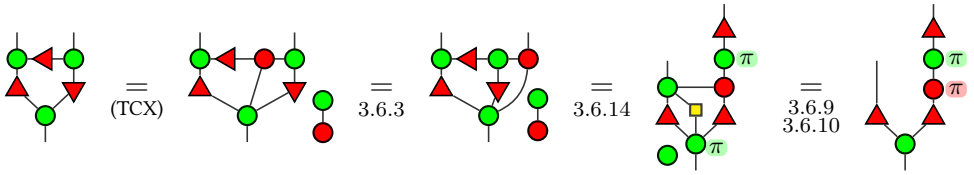


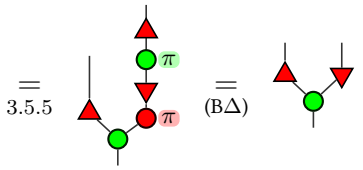
Let n be the number of triangles in the first two diagrams.

• $n = 0$: The first equality is (HL), the second is equivalent to the third, and already proven 3.6.6.

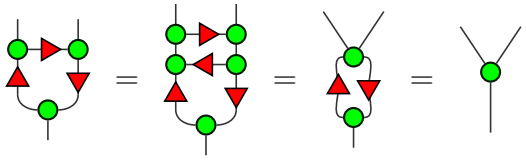
• $n = 1$: The first equality is 3.6.9, the second is 3.5.4 and the third is 5.1.1.

• $n = 2$: The first equality is given by Lemma 5.4.1. Then:

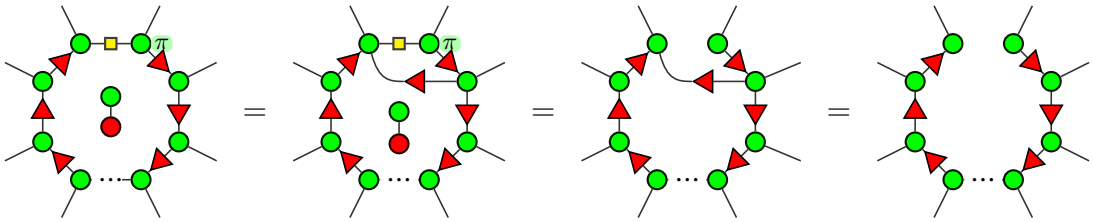




Finally:



• n: Suppose we have the result for $n-1$ and $n=2$. Then:

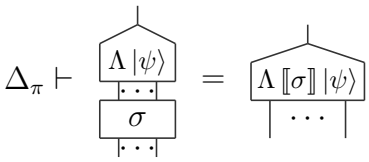


The same trick is used for the two other equalities.

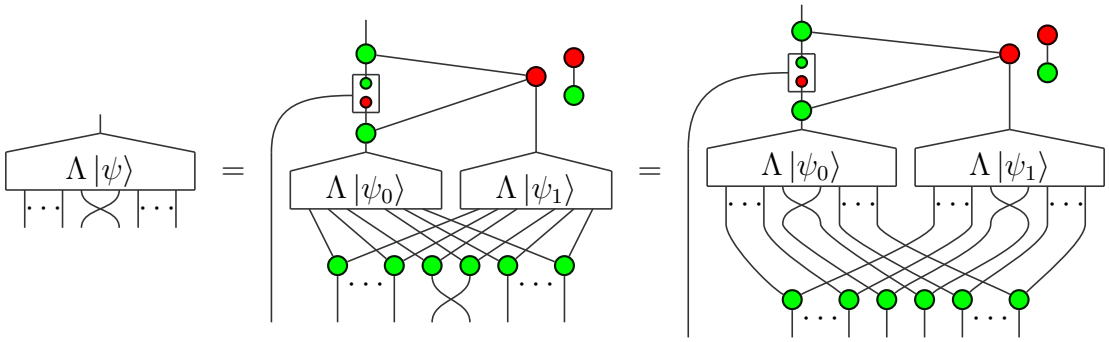
5.5 Compositions of Normal Forms

We now use the results of Section 5.4 to prove that the compositions (spatial and sequential) of two diagrams in S-CNF can be put in S-CNF.

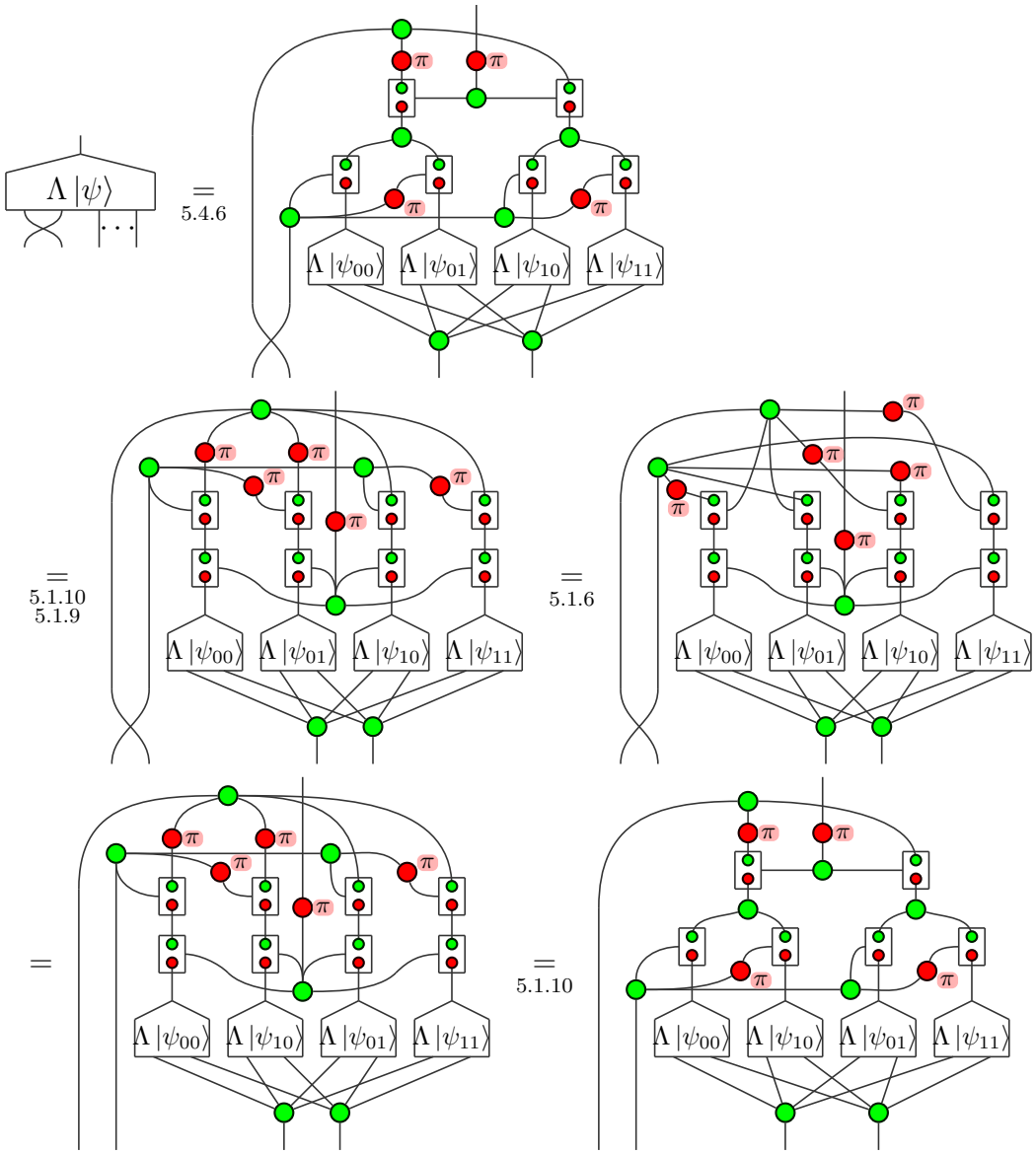
Proposition 5.5.1 (Permutation). *For any* $|\psi\rangle : 0 \to n \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}},e^{iF}]}$, *and any permutation* σ *on* n *wires:*



Proof ► Any permutation can be decomposed in a sequence of adjacent transpositions, which in ZX translates as swaps σ. If $|\psi\rangle$ is a state on 0 or 1 qubit, the only permutation allowed is the identity. Otherwise, let $|\psi\rangle = |0\rangle\,|\psi_0\rangle + |1\rangle\,|\psi_1\rangle = |00\rangle\,|\psi_{00}\rangle + |01\rangle\,|\psi_{01}\rangle + |10\rangle\,|\psi_{10}\rangle + |11\rangle\,|\psi_{11}\rangle$. If the first wire is not affected by the swap:

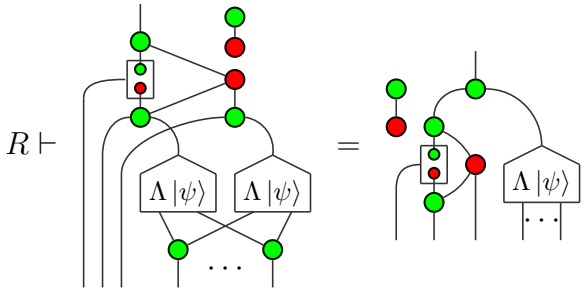


which can be set in normal form by induction. If a swap occurs on the two first outputs:



◀

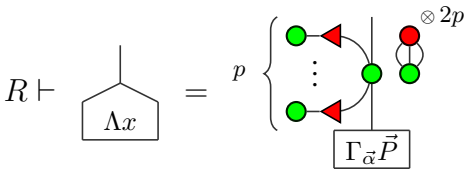
Lemma 5.5.2.



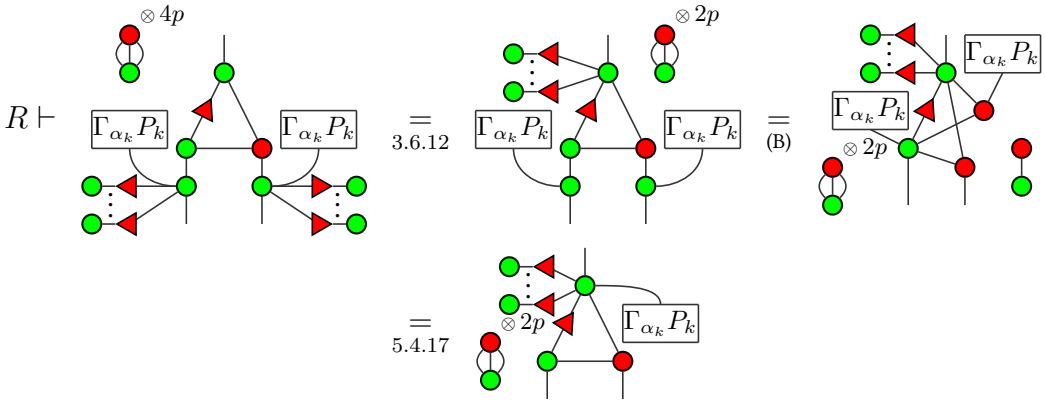
Proof ▶ By induction on the number n of outputs of $|\psi\rangle$:

• $n = 0$: Let $x \in \mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$. There exist p, $\vec{\alpha} = (\alpha_k)_k$ and $\vec{P} = (P_k)_k$ such that

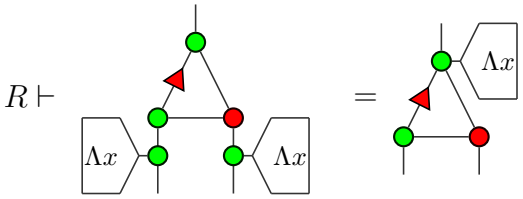
$x = \frac{1}{2^p} \sum_k P(e^{i\alpha_k})$. The conditions for Theorem 5.3.1 imply that:



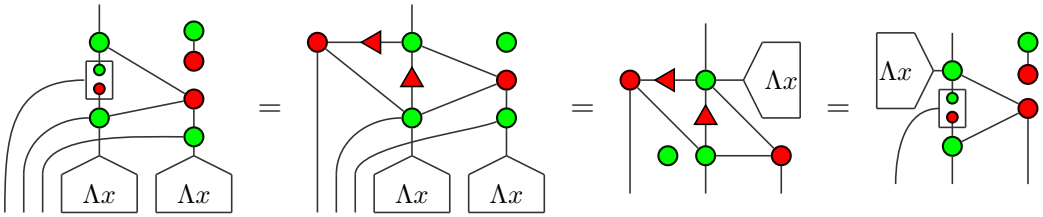
Then:



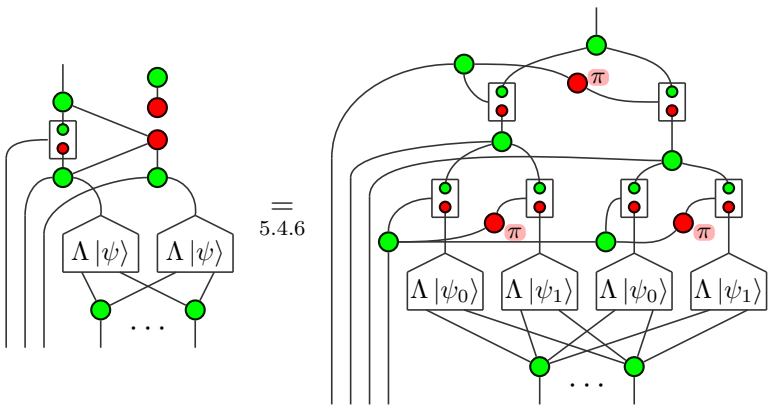
Hence:

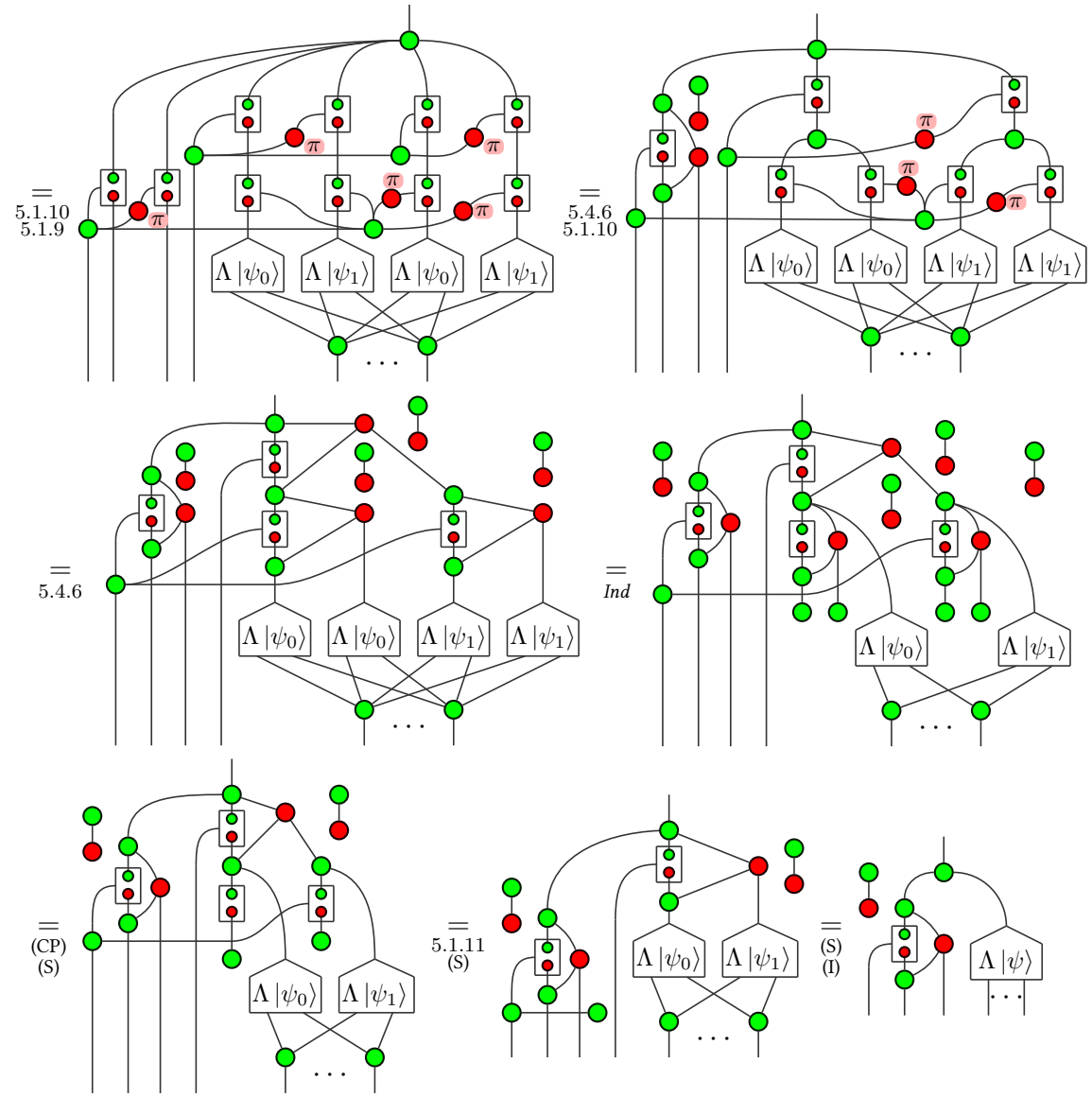


Then:



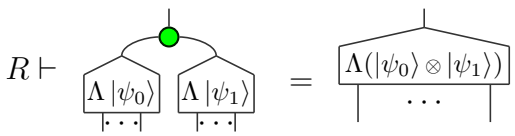
• $n \geq 1$: In this case, let $|\psi\rangle = |0\rangle |\psi_0\rangle + |1\rangle |\psi_1\rangle$, and





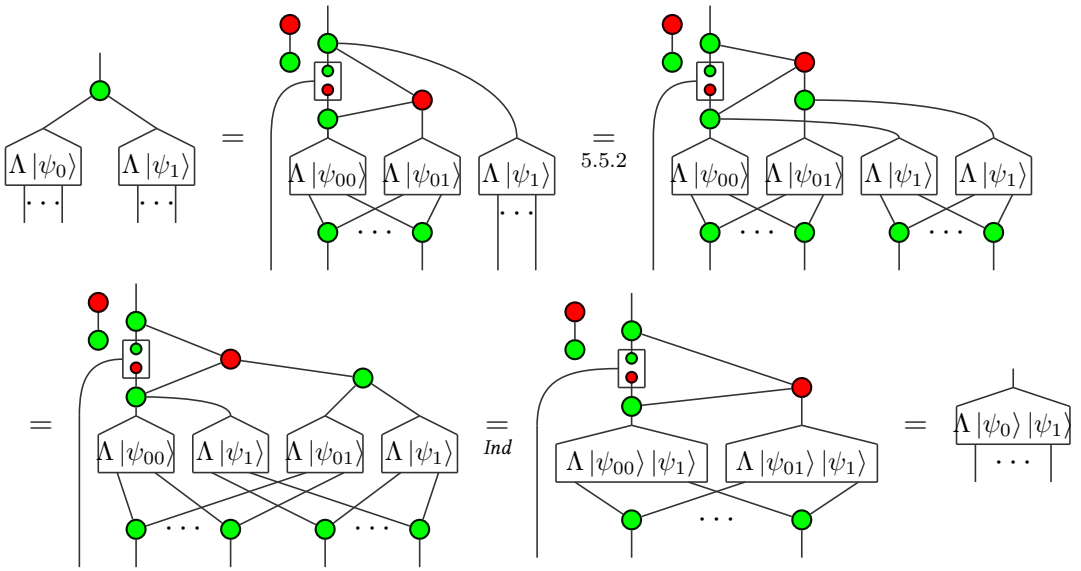
◀

Proposition 5.5.3 (Tensor Product). *For any* $|\psi_0\rangle : 0 \to n, |\psi_1\rangle : 0 \to m \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}$, *and any* R *such that* $R \vdash \Delta_\pi^+$ +(Cond)*:*



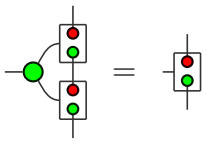
Proof ▶ By induction on the number of outputs of $|\psi_0\rangle$ and $|\psi_1\rangle$:
• If both states are scalars, this case is handled by the condition in Theorem 5.3.1.

• If one of the two states has at least one output – say $|\psi_0\rangle = |0\rangle\,|\psi_{00}\rangle + |1\rangle\,|\psi_{01}\rangle$:

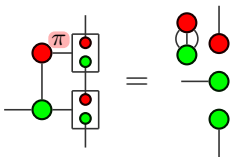


◀

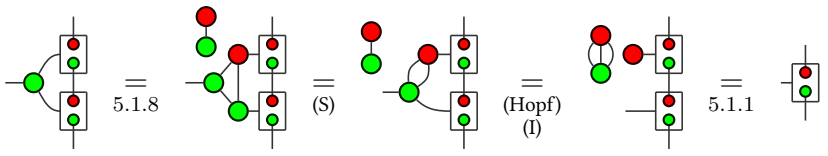
Lemma 5.5.4.

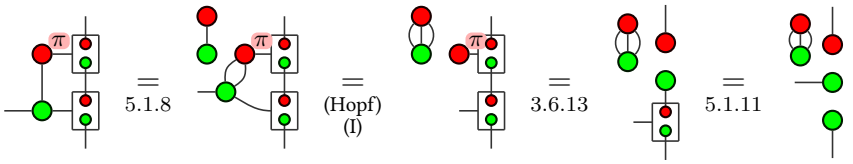


Lemma 5.5.5.



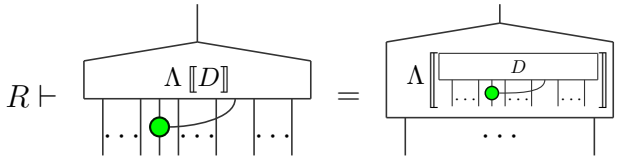
Proof ►





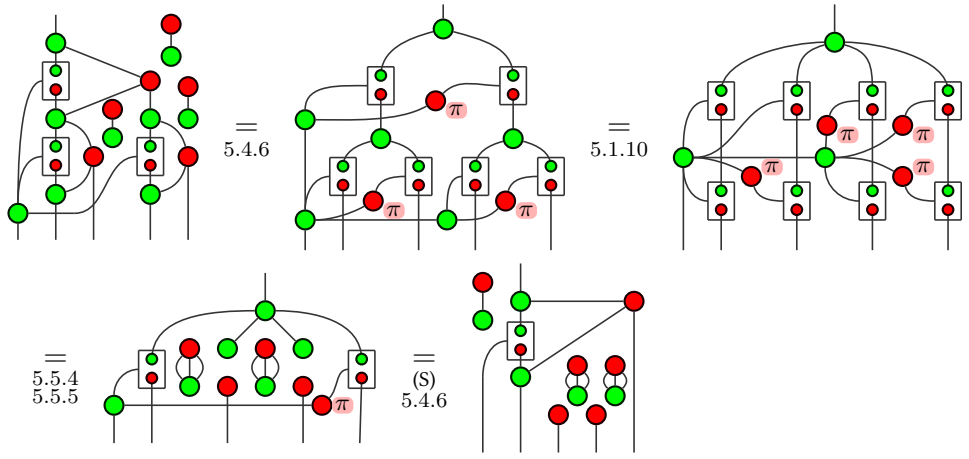
◀

Proposition 5.5.6 ($R_Z^{(2,1)}$). *For any $D : 0 \to n+2$, and any R such that $R \vdash \Delta_\pi$ +(Cond):*

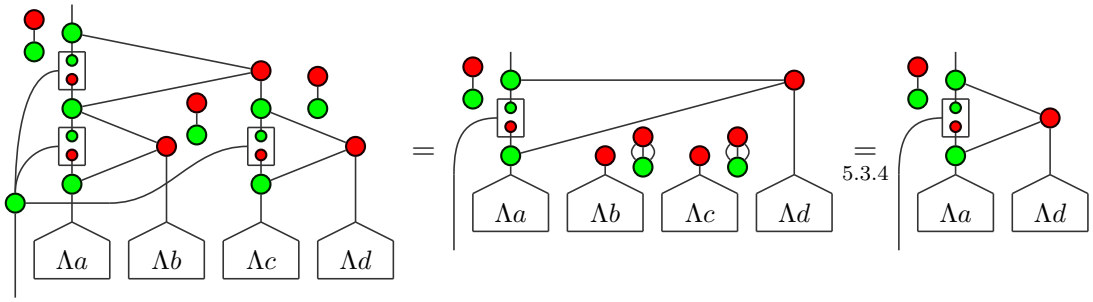


Proof ▶ By induction on the number n of outputs of $|\psi\rangle$.

• $n = 2$: First notice:

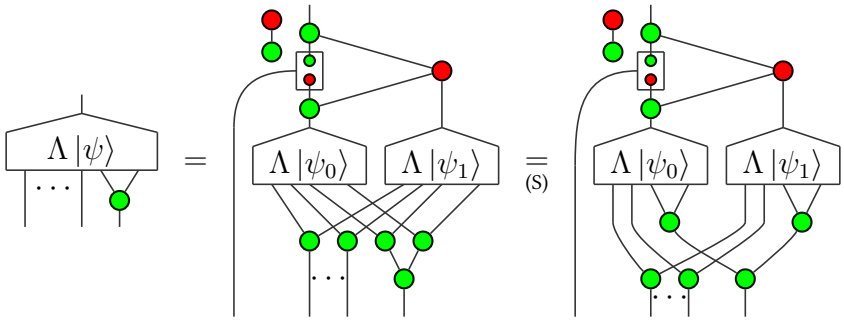


Then, if $|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + |11\rangle$:



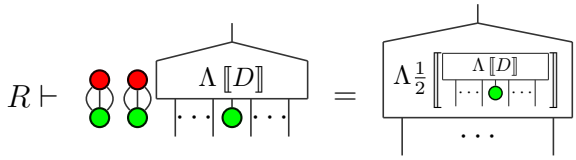
which is in normal form.

• $n \geq 3$: Using Proposition 5.5.1, we can impose  to be applied on the two last wires. Then:

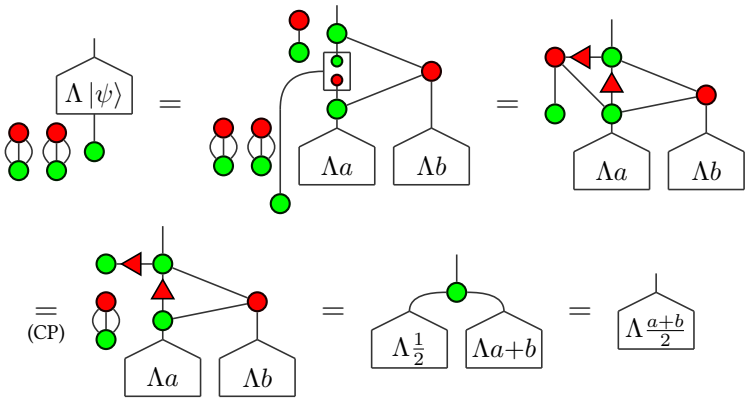


◀

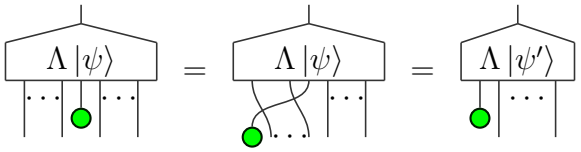
Proposition 5.5.7 ($R_Z^{(1,0)}$). *For any diagram $D : 0 \to n+1$, and any R such that $R \vdash \Delta_\pi$ +(Cond):*



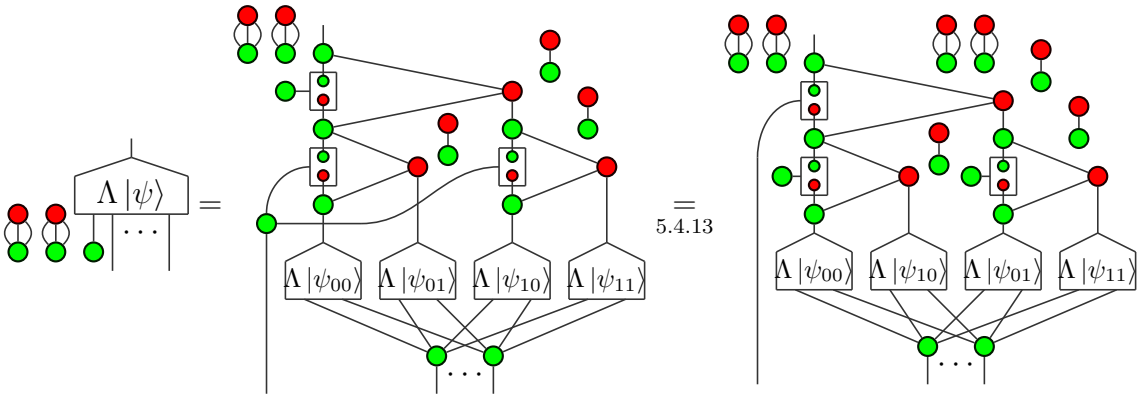
Proof ▶ By induction of the number n of wires of $|\psi\rangle$:
• $n = 1$: Let $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. Then:



• $n \geq 2$: First, using Proposition 5.5.1 if needs be,

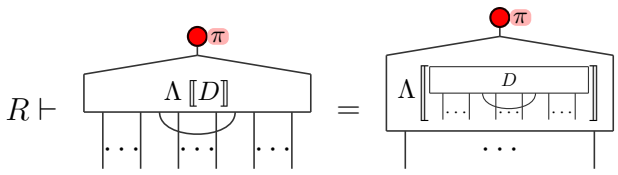


then,

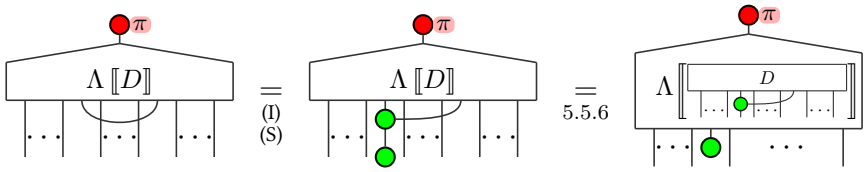


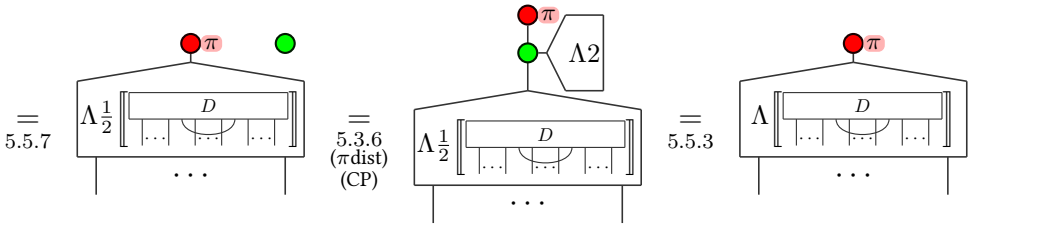
◀

Proposition 5.5.8 (Trace). *For any diagram $D : 0 \to n + 1$, and any R such that $R \vdash \Delta_\pi$ +(Cond):*



Proof ▶

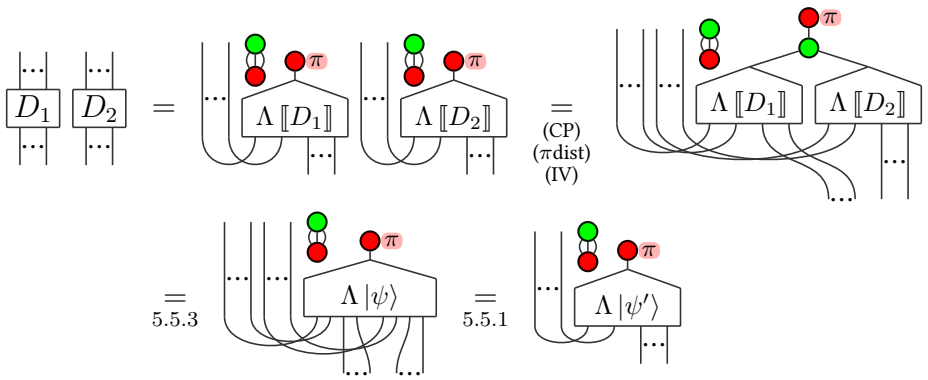




◀

Proposition 5.5.9. *With the hypothesis of Theorem 5.3.1, for any D_0, D_1 in S-NF, $D_0 \otimes D_1$ can be transformed into a diagram in S-NF.*

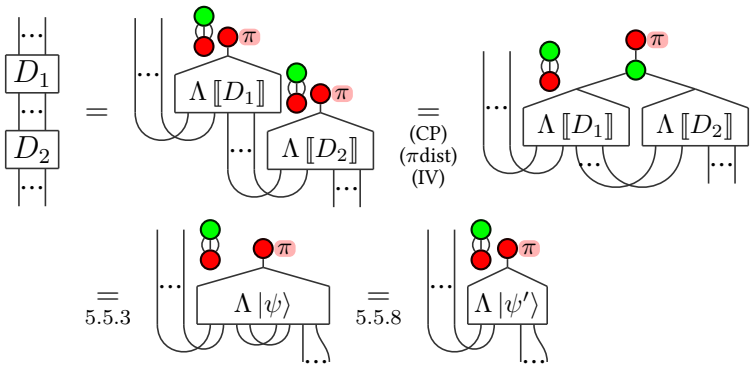
Proof ▶



◀

Proposition 5.5.10. *With the hypothesis of Theorem 5.3.1, for any $D_0 : n \to m$ and $D_1 : m \to k$ in S-NF, $D_1 \circ D_0 : n \to k$ can be transformed into a diagram in S-NF.*

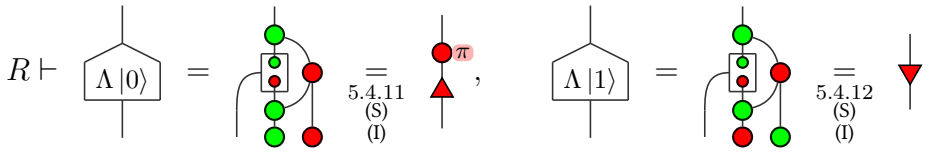
Proof ▶



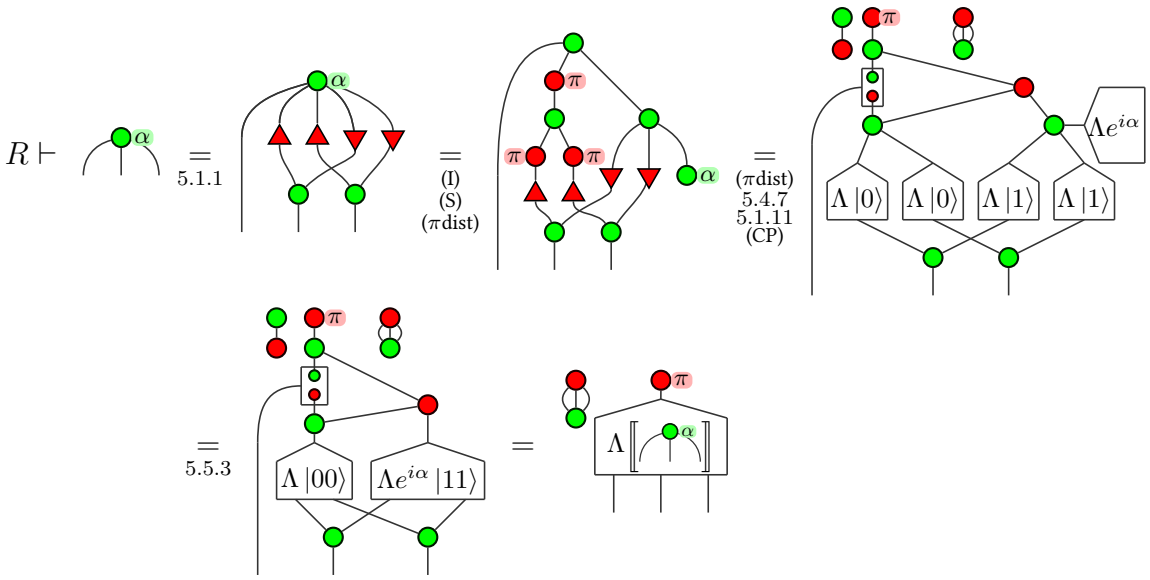
◀

Proposition 5.5.11. *With the hypothesis of Theorem 5.3.1, each generator can be transformed into a diagram in S-NF.*

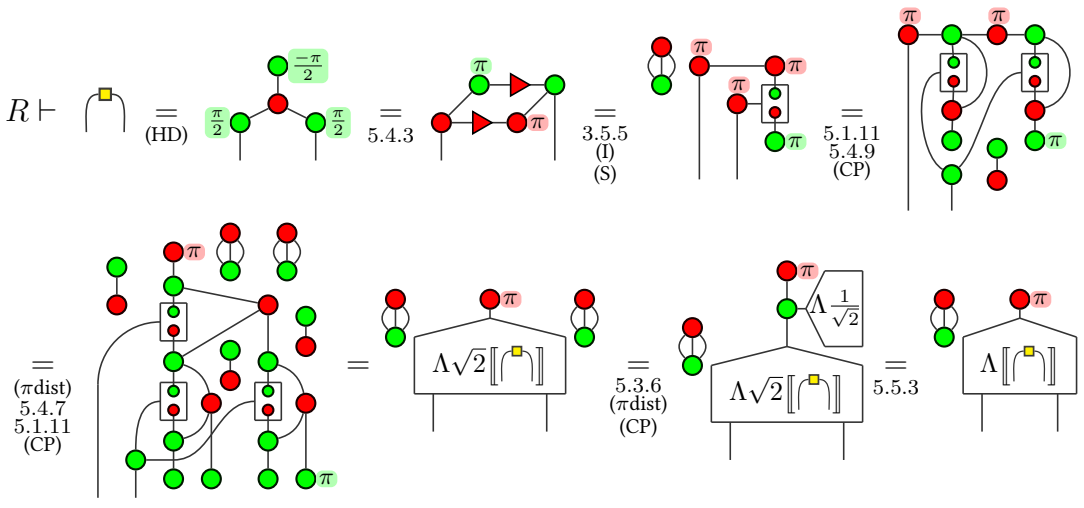
Proof ▶ We will prove the result for states, for the three-legged green dot, the Hadamard node and the empty diagram. All the other generators can be built from them and the Propositions 5.5.1, 5.5.3, 5.5.6, 5.5.8 and 5.5.7: First, notice that:



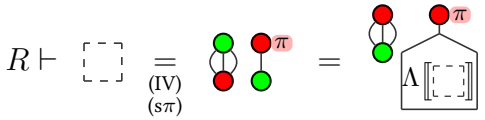
Then:



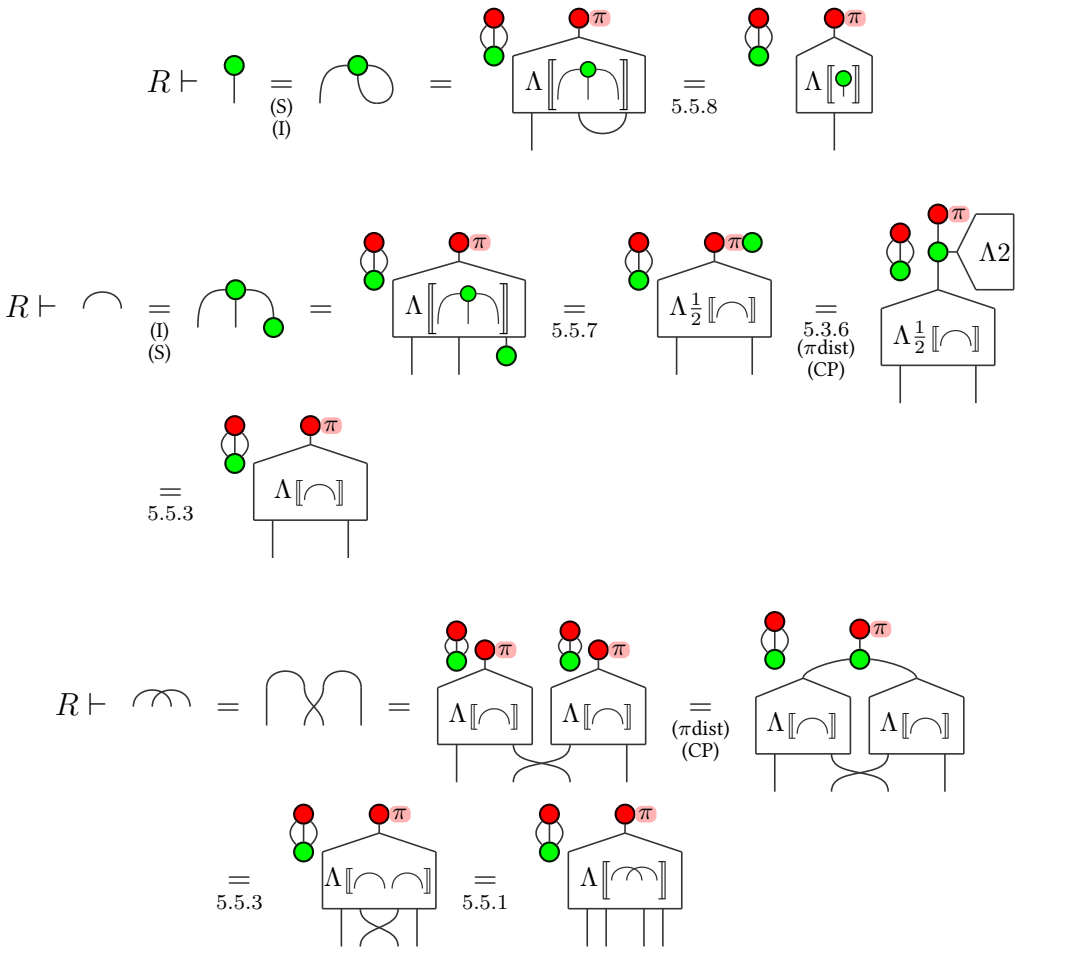
and:



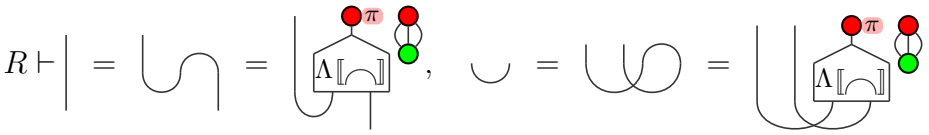
and:



Then:



Any green dot with arity larger than 3 can be decomposed as a 3-legged dots thanks to (S), and any red dot is a green dot with Hadamard gates on its adjacent wires. Then, any diagram can be built from the states by simple topological transformations. E.g:



◀

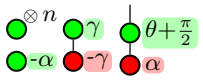
In the next sections, we will consider several fragments of the ZX-calculus for which we will exhibit a diagrammatic representation of controlled states. For some fragments, the above equations are provable, implying the completeness of the ZX-calculus for these fragments. For other fragments, we will need the help of some additional axioms to prove the above equations, implying the completeness of a ZX-calculus augmented with these additional axioms.

5.6 Normal Forms with Arbitrary Angles

In the case of the general ZX-calculus, we know (Theorem 4.6.1) that the language is complete with the set of rules ZX (Figure 4.3).

Definition 5.6.1: Let $\Lambda_{\mathbb{R}} : \mathbb{C} \to \mathbf{ZX}[1,0]$ be the map defined as:

- $\Lambda_{\mathbb{R}}(0) =$ 
- $\forall \rho > 0, \forall \theta \in [0, 2\pi)$, $\Lambda_{\mathbb{R}}(\rho e^{i\theta}) :=$



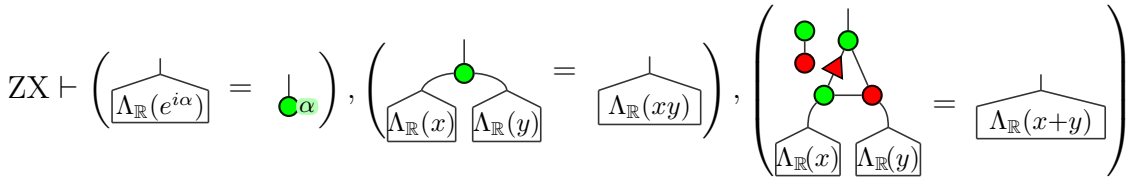
$$\text{with} \begin{cases} \alpha := 2\arctan(\rho) \\ n := \max(0, \lceil -\log_2(1+\cos(\alpha)) \rceil - 2) \\ \gamma := \arccos\left(\frac{1}{2^{n+1}(1+\cos(\alpha))}\right) \end{cases}$$

and $S_{\mathbb{R}} := \{\Lambda_{\mathbb{R}}(x) \mid x \in \mathbb{C}\}$.

Lemma 5.6.2. *For any $x \in \mathbb{C}$, $\Lambda_{\mathbb{R}}(x)$ is a controlled scalar, and $[\![\Lambda_{\mathbb{R}}(x)]\!]\,|1\rangle = x$.*

Proof ▶ This is routine (and can use Corollary 4.7.20). ◀

Lemma 5.6.3. *The map $\eta_{\mathbb{R}} : S_{\mathbb{R}} \to \mathbb{C} = D \to [\![D]\!]\,|1\rangle$ is bijective, and $\Lambda_{\mathbb{R}} = \eta_{\mathbb{R}}^{-1}$. Moreover:*



Proof ▶ The proof for the the first equation was done in Proposition 4.8.9 and the ones for the two other equations are similar to the proofs of rules $1b$ and $4a$ of Proposition 4.8.10. ◀

We can now reprove the completeness of $\mathbf{ZX}/$ ZX. By Proposition 4.8.5, ZX $\vdash \mathrm{ZX}_{\pi/4}$ and by Proposition 4.4.2 $\mathrm{ZX}_{\pi/4} \vdash \Delta_{\pi/4}$. By Lemma 5.6.3, the conditions (Cond) are met, so by Theorem 5.3.1, the language is complete.

5.7 Completeness and Normal Forms with Rational Angles

In this section, we consider the case where the angles are rational multiples of π, i.e. fragments $F \in \mathcal{F}_{\mathbb{Q}} := \{F \in \mathcal{F} \mid F \subseteq \mathbb{Q}\pi\}$. Among the rational angles, dyadic angles, i.e. $\mathcal{F}_{\mathbb{D}} := \{F \in \mathcal{F} \mid F \subseteq \mathbb{D}\pi\}$, where $\mathbb{D} := \{\frac{p}{2^q} \mid p, q \in \mathbb{N}\}$ enjoy some particular properties, and are considered in details in the next section.

Incompleteness and a new Rule for Cancelling Scalars

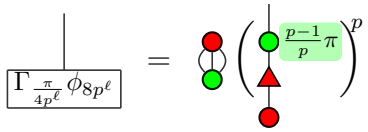
An interesting set of equations comes from the controlled scalars parametrised by integer polynomials, more precisely from those parametrised by cyclotomic polynomials. Indeed for any $n > 0$, $\left[\!\left[\Gamma_{\frac{2\pi}{n}}(\phi_n)\right]\!\right]|1\rangle = \phi_n(e^{\frac{i2\pi}{n}}) = 0$ (where ϕ_n is the n^{th} cyclotomic polynomial), thus $\left[\!\left[\Gamma_{\frac{2\pi}{n}}(\Phi_n)\right]\!\right] = \left[\!\left[$  $\right]\!\right]$. However, the corresponding equations are

not provable with $\mathrm{ZX}_{\pi/4}$ when $n = 8p$ with p an odd prime number, implying the incompleteness of any fragment of rational angles which contains at least one angle of the form $\frac{\pi}{4p}$:

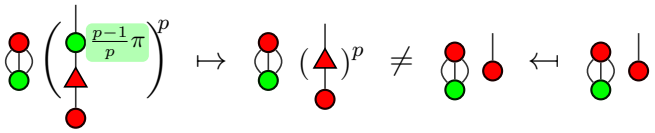
Lemma 5.7.1 (Incompleteness). *For any $F \in \mathcal{F}_{\mathbb{Q}} \setminus \mathcal{F}_{\mathbb{D}}$, there exists an odd prime number p such that $\Gamma_{\frac{\pi}{4p}}(\Phi_{8p}) \in \mathbf{ZX}[F]$ and*

$$\mathrm{ZX}_{\pi/4} \not\vdash \Gamma_{\frac{\pi}{4p}}(\Phi_{8p}) =$$ 

Proof ▶ Let p be an odd prime number and ℓ an integer ≥ 1. The formula of the cyclotomic polynomial for a number with at most one odd prime factor gives: $\phi_{8p^\ell}(x) = \sum_{k=0}^{p-1}(-1)^k x^{4kp^{\ell-1}}$. Moreover, $(-1)^k e^{i\frac{\pi}{4p^\ell}\times 4kp^{\ell-1}} = e^{i\frac{p+1}{p}k\pi}$. After telescoping:

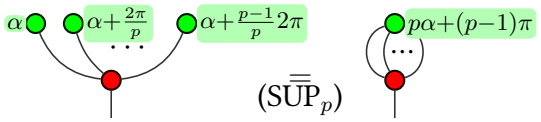


Since p and 4 are coprime, there exists k such that $kp\frac{\pi}{4} = \frac{\pi}{4}$. Let us then consider the interpretation $[.]_{kp}$ which multiplies all the angles by kp: $D_1 \otimes D_2 \mapsto [D_1]_{kp} \otimes [D_2]_{kp}$, $D_1 \circ D_2 \mapsto [D_1]_{kp} \circ [D_2]_{kp}$, $R_Z^{(n,m)}(\alpha) \mapsto R_Z^{(n,m)}(kp\alpha)$, $R_X^{(n,m)}(\alpha) \mapsto R_X^{(n,m)}(kp\alpha)$, Id otherwise. It is routine to show that the rules of $\mathrm{ZX}_{\pi/4}$ hold under this interpretation, but:

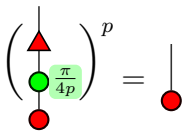


◀

Notice that a similar proof of incompleteness can be derived using cyclotomic supplementarity instead: For any $F \in \mathcal{F}_{\mathbb{Q}} \setminus \mathcal{F}_{\mathbb{D}}$, there exists an odd prime number p such that (SUP_p) is not provable in $\mathrm{ZX}_{\pi/4}$:

$\mathrm{ZX}_{\pi/4} \not\vdash$ 

Hence the ZX-calculus needs to be completed to deal with rational angles. One possible way of doing this is to add the previous set of equations as axioms: $\Gamma_{\frac{\pi}{4p}}(\Phi_{8p}) =$  . This would translate as:



with p prime

and – as we will see in the following – would be enough for completeness. However, instead of adding one or several new equations, we propose to add a simple and very natural rule to $\mathrm{ZX}_{\pi/4}$, the *cancellation rule* which allows one to simplify non zero scalars:

⌜ **Definition 5.7.2** (Cancellation rule)**:** The cancellation rule (Cancel) is defined as follows. For any diagrams of the ZX-calculus D_1 and D_2:

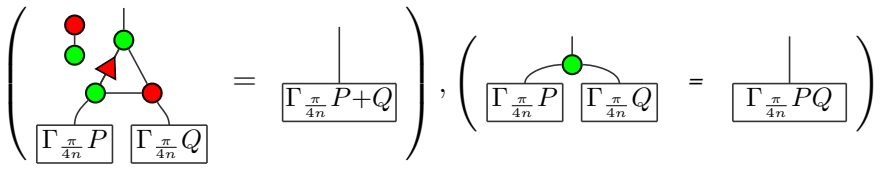
$$\forall \alpha \neq \pi \bmod 2\pi, \quad \mathrm{ZX}_{\pi/4} \vdash D_1 \otimes \alpha = D_2 \otimes \alpha \underset{\text{(Cancel)}}{\Longrightarrow} \mathrm{ZX} \vdash D_1 = D_2$$

⌟

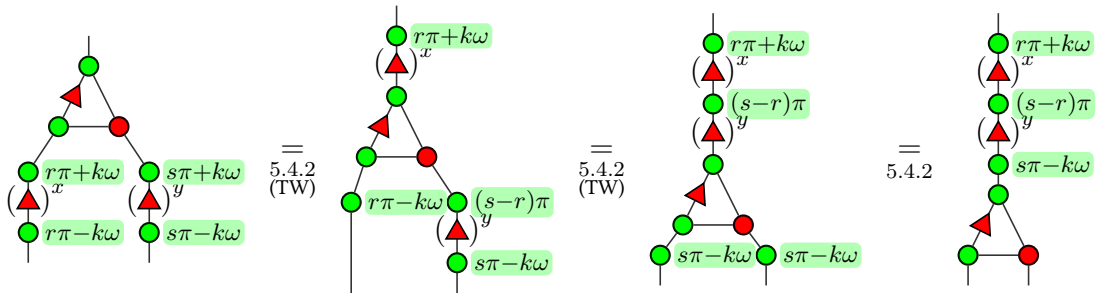
When paired with the cancellation rule, $\mathrm{ZX}_{\pi/4}$ becomes $\mathrm{ZX}_{\mathbb{Q}}$.

To prove the equation $\Gamma_{\frac{\pi}{4n}}(\Phi_{8n}) =$  on cyclotomic polynomials, we need to be able to perform the sum and the product of polynomials:

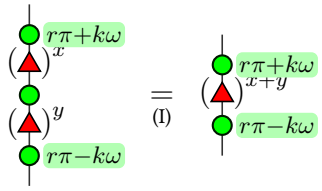
Lemma 5.7.3. *For any polynomials P and Q in $\mathbb{Z}[X]$:*

$\mathrm{ZX}_{\pi/4} \vdash$ 

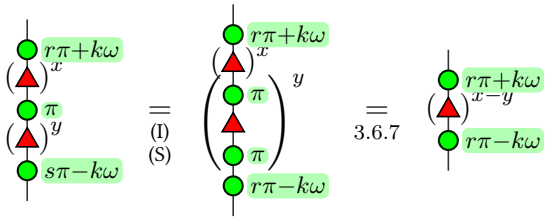
Proof ▶ First, if $x, y \in \mathbb{N}$:



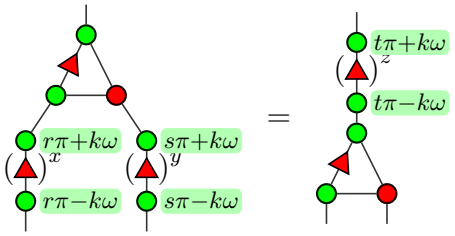
If $r = s$:



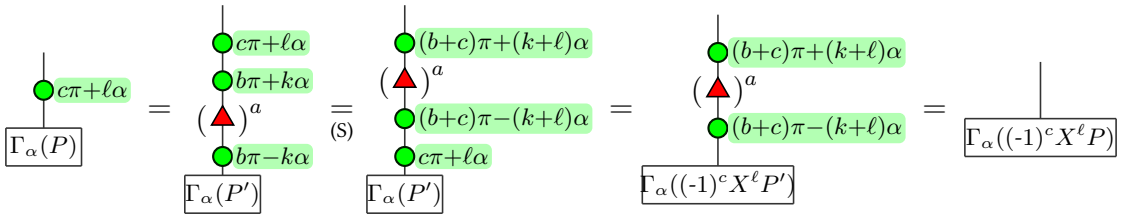
Otherwise, if $r \neq s$ and $x \geq y$:



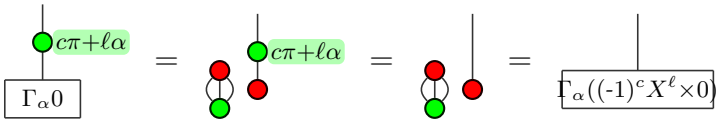
The case $r \neq s$ and $x \leq y$ is similar. In the end:



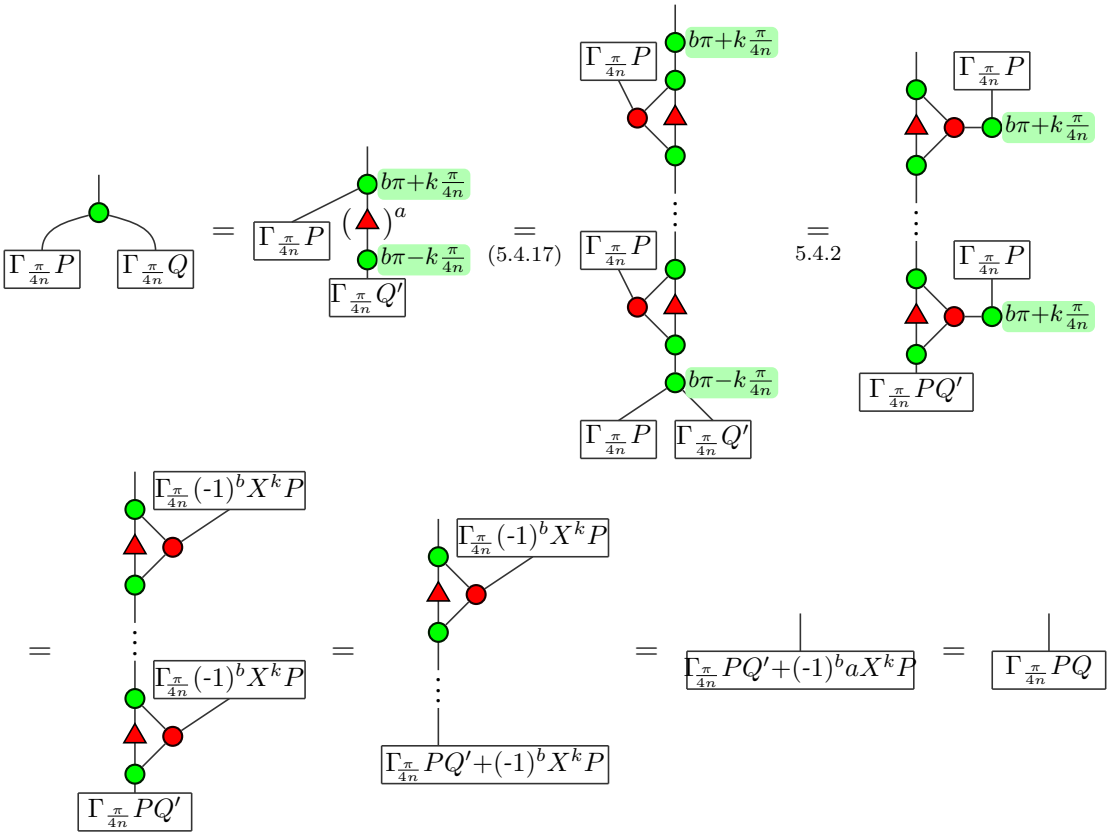
with $(-1)^t z = (-1)^r x + (-1)^s y$. The result for the sum immediately follows by induction (if 0 is involved, the result is obvious). For the product, first, if $P(X) = P'(X) + (-1)^b a X^k$:



and



Then, if Q is non-null:



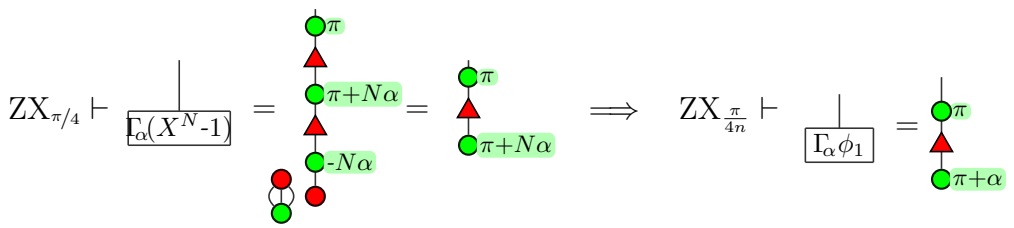
and if $Q = 0$, the result is obvious. ◀

Now, thanks to the new rule (Cancel) together with the previous lemma, we get:

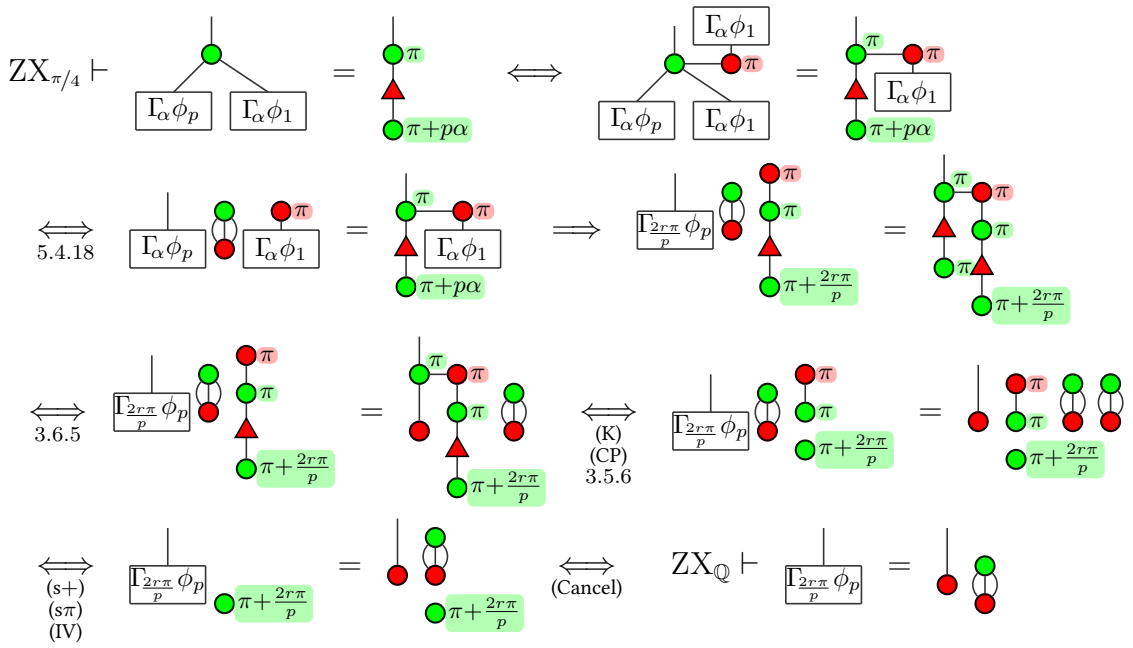
Proposition 5.7.4. *For any $n > 0$,*

$$\mathrm{ZX}_{\mathbb{Q}} \vdash \Gamma_{\frac{\pi}{4n}}(\Phi_{8n}) =$$ 

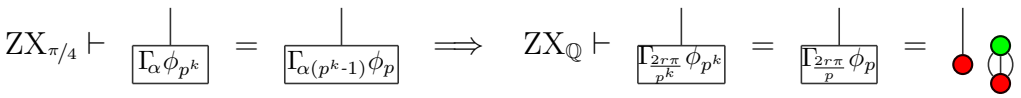
Proof ▶ First of all, we can easily derive for any N:



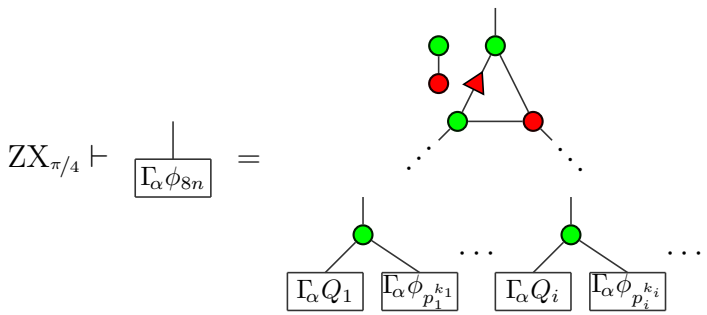
Now, assume p is prime. Then, $\phi_1(X)\phi_d(X) = \prod_{d|p} \phi_d(X) = X^p - 1$. Since sums and products of control polynomials are derivable in ZX (Lemma 5.7.3), it means:

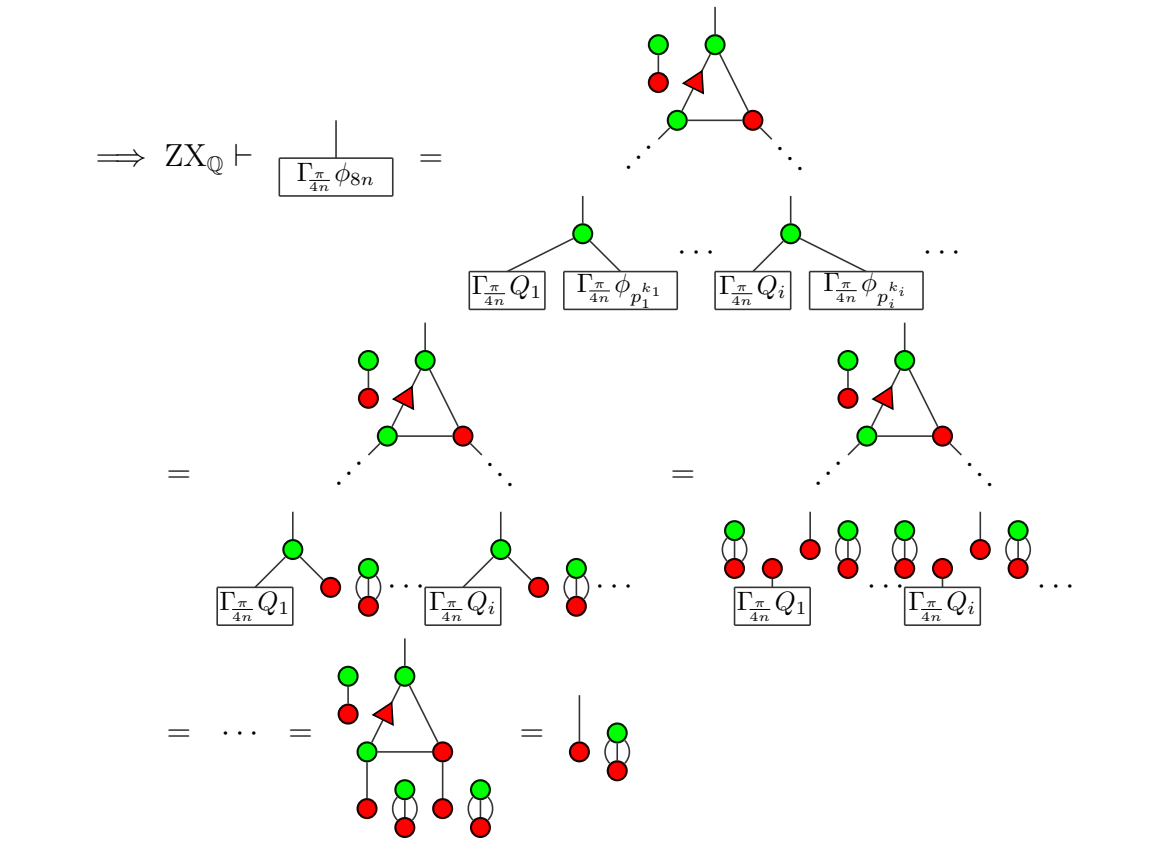


Now, if p is still prime, the case of p^k is handled with the equation $\phi_{p^k}(X) = \phi_p(X^{p^{k-1}})$ which translates as:



Finally, in the general case, let $8n = \prod_i p_i^{k_i}$ with all p_i primes. Then, the polynomial ϕ_{8n} is $\phi_{8n}(X) = \gcd_i\left(\phi_{p_i^{k_i}}(X^{p_i^{k_i-1}})\right)$. By Bézout's identity, $\phi_{8n}(X) = \sum_i Q_i(X)\phi_{p_i^{k_i}}(X^{p_i^{k_i-1}})$ where the Q_i are some unitary polynomials. This translates as:





◀

We show in the next subsection that the ZX-calculus augmented with the new cancellation rule makes the ZX-calculus complete for rational angles.

Normal forms

First, let $F \in \mathcal{F}_{\mathbb{Q}} \setminus \mathcal{F}_{\mathbb{D}}$ be finite. Then, there exists n such that F is generated by $\frac{\pi}{4n}$ (i.e. $F = \{\frac{k\pi}{4n} \mid k \in \mathbb{N}\}$), and for any x in $\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$, there exists a polynomial $P \in \mathbb{D}[X]$ such that $x = P(e^{i\frac{\pi}{4n}})$.

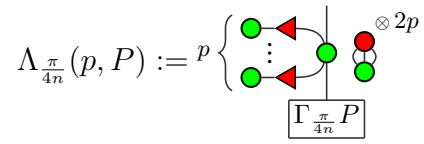
This representation is not ideal. First of all, we can factor the powers of $\frac{1}{2}$ and write P as $\frac{1}{2^p}Q$ where $Q \in \mathbb{Z}[X]$. The power p can be uniquely chosen if we ensure that Q is not a multiple of 2 if $p > 0$ i.e. $\forall Q' \in \mathbb{Z}[X], p > 0 \implies Q \neq 2Q'$.

This expression is still not unique, because the evaluation of two different polynomials in $e^{i\frac{\pi}{4n}}$ can yield the same value (e.g. $(e^{i\frac{\pi}{4n}})^{8n} = 1$). To palliate this problem, we need to work in $\mathbb{Z}[X]/\phi_{8n}(X)$ where ϕ_{8n} is the $8n^{\text{th}}$ cyclotomic polynomial. Indeed, ϕ_{8n} is the unique irreducible polynomial with $e^{\frac{2i\pi}{8n}}$ as root. Then, applying the Euclidean division of Q by ϕ_{8n}:

$$Q = Q'\phi_{8n} + R \tag{DIV}$$

where R and Q' are uniquely chosen so that $\deg(R) < \deg(\phi_{8n}) = \varphi(8n)$. Then, $Q(e^{i\frac{\pi}{4n}}) = R(e^{i\frac{\pi}{4n}})$.

⌜ **Definition 5.7.5:** Let $\Lambda_{\frac{\pi}{4n}} : \mathbb{N} \times \mathbb{Z}[X] \to \mathbf{ZX}[1 \to 0]$ be the map such that

$\Lambda_{\frac{\pi}{4n}}(p, P) :=$ 

We then define $S_{\frac{\pi}{4n}} := \left\{ \Lambda_{\frac{\pi}{4n}}(p, P) \;\middle|\; \begin{array}{l} P \in \mathbb{Z}[X],\ p \in \mathbb{N}, \\ \deg(P) < \varphi(8n), \\ \forall Q \in \mathbb{Z}[X],\ p > 0 \implies P \neq 2Q \end{array} \right\}$ ⌟

Remark 5.7.6. Notice that if $P = 0$, only $\Lambda_{\frac{\pi}{4n}}(0, 0)$ is part of $S_{\frac{\pi}{4n}}$. Indeed, if $P = 0$, then $P = 2 \times 0 = 2P$, so the last constraint imposes that $p = 0$.

Lemma 5.7.7. $[\![\Lambda_{\frac{\pi}{4n}}(p, P)]\!] \, |1\rangle = \frac{1}{2^p} P(e^{i\frac{\pi}{4n}})$

Proof ▶ By construction. ◀

Moreover:

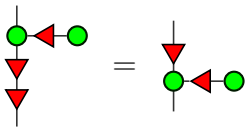
Lemma 5.7.8. *The map* $\eta_{\frac{\pi}{4n}} : S_{\frac{\pi}{4n}} \to \mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}] = D \to [\![D]\!] \, |1\rangle$ *is bijective.*

Proof ▶ Every element of $\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]$ is uniquely defined as the quantity $\frac{1}{2^p} P(e^{i\frac{\pi}{4n}})$ where $\deg(P) < \varphi(8n)$, and $\forall Q \in \mathbb{Z}[X],\ p > 0 \implies P \neq 2Q$. ◀

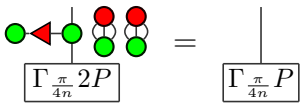
We now need to meet the conditions of Theorem 5.3.1. First we notice that we can operate the sum and the product on controlled polynomials thanks to Lemma 5.7.3.

Two problems arise when trying to do the same with diagrams of $S_{\frac{\pi}{4n}}$. First of all, the sum of two diagrams in normal form can have a parity issue. For instance $\frac{1}{2}(2 + X) + \frac{1}{2}(X + 2X^2) = \frac{1}{2}(2 + 2X + 2X^2)$ which shall be reduced to $1 + X + X^2$. This is dealt with thanks to the following lemmas:

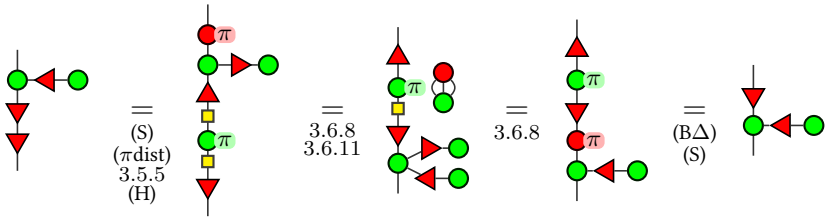
Lemma 5.7.9.



Lemma 5.7.10.

$\mathrm{ZX}_{\pi/4} \vdash$ 

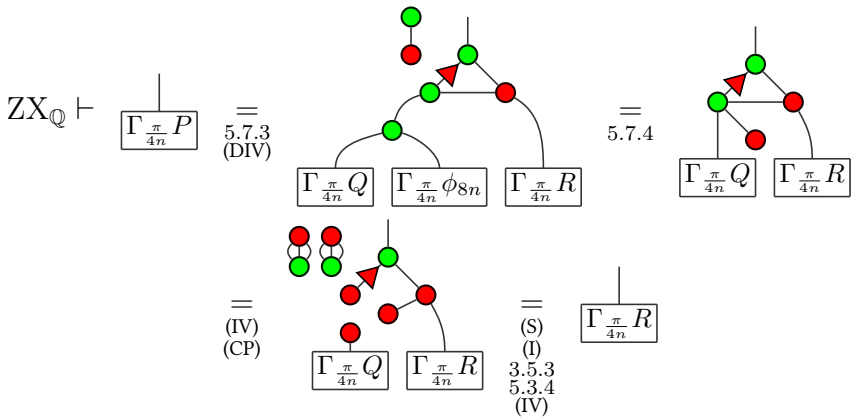
Proof ▶ First:



The second lemma is then proven by induction, using Lemma 5.7.9. ◀

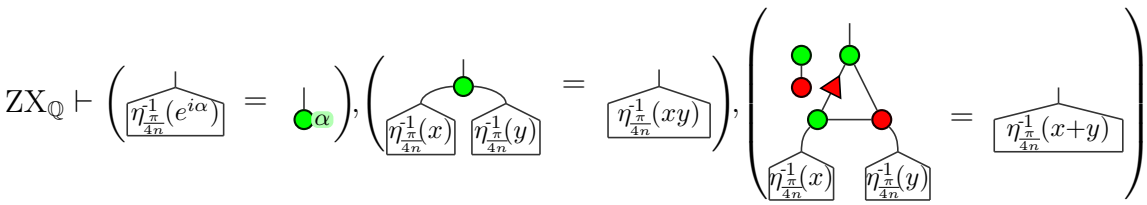
Secondly, the product of two polynomials may well end up with a degree larger than $\varphi(8n)$. However, since we can operate the sum and product of controlled polynomials

thanks to Lemma 5.7.3, we can derive the controlled version of the Euclidean division (DIV). Combined with Lemma 5.7.4, we get, assuming $P = Q\phi_{8n} + R$:

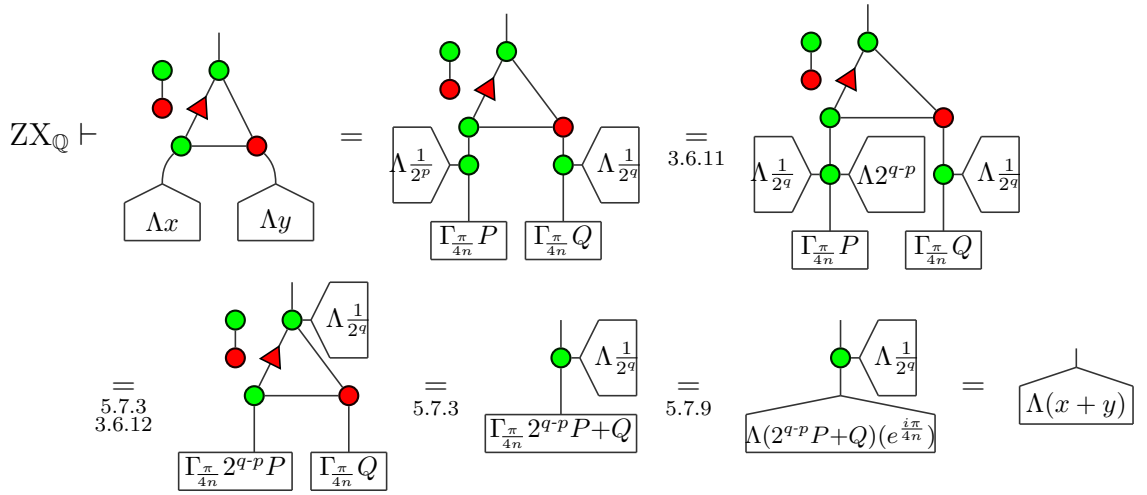


All in all, any controlled scalar in the form $\Lambda_{\frac{\pi}{4n}} P$ can be reduced to a diagram in $S_{\frac{\pi}{4n}}$.

Lemma 5.7.11.



Proof ▶ The product is obvious when we have Lemmas 5.7.3 and 5.7.4. For the sum, let $x = \frac{1}{2^p} P(e^{i\frac{\pi}{4n}})$, $y = \frac{1}{2^q} Q(e^{i\frac{\pi}{4n}})$. W.l.o.g., assume $p \leq q$. Then:



The ante-penultimate diagram may not directly be in normal form, for there may be S such that $2^{q-p} P + Q = 2S$, but this is dealt with with Lemma 5.7.9. ◀

Theorem 5.7.12. *The language* $\mathbf{ZX}[\frac{\pi}{4n}]/\,\mathrm{ZX}_{\mathbb{Q}}$ *is complete, the functor* $\mathbf{ZX}[\frac{\pi}{4n}]/\,\mathrm{ZX}_{\mathbb{Q}} \xrightarrow{[\![\cdot]\!]} \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{i\frac{\pi}{4n}}]}$ *is full and faithful.*
Moreover, any $\mathbf{ZX}[\frac{\pi}{4n}]$*-diagram can be put into a normal form with respect to* $S_{\frac{\pi}{4n}}$.

Proof ▶ By application of Theorem 5.3.1. ◀

Corollary 5.7.13. *For any $F \in \mathcal{F}_{\mathbb{Q}}$ (finite or not), the language $\mathbf{ZX}[F]/\operatorname{ZX}_{\mathbb{Q}}$ is complete, the functor $\mathbf{ZX}[F]/\operatorname{ZX}_{\mathbb{Q}} \xrightarrow{[\![.]\!]} \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}$ is faithful.*
Moreover, any $\mathbf{ZX}[F]$-diagram can be put into a normal form with respect to $S_F := \bigcup_{\frac{\pi}{4n} \in F} S_{\frac{\pi}{4n}}$.

Proof ▶ Let F be a subgroup of $\mathbb{Q}\pi$, and D_1 and D_2 be two diagrams of the fragment F, such that $[\![D_1]\!] = [\![D_2]\!]$. If F is finite, Theorem 5.7.12 directly gives the result. Otherwise, there exists $n \in \mathbb{N}$ such that $\frac{\pi}{4n} \in F$ and both diagrams are in the $\frac{\pi}{4n}$-fragment of the ZX-calculus. By completeness (Theorem 5.7.12): $\operatorname{ZX}_{\mathbb{Q}} \vdash D_1 = D_2$. ◀

The completeness for $\mathbb{Q}\pi$ is obtained thanks to the meta-rule (Cancel). It can be beneficial to avoid second-order axioms like this one. Thankfully, it has been proven later on that the axiomatisation $\operatorname{ZX}_{\pi/4}$ together with the family of axioms (SUP_p) made $\mathbf{ZX}[\mathbb{Q}\pi]$ complete [Jea18].

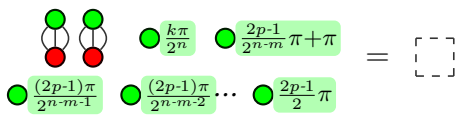
Theorem 5.7.14 ([Jea18]). *The functor $\mathbf{ZX}[\mathbb{Q}\pi]/\operatorname{ZX}_{\pi/4} + (\text{SUP}_p) \xrightarrow{[\![.]\!]} \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{i\mathbb{Q}\pi}]}$ is full and faithful.*

5.8 Normal Forms with Dyadic Angles

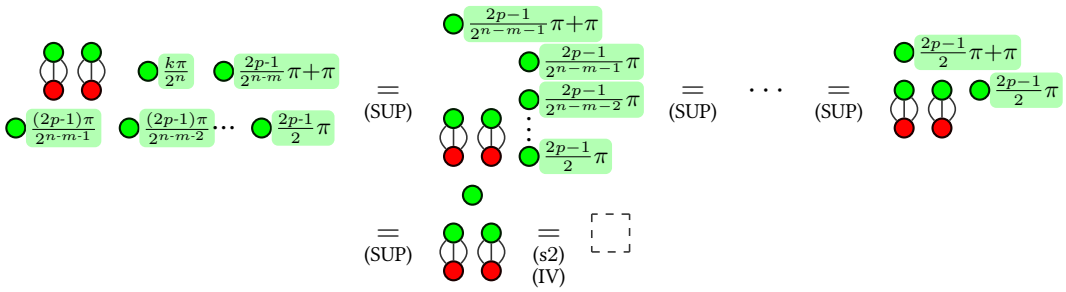
In this section we focus on a particular case of dyadic angles, a subgroup of $\mathbb{D}\pi$ which contains $\frac{\pi}{4}$ (i.e. $F \in \mathcal{F}_{\mathbb{D}}$). In the previous section, we introduced the cancellation rule which makes the $\operatorname{ZX}_{\pi/4}$ complete for rational angles.

Notice that, given a fragment $F \in \mathcal{F}$, the cancellation rule can be derived from the other rules if for every $\alpha \in F$, $\alpha \neq 0 \bmod \pi$, there exists an inverse of α, i.e. a diagram $D : 0 \to 0 \in \mathbf{ZX}[F]$ s.t. $[\![D \otimes \alpha]\!] = 1$, and moreover this equation is provable: $\operatorname{ZX}_{\pi/4} \vdash D \otimes \alpha =$. This is the case in any fragment of dyadic angles:

Lemma 5.8.1. *For any $n \geq 1$, and any $k \in \{-2^n + 1, \cdots, 2^{n+1} - 1\}$, $\frac{k\pi}{2^n}$ has an inverse. There exist $0 \leq m < n$ and $p \in \mathbb{Z}$ such that:*



Proof ▶ If $k \in \{-2^n + 1, \cdots, 2^{n+1} - 1\}$, then there exist $0 \leq m < n$ and $p \in \mathbb{Z}$ such that $k = 2^m(2p-1)$i.e. $\frac{k\pi}{2^n} = \frac{2p-1}{2^{n-m}}\pi$ where $2^{n-m} \geq 2$. Then:



◀

Theorem 5.8.2. *For any $n \geq 2$, the language $\mathbf{ZX}[\frac{\pi}{2^n}]/\operatorname{ZX}_{\pi/4}$ is complete, the functor $\mathbf{ZX}[\frac{\pi}{2^n}]/\operatorname{ZX}_{\pi/4} \overset{[\![.]\!]}{\to} \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{i\frac{\pi}{2^n}}]}$ is full and faithful.*
Any $\mathbf{ZX}[\frac{\pi}{2^n}]$-diagram can be put into a normal form with respect to $S_{\frac{\pi}{2^n}} = S_{\frac{\pi}{4\times 2^{n-2}}}$.

Corollary 5.8.3. *For any $F \in \mathcal{F}_{\mathbb{D}}$ (finite or not), the language $\mathbf{ZX}[F]/\operatorname{ZX}_{\pi/4}$ is complete, the functor $\mathbf{ZX}[F]/\operatorname{ZX}_{\pi/4} \overset{[\![.]\!]}{\to} \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{\sqrt{2}}, e^{iF}]}$ is faithful.*
Any $\mathbf{ZX}[F]$-diagram can be put into a normal form with respect to $S_F := \bigcup_{\frac{\pi}{2^n} \in F} S_{\frac{\pi}{2^n}}$.

Proof ▶ The proof is the same as that of Corollary 5.7.13, except we use the completeness of $\mathbf{ZX}[\frac{\pi}{2^n}]/\operatorname{ZX}_{\pi/4}$ (Theorem 5.8.2). ◀

5.9 Normal Forms for Linear Diagrams

We show in this section that we can extend the results of universality and completeness to linear diagrams, and at no cost. We take $F \in \mathcal{F}$ an arbitrary fragment that contains $\frac{\pi}{4}$. The standard interpretation is a functor $[\![.]\!] : \mathbf{ZX}[F] \to \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$, which is full by Theorem 5.2.10. Recall that when extending ZX-diagrams to linear diagrams, the interpretation became $[\![.]\!] : \mathbf{ZX}[\vec{\alpha}, F] \to \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$ where:

$$\mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]} = \left\{ \vec{\alpha} \mapsto P(e^{i\alpha_1}, \ldots, e^{i\alpha_k}) \;\middle|\; P \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}[X_1, \ldots, X_k] \right\}$$

We can now easily show that this functor is full.

Theorem 5.9.1. *For any $F \in \mathcal{F}$, $\mathbf{ZX}[\vec{\alpha}, F]$ is universal for $\mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$:*

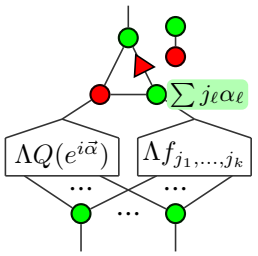
$$\forall f \in \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]},\ \exists D \in \mathbf{ZX}[\vec{\alpha}, F],\ [\![D]\!] = f$$

In other words, the functor $\mathbf{ZX}[\vec{\alpha}, F] \overset{[\![.]\!]}{\to} \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$ is full.

Proof ▶ By map/state duality, we can w.l.o.g. restrict ourselves to states. Let $f : 0 \to n \in \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$. Then, there exists P a multivariate polynomial on k variables with coefficients in $\mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$ such that $f = \vec{\alpha} \mapsto P(e^{i\alpha_1}, \ldots, e^{i\alpha_k})$. Every element of $\mathbb{Z}[\frac{1}{2}, e^{iF}]$ can be controlled, so using construction Λ of Definition 5.3.3, we can build Λg for every $g \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$, hence every coefficient of P can be associated with a diagram that controls it.

We can then extend Λ to linear diagrams inductively as:

$$\left(\vec{\alpha} \mapsto f_{j_1,\ldots,j_k} e^{i\sum j_\ell \alpha_\ell} + Q(e^{i\alpha_1}, \ldots, e^{i\alpha_k})\right) \mapsto$$



It is then routine to show that:

$$[\![\Lambda f]\!]\,|1\rangle = [\![\Lambda\left(\vec{\alpha} \mapsto P(e^{i\alpha_1}, \ldots, e^{i\alpha_k})\right)]\!]\,|1\rangle = \vec{\alpha} \mapsto P(e^{i\alpha_1}, \ldots, e^{i\alpha_k}) = f$$

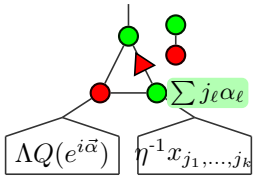
◀

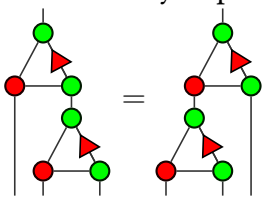
Fullness is not the only property that is preserved when extending to linear diagrams. We also have:

Theorem 5.9.2. *Let $F \in \mathcal{F}$. If there exists $S \subseteq \mathbf{ZX}[F]$ a set of controlled scalars such that the map $\eta : S \to \mathbb{Z}[\frac{1}{2}, e^{iF}] = D \mapsto [\![D]\!]\,|1\rangle$ is bijective, if $R \vdash \mathrm{ZX}_{\pi/4}+(\mathrm{Cond})$, then $\mathbf{ZX}[\vec{\alpha}, F]/R$ is complete i.e. the functor $\mathbf{ZX}[\vec{\alpha}, F]/R \xrightarrow{[\![.]\!]} \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$ is faithful.*

Proof ▶ Let $x \in \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}[0, 0]$. There exists $P \in \mathbb{Z}[\frac{1}{2}, e^{iF}][X_1, \ldots, X_k]$ such that $x = \vec{\alpha} \mapsto P(e^{i\alpha_1}, \ldots, e^{i\alpha_k})$. Since η is surjective, we can define inductively Λx:

$$\left(\vec{\alpha} \mapsto x_{j_1,\ldots,j_k} e^{i\sum j_\ell \alpha_\ell} + Q(e^{i\alpha_1}, \ldots, e^{i\alpha_k})\right) \mapsto$$



Notice that any ambiguity can be lifted by imposing an ordering on the powers in Q, or diagrammatically thanks to  . We can then define $S_{\vec{\alpha}} := \{\Lambda x \mid x \in \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}[0, 0]\}$. We can then notice that the map $\eta_{\vec{\alpha}} : S_{\vec{\alpha}} \to \mathbf{Qubit}^{\mathbb{R}^k}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}[0, 0] = D \mapsto [\![D]\!]\,|1\rangle$ is bijective by uniqueness of P in $x = \vec{\alpha} \mapsto P(e^{i\alpha_1}, \ldots, e^{i\alpha_k})$.

One can then check that the compositions of normal forms are still valid with variables. Any diagram of $\mathbf{ZX}[\vec{\alpha}, F]$ can hence be put in normal form.

◀

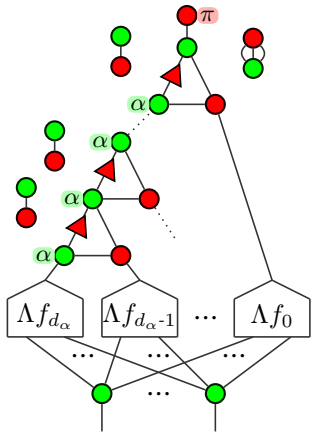
Notice that this result is a refinement of Theorem 4.2.1, for here the "constant" diagrams of $\mathbf{ZX}[F]$ need a normal form. However we see that in this case the notion of normal naturally extends to linear diagrams of the same fragment.

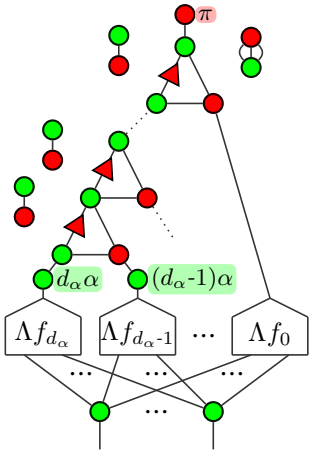
Factoring

Let $F \in \mathcal{F}$, and let $f \in \mathbf{Qubit}^{\mathbb{R}}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$, i.e. f has only one variable. Every entry of f is of the form of $P(e^{i\alpha})$ where P is a polynomial with coefficients in $\mathbb{Z}[\frac{1}{2}, e^{iF}]$. f can actually be seen as $f = \sum f_k e^{ik\alpha}$ with $f_k \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$. We can naturally define a notion of degree of α in f, $d_\alpha(f)$, as the largest value of k for which $f_k \neq 0$. Then, we can build a $\mathbf{ZX}[\alpha, F]$-diagram that represents f using only d_α occurrences of α.

Proposition 5.9.3. *Let $F \in \mathcal{F}$, and $f \in \mathbf{Qubit}^{\mathbb{R}}_{\mathbb{Z}[\frac{1}{2}, e^{iF}]}$. Let d_α be the degree of the variable α in f. There exists a $\mathbf{ZX}[\alpha, F]$-diagram D_1 with d_α occurrences of α and no occurrence of $k\alpha$ for $k > 1$, such that $[\![D_1]\!] = f$. There also exists a $\mathbf{ZX}[\alpha, F]$-diagram D_2 with at most one occurrence of $k\alpha$ for each $k \in \{1, \ldots, d_\alpha\}$ such that $[\![D_2]\!] = f$.*

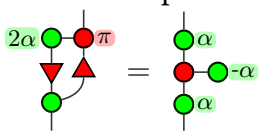
Proof ▶ Let $f : 0 \to n \in \mathbf{Qubit}^{\mathbb{R}}_{\mathbb{Z}[\frac{1}{2},e^{iF}]}$. There exist $f_k \in \mathbf{Qubit}_{\mathbb{Z}[\frac{1}{2},e^{iF}]}$ such that $f = \sum f_k e^{ik\alpha}$. We can build a diagram that represents their controlled version Λf_k. These diagrams are in in $\mathbf{ZX}[F]$. We define D_1 and D_2 as:

$D_1 :=$ 

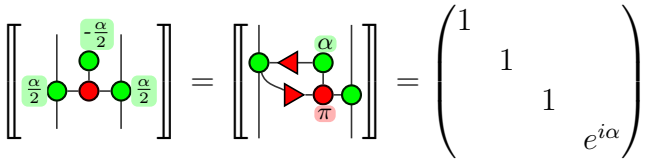
$D_2 :=$ 

Both diagrams use the sum of controlled scalars. D_2 directly represents $\sum f_k e^{ik\alpha}$, while D_1 represents the Horner expansion $f = f_0 + e^{i\alpha}(f_1 + e^{i\alpha}(\ldots))$. Notice that we can easily transform one into the other using Lemma 5.4.2. ◀

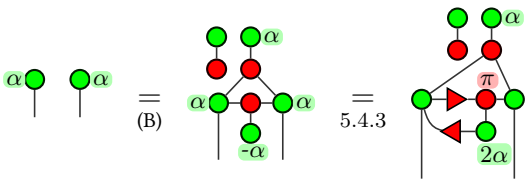
Example 5.9.4. The quantum Fourier transform on n wires is in the $\frac{\pi}{2^n}$-fragment. The usual quantum circuit implementing it with the gate set (H, $R_Z(\alpha)$, CNot) uses $3(n-2)$ occurrences of $\frac{\pi}{8}$, $3(n-3)$ occurrences of $\frac{\pi}{16}$, ..., and 3 occurrences of $\frac{\pi}{2^n}$. In ZX-Calculus, the QFT can be represented with $n-2$ occurrences of $\frac{\pi}{2^n}$ and zero occurrence of $\frac{\pi}{2^j}$ with $3 \leq j < n$; or with exactly one occurrence of each $\frac{\pi}{2^j}$ for $3 \leq j \leq n$.

One way to reduce the count of phases outside Clifford+T, is to use the seemingly innocent Lemma 5.4.3: 

. This is actually pretty powerful. Indeed, notice that



Hence it represents the control of the phase α. While this is usually obtained thanks to the half phase $\frac{\alpha}{2}$ (first diagram), it can be done with one occurrence of α and a diagram of $\mathbf{ZX}[\frac{\pi}{4}]$ (actually of $\Delta\mathbf{ZX}[\pi]$). Thanks to this, we can create a diagram that given an angle α copies  while only using angles in $\frac{\pi}{4}\mathbb{Z} \cup \{2\alpha\}$:



Doing this transformation inductively (together with (S) and (H)), we can get rid of all occurrences of α except one. We can then use the same process to remove all occurrences of 2α but one, etc...

Conclusion

In this thesis, we have provided axiomatisations for different fragments and extensions of the graphical language ZX-Calculus, used for quantum computing. For each axiomatisation, we proved its completeness, thanks to mainly two proof methods. The first one is a transport of completeness from one language to another, using adequate systems of translations. The starting point for this method is the completeness of two fragments of the ZW-Calculus, another graphical language for quantum computing in which there exists a nice notion of normal form. The second method is precisely to define normal forms directly in the ZX-Calculus.

A problem related to that of completeness, and addressed for one of the axiomatisations is minimality. For most of the provided axiomatisation, it is as of now unclear whether all the rules are necessary, or if they can be simplified, although a great deal of work was made in order to provide the simplest axiomatisations possible. This question is all the more relevant for the two rules (BW) and (C) of $\mathrm{ZX}_{\pi/4}$.

Now thanks to the completeness of the language, any reasoning can theoretically be performed inside the ZX-Calculus itself. However, some questions can still be hard to answer. We can now check whether two diagrams are equivalent by turning them into their normal forms. This is however not efficient, so it could be beneficial to find invariants of the calculus. An obvious one is the number of input and output wires. Also, in any fragment that does not contain $\frac{\pi}{4}$, there exists an invariant [JPVW17]. Can we find other invariants, ideally that work in any fragment?

So far the strategies for simplification used for instance in [DG18] or [KvdW19] do not use axioms outside $\mathrm{ZX}_{\pi/2}$. A research direction would hence be to find such strategies, that for instance require (BW) or (C). More generally, it would be interesting now to find applications of the ZX-Calculus that use the larger axiomatisations. I am currently working on an adaptation of sum-over-paths [Amy19] for ZX-diagrams, with in mind the idea of seeing how a variable reduction in the sum-over-path formalism shows in the associated ZX-diagram.

In the proof of completeness of $\mathbf{ZX}/\mathrm{ZX}$, we introduced the SVD form of cycle-free $0 \to 1$ and $1 \to 1$ ZX-diagrams. Although this was enough for the proof, since this form derives from the SVD decomposition of the underlying matrix, one could definitely define the SVD form for any ZX-diagram. This could be an interesting alternative normal form, with practical applications.

Still concerning the axiomatisation ZX, we have shown in the ZX-Calculus that adding a rule characterising one-qubit unitaries (EU) to a complete set of rules for the many-qubit Clifford fragment ($\mathrm{ZX}_{\pi/2}$) was enough to get the completeness in the unrestricted language. A natural question is now whether this is true for quantum circuits as well (we know a complete axiomatisation for Clifford and (EU) can easily be expressed

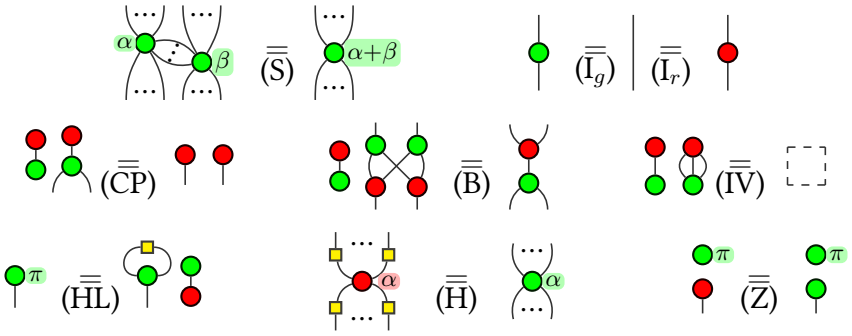
in this formalism), or are the specific features of the ZX-Calculus (such as the compact-closed structure) necessary?

Finally, one last research direction for the ZX axiomatisations, would be to provide adequate and ideally complete languages for qudit quantum computing.

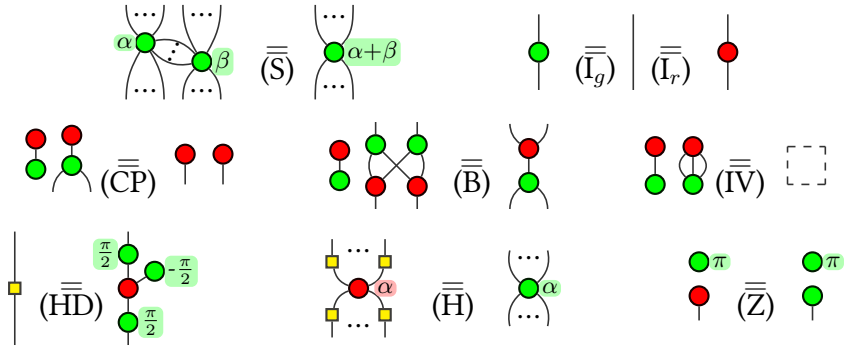
Cheat Sheet

Axiomatisations

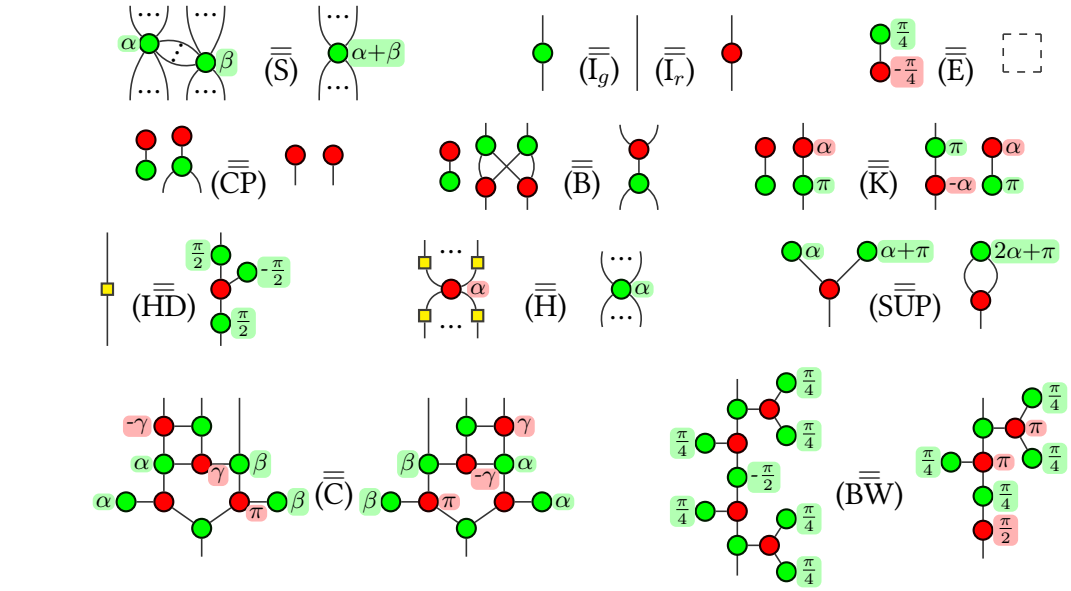
ZX$_{\pi}$



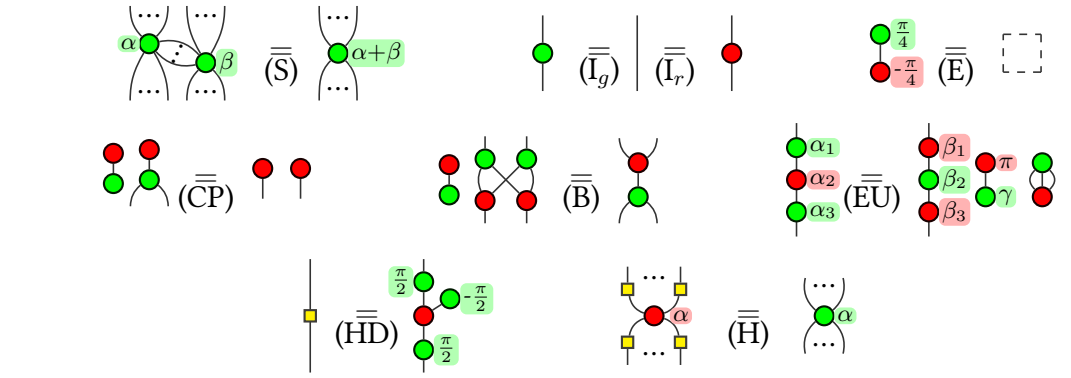
ZX$_{\pi/2}$



$\mathrm{ZX}_{\pi/4}$

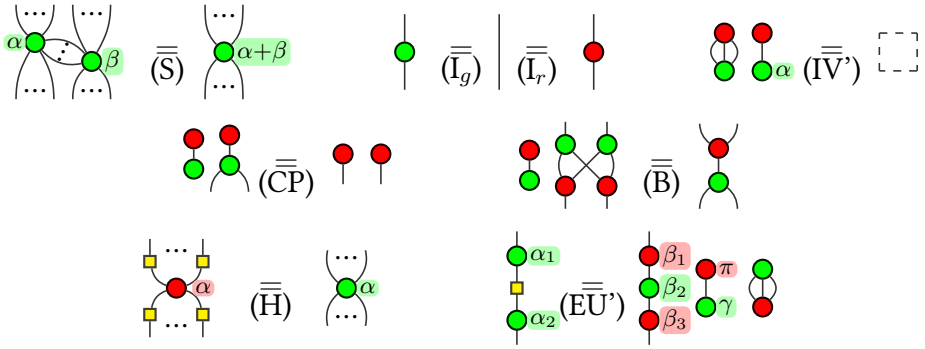


ZX



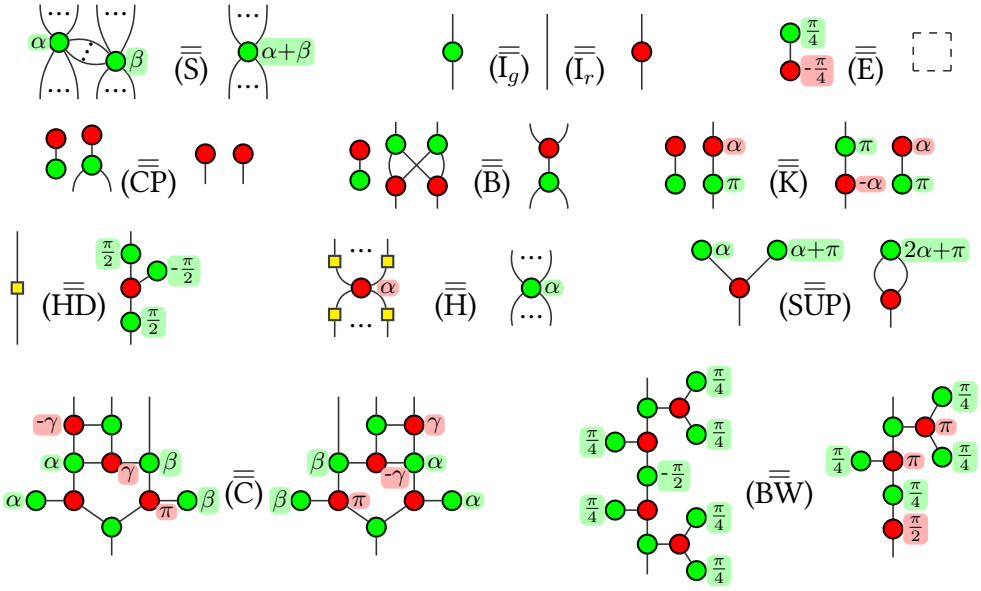
$x^+ := \frac{\alpha_1+\alpha_3}{2}$; $x^- := x^+ - \alpha_3$; $z := \cos\left(\frac{\alpha_2}{2}\right)\cos\left(x^+\right) + i\sin\left(\frac{\alpha_2}{2}\right)\cos\left(x^-\right)$; $z' := \cos\left(\frac{\alpha_2}{2}\right)\sin\left(x^+\right) - i\sin\left(\frac{\alpha_2}{2}\right)\sin\left(x^-\right)$; $\beta_1 = \arg z + \arg z$; $\beta_2 = 2\arg\left(i + \left|\frac{z}{z'}\right|\right)$; $\beta_3 = \arg z - \arg z'$; $\gamma = x^+ - \arg(z) + \frac{\alpha_2-\beta_2}{2}$;

ZX′



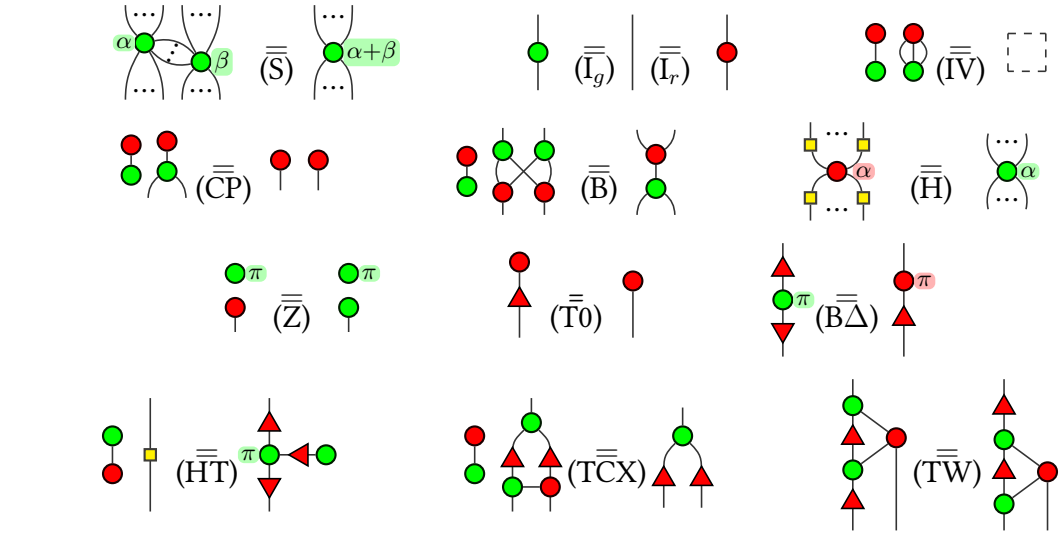
$x^+ := \frac{\alpha_1+\alpha_2}{2}$; $x^- := x^+ - \alpha_2$; $z := -\sin(x^+) + i\cos(x^-)$; $z' := \cos(x^+) - i\sin(x^-)$;
$\beta_1 = \arg z + \arg z'$; $\beta_2 = 2\arg\left(i + \left|\frac{z}{z'}\right|\right)$; $\beta_3 = \arg z - \arg z'$; $\gamma = x^+ - \arg(z) + \frac{\pi-\beta_2}{2}$

ZX$_\mathbb{Q}$

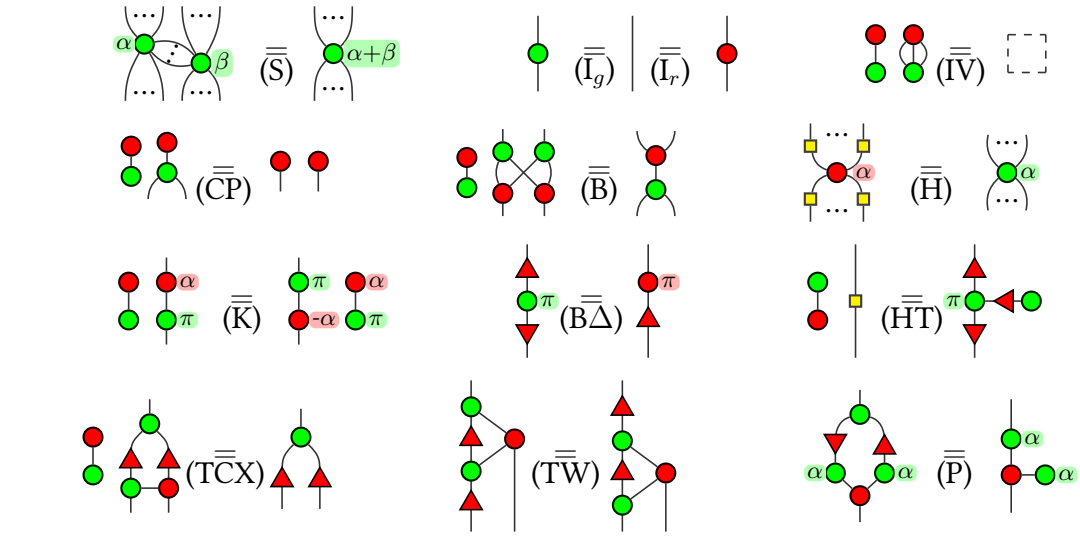


$\forall \alpha \neq \pi \bmod 2\pi, \quad \mathrm{ZX}_{\pi/4} \vdash D_1 \otimes \bullet\!\!\!\bullet\,\alpha = D_2 \otimes \bullet\!\!\!\bullet\,\alpha \underset{\text{(Cancel)}}{\Longrightarrow} \mathrm{ZX} \vdash D_1 = D_2$

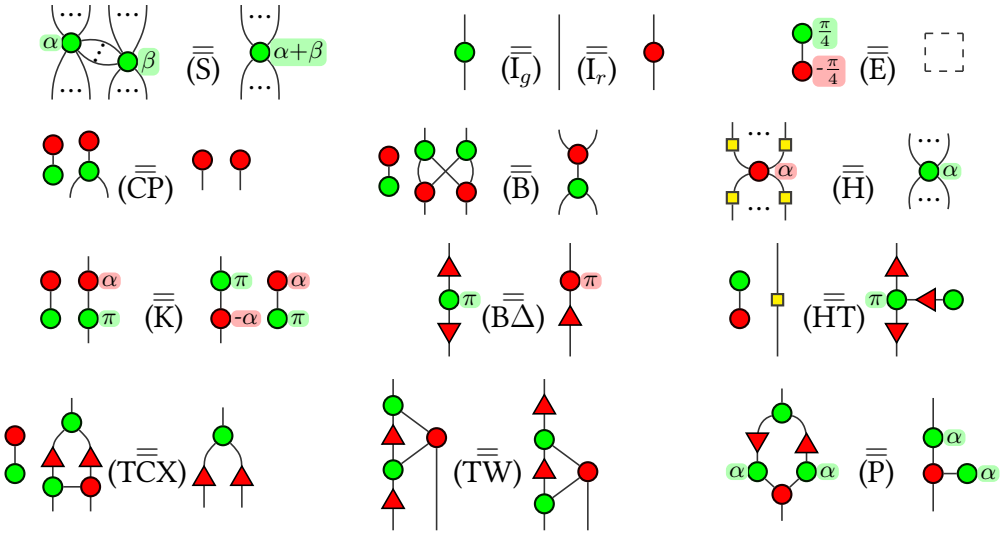
Δ_π



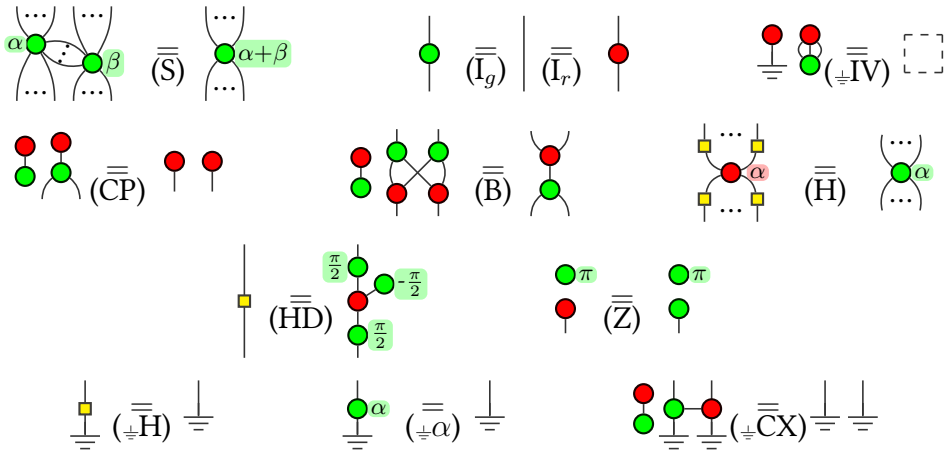
Δ_π^+



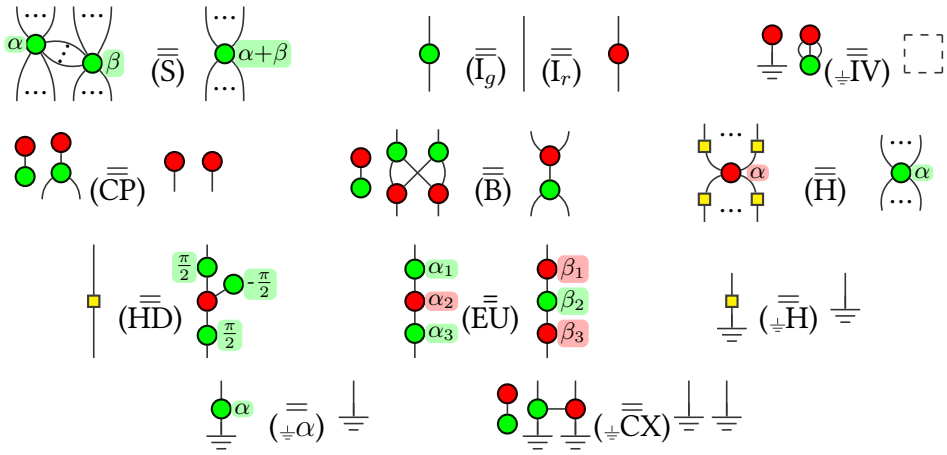
$\Delta_{\pi/4}$



$ZX^{\frac{1}{2}}_{\pi/2}$

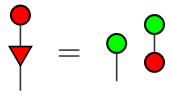


$ZX^{\frac{1}{2}}$

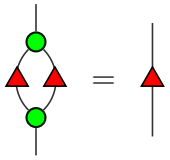


Lemmas

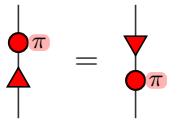
Lemma 3.5.3.



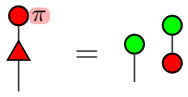
Lemma 3.5.4.



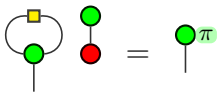
Lemma 3.5.5.



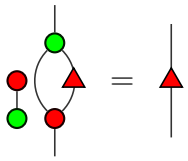
Lemma 3.5.6.



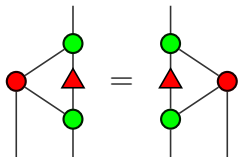
Lemma 3.5.7.



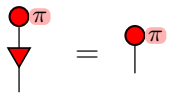
Lemma 3.6.2.



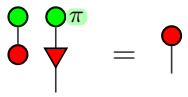
Lemma 3.6.3.



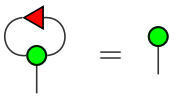
Lemma 3.6.4.



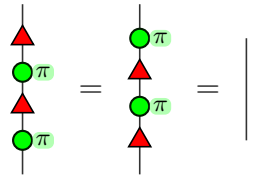
Lemma 3.6.5.



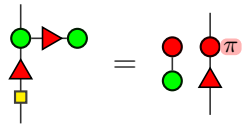
Lemma 3.6.6.



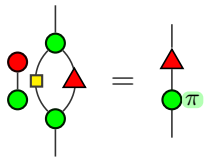
Lemma 3.6.7.



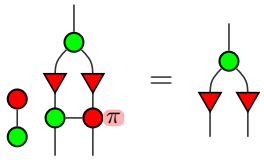
Lemma 3.6.8.



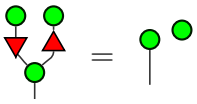
Lemma 3.6.9.



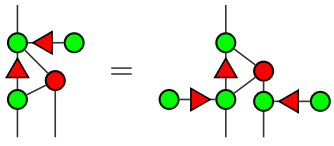
Lemma 3.6.10.



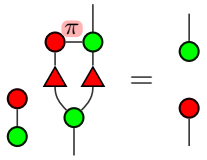
Lemma 3.6.11.



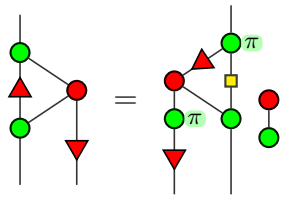
Lemma 3.6.12.



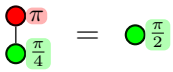
Lemma 3.6.13.



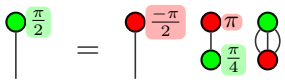
Lemma 3.6.14.



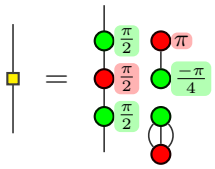
Lemma 3.8.3.



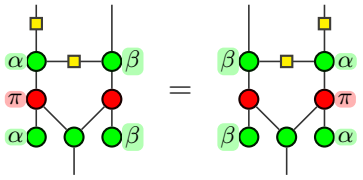
Lemma 3.8.4.



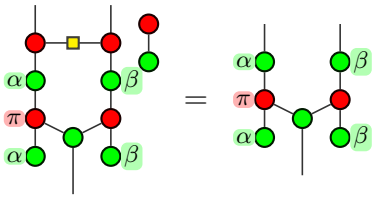
Lemma 3.8.5.



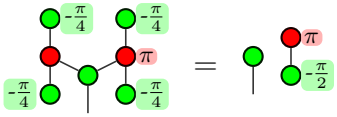
Lemma 3.8.6.



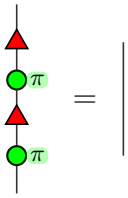
Lemma 3.8.7.



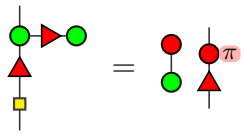
Lemma 3.8.8.



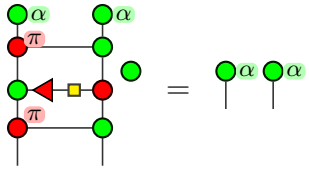
Lemma 3.8.9.



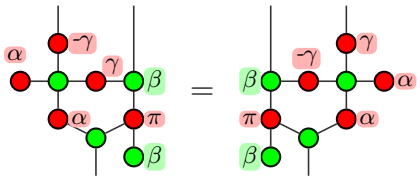
Lemma 3.8.10.



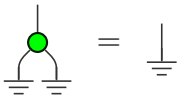
Lemma 3.8.11.



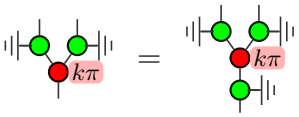
Lemma 3.8.12.



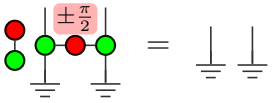
Lemma 4.10.25.



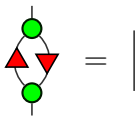
Lemma 4.10.26.



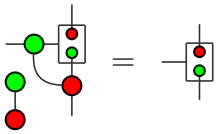
Lemma 4.10.27.



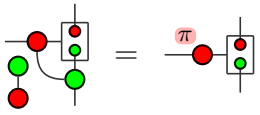
Lemma 5.1.1.



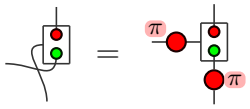
Lemma 5.1.4.



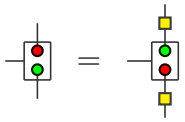
Lemma 5.1.5.



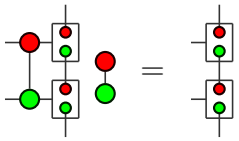
Lemma 5.1.6.



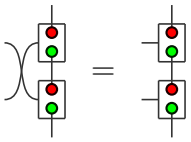
Lemma 5.1.7.



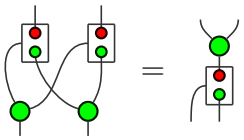
Lemma 5.1.8.



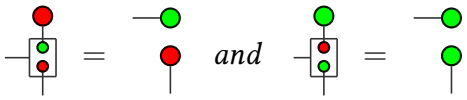
Lemma 5.1.9.



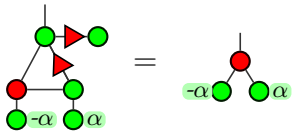
Lemma 5.1.10.



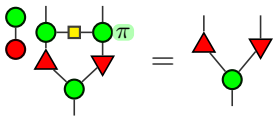
Lemma 5.1.11.



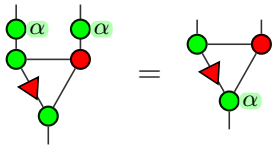
Lemma 5.3.5.



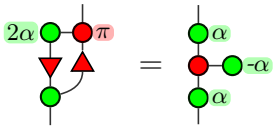
Lemma 5.4.1.



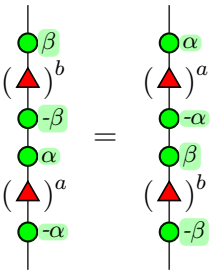
Lemma 5.4.2.



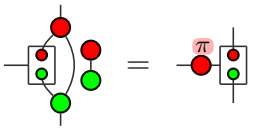
Lemma 5.4.3.



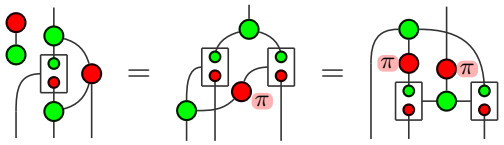
Lemma 5.4.4.



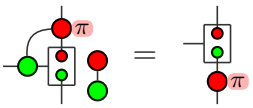
Lemma 5.4.5.



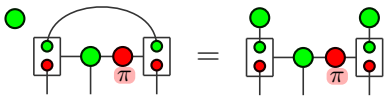
Lemma 5.4.6.



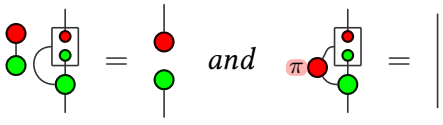
Lemma 5.4.7.



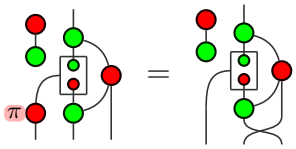
Lemma 5.4.8.



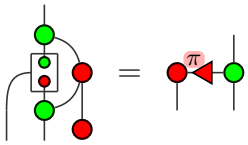
Lemma 5.4.9.



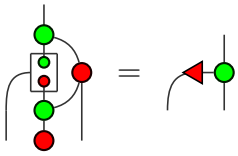
Lemma 5.4.10.



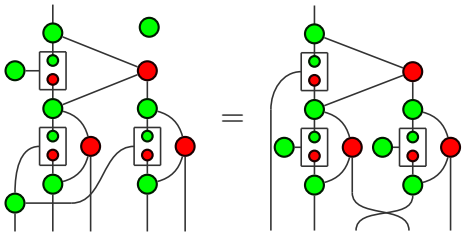
Lemma 5.4.11.



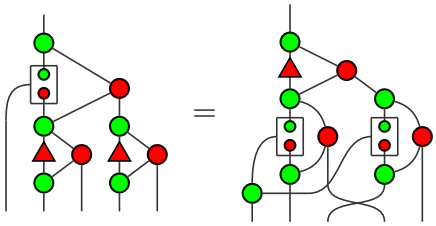
Lemma 5.4.12.



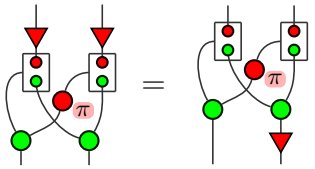
Lemma 5.4.13.



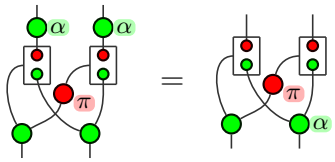
Lemma 5.4.14.



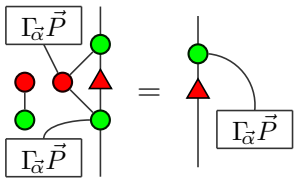
Lemma 5.4.15.



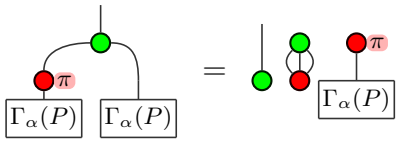
Lemma 5.4.16.



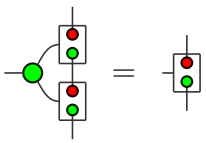
Lemma 5.4.17.



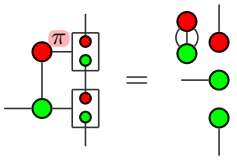
Lemma 5.4.18.



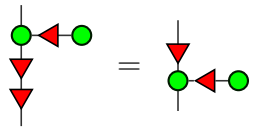
Lemma 5.5.4.



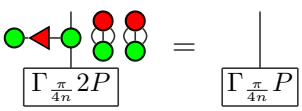
Lemma 5.5.5.



Lemma 5.7.9.



Lemma 5.7.10.

$\mathrm{ZX}_{\pi/4} \vdash$ 

Index

Bibliography

[AB06] Charalambos D. Aliprantis and Kim C. Border. *Infinite-dimensional analysis*. Springer; 3rd edition, 2006.

[AC04] S. Abramsky and B. Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, 2004.*, pages 415–425, Jul 2004.

[AC09] Samson Abramsky and Bob Coecke. Categorical quantum mechanics. In *Handbook of Quantum Logic and Quantum Structures*, pages 261–323. Elsevier, 2009.

[ACR18] Matthew Amy, Jianxin Chen, and Neil J. Ross. A finite presentation of CNOT-dihedral operators. In Bob Coecke and Aleks Kissinger, editors, *Proceedings 14th International Conference on Quantum Physics and Logic, Nijmegen, The Netherlands, 3-7 July 2017*, volume 266 of *Electronic Proceedings in Theoretical Computer Science*, pages 84–97, 2018.

[AG04] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328, Nov 2004.

[Aha03] Dorit Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. *eprint arXiv:quant-ph/0301040*, Jan 2003.

[Amy19] Matthew Amy. Towards large-scale functional verification of universal quantum circuits. In Peter Selinger and Giulio Chiribella, editors, *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 1–21, 2019.

[AP05] Koenraad M. R. Audenaert and Martin B. Plenio. Entanglement on mixed stabilizer states: Normal forms and reduction procedures. *New Journal of Physics*, 7:170–170, Aug 2005.

[Bac14a] Miriam Backens. The ZX-calculus is complete for stabilizer quantum mechanics. In *New Journal of Physics*, volume 16, page 093021. IOP Publishing, Sep 2014.

[Bac14b] Miriam Backens. The ZX-calculus is complete for the single-qubit clifford+t group. In Bob Coecke, Ichiro Hasuo, and Prakash Panangaden, editors, *Proceedings of the 11th workshop on Quantum Physics and Logic,*

Kyoto, Japan, 4-6th June 2014, volume 172 of *Electronic Proceedings in Theoretical Computer Science*, pages 293–303, 2014.

[Bac15] Miriam Backens. Making the stabilizer ZX-calculus complete for scalars. In Chris Heunen, Peter Selinger, and Jamie Vicary, editors, *Proceedings of the 12th International Workshop on Quantum Physics and Logic, Oxford, U.K., July 15-17, 2015*, volume 195 of *Electronic Proceedings in Theoretical Computer Science*, pages 17–32, 2015.

[BBT05] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, Nov 2005.

[BCJ11] Jacob D. Biamonte, Stephen R. Clark, and Dieter Jaksch. Categorical tensor network states. *AIP Advances*, 1(4):042172, 2011.

[BE15] John C. Baez and Jason Erbele. Categories in control. In *Theory and Applications of Categories*, volume 30, pages 836–881, 2015.

[Bel64] John S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195–200, Nov 1964.

[BK02] Sergey B. Bravyi and Alexei Yu. Kitaev. Fermionic quantum computation. *Annals of Physics*, 298(1):210–226, May 2002.

[BPW17a] Miriam Backens, Simon Perdrix, and Quanlong Wang. A simplified stabilizer ZX-calculus. In Ross Duncan and Chris Heunen, editors, *Proceedings 13th International Conference on Quantum Physics and Logic, Glasgow, Scotland, 6-10 June 2016*, volume 236 of *Electronic Proceedings in Theoretical Computer Science*, pages 1–20, 2017.

[BPW17b] Miriam Backens, Simon Perdrix, and Quanlong Wang. Towards a Minimal Stabilizer ZX-calculus. *ArXiv e-prints*, Sep 2017.

[BSZ17] Filippo Bonchi, Paweł Sobociński, and Fabio Zanasi. Interacting Hopf algebras. *Journal of Pure and Applied Algebra*, 221(1):144 – 184, 2017.

[BW95] Michael Barr and Charles Wells. *Category Theory for Computing Science*. Prentice Hall, 1995.

[CD11] Bob Coecke and Ross Duncan. Interacting quantum observables: Categorical algebra and diagrammatics. *New Journal of Physics*, 13(4):043016, Apr 2011.

[CH16] Bob Coecke and Chris Heunen. Pictures of complete positivity in arbitrary dimension. *Information and Computation*, 250:50–58, 2016.

[CHT05] Claudio Carmeli, Teiko Heinonen, and Alessandro Toigo. On the coexistence of position and momentum observables. *Journal of Physics A: Mathematical and General*, 38(23):5253–5266, May 2005.

[CJPV19] Titouan Carette, Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Completeness of Graphical Languages for Mixed States Quantum Mechanics. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, editors, *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, volume 132 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 108:1–108:15, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[CK10] Bob Coecke and Aleks Kissinger. The compositional structure of multipartite quantum entanglement. In *Automata, Languages and Programming*, pages 297–308. Springer Berlin Heidelberg, 2010.

[CK17] Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, 2017.

[CKR+16] Nicholas Chancellor, Aleks Kissinger, Joschka Roffe, Stefan Zohren, and Dominic Horsman. Graphical structures for design and verification of quantum error correction. arXiv:1611.08012, 2016.

[Coe08] Bob Coecke. Axiomatic description of mixed states from Selinger's CPM-construction. *Electronic Notes in Theoretical Computer Science*, 210:3 – 13, 2008. Proceedings of the 4th International Workshop on Quantum Programming Languages (QPL 2006).

[CP08] Bob Coecke and Éric Oliver Paquette. POVMs and Naimark's theorem without sums. *Electronic Notes in Theoretical Computer Science*, 210:15 – 31, 2008. Proceedings of the 4th International Workshop on Quantum Programming Languages (QPL 2006).

[CP12] Bob Coecke and Simon Perdrix. Environment and Classical Channels in Categorical Quantum Mechanics. *Logical Methods in Computer Science*, Volume 8, Issue 4, Nov 2012.

[CPP08] Bob Coecke, Éric Oliver Paquette, and Simon Perdrix. Bases in diagrammatic quantum protocols. *Electronic Notes in Theoretical Computer Science*, 218:131–152, Oct 2008.

[CPV12] Bob Coecke, Dusko Pavlovic, and Jamie Vicary. A new description of orthogonal bases. *Mathematical Structures in Computer Science*, 23(03):555–567, Nov 2012.

[CW18] Bob Coecke and Quanlong Wang. ZX-rules for 2-qubit Clifford+T quantum circuits, 2018. arXiv:1804.05356.

[dBDHP19] Niel de Beaudrap, Ross Duncan, Dominic Horsman, and Simon Perdrix. Pauli fusion: a computational model to realise quantum transformations from ZX terms, 2019.

[dBH17] Niel de Beaudrap and Dominic Horsman. The ZX-calculus is a language for surface code lattice surgery. *CoRR*, abs/1704.08670, 2017.

[DD16] Ross Duncan and Kevin Dunne. Interacting Frobenius algebras are Hopf. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS 2016, pages 535–544, New York, NY, USA, 2016. ACM.

[DG18] Ross Duncan and Liam Garvie. Verifying the smallest interesting colour code with quantomatic. In Bob Coecke and Aleks Kissinger, editors, *Proceedings 14th International Conference on Quantum Physics and Logic, Nijmegen, The Netherlands, 3-7 July 2017*, volume 266 of *Electronic Proceedings in Theoretical Computer Science*, pages 147–163, 2018.

[Dir28] Paul Dirac. The quantum theory of the electron. In *Proc. R. Soc. Lond. A*, volume 117, 1928.

[DKPvdW19] Ross Duncan, Aleks Kissinger, Simon Perdrix, and John van de Wetering. Graph-theoretic simplification of quantum circuits with the ZX-calculus, 2019.

[DL14] Ross Duncan and Maxime Lucas. Verifying the Steane code with Quantomatic. In Bob Coecke and Matty Hoban, editors, *Proceedings of the 10th International Workshop on Quantum Physics and Logic, Castelldefels (Barcelona), Spain, 17th to 19th July 2013*, volume 171 of *Electronic Proceedings in Theoretical Computer Science*, pages 33–49. Open Publishing Association, 2014.

[DP09] Ross Duncan and Simon Perdrix. Graphs states and the necessity of Euler decomposition. *Mathematical Theory and Computational Practice*, 5635:167–177, 2009.

[DP10] Ross Duncan and Simon Perdrix. Rewriting measurement-based quantum computations with generalised flow. *Lecture Notes in Computer Science*, 6199:285–296, 2010.

[DP14] Ross Duncan and Simon Perdrix. Pivoting makes the ZX-calculus complete for real stabilizers. In Bob Coecke and Matty Hoban, editors, *Proceedings of the 10th International Workshop on Quantum Physics and Logic, Castelldefels (Barcelona), Spain, 17th to 19th July 2013*, volume 171 of *Electronic Proceedings in Theoretical Computer Science*, pages 50–62, 2014.

[Dun13] Ross Duncan. A graphical approach to measurement-based quantum computing. In *Quantum Physics and Linguistics*, pages 50–89. Oxford University Press, Feb 2013.

[DVC00] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62:062314, 2000.

[EEC08] Matthew B. Elliott, Bryan Eastin, and Carlton M. Caves. Graphical description of the action of clifford operators on stabilizer states. *Phys. Rev. A*, 77:042307, Apr 2008.

[Ein05] Albert Einstein. Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt. *Annalen der Physik*, 322(6):132–148, 1905.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, May 1935.

[Eul76] Leonhard Euler. Formulae generales pro translatione quacunque corporum rigidorum. In *Novi Commentarii academiae scientiarum Petropolitanae 20*, pages 189–207, 1776.

[FLSL66] Richard P. Feynman, Robert B. Leighton, Matthew Sands, and R. Bruce Lindsay. The Feynman lectures on physics, vol. 3: Quantum mechanics. *Physics Today*, 19(11):80–83, Nov 1966.

[GHZ89] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going beyond bell's theorem. In *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, pages 69–72. Springer Netherlands, 1989.

[Had15] Amar Hadzihasanovic. A diagrammatic axiomatisation for qubit entanglement. In *2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 573–584, Jul 2015.

[Had17] Amar Hadzihasanovic. *The Algebra of Entanglement and the Geometry of Composition*. PhD thesis, University of Oxford, 2017.

[HdFN18] Amar Hadzihasanovic, Giovanni de Felice, and Kang Feng Ng. A diagrammatic axiomatisation of fermionic quantum circuits. *CoRR*, abs/1801.01231, 2018.

[Hil11] Anne Hillebrand. Quantum protocols involving multiparticle entanglement and their representations. Master's thesis, University of Oxford, 2011.

[HJ85] Roger A. Horn and Charles R. Johnson. Positive definite matrices. In *Matrix analysis*, pages 391–486. Cambridge University Press, 1985.

[HNW18] Amar Hadzihasanovic, Kang Feng Ng, and Quanlong Wang. Two complete axiomatisations of pure-state qubit quantum computing. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 502–511, New York, NY, USA, 2018. ACM.

[Hor11] Clare Horsman. Quantum picturalism for topological cluster-state computing. *New Journal of Physics*, 13(9):095011, Sep 2011.

[HS19] Mathieu Huot and Sam Staton. Universal properties in quantum theory. In Peter Selinger and Giulio Chiribella, editors, *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 213–223, 2019.

[Jea18] Emmanuel Jeandel. The rational fragment of the ZX-calculus, 2018.

[JPV18a] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 559–568, New York, NY, USA, 2018. ACM.

[JPV18b] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Diagrammatic reasoning beyond Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 569–578, New York, NY, USA, 2018. ACM.

[JPV18c] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A generic normal form for ZX-diagrams and application to the rational angle completeness, 2018. Accepted at LiCS'19.

[JPV18d] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Y-calculus: A language for real matrices derived from the zx-calculus. In Bob Coecke and Aleks Kissinger, editors, *Proceedings 14th International Conference on Quantum Physics and Logic, Nijmegen, The Netherlands, 3-7 July 2017*, volume 266 of *Electronic Proceedings in Theoretical Computer Science*, pages 23–57, 2018.

[JPVW17] Emmanuel Jeandel, Simon Perdrix, Renaud Vilmart, and Quanlong Wang. ZX-calculus: Cyclotomic supplementarity and incompleteness for Clifford+T quantum mechanics. In Kim G. Larsen, Hans L. Bodlaender, and Jean-Francois Raskin, editors, *42nd International Symposium on Mathematical Foundations of Computer Science (MFCS 2017)*, volume 83 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:13, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[JS91] André Joyal and Ross Street. The geometry of tensor calculus, i. *Advances in Mathematics*, 88(1):55 – 112, 1991.

[KDD+11] Aleks Kissinger, Lucas Dixon, Ross Duncan, Benjamin Frot, Alex Merry, David Quick, Matvey Soloviev, and Vladimir Zamdzhiev. Quantomatic, 2011.

[KDT95] G. Knöchlein, D. Drechsel, and L. Tiator. Photo- and electroproduction of eta mesons. *Zeitschrift für Physik A Hadrons and Nuclei*, 352(3):327–343, Sep 1995.

[KvdW18] Aleks Kissinger and John van de Wetering. Pyzx, 2018.

[KvdW19] Aleks Kissinger and John van de Wetering. Reducing T-count with the ZX-calculus, 2019.

[KZ15] Aleks Kissinger and Vladimir Zamdzhiev. Quantomatic: A proof assistant for diagrammatic reasoning. In Amy P. Felty and Aart Middeldorp,

editors, *Automated Deduction - CADE-25*, pages 326–336, Cham, 2015. Springer International Publishing.

[Lac04] Stephen Lack. Composing PROPs. In *Theory and Applications of Categories*, volume 13, pages 147–163, 2004.

[MA08] Ken Matsumoto and Kazuyuki Amano. Representation of Quantum Circuits with Clifford and $\pi/8$ Gates, Jun 2008.

[ML13] Saunders Mac Lane. *Categories for the Working Mathematician*, volume 5. Springer Science & Business Media, 2013.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[Pla01] Max Planck. Ueber das Gesetz der Energieverteilung im Normalspectrum. *Annalen der Physik*, 309(3):553–563, 1901.

[PW16] Simon Perdrix and Quanlong Wang. Supplementarity is necessary for quantum diagram reasoning. In *41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016)*, volume 58 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 76:1–76:14, Krakow, Poland, Aug 2016.

[SB15] Peter Selinger and Xiaoning Bian. Relations for Clifford+T operators on two qubits, 2015.

[SdWZ14] Christian Schröder de Witt and Vladimir Zamdzhiev. The ZX-calculus is incomplete for quantum mechanics. In Bob Coecke, Ichiro Hasuo, and Prakash Panangaden, editors, *Proceedings of the 11th workshop on Quantum Physics and Logic, Kyoto, Japan, 4-6th June 2014*, volume 172 of *Electronic Proceedings in Theoretical Computer Science*, pages 285–292, 2014.

[Sel07] Peter Selinger. Dagger compact closed categories and completely positive maps. *Electronic Notes in Theoretical Computer Science*, 170:139–163, Mar 2007.

[Sel10] Peter Selinger. A survey of graphical languages for monoidal categories. In *New Structures for Physics*, pages 289–355. Springer, 2010.

[Sel15] Peter Selinger. Generators and Relations for n-qubit Clifford Operators. *Logical Methods in Computer Science*, Volume 11, Issue 2, Jun 2015.

[Shi03] Yaoyun Shi. Both Toffoli and controlled-not need little help to do universal quantum computing. *Quantum Information & Computation*, 3(1):84–92, 2003.

[vdW] John van de Wetering. Personal communication.

[Vil18] Renaud Vilmart. A near-optimal axiomatisation of ZX-calculus for pure qubit quantum mechanics, 2018. Accepted at LiCS'19.

[Vil19] Renaud Vilmart. A ZX-calculus with triangles for Toffoli-Hadamard, Clifford+T, and beyond. In Peter Selinger and Giulio Chiribella, editors, *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 313–344, 2019.

[vN32] John von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Feb 1932.

[Zam12] Vladimir Zamdzhiev. An abstract approach towards quantum secret sharing. Master's thesis, University of Oxford, 2012.

[Zan15] Fabio Zanasi. *Interacting Hopf Algebras – the theory of linear systems*. PhD thesis, Université de Lyon, 2015.

Résumé

Le ZX-Calculus est un langage graphique puissant et intuitif, issu de la théorie des catégories, et qui permet de raisonner et calculer en quantique. Les évolutions quantiques sont vues dans ce formalisme comme des graphes ouverts, ou diagrammes, qui peuvent être transformés localement selon un ensemble d'axiomes qui preservent le résultat du calcul. Un aspect des plus importants du langage est sa complétude : Étant donnés deux diagrammes qui représentent la même évolution quantique, puis-je transformer l'un en l'autre en utilisant seulement les règles graphiques permises par le langage ? Si c'est le cas, cela veut dire que le langage graphique capture entièrement la mécanique quantique.

Le langage est connu comme étant complet pour une sous-classe (ou fragment) particulière d'évolutions quantiques, appelée Clifford. Malheureusement, celle-ci n'est pas universelle : on ne peut pas représenter, ni même approcher, certaines évolutions. Dans cette thèse, nous proposons d'élargir l'ensemble d'axiomes pour obtenir la complétude pour des fragments plus grands du langage, qui en particulier sont approximativement universels, voire universels.

Pour ce faire, dans un premier temps nous utilisons la complétude d'un autre langage graphique et transportons ce résultat au ZX-Calculus. Afin de simplifier cette fastidieuse étape, nous introduisons un langage intermédiaire, intéressant en lui-même car il capture un fragment particulier mais universel de la mécanique quantique : Toffoli-Hadamard. Nous définissons ensuite la notion de diagramme linéaire, qui permet d'obtenir une preuve uniforme pour certains ensembles d'équations. Nous définissons également la notion de décomposition d'un diagramme en valeurs singuliaires, ce qui nous permet de nous épargner un grand nombre de calculs.

Dans un second temps, nous définissons une forme normale qui a le mérite d'exister pour une infinité de fragments du langage, ainsi que pour le langage lui-même, sans restriction. Grâce à cela, nous reprouvons les résultats de complétude précédents, mais cette fois sans utiliser de langage tiers, et nous en dérivons de nouveaux, pour d'autres fragments. Les états contrôlés, utilisés pour la définition de forme normale, s'avèrent en outre utiles pour réaliser des opérations non-triviales telles que la somme, le produit terme-à-terme, ou la concaténation.

Mots-clés: Mécanique Quantique Catégorique, ZX-Calculus, Complétude, Universalité, Formes Normales, CPM.

Abstract

The ZX-Calculus is a powerful and intuitive graphical language, based on category theory, that allows for quantum reasoning and computing. Quantum evolutions are seen in this formalism as open graphs, or diagrams, that can be transformed locally according to a set of axioms that preserve the result of the computation. One of the most important aspects of language is its completeness: Given two diagrams that represent the same quantum evolution, can I transform one into the other using only the graphical rules allowed by the language? If this is the case, it means that the graphical language captures quantum mechanics entirely.

The language is known to be complete for a particular subclass (or fragment) of quantum evolutions, called Clifford. Unfortunately, this one is not universal: we cannot represent, or even approach, certain quantum evolutions. In this thesis, we propose to extend the set of axioms to obtain completeness for larger fragments of the language, which in particular are approximately universal, or even universal.

To do this, we first use the completeness of another graphical language and transport this result to the ZX-Calculus. In order to simplify this tedious step, we introduce an intermediate language, interesting in itself as it captures a particular but universal fragment of quantum mechanics: Toffoli-Hadamard. We then define the notion of a linear diagram, which provides a uniform proof for some sets of equations. We also define the notion of singular value decomposition of a diagram, which allows us to avoid a large number of calculations.

In a second step, we define a normal form that exists for an infinite number of fragments of the language, as well as for the language itself, without restriction. Thanks to this, we reprove the previous completeness results, but this time without using any third party language, and we derive new ones for other fragments. The controlled states, used for the definition of the normal form, are also useful for performing non-trivial operations such as sum, term-to-term product, or concatenation.

Keywords: Categorical Quantum Mechanics, ZX-Calculus, Completeness, Universality, Normal Forms, CPM.