An application of Khovanov homology to quantum codes

Benjamin Audoux

AN APPLICATION OF KHOVANOV HOMOLOGY TO QUANTUM CODES

BENJAMIN AUDOUX

Abstract. We use Khovanov homology to define families of LDPC quantum error-correcting codes: unknot codes with asymptotical parameters $\left[\!\left[\frac{3^{2\ell+1}}{\sqrt{8\pi\ell}}; 1; 2^\ell \right]\!\right]$; unlink codes with asymptotical parameters $\left[\!\left[\sqrt{\frac{3}{2\pi\ell}}6^\ell; 2^\ell; 2^\ell \right]\!\right]$ and $(2,\ell)$–torus link codes with asymptotical parameters $[\![n; 1; d_n]\!]$ where $d_n > \frac{\sqrt{n}}{1.62}$.

Introduction

Classical error–correcting codes have been now studied for decades. Among them, some codes ([Gal62]), defined by sparse matrices and called LDPC (Low Density Parity Check), noteworthily come with fast decoding algorithms. Since the end of the last century, error–correcting codes for quantum computing were also known to exist and explicit constructions were given. A. R. Calderbank, P. Shor and A. Steane ([CS96],[Ste96]) described, for instance, a way to associate such a code to any pair $(\mathbf{H}_X, \mathbf{H}_Z)$ of $\mathbb{F}_2$–matrices with $\mathbf{H}_X\mathbf{H}_Z^t = 0$. This procedure allows the construction of several codes with good parameters ; it means infinite families of quantum codes whose dimension (usually denoted by k) and number of rectifiable errors (which is related to the minimum distance, usually denoted by d) are both linear in the length of codewords (usually denoted by n).

However, quickness in quantum decoding is all the more crucial since corrections should occur as fast as quantum decoherence arises. It is then natural to try to transpose the LDPC notion for classical codes into a quantum counterpart, looking for pairs of matrices $(\mathbf{H}_X, \mathbf{H}_Z)$ with minimally weighted rows. Surprisingly, topology appeared to be a fruitful field for such a project. This was initiated by Kitaev codes ([Kit03]) who defined such a family of, so-called toric, codes by considering a $m \times m$–squared tessellation of the $S^1 \times S^1$–torus. It led to codes with parameters equal to $[\![n; k; d]\!] = [\![2m^2; 2; m]\!]$. Toric codes were then generalized to surface ([BMD07]) and color ([BMD06]) codes. Other LDPC quantum codes were also defined; see for instance the constructions given by M. Freedman, D. Meyer and F. Luo in [FML02] with asymptotical parameters $[\![n; a\sqrt{n}; b\sqrt{n}\ln(n)]\!]$ or by J.-P. Tillich and G. Zemor in [TZ09] with asymptotical parameters $[\![n; cn; d\sqrt{n}]\!]$, where a, b, c and d are some constants. It is striking that none of these, and even none of any known LDPC quantum error-correcting codes families, has a minimum distance d that grows faster than n^α for any $\alpha > 1/2$. It is still an open question to know whether there is actually a general square root barrier for minimum distance in LDPC quantum codes or if this is only due to an "excess of structure" in these constructions. Indeed, constructing LDPC quantum codes remains challenging, and the few examples which are known to date carry lots of structure — in particular, a duality structure — and symmetry. This enables exact comptutation of parameters but may yield artificial restrictions. The square root barrier has been proved for local euclidian codes ([BPT10]) and for surfaces and color codes ([Del13],[Fet12]). There is thus a need for new constructions.

In this paper, we explore a new side of topology which is likely to hold interesting quantum codes. Khovanov homology is a link invariant defined in [Kho00]. To any diagram representation of a link, it associates a chain complex whose homology depends on the underlying link only. The chain complex is actually bigraded and its Euler characteristic is famed for categorifying the Jones polynomial, however we will not be interested here in this second non homological grading. Khovanov homology has a rich structure, in particular a Poincaré duality property, that makes easier the computation of minimum distances. As a matter of fact, we study three families of codes, associated to some very simple knots and links, and compute explicitly their parameters. Asymptotically, we respectively obtain $\left[\!\left[\frac{3^{2\ell+1}}{\sqrt{8\pi\ell}}; 1; 2^\ell \right]\!\right]$, $\left[\!\left[\sqrt{\frac{3}{2\pi\ell}}6^\ell; 2^\ell; 2^\ell \right]\!\right]$ and $[\![n; 1; a\sqrt{n}]\!]$ with a a constant. This is below the parameters of Freedman–Meyer–Luo and Tillich–Zemor codes, but reaches, and

Date: January 19, 2016.

even beats, toric codes and most other known ones. Moreover, there are still many others candidates among link diagrams to look at and other codes properties to study such as minimal amount of energy needed to reach an unrectifiable error. Moreover, it is worthwhile to note that, even if the construction drastically differs from its predecessors, it seems to run into the same square root bound for minimum distance. Finally, even if this study was initially motivated by quantum computing interests, it opens some questions (see *e.g.* question 2.6) that may result on interesting properties of Khovanov homology, even from the knot theory point of view.

This paper aims at being readable by both topologists and code theorists. It begins by a review of LDPC CSS codes followed by a review of chain complexes and homology. The first part ends with a generic way to define one of the former using the latter. The second part is devoted to the definition of Khovanov homology and to some of its properties. Third, fourth and fifth parts deal each with a family of codes associated, respectively, to diagrams of the unknot, of the unlinks and of the $(2, n)$–torus knots and links. All the parameters of the codes are computed there. Finally, in order to lighten the core of the text, a technical appendix gathers some analytical proofs needed on the way.

Acknowledgement. The author thanks Alain Couvreur and Gilles Zemor for introducing him to quantum codes and to their connection with topology. He is also deeply grateful to Nicolas Delfosse for answering all his (numerous) questions on quantum computing. He finally wants to thank Rinat Kashaev for a simplification in the proof of Prop. A.1. The author is supported by ANR project VasKho and CNRS PEPS project TOCQ.

1. Chain complex codes

1.1. **From quantum errors to codes.** For more details, the author recommends [NC10], [Pre] or the (french) introduction of [Del12] to the reader. This section is a rough overview of error–correcting quantum codes adressed to non specialists.

1.1.1. *Qubits and their errors.* In quantum theory, the elementary piece of information is the qubit. It is a unitary element in the $\mathbb{C}$–vector space $\mathcal{H}$ spanned by two generators, usually denoted by $|0\rangle$ and $|1\rangle$. We denote the space of qubits by $\mathcal{H}_1$. Actually, only the images in the projective quotient can be physically apprehended, but since it will be fruitful to deal with signs issues, we will often switch between the (non commutative) affine and the (commutative) projective cases. For convenience, we will use notation with tildas each time we deal with affine elements.

Unlike the classical case, multiple qubits do not just concatenate: they can entangle. From the postulates of quantum mechanics, n qubits are described by unitary elements in $\mathcal{H}^{\otimes n}$; they are of the form $\sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$ with $\sum_x |\alpha_x|^2 = 1$. We denote the space of such n–qubits by $\mathcal{H}_1^n$.

Transmitting, or even just keeping stored, an n–qubit may alter it. On a single qubit, a set of possible alterations is the Pauli group $\widetilde{\mathcal{G}}_1$, generated by three elements:

$$\widetilde{X}: \begin{array}{ccc} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{array}, \qquad \widetilde{Y}: \begin{array}{ccc} |0\rangle & \mapsto & -i|1\rangle \\ |1\rangle & \mapsto & i|0\rangle \end{array}, \qquad \widetilde{Z}: \begin{array}{ccc} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{array}.$$

Of course, they are not the only errors which may occur, but they are an orthogonal basis for them. For this reason, it is sufficient to focus our effort on them. We can note that every such Pauli error is of the form εA with $\varepsilon \in S := \{\pm 1, \pm i\}$ and $A \in \widetilde{\mathbb{E}} := \{I, \widetilde{X}, \widetilde{Y}, \widetilde{Z}\}$ and that any two errors always do commute or anti-commute. We denote by $\mathcal{G}_1$ the projective quotient of $\widetilde{\mathcal{G}}_1$. It is an abelian group which is generated by only two elements, for instance X and Z, the images of $\widetilde{X}$ and $\widetilde{Z}$. On an n–qubit, every factor can be altered by an error. The group $\widetilde{\mathcal{G}}_n = \widetilde{\mathcal{G}}_1^{\otimes n}$, defined as the set $\widetilde{\mathbb{E}}^n \times S$ with the obvious product, forms an orthogonal basis for errors on n–qubits. Here again, every two elements do commute or anti-commute; and the projective quotient $\mathcal{G}_n$ of $\widetilde{\mathcal{G}}_n$ is $\mathbb{E}^n$, where $\mathbb{E} := \{I, X, Z, XZ\}$. The group $\mathcal{G}_n$ is abelian but we say that two elements commute (resp. anti-commute) only if their lifts in $\widetilde{\mathcal{G}}_n$ do commute (resp. anti-commute). Note that it does not depend on the choosen lifts.

1.1.2. *CSS codes.* A quantum code C of length $n \in \mathbb{N}^*$ and dimension $k \in [\![1, n]\!]$ is a 2^k–dimensional subspace of $\mathcal{H}^{\otimes n}$. It makes possible the storage of a k–qubit in the form of an n–qubit, what enables, as we will see, a correction process for small alterations of the encoding n–qubits. The terminology, here, may be misleading since the dimension of a quantum code refers to the number of encoded qubits and not to the actual dimension of the code as a $\mathbb{C}$–vector space. We define a *codeword* as any element of C.

Let G be a subgroup of $\mathcal{G}_n$ such that G is liftable to a group $\widetilde{G} \subset \widetilde{\mathcal{G}_n}$. For every $g \in G$, we denote by $\widetilde{g}$ its lift in $\widetilde{G}$. We define C_G as $\mathrm{Fix}_{\widetilde{G}}(\mathcal{H}_1^n) := \{x \in \mathcal{H}_1^n \mid \forall \widetilde{g} \in \widetilde{G}, \widetilde{g}(x) = x\}$. Note that it only depends on G and not on the choosen lift $\widetilde{G}$. If G is generated by $(n-k)$ independent elements of $\mathcal{G}_n$, then one can prove that C_G is a code, so-called *stabilizer code*, of dimension k.

We say that C_G is a *CSS* — for Calderbank, Shor and Steane code — if G is even more restrictively generated by elements in $\mathbb{E}_X^n \cup \mathbb{E}_Z^n$ with $\mathbb{E}_X := \{1, X\}$ and $\mathbb{E}_Z := \{1, Z\}$. Since $\mathbb{E}_X^n$ and $\mathbb{E}_Z^n$ are both abelian and made of order 2 elements, they are both isomorphic to $\mathbb{F}_2^n$. As a matter of fact, such a set of generators can be described as the rows of two matrices $\mathbf{H}_X, \mathbf{H}_Z \in \bigcup_{p \in \mathbb{N}^*} \mathrm{Mat}_{\mathbb{F}_2}(p, n)$: to a row $(a_1, \cdots, a_n) \in \mathbb{F}_2^n$ of A_α with $\alpha = X$ or Z, we associate $(\alpha^{a_1}, \cdots, \alpha^{a_n}) \in \mathbb{E}_\alpha^n$.

The fact that G is liftable in $\widetilde{\mathcal{G}_n}$ means that every two generators x and y commute. Of course, if $x, y \in \mathbb{E}_X^n$ or $x, y \in \mathbb{E}_Z^n$, this is trivially satisfied; but since $\widetilde{X}$ and $\widetilde{Z}$ anticommute, $x \in \mathbb{E}_X^n$ and $y \in \mathbb{E}_Z^n$ do commute iff they share an even number of non-zero entries, that is if the product of the associated rows in $\mathbf{H}_X$ and in $\mathbf{H}_Z$ is zero. In short, G is liftable iff $\mathbf{H}_X \mathbf{H}_Z^t = 0$.

Finally, generators in $\mathbb{E}_X^n$ are necessarily independent from those in $\mathbb{E}_Z^n$, so the minimal number of independent generators for G is $\mathrm{rk}(\mathbf{H}_X) + \mathrm{rk}(\mathbf{H}_Z)$. As a matter of fact, two matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ such that $\mathbf{H}_X \mathbf{H}_Z^t = 0$ being given, the length n of the associated CSS code is their common number of columns, and the dimension is $k = n - \mathrm{rk}(\mathbf{H}_X) - \mathrm{rk}(\mathbf{H}_Z)$.

1.1.3. *Decoding and minimum distance.* In quantum physics, certain measurements can be seen as orthogonal projections. More precisely, for a given orthogonal decomposition $\mathcal{H}^n = \overset{\perp}{\oplus} V_i$, there is an associated measure which sends a unitary element $\sum x_i \in \mathcal{H}_1^n$ to $\frac{1}{\|x_{i_0}\|} x_{i_0}$ with probability $\|x_{i_0}\|^2$.

Now, let C_G be a CSS code and $\{E_1, \cdots, E_{n-k}\}$ be a minimal set of $n-k$ generators for G. For every $\sigma := (s_1, \cdots, s_{n-k}) \in \mathbb{F}_2^{n-k}$, we set $C(\sigma) := \{x \in \mathcal{H}_1^n \mid \forall i \in [\![1, n-k]\!], \widetilde{E_i}(x) = (-1)^{s_i} x\}$. For every error $E \in \mathcal{G}^n$, we define its syndrome $\sigma(E) := \big(s_1(E), \cdots, s_{n-k}(E)\big) \in \mathbb{F}_2^{n-k}$ by $s_i(E) = 0$ iff E commutes with E_i. We can note that if $x \in C_G$ and $E \in \mathcal{G}_n$, then $\widetilde{E}(x) \in C(\sigma(E))$. The *weight* of an error is the number of qubits it alters. For every $\sigma \in \mathbb{F}_2^{n-k}$, we choose a minimally weighted error E_σ of syndrome σ.

The decomposition $\mathcal{H}^n = \overset{\perp}{\bigoplus_{\sigma \in \mathbb{F}_2^{n-k}}} C(\sigma)$ holds and the associated measure discretizes the set of possible alterations of a codeword. Indeed, let $e(x_0)$ be a codeword $x_0 \in C_G = \mathrm{Fix}_{\widetilde{G}}(\mathcal{H}_1^n)$ altered by an error e and let assume that the measure projects it to $E(x_0)$ where E is a Pauli error of syndrome σ_E. Then one can try to correct the error by computing $\overline{x_0} := \widetilde{E}_{\sigma_E} \widetilde{E}(x_0)$. By construction, $\widetilde{E}_{\sigma_E} \widetilde{E}$ has a syndrome equal to zero, so it commutes with all elements in G. If it is actually in G, then $\overline{x_0} = x_0$ and we got back the initial codeword. However, it may happen that $\widetilde{E}_{\sigma_E} \widetilde{E}$ does not belong to G. Then the decoding process fails.

The *minimum distance* of a code is the minimal weight of a non detectible error that does alter codewords. For a CSS code C_G, it is the minimal weight of an error which commutes with all the elements of G but does not belong to G. It corresponds, as we will see in the proof of Prop. 1.7, to the minimal weight of a vector which is in the kernel of one of the matrices $\mathbf{H}_X$ or $\mathbf{H}_Z$ without being spanned by the rows of the other.

Notation 1.1. For any code, we denote its parameters by $[\![n; k; d]\!]$ where n is the length of the code, k its dimension and d its minimum distance.

1.2. **From codes to chain complexes.** For further details, the reader can refer to [Wei94], [HS97], [ML95] or [Lan02].

1.2.1. *Homology and cohomology.* Before relating them to quantum codes, we recall some basic definitions on chain complexes. We will focus here on $\mathbb{F}_2$, but up to signs issues, everything remains true for any field. Everything but the Künneth formula, which has then a more sophisticated statement, remains even true for any ring.

Definition 1.2. An increasing (resp. decreasing) chain complex C is a $\mathbb{Z}$–graded $\mathbb{F}_2$–vector space $\underset{i\in\mathbb{Z}}{\oplus} C^i$ (resp. $\underset{i\in\mathbb{Z}}{\oplus} C_i$) together with a linear map $\partial\colon C \longrightarrow C$ which increases (resp. decreases) the grading by one and satisfies $\partial^2 \equiv 0$. It is often denoted as

$$\cdots \xrightarrow{\partial} C^i \xrightarrow{\partial} C^{i+1} \xrightarrow{\partial} \cdots .$$

The grading is called *homological grading*. If C is non zero for only a finite number of homological degrees, then we omit all the redundant zero spaces.

Remark 1.1. Unless otherwise specified, chain complexes will be assumed to be increasing. This convention is opposite to the usual one, but it sticks to the standard appellation "Khovanov homology", which should be more appropriately called "Khovanov cohomology".

Definition 1.3. If $C := \left(\underset{i\in\mathbb{Z}}{\oplus} C^i, \partial\right)$ is a chain complex, then its dual $C^\vee$ is the decreasing chain complex $\left(\underset{i\in\mathbb{Z}}{\oplus} C_i^\vee, \partial^\vee\right)$ defined, for every $i \in \mathbb{Z}$, by $C_i^\vee = \mathrm{Hom}(C^i, \mathbb{F}_2)$ and $\big(\partial^\vee(f)\big)(c) = f\big(\partial(c)\big)$ for every $f \in C_i^\vee$ and $c \in C^{i-1}$.

Definition 1.4. If $C := \left(\underset{i\in\mathbb{Z}}{\oplus} C^i, \partial\right)$ is a chain complex, then its homology $H^*(C)$ is the graded space $\underset{i\in\mathbb{Z}}{\oplus} H^i(C) := \underset{i\in\mathbb{Z}}{\oplus} \Big(\mathrm{Ker}(\partial) \cap C^i\Big) \Big/ \Big(\mathrm{Im}(\partial) \cap C^i\Big)$ and its cohomology $H_*(C)$ the graded space $\underset{i\in\mathbb{Z}}{\oplus} H_i(C) := \underset{i\in\mathbb{Z}}{\oplus} \Big(\mathrm{Ker}(\partial^\vee) \cap C_i^\vee\Big) \Big/ \Big(\mathrm{Im}(\partial^\vee) \cap C_i^\vee\Big)$ where $C^\vee$ is the dual of C.

For every $x \in \mathrm{Ker}(\partial)$ (resp. $x \in \mathrm{Ker}(\partial^\vee)$), we denote by $[x]$ its image in $H^*(C)$ (resp. $H_*(C)$).

Now, we prove a very elementary lemma which will be central in the proof of Prop. 5.3.

Lemma 1.1. *Let $C := \left(\underset{i\in\mathbb{Z}}{\oplus} C^i, \partial\right)$ be a chain complex, r an integer and $\{\alpha_i\}_{i\in I} \subset \mathrm{Ker}(\partial) \cap C^r$ a finite set such that $\big\{[\alpha_i]\big\}_{i\in I}$ generates $H^r(C)$. Then every $\varphi \in \mathrm{Ker}(\partial^\vee) \cap C_r^\vee$ satisfying $\varphi(\alpha_i) = 0$ for every $i \in I$ is null in $H_r(C)$.*

Proof. Since $\big\{[\alpha_i]\big\}_{i\in I}$ generates $H^r(C)$, every $x \in \mathrm{Ker}(\partial) \cap C^r$ can be written $x = \sum_{i\in I'\subset I} \alpha_i + \partial(y)$ with $y \in C^{r-1}$. Then $\varphi(x) = \varphi\big(\partial(y)\big) = \big(\partial^*(\varphi)\big)(y) = 0$ and $\varphi_{|\mathrm{Ker}(\partial)} \equiv 0$. Now, consider a basis $\{\beta_j\}_{j\in J}$ of $\mathrm{Ker}(\varphi)^\perp \subset \mathrm{Ker}(\partial)^\perp$ in C^r, set $\beta'_j = \partial(\beta_j) \neq 0$ for all $j \in J$ and define $g \in \mathrm{Hom}(C^{r+1}, \mathbb{F}_2)$ by $g(\beta'_j) = \varphi(\beta_j)$ for all $j \in J$ and $g_{|\mathbb{F}_2^\perp <\beta'_j>} \equiv 0$. Then $\varphi = g \circ \partial \in \mathrm{Im}(\partial^\vee)$ and $[\varphi] = 0$. □

1.2.2. *Operations on chain complexes.* Later on the paper, we will need the following definitions and propositions.

Definition 1.5. If $C_1 := \left(\underset{i\in\mathbb{Z}}{\oplus} C_1^i, \partial_1\right)$ and $C_2 := \left(\underset{i\in\mathbb{Z}}{\oplus} C_2^i, \partial_2\right)$ are two chain complexes, then $C_1 \otimes C_2$ is the chain complex $\left(\underset{i\in\mathbb{Z}}{\oplus} C^i, \partial\right)$ defined by $C^i = \underset{j\in\mathbb{Z}}{\oplus} \left(C_1^j \otimes C_2^{i-j}\right)$ and $\partial(c_1 \otimes c_2) = \partial_1(c_1) \otimes c_2 + c_1 \otimes \partial_2(c_2)$ for every $c_1 \in C_1$ and $c_2 \in C_2$.

Proposition 1.2 (Künneth formula)**.** *If C_1 and C_2 are two chain complexes, then $H^*(C_1 \otimes C_2) \cong H^*(C_1) \otimes H^*(C_2)$ and $H_*(C_1 \otimes C_2) \cong H_*(C_1) \otimes H_*(C_2)$ as graded spaces.*

Definition 1.6. If $C_1 := \left(\underset{i\in\mathbb{Z}}{\oplus} C_1^i, \partial_1\right)$ and $C_2 := \left(\underset{i\in\mathbb{Z}}{\oplus} C_2^i, \partial_2\right)$ are two chain complexes, then $f := \left(f^i\colon C_1^i \longrightarrow C_2^i\right)_{i\in\mathbb{Z}}$ is a chain map iff it commutes with the differentials, *i.e.* iff $\partial_2 \circ f = f \circ \partial_1$.

The *cone* of f is the chain complex $\mathrm{Cone}(f) := \left(\underset{i\in\mathbb{Z}}{\oplus} C^i, \partial\right)$ defined by $C^i := C_1^i \oplus C_2^{i-1}$ for every $i \in \mathbb{Z}$ and $\partial = \begin{pmatrix} \partial_1 & 0 \\ f & \partial_2 \end{pmatrix}$.

Proposition 1.3. *A chain map $f\colon C_1 \longrightarrow C_2$ between two chain complexes C_1 and C_2 induces maps at the level of homology and cohomology which are denoted by $f^*\colon H^*(C_1) \longrightarrow H^*(C_2)$ and $f_*\colon H_*(C_1) \longrightarrow H_*(C_2)$*

1.2.3. *Exact sequences.* The following notion will be usefull to compute homologies.

Definition 1.7. An exact sequence is a chain complex (C, ∂) with homology equal to zero in all degrees. It means that $\mathrm{Ker}(\partial) = \mathrm{Im}(\partial)$.

Proposition 1.4. *If (C_0, ∂_0), (C_1, ∂_1) and (C_2, ∂_2) are three chain complexes such that, for every $n \in \mathbb{Z}$, there are maps $\iota_n \colon C_0^n \longrightarrow C_1^n$ and $\pi_n \colon C_1^n \longrightarrow C_2^n$ which commute with the differentials ∂_0, ∂_1 and ∂_2 and such that*

$$0 \longrightarrow C_0^n \xrightarrow{\iota_n} C_1^n \xrightarrow{\pi_n} C_2^n \longrightarrow 0$$

is an exact sequence, then

$$\cdots \xrightarrow{f_{n-1}^*} H^n(C_0) \xrightarrow{\iota_n^*} H^n(C_1) \xrightarrow{\pi_n^*} H^n(C_2) \xrightarrow{f_n^*} H^{n+1}(C_0) \xrightarrow{\iota_{n+1}^*} \cdots$$

is an exact sequence , where, for all $n \in \mathbb{Z}$, ι_n^* and π_n^* are the maps induced in homology by ι_n and π_n and f_n^* is some connecting map.

Remark 1.2. The condition on the short exact sequence just states that maps ι_n are injective, maps π_n are surjective and $\mathrm{Ker}(\pi_n) = \mathrm{Im}(\iota_n)$.

Proposition 1.5. *If $f \colon C_1 \longrightarrow C_2$ is a chain map, then* $\mathrm{Cone}(f) := \bigoplus_{i \in \mathbb{Z}} C^i$ *fits the following short exact sequence in every degree $n \in \mathbb{N}$:*

$$0 \longrightarrow C_2^{n-1} \xrightarrow{\iota_n} C^n \xrightarrow{\pi_n} C_1^n \longrightarrow 0 \ .$$

Corollary 1.6. *If $f \colon C_1 \longrightarrow C_2$ is a chain map, then*

$$\cdots \xrightarrow{f_{n-1}^*} H^{n-1}(C_2) \xrightarrow{\iota_n^*} H^n\big(\mathrm{Cone}(f)\big) \xrightarrow{\pi_n^*} H^n(C_1) \xrightarrow{f_n^*} H^n(C_2) \xrightarrow{\iota_{n+1}^*} \cdots$$

is an exact sequence. In this case, maps f_n^* are the maps induced in homology by f.

1.2.4. *Chain complex codes.* Now, we can state the purpose of this section.

Proposition 1.7. *To any length 3 piece of chain complex $C := \left(C^{i_0-1} \xrightarrow{\partial} C^{i_0} \xrightarrow{\partial} C^{i_0+1}\right)$ given with a basis $\mathcal{B}$, one can associate a CSS code C_C with parameter $[\![n; k; d]\!]$ where $n = \dim(C^{i_0})$, $k = \dim\left(H^{i_0}(C)\right)\Big($ $= \dim\left(H_{i_0}(C)\right)\Big)$ and $d = \min\left\{|x|_{\mathcal{B}} \;\middle|\; [x] \in H^{i_0}(C) \sqcup H_{i_0}(C), [x] \neq 0\right\}$, where $|\,.\,|_{\mathcal{B}}$ denotes the $\mathcal{B}$–weight, that is the number of non trivial coordinates in the basis $\mathcal{B}$.*

Proof. We set $\mathbf{H}_X := \mathrm{Mat}_{\mathcal{B}}(\partial_{|C^{i_0}})$ and $\mathbf{H}_Z := \mathrm{Mat}_{\mathcal{B}}(\partial_{|C^{i_0-1}})^t$. Since $\partial^2 = 0$, we have that $\mathbf{H}_X \mathbf{H}_Z^t = 0$ and the matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ define a CSS code C_C. Its length is trivially $\dim(C^{i_0})$. Its dimension is

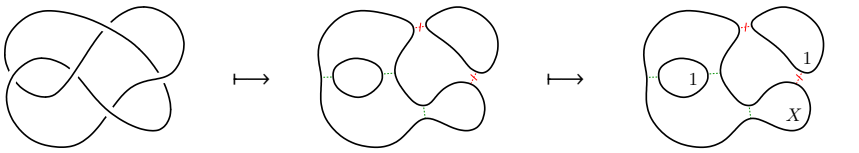
$$\begin{aligned} n - \mathrm{rk}(\mathbf{H}_X) - \mathrm{rk}(\mathbf{H}_Z) &= \dim(C^{i_0}) - \mathrm{rk}(\partial_{|C^{i_0}}) - \mathrm{rk}(\partial_{|C^{i_0-1}}) \\ &= \dim\left(\mathrm{Ker}(\partial_{|C^{i_0}})\right) - \mathrm{rk}(\partial_{|C^{i_0-1}}) \\ &= \dim\left(\mathrm{Ker}(\partial_{|C^{i_0}}) \Big/ \mathrm{Im}(\partial_{|C^{i_0-1}})\right) \ = \ \dim\left(H^{i_0}(C)\right). \end{aligned}$$

To compute the minimum distance, we consider an error E which commutes with every element of G but which is not in G.

If E only involves Z alterations, then it can be described by a vector $v_E \in \mathbb{F}_2^n$ and the weight of E is exactly $|v_E|_{\mathcal{B}}$. Since E commutes with all the generators of G induced by the rows of $\mathbf{H}_X$, the vector v_E is orthogonal to all these rows and $v_E \in \mathrm{Ker}(\partial_{|C^{i_0}})$. But $E \notin G$, so v_E is not spanned by rows of $\mathbf{H}_Z$ and $v_E \notin \mathrm{Im}(\partial_{|C^{i_0-1}})$. It follows that E is non detectible iff $[v_E]$ is non zero in $H^{i_0}(C)$.

If E only involves X alterations, then a similar reasoning at the dual level shows that E is non detectible iff $[v_E]$ is non zero in $H_{i_0}(C)$.

Now, for a general E, we factorize it as a product $E_X E_Z$ where E_α only involves α alterations. Since every given generator of G involves only X alterations or only Z ones, the fact that E commutes with them implies that E_X and E_Z do. But $E \notin G$, so at least one of E_X or E_Z is not in G. We conclude by noting that the weight of E is greater than each of the weights of E_X and E_Z. □



a diagram a resolution an enhanced resolution

Figure 1: From diagrams to enhanced resolutions

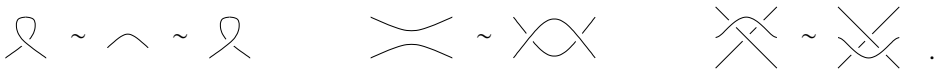
2. Khovanov homology

For more details on knot theory, the reader can refer to [Lic97] or [Kau87]. For details on Khovanov homology, the author advises Khovanov's seminal paper [Kho00] for the general definition, [Kho03] for the reduced case, Viro's elementary reformulation [Vir04] and Shumakovich's survey [Shu11].

2.1. **Link diagrams.** A link is an embedding of a disjoint union of circles in $\mathbb{R}^3$ considered up to ambient isotopies in $\mathbb{R}^3$. Two maps $f, g\colon X \longrightarrow Y$ are said ambient isotopic in Y if there exists a continuous path of homeomorphisms $\phi_t\colon Y \longrightarrow Y$ such that $\phi_0 = \mathrm{Id}_Y$ and $g = \phi_1 \circ f$.

The notion can be turned combinatorial by considering link diagrams. They are generic projections, *i.e.* with regular points and a finite number of transverse double points, of links into the plane $\mathbb{R}^2 \times \{0\}$ together with an over/underpassing information for the strands at each double point.

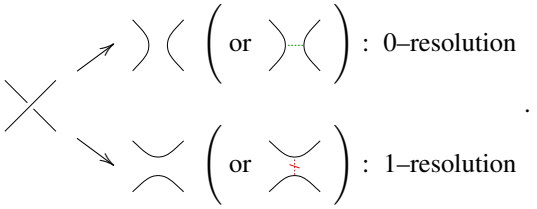
Theorem 2.1 ([Rei72])**.** *Every link admits diagrams and two given diagrams describe the same link iff they can be connected by ambient isotopies in* $\mathbb{R}^2$ *and a finite number of the following Reidemeister moves:*



R1$^+$ & R1$^-$ R2 R3

Two diagrams are connected by a Reidemeister move if they are identical outside a disk inside which they respectively correspond to the given pictures.

A double point with over/underpassing information is called *a crossing*. There are two canonical ways to smooth (or resolve) a crossing:



The second pictures aim at keeping tracks of the resolved crossing. If D is a link diagram, we call *resolution of* D any map $\phi\colon \{\text{crossings of } D\} \longrightarrow \{0,1\}$, or equivalently the diagram D_ϕ obtained from D by $\phi(c)$–resolving every crossing c of D. Resolution diagrams are <u>not</u> considered up to isotopies and different maps ϕ always lead to different resolution diagrams D_ϕ. Note that D_ϕ is a union of disjoint circles embedded in the plane. An *enhanced resolution* D_ϕ^σ of D is a resolution D_ϕ of D together with a labelling map $\sigma\colon \{\text{circles of } D_\phi\} \longrightarrow \{1, X\}$. The labels can be seen as elements of $\mathbb{F}_2[X]\big/X^2$, and later, when dealing with combinations of enhanced diagrams, we will assume multi-linearity for the labels. Note that this X is not related in any sense to the eponym Pauli error, and actually, this notation will be dropped out by the end of the section.

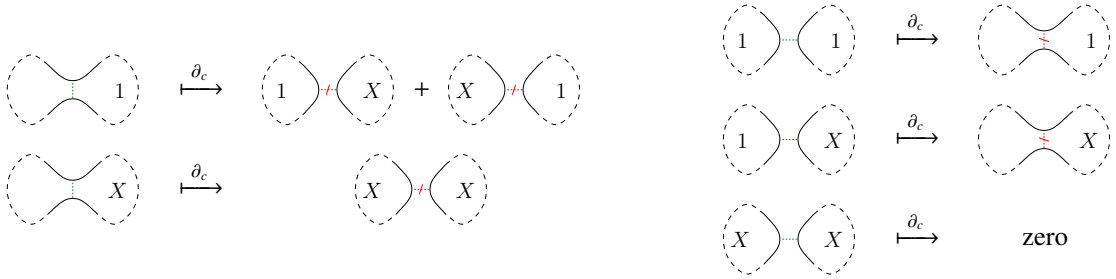


Figure 2: Rules for labelling in the differential: here (and throughout the paper), only the modified part is depicted, the rest of the resolutions being identical on both sides of the arrows

2.2. **Khovanov chain complex.** To any diagram D with $n \in \mathbb{N}$ crossings, Khovanov theory associates a length $n+1$ chain complex

$$C(D) := \; 0 \longrightarrow C^0 \xrightarrow{\partial_D} C^1 \xrightarrow{\partial_D} \cdots \xrightarrow{\partial_D} C^n \longrightarrow 0$$

defined as follows. For $i \in [\![0, n]\!]$, C^i is spanned over $\mathbb{F}_2$ by enhanced resolutions of D with exactly i 1–resolved crossings. The map ∂_D is the $\mathbb{F}_2$–linear map defined for a generator D^σ_ϕ by

$$\partial_D(D^\sigma_\phi) = \sum_{c \in \phi^{-1}(0)} \partial_c(D^\sigma_\phi)$$

where $\partial_c(D^\sigma_\phi)$ is a sum of enhanced resolutions over $D_{\phi+\delta_c}$, with δ_c the Kronecker delta. The resolution $D_{\phi+\delta_c}$ is nothing but the resolution obtained by changing the smoothing of c. Before stating the enhancing rules, let us note that $D_{\phi+\delta_c}$ differs from D_ϕ by the merging of two circles into one or the splitting of a circle into two. Now, the rules are:

- the untouched circles keep their labels unchanged;
- if two circles are merging, then the resulting circle is labelled by the product of the labels in $\mathbb{F}_2[X]/X^2$. Note that a 0–label just means no contribution;
- if one 1–labelled circle is splitting, then there are two contributions obtained as the two ways to distribute 1 and X to the two new circles;
- if one X–labelled circle is splitting, then there is only one contribution obtained by labelling both new circles by X.

These rules are summarized in Fig. 2.

Proposition 2.2 ([Kho00] Prop. 8, [Vir04] Th. 5.3.A)**.** *The map ∂_D satisfies $\partial_D \circ \partial_D = 0$.*

Remarks 2.1.

(1) The construction was originally given with $\mathbb{Z}$–coefficients instead of $\mathbb{F}_2$–ones. It can therefore be adapted to any ring.
(2) Khovanov homology is usually defined with a second grading j on $C(D)$, namely $j(D^\sigma_\phi) = |\sigma^{-1}(X)| - |\sigma^{-1}(1)| - |\phi^{-1}(1)|$ where $|\,.\,|$ stands for cardinality. Since the differential ∂_D respects this grading j, the chain complex $C(D)$ splits into several chain complexes, one for each value of j. However, this grading is not relevant for the purpose of the present paper.

2.3. **Change of variable.** With this basis, Khovanov complexes are not really efficient for quantum codes since non trivial homology elements can easily have small weight. To change this matter of fact, we consider another set of generators, where labels are not anymore 1 and X but signs $- := 1$ and $+ := 1 + X$. A label $+$ for a circle means the sum of the two generators for which the circle is labelled by 1 or by X, all the others circles being identically labelled. The differential is then kind of symmetrized as pointed in Fig. 3.

Remark 2.2. The new set of generators is not anymore graded with regard to the second grading j. That is essentially why j is not relevant here.

Figure 3: Modified rules for labelling in the differential: here, ε and η are element of $\{-,+\}$ and the product is the obvious one

2.4. **Reidemeister moves invariance.** The Khovanov complex $C(D)$ depends heavily on the diagram D, but if considering the homology, then $\mathrm{Kh}(D) := H^*\big(C(D)\big)$ depends essentially on the underlying link. Indeed, the following theorem makes explicit the behavior of $\mathrm{Kh}(D)$ under Reidemeister moves.

Theorem 2.3 ([Vir04] sections 5.6 & 5.7, [Ito11])**.** *Let D_1 and D_2 be two link diagrams connected by a Reidemeister move (with D_2 having greater or equal number of crossings than D_1). Then the chain maps given in Fig. 4 induce isomorphisms between $\mathrm{Kh}(D_2)$ and $\mathrm{Kh}(D_1)\{\eta\}$ where $\{\,.\,\}$ denotes a shift in the grading and $\eta = 1$ if the Reidemeister move is $\mathrm{R1}^-$ or R2 and $\eta = 0$ otherwise.*

Remark 2.3. There is a canonical way to shift Khovanov homology so it becomes really invariant under Reidemeister moves ([Kho00]), but this is not relevant for our purpose.

2.5. **Basic properties.** Khovanov homology does behave quite nicely under certain usual operations on knots.

Proposition 2.4 ([Kho00] Cor. 12)**.** *If D_1 and D_2 are two link diagrams, then $C(D_1 \sqcup D_2) \cong C(D_1) \otimes C(D_2)$ so $\mathrm{Kh}(D_1 \sqcup D_2) \cong \mathrm{Kh}(D_1) \otimes \mathrm{Kh}(D_2)$.*

Proposition 2.5 ([Kho00] Prop. 32)**.** *For any link D with n crossings and for every $i \in [\![0, n]\!]$, $\mathrm{Kh}^i(D!) \cong \mathrm{Kh}^\vee_{n-i}(D)$ where $D!$ is the mirror image of D, i.e. the link obtained by swapping the under and the over strands at every crossings, and $\vee$ stands for duality. Besides, the isomorphism is induced by the generator-to-generator chain map $m\colon C^\vee_{n-i}(D) \longrightarrow C^i(D!)$ defined by $m(D^{\sigma\vee}_\phi) = D!^{-\sigma}_{1-\phi}$.*

Remark 2.4. This analogue of Poincaré duality is of special interest since it enables to deal with dual chain complexes while staying in the frame of Khovanov complexes.

2.6. **Reduced Khovanov homology.** There is a reduced Khovanov homology defined for pointed links, *i.e.* links with a marked point on it. The definition is nearly the same except the marked point induces a pointed circle in every resolution, and we force it to be labelled by X, that is the sum of labels $-$ and $+$. It leads to the additional labelling rules for the differential given in Fig. 5.

Proposition 2.6 ([Shu11] Theo. 2.6)**.** *If $D_\bullet$ is a pointed version of a link diagram D, then $\mathrm{Kh}(D) \cong \mathrm{Kh}(D_\bullet) \oplus \mathrm{Kh}(D_\bullet)$.*

Proposition 2.7. *If D_1 and D_2 are two pointed link diagrams, then $C(D_1 \# D_2) \cong C(D_1) \otimes C(D_2)$ so $\mathrm{Kh}(D_1 \# D_2) \cong \mathrm{Kh}(D_1) \otimes \mathrm{Kh}(D_2)$, where $\#$ is the connected sum operation done on the two marked points (see Fig. 6).*

2.7. **Exact sequence.** Let D be a link diagram (possibly pointed) and c a crossing of D. We denote by D_0 and D_1 the diagrams obtained, respectively, by 0–resolving and 1–resolving c. It follows from the definition that:

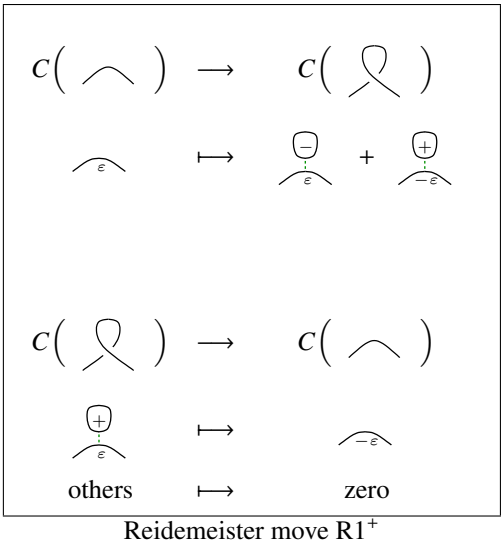
Proposition 2.8. $C(D) \cong \mathrm{Cone}\big(\partial_c\colon C(D_0) \longrightarrow C(D_1)\big)$.

If denoting by $\alpha\colon C(D_1) \longrightarrow C(D)$ and $\beta\colon C(D) \longrightarrow C(D_2)$ the natural injection and surjection, then Prop. 1.6 implies:

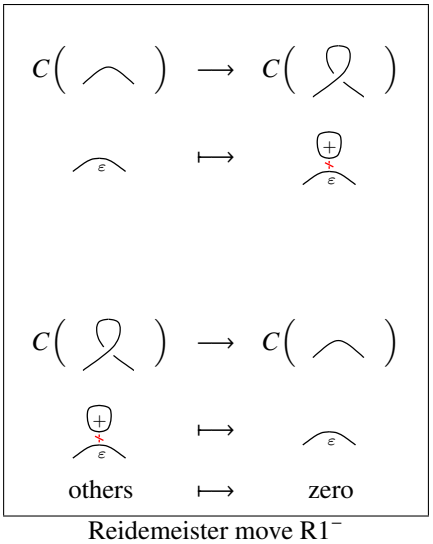
Corollary 2.9 ([Vir04] section 6.2)**.** *The long sequence*

$$\cdots \xrightarrow{\partial_c^*} \mathrm{Kh}^{i-1}(D_1) \xrightarrow{\alpha^*} \mathrm{Kh}^i(D) \xrightarrow{\beta^*} \mathrm{Kh}^i(D_0) \xrightarrow{\partial_c^*} \mathrm{Kh}^i(D_1) \xrightarrow{\alpha^*} \cdots .$$

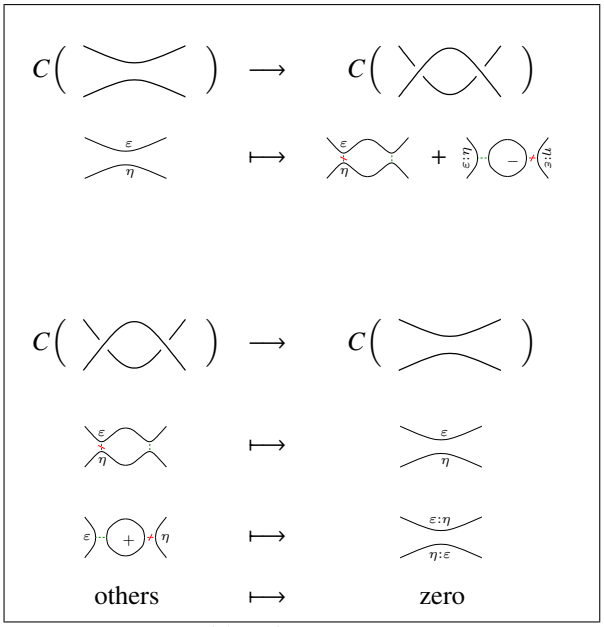
is exact.



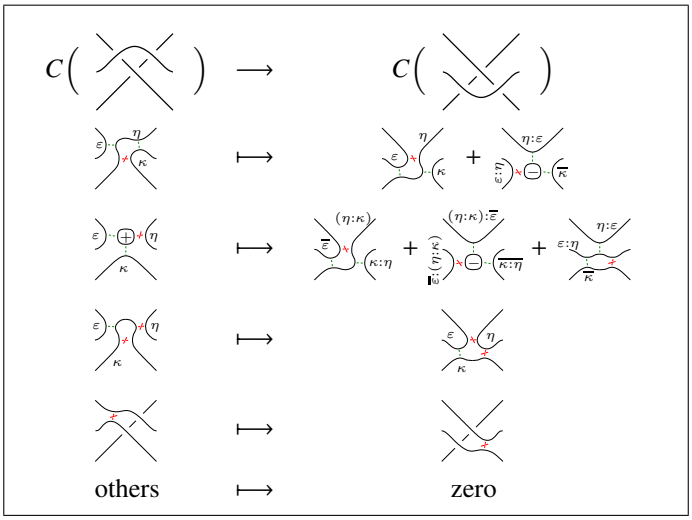
Reidemeister move R1$^+$



Reidemeister move R1$^-$



Reidemeister move R2



Reidemeister move R3

Figure 4: Invariance chain maps: only the part involved in the Reidemeister move is depicted, the rest of the diagrams are identical on each side; $\varepsilon{:}\eta$ and $\eta{:}\varepsilon$ are the two labels (maybe a sum of) obtained when merging/splitting circles with labels ε and η; overlining a label means that it may be modified if, outside the depicted part, its circle is connected to the splitting/merging ones; a unresolved crossing stands for any of its resolutions, the map is then the natural one-to-one one

Figure 5: Extra rules for labelling in the reduced differential: here ε is an element of $\{-,+\}$

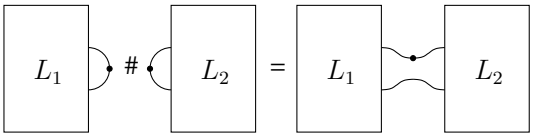


Figure 6: Connected sum for pointed links

2.8. **Weight considerations.** As far as the author knows, weight of representives for non-zero elements in Khovanov homology have not been studied yet. This section aims at presenting some first thoughts toward this direction.

For every chain complex $C := \oplus_{i\in\mathbb{Z}} C^i$ and every integer $i \in \mathbb{Z}$, we denote by $d^i_C := \min\left\{|x| \;\middle|\; x \in C^i, [x] \in H^i(C) \setminus \{0\}\right\}$. In the case of Khovanov homology, we will write, for a diagram D and an integer $i \in \mathbb{N}$, d^i_D for $d^i_{C(D)}$.

Proposition 2.10. *Let C_1 and C_2 be two chain complexes. If a chain map (which possibly shifts the homological grading) $\psi\colon C^i_1 \longrightarrow C^j_2$, with $i, j \in \mathbb{N}$, induces an injective map in homology, then $kd^i_{C_1} \geq d^j_{C_2}$ where $k := \max\left\{|\psi(x)| \;\middle|\; x \text{ generator of } C^i_1\right\}$.*
Moreover, if $k = 1$, if the map ψ is also injective and if a minimally weighted homology-surviving element of C^j_2 is on the image of ψ, then the inequality becomes an equality.

Proof. Let $x \in C^i_1$ be such that $[x] \neq 0$ and $|x| = d^i_{C_1}$. In one hand, we have $|\psi(x)| \leq k|x|$ but on the other hand, since ψ^* is injective, $\psi^*\big([x]\big) = \big[\psi(x)\big] \neq 0$ so $|\psi(x)| \geq d^j_{C_2}$.

Now, if all the conditions of the second part of the statement hold, we can find $y \in C^j_2$ and $x \in C^i_1$ such that $[y] \neq 0$, $|y|$ is minimal and $\psi(x) = y$. Then $\psi\big(\partial_{C_1}(x)\big) = \partial_{C_2}(y) = 0$, but ψ is injective so $\partial_{D_1}(x) = 0$ and since $\psi^*\big([x]\big) = [y] \neq 0$, $[x] \neq 0$. But ψ is injective and $k = 1$ so $|y| = \big|\psi(x)\big| = |x|$. It follows that $d^i_{C_1} \leq d^j_{C_2}$ and hence $d^i_{C_1} = d^j_{C_2}$. □

Corollary 2.11. *With obvious notation for diagrams differing from Reidemeister moves, we have for any $i \in \mathbb{N}$*

$$d^i_{\text{⟲}} = 2d^i_{\text{⌒}} \qquad\qquad d^{i+1}_{\text{⟲}} = d^i_{\text{⌒}}$$

$$\tfrac{1}{3}d^i_{\text{><}} \leq d^{i+1}_{\text{><}} \leq 2d^i_{\text{><}} \qquad\qquad \tfrac{1}{8}d^i_{\text{⋈}} \leq d^i_{\text{⋈}} \leq 8d^i_{\text{⋈}}$$

Proof. Most of the statement is a direct application of Prop. 2.3 and 2.10. Only $d^i_{\text{⟲}} \geq 2d^i_{\text{⌒}}$ needs a further argumentation. Let $x \in C^i(\,\text{⟲}\,)$ be a representative of a non-zero element of the homology. We can decompose it as $x = a_+ + a_- + b$ with a_+ (resp. a_-) a sum of generators of the form $\oplus_{\varepsilon}$ (resp. $\ominus_{\varepsilon}$) and b a sum of generators of the form $\,\text{⟲}\,$. Since x represents an element of the homology, we know that $\partial_{\text{⟲}}(x) = 0$. Looking at the part which lies in resolutions of the form $\,\text{⟲}\,$, we obtain $A_+ + A_- + \partial_{\text{⟲}}(b) = 0$ where A_- (resp. A_+) is an element of $\,\text{⟲}\,$ obtained from a_- (resp. a_+) by removing the "$-$"–labelled

circle and performing a small isotopy (resp. removing the "+"–labelled circle, inverting the sign of ε and performing a small isotopy). In particular $|A_+| = |a_+|$ and $|A_-| = |a_-|$. Applying backward the small isotopy, we obtain $\widetilde{A}_+ + \widetilde{A}_- + \partial_{\frown}(\widetilde{B}) = 0$ in $C^i(\frown)$. We deduce that $[\widetilde{A}_+] = [\widetilde{A}_-]$ in $\mathrm{Kh}^i(\frown)$. But the image of x under the R1$^+$–chain quasi-isomorphism is precisely $\widetilde{A}_+$. So $[\widetilde{A}_+] = [\widetilde{A}_-] \neq 0$ and $|\widetilde{A}_+|, |\widetilde{A}_-| \geq d^i_{\frown}$. Finally, $|x| \geq |a_+| + |a_-| = |\widetilde{A}_+| + |\widetilde{A}_-| \geq 2d^i_{\frown}$. □

Remark 2.5. Computations and the fact that awkward generators are part of acyclic subcomplexes suggest that those naïve bounds are far from being sharp for Reidemeister moves R2 and R3.

Question 2.6. Do Reidemeister moves R2 always double minimal distances, and do Reidemeister moves R3 always preserve it ? If true, Khovanov homology would hide inner invariants on each degree supporting a non trivial homology.

3. Unknot codes

For every $\ell \in \mathbb{N}$, we consider the following diagram D^{uk}_ℓ of the pointed unknot with 2ℓ crossings:

We call ℓ^{th} *unknot code* the code obtained from $\left(C^{\ell-1}(D^{\mathrm{uk}}_\ell) \xrightarrow{\partial_{D^{\mathrm{uk}}_\ell}} C^{\ell}(D^{\mathrm{uk}}_\ell) \xrightarrow{\partial_{D^{\mathrm{uk}}_\ell}} C^{\ell+1}(D^{\mathrm{uk}}_\ell)\right)$. Its parameters are denoted by $[\![n_\ell; k_\ell; d_\ell]\!]$.

3.1. **Length.**

Proposition 3.1. *$n_\ell \sim \frac{3^{2\ell+1}}{\sqrt{8\pi\ell}}$ as ℓ tends to infinity.*

Proof. When 0–resolving all the crossings, we obtain  with ℓ undotted circles. Swapping the resolution of one of the ℓ crossings on the left creates a new undotted circle. On the contrary, swapping the resolution of one of the ℓ crossings on the right reduces by one the number of undotted circles. Now we gather the generators of $C^\ell(D^{\mathrm{uk}}_\ell)$ according to the number of 1–resolved crossings among the ℓ left ones. We obtain $n_\ell = \sum_{r=0}^{\ell} \binom{\ell}{r}\binom{\ell}{\ell-r} 2^{\ell+r-(\ell-r)} = \sum_{r=0}^{\ell} \left[\binom{\ell}{r} 2^r\right]^2$. Then, using the formula of Prop. A.1 for $x = 2$, we get $n_\ell \sim \frac{3^{2\ell+1}}{\sqrt{8\pi\ell}}$. □

3.2. **Dimension and minimum distance.**

Proposition 3.2. *$k_\ell = 1$ and $d_\ell = 2^\ell$.*

Proof. To pass from D^{uk}_ℓ to $D^{\mathrm{uk}}_{\ell+1}$, one can perform two R1 moves (one R1$^+$ and one R1$^-$). Now the statement on k_ℓ follows from Prop. 2.3 and the statement on d_ℓ from Prop. 2.11. □

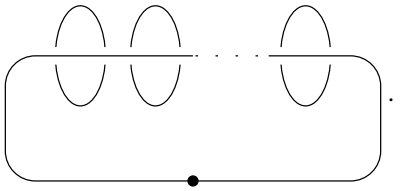
3.3. **Sparseness.**

Proposition 3.3. *The weight of each row in the ℓ^{th} unknot code is $O\big(\ln(n_\ell)\big)$ as ℓ increases.*

Proof. It is clear from Khovanov homology construction that each row has between $\ell + 1$ and $2(\ell + 1)$ non trivial entries. Since $8^\ell \leq n_\ell \leq 9^\ell$ for sufficiently large ℓ, the result follows. □

4. Unlink codes

For every $\ell \in \mathbb{N}$, we consider the following diagram D_ℓ^{ul} of the pointed $(\ell+1)$–unlink:



We call ℓ^{th} *unlink code* the code obtained from $\left(C^{\ell-1}(D_\ell^{\mathrm{ul}}) \xrightarrow{\partial_{D_\ell^{\mathrm{ul}}}} C^{\ell}(D_\ell^{\mathrm{ul}}) \xrightarrow{\partial_{D_\ell^{\mathrm{ul}}}} C^{\ell+1}(D_\ell^{\mathrm{ul}})\right)$. Its parameters are denoted by $[\![n_\ell; k_\ell; d_\ell]\!]$.

4.1. **Case $\ell = 1$.** It follows from Prop. 2.7 that $C(D_\ell^{\mathrm{ul}}) \cong C(D_1^{\mathrm{ul}})^{\otimes \ell}$. It is hence worthwhile to deal with the case $\ell = 1$ in detail.

It can be directly computed that $C(D_1^{\mathrm{ul}}) \cong C^\vee(D_1^{\mathrm{ul}})$ has six generators:

degree 0 : $a :=$ 

degree 1 : $b_1 :=$  , $b_2 :=$  , $b_3 :=$  , $b_4 :=$ 

degree 2 : $c :=$ 

The differential is $\partial_{D_1^{\mathrm{ul}}}(a) = b_1 + b_2 + b_3 + b_4$ and $\partial_{D_1^{\mathrm{ul}}}(b_1) = \partial_{D_1^{\mathrm{ul}}}(b_2) = \partial_{D_1^{\mathrm{ul}}}(b_3) = \partial_{D_1^{\mathrm{ul}}}(b_4) = c$. The non-zero elements of the homology are then represented by sums $b_i + b_j$ with $i \neq j \in [\![1, 4]\!]$ and two such sums are equivalent iff their supports are disjoint. The homology is then of rank 2 and its three non trivial elements are $[b_1 + b_2] = [b_3 + b_4]$, $[b_1 + b_3] = [b_2 + b_4]$ and $[b_1 + b_4] = [b_2 + b_3]$.

4.2. **Length.**

Proposition 4.1. *$n_\ell \sim \sqrt{\frac{3}{2\pi\ell}} 6^\ell$ as ℓ tends to infinity.*

Proof. Since Prop. 2.7, we have $C(D_\ell^{\mathrm{ul}}) = C(D_1^{\mathrm{ul}})^{\otimes \ell}$. It follows then that $\dim\left(C^\ell(D_\ell^{\mathrm{ul}})\right)$ is the coefficient of degree ℓ in $(1 + 4t + t^2)^\ell$, that is the constant term in $(t^{-1} + 4 + t)^\ell$. But

$$(t^{-1} + 4 + t)^\ell = \left((t^{-\frac{1}{2}} + t^{\frac{1}{2}})^2 + 2\right)^\ell = \sum_{r=0}^{\ell} \binom{\ell}{r} (t^{-\frac{1}{2}} + t^{\frac{1}{2}})^{2r} 2^{\ell-r} = 2^\ell \sum_{r=0}^{\ell} \frac{\binom{\ell}{r}}{2^r} \sum_{l=0}^{2r} \binom{2r}{l} t^{r-l}$$

so $n_\ell = 2^\ell \sum_{r=0}^{\ell} \frac{\binom{\ell}{r}\binom{2r}{r}}{2^r}$. Then we use Prop. A.2 to conclude. □

4.3. **Dimension.**

Proposition 4.2. *$k_\ell = 2^\ell$.*

This is a direct consequence of Prop. 2.7.

4.4. **Minimum distance.**

Proposition 4.3. *$d_\ell = 2^\ell$.*

Proof. It is easily seen that there is a differential-preserving one-to-one correspondance between generators of $C(D_\ell^{\mathrm{ul}})$ and $C(D_\ell^{\mathrm{ul}}!) \cong C^\vee(D_\ell^{\mathrm{ul}})$. It is hence sufficent to deal with $C(D_\ell^{\mathrm{ul}})$.

By induction on ℓ, we prove a sligthly stronger result: 2^ℓ is the minimum distance and it is reached for any non trivial element of the homology. This is trivial for $\ell = 0$ (and it has been checked for $\ell = 1$). Now, we assume the assertion is true for a given $\ell \in \mathbb{N}$.

Since $C(D^{\text{ul}}_{\ell+1}) \cong C(D^{\text{ul}}_{\ell}) \otimes C(D^{\text{ul}}_{1})$, any element A of $C^k(D^{\text{ul}}_{\ell+1})$, for $k \in [\![0, 2\ell+2]\!]$ can be decomposed into the following form

$$A = \begin{cases} x \otimes a & \in C^k(D^{\text{ul}}_{\ell}) \otimes C^0(D^{\text{ul}}_{1}) \\ + & \\ \sum_{i=1}^4 y_i \otimes b_i & \in C^{k-1}(D^{\text{ul}}_{\ell}) \otimes C^1(D^{\text{ul}}_{1}) \\ + & \\ z \otimes c & \in C^{k-2}(D^{\text{ul}}_{\ell}) \otimes C^2(D^{\text{ul}}_{1}) \end{cases}.$$

Thus, we have

$$\partial_{D^{\text{ul}}_{\ell+1}}(A) = \begin{cases} \partial_{D^{\text{ul}}_{\ell}}(x) \otimes a & \in C^{k+1}(D^{\text{ul}}_{\ell}) \otimes C^0(D^{\text{ul}}_{1}) \\ + & \\ \sum_{i=1}^4 \left(x + \partial_{D^{\text{ul}}_{\ell}}(y_i)\right) \otimes b_i & \in C^{k}(D^{\text{ul}}_{\ell}) \otimes C^1(D^{\text{ul}}_{1}) \\ + & \\ \left(y_1 + y_2 + y_3 + y_4 + \partial_{D^{\text{ul}}_{\ell}}(z)\right) \otimes c & \in C^{k-1}(D^{\text{ul}}_{\ell}) \otimes C^2(D^{\text{ul}}_{1}) \end{cases}.$$

Lemma 4.4. *If* $\left([w_1], \cdots, [w_{2^\ell}]\right)$ *is a basis for* $\text{Kh}(D^{ul}_{\ell})$*, then*

$$\left(\left[w_1 \otimes (b_1 + b_2)\right], \cdots, \left[w_{2^\ell} \otimes (b_1 + b_2)\right], \left[w_1 \otimes (b_1 + b_3)\right], \cdots, \left[w_{2^\ell} \otimes (b_1 + b_3)\right]\right)$$

is a basis for $\text{Kh}(D^{ul}_{\ell+1})$.

Proof. Elements of the form $w_i \otimes (b_i + b_j)$, for $i, j \in [\![1, 4]\!]$ are clearly in the kernel of $\partial_{D^{\text{ul}}_{\ell+1}}$. If

$$\sum_{i=1}^{2^\ell} \alpha_i \left[w_i \otimes (b_1 + b_2)\right] + \beta_i \left[w_i \otimes (b_1 + b_3)\right] = 0$$

with $(\alpha_i), (\beta_i) \in \mathbb{F}_2^{2^\ell}$, then there exists $A \in C_\ell(D^{\text{ul}}_{\ell+1})$ such that

$$\sum_{i=1}^{2^\ell} \alpha_i w_i \otimes (b_1 + b_2) + \beta_i w_i \otimes (b_1 + b_3) = \partial_{D^{\text{ul}}_{\ell+1}}(A)$$

and hence, with the notation above, and by looking at the $\ . \otimes b_i$ parts,

$$\begin{cases} x + \partial_{D^{\text{ul}}_{n}}(y_1) = \sum_{i=1}^{2^\ell} (\alpha_i + \beta_i) w_i \\ x + \partial_{D^{\text{ul}}_{n}}(y_2) = \sum_{i=1}^{2^\ell} \alpha_i w_i \\ x + \partial_{D^{\text{ul}}_{n}}(y_3) = \sum_{i=1}^{2^\ell} \beta_i w_i \\ x + \partial_{D^{\text{ul}}_{n}}(y_4) = 0 \end{cases}.$$

It follows that $\sum_{i=1}^{2^\ell} \alpha_i w_i = \partial_{D^{\text{ul}}_{\ell}}(y_2 + y_4)$ and $\sum_{i=1}^{2^\ell} \beta_i w_i = \partial_{D^{\text{ul}}_{\ell}}(y_3 + y_4)$. This means that $\sum_{i=1}^{2^\ell} \alpha_i [w_i] = \sum_{i=1}^{2^\ell} \beta_i [w_i] = 0$ and hence that $\alpha_i = \beta_i = 0$ for every $i \in [\![1, 2^\ell]\!]$. □

Lemma 4.5. *If* $[A]$ *is a non trivial element of* $\text{Kh}(D^{ul}_{\ell+1})$ *then* $|A| \geq 2^{\ell+1}$.

Proof. If $A = \alpha \otimes a + \sum_{i=1}^4 \beta_i \otimes b_i + \gamma \otimes c$, then $|A| = |\alpha| + \sum_{i=1}^4 |\beta_i| + |\gamma|$. According the precedent lemma, there exists $(v, w) \in \text{Ker}(\partial_{D^{\text{ul}}_{\ell}})$ such that $[A] = \left[(v + w) \otimes b_1 + v \otimes b_2 + w \otimes b_3\right]$ with $([v], [w]) \neq (0, 0)$. As above, it follows, that

$$\begin{cases} x + \partial_{D^{\text{ul}}_{\ell}}(y_1) = \beta_1 + v + w \\ x + \partial_{D^{\text{ul}}_{\ell}}(y_2) = \beta_2 + v \\ x + \partial_{D^{\text{ul}}_{\ell}}(y_3) = \beta_3 + w \\ x + \partial_{D^{\text{ul}}_{\ell}}(y_4) = \beta_4. \end{cases}$$

If $[v] \neq 0$, then $\beta_1 + \beta_3 = v + \partial_{D^{\text{ul}}_{\ell}}(y_1 + y_3)$ and $\beta_2 + \beta_4 = v + \partial_{D^{\text{ul}}_{\ell}}(y_2 + y_4)$ so $[\beta_1 + \beta_3] = [\beta_2 + \beta_4]$ is a non trivial element of $\text{Kh}(D^{\text{ul}}_{\ell})$ so $|\beta_1 + \beta_3| \geq 2^\ell$ and $|\beta_2 + \beta_4| \geq 2^\ell$. Finally

$$|A| \geq |\beta_1| + |\beta_2| + |\beta_3| + |\beta_4| \geq |\beta_1 + \beta_3| + |\beta_2 + \beta_4| \geq 2^{\ell+1}.$$

If $[v] = 0$ then we replace v by w. □

□

Remark 4.1. This proposition would be a direct application of question 2.6 if it were answered true. It is also an example of chain complexes product with minimum distance equal to the product of the minimum distances.

Remark 4.2. It is explicit in the proof that minimally weighted homology-surviving elements are carried by 4^ℓ generators only, namely those of $C_1(D_1^{\mathrm{ul}})^{\otimes \ell}$.

Question 4.3. Can unlink codes be swept out, for instance by removing acyclic subcomplexes, so they reach parameter $[\![4^\ell; 2^\ell; 2^\ell]\!]$? Since it would share almost the same dimension and same logarithmic sparseness property, would it be somehow related to Couvreur–Delfosse–Zemor codes ([CDZ12]) ?

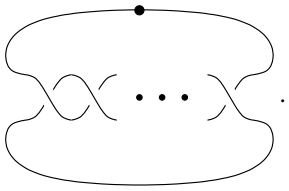
4.5. **Sparseness.**

Proposition 4.6. *The weight of each row in the ℓ^{th} unlink code is $O\big(\ln(n_\ell)\big)$ as ℓ increases.*

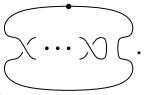
Proof. It is clear from Khovanov homology construction that each row has between $\ell + 1$ and $2(\ell + 1)$ non trivial entries. Since $4^\ell \leq n_\ell \leq 6^\ell$, the result follows. □

5. $(2, n)$–TORUS LINK CODES

For every $\ell \in \mathbb{N}$, we consider the following diagram D_ℓ^{tl} of the pointed $(2, \ell)$–torus link:



For every $r \in [\![2, \ell]\!]$, the code obtained from $\big(C^{r-1}(D_\ell^{\mathrm{tl}}) \xrightarrow{\partial_{D_\ell^{\mathrm{tl}}}} C^r(D_\ell^{\mathrm{tl}}) \xrightarrow{\partial_{D_\ell^{\mathrm{tl}}}} C^{r+1}(D_\ell^{\mathrm{tl}})\big)$ is called $(\ell, r)^{th}$ $(2, n)$–*torus link code*. Its parameters are denoted by $[\![n_{\ell,r}; k_{\ell,r}; d_{\ell,r}]\!]$.

5.1. **Homology.** For convenience, we introduce, for every $\ell \in \mathbb{N}$ the diagram $U_\ell :=$  . It follows from Prop. 2.3 that $\mathrm{Kh}(U_\ell)$ and $\mathrm{Kh}(U_\ell!)$ have only one non-zero element, respectively in degree ℓ and 0. Then the exact long sequence presented in section 2.7, applied to the rightmost crossing, gives for every $\ell \in \mathbb{N}^*$

$$0 \longrightarrow \mathrm{Kh}^r(D_\ell^{\mathrm{tl}}) \xrightarrow{\beta_\ell^r} \mathrm{Kh}^r(D_{\ell-1}^{\mathrm{tl}}) \longrightarrow 0 \quad \text{for } r \in [\![0, \ell - 2]\!]$$

$$0 \longrightarrow \mathrm{Kh}^{\ell-1}(D_\ell^{\mathrm{tl}}) \xrightarrow{\beta_\ell^{\ell-1}} \mathrm{Kh}^{\ell-1}(D_{\ell-1}^{\mathrm{tl}}) \longrightarrow \underset{\mathbb{F}_2}{\mathrm{Kh}^{\ell-1}(U_{\ell-1})} \xrightarrow{\alpha_\ell} \mathrm{Kh}^\ell(D_\ell^{\mathrm{tl}}) \longrightarrow 0$$

$$0 \longrightarrow \mathrm{Kh}^{r-1}(D_{\ell-1}^{\mathrm{tl}}!) \xrightarrow{\alpha_\ell^r} \mathrm{Kh}^r(D_\ell^{\mathrm{tl}}!) \longrightarrow 0 \quad \text{for } r \in [\![2, \ell]\!]$$

$$0 \longrightarrow \mathrm{Kh}^0(D_\ell^{\mathrm{tl}}!) \xrightarrow{\beta_\ell} \underset{\mathbb{F}_2}{\mathrm{Kh}^0(U_{\ell-1}!)} \longrightarrow \mathrm{Kh}^0(D_{\ell-1}^{\mathrm{tl}}!) \xrightarrow{\alpha_n^1} \mathrm{Kh}^1(D_\ell^{\mathrm{tl}}!) \longrightarrow 0\ .$$

But $\mathrm{Kh}^\ell(D_\ell^{\mathrm{tl}}) \neq 0$ since $\partial_{D_\ell^{\mathrm{tl}}} \colon C^{\ell-1}(D_\ell^{\mathrm{tl}}) \longrightarrow C^\ell(D_\ell^{\mathrm{tl}})$ involves only splitting circles, so the weight of any image is necessarily even and every single generator survives in homology. Similarly, it is easy to produce a

non trivial element in the kernel of $\partial_{D_\ell^{\mathrm{tl}}!}\colon C^0(D_\ell^{\mathrm{tl}}!) \longrightarrow C^1(D_\ell^{\mathrm{tl}}!)$ and since there is nothing to quotient by, it follows that $\mathrm{Kh}^0(D_\ell^{\mathrm{tl}}!) \neq 0$.

Then, by induction, we can deduce that all the named maps are isomorphisms and that:

$$\mathrm{Kh}_r(D_\ell^{\mathrm{tl}}) = \begin{cases} \mathbb{F}_2 \text{ for } r = 0 \text{ and } r \in [\![2, \ell]\!] \\ 0 \text{ otherwise} \end{cases} \qquad \mathrm{Kh}_r(D_\ell^{\mathrm{tl}}!) = \begin{cases} \mathbb{F}_2 \text{ for } r \in [\![0, \ell-2]\!] \text{ and } r = \ell \\ 0 \text{ otherwise} \end{cases}.$$

5.2. **Length and dimension.**

Proposition 5.1. *$n_{\ell,r} = 2^{r-1}\binom{\ell}{r}$ and $k_{\ell,r} = 1$.*

Proof. Concerning the length, one has to choose the r 1–resolved crossings and then it remains $r-1$ undotted circles to label.

The dimension has been computed in the previous section. □

5.3. **Minimum distance.**

Proposition 5.2. *For $r \in [\![2, \ell]\!]$, $d^r_{D_\ell^{\mathrm{tl}}} = \binom{\ell}{r}$ and $d^0_{D_\ell^{\mathrm{tl}}} = 2$.*

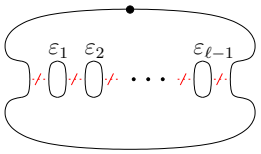
Proof. Within the framework of this proof and for simplicity, we will denote D_ℓ^{tl} by D and $\{+,-\}^{\ell-1}$ by S.

Equality $d^0_{D_\ell^{\mathrm{tl}}} = 2$ follows from the fact that $C^0(D)$ has only two generators with equal non-zero image throught ∂_D.

Now, we consider $r \in [\![2, \ell]\!]$. First we note that the cardinal of the set $E_r := \left\{\phi\colon \{\text{crossings of } D\} \longrightarrow \{0,1\} \;\middle|\; |\phi^{-1}(1)| = r\right\}$ is $\binom{\ell}{r}$. Then, we construct a map

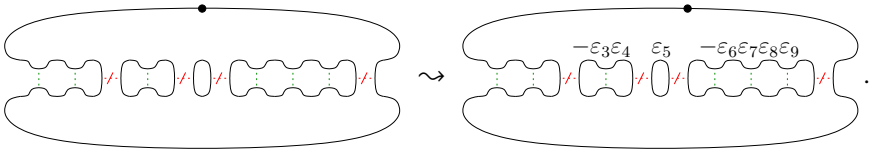
$$\begin{array}{ccc} E_r & \longrightarrow & \{\text{labelling maps}\} \\ \phi & \longmapsto & \sigma_\phi \end{array}$$

so that $\sum_{\phi\in E_r} D_\phi^{\sigma_\phi}$ is in the kernel of $\partial_D\colon C^r(D) \longrightarrow C^{r+1}(D)$. To this end, we choose $\underline{\varepsilon} := (\varepsilon_1, \cdots, \varepsilon_{\ell-1}) \in S$. When 1–resolving all the crossing of D, we obtain a resolution $D_{\underline{\varepsilon}}$ with $\ell-1$ undotted circles and we label them, from left to right with $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{\ell-2}$ and $\varepsilon_{\ell-1}$:

$D_{\underline{\varepsilon}} :=$ 

.

To $\phi \in E_r$ corresponds a resolution of D where $\ell - r$ crossings are turned into 0–resolutions. Roughly, we define $D^r_{\underline{\varepsilon}}$ as the image of $D_{\underline{\varepsilon}}$ under the partial maps ∂_c^{-1}, for c successively all these $\ell - r$ crossings. Explicitly, the $\ell - 1$ circles merge into $r - 1$ ones and there are numbers $a, b_1, \cdots, b_{r-1}, c \in \mathbb{N}$ such that the first a and the last c crossings are 0–resolved, and the i^{th} circle, numbered from left to right, contains b_i 0–resolved crossings. Note that the $(r+1)$-uple $(a, b_1, \cdots, b_{r-1}, c)$ determines ϕ. Then we denote by B_i the sum $1 + a + \sum_{j=1}^{i-1}(1+b_i)$ and we define σ_ϕ the map which label the i^{th} circle by $\Lambda_i := (-1)^{1+b_i}\varepsilon_{B_i}\varepsilon_{B_i+1}\cdots\varepsilon_{B_i+b_i}$.
For instance, the case $\ell = 10$, $r = 4$, $a = 2$, $b_1 = 1$, $b_2 = 0$, $b_3 = 3$ and $c = 0$ gives



.

We denote $\sum_{\phi\in E_r} D_\phi^{\sigma_\phi}$ by $D^r_{\underline{\varepsilon}}$ and claim that $\partial_D(D^r_{\underline{\varepsilon}}) = 0$. It is sufficient to show that for any given $\varphi \in E_{r+1}$ the contributions of the form D_φ^σ cancel. So let us choose such a φ. As above, we can describe it by integers

$a, b_1, \cdots, b_r, c$. The elements of E_r such that $\partial_D(D_\phi^{\sigma_\phi})$ contributes are

$$\begin{array}{c} (a+1+b_1, b_2, \cdots, b_r, c); \\ (a, b_1, \cdots, b_{i-1}, b_i+1+b_{i+1}, b_{i+2}, \cdots, b_r, c) \quad \text{for } i \in [\![1, r-1]\!]; \\ (a, b_1, \cdots, b_{r-1}, b_r+1+c). \end{array}$$

The labels of their circles, given from left to right and using the same notation Λ_i as above are

$$\begin{array}{c} \big(\Lambda_2, \cdots, \Lambda_r\big); \\ \big(\Lambda_1, \cdots, \Lambda_{i-1}, -\Lambda_i\Lambda_{i+1}, \Lambda_{i+2}, \cdots, \Lambda_r\big) \quad \text{for } i \in [\![1, r-1]\!]; \\ \big(\Lambda_1, \cdots, \Lambda_{r-1}\big). \end{array}$$

And their contributions, again given by the labels of the circles, are

$$\begin{array}{c} \big(\Lambda_1, \Lambda_2, \cdots, \Lambda_r\big) \ ; \ \big(-\Lambda_1, \Lambda_2, \cdots, \Lambda_r\big) \\ \big(\Lambda_1, \cdots, \Lambda_{i-1}, -\Lambda_i, \Lambda_{i+1}, \Lambda_{i+2}, \cdots, \Lambda_r\big) \ ; \ \big(\Lambda_1, \cdots, \Lambda_{i-1}, \Lambda_i, -\Lambda_{i+1}, \Lambda_{i+2}, \cdots, \Lambda_r\big) \quad \text{for } i \in [\![1, r-1]\!]; \\ \big(\Lambda_1, \Lambda_2, \cdots, -\Lambda_r\big) \ ; \ \big(\Lambda_1, \Lambda_2, \cdots, \Lambda_r\big); \end{array}$$

They do cancel indeed. The element $D^r_{\underline{\varepsilon}}$ is hence an element of the kernel of ∂_D which contains exactly one element for each resolution of E_r. But the map ∂_D only splits circles, so it produces even numbers of contributions for each resolution of E_r. So $D^r_{\underline{\varepsilon}}$ cannot be in the image of ∂_D and it survives in homology. Moreover, it is of weight $\binom{\ell}{r}$.

Now, we assume *ad absurdum* that there exists $x \in \ker(\partial_{D|C^r(D)})$, surviving in homology and satisfying $|x| < |D^r_{\underline{\varepsilon}}|$. Then there is a resolution of E_r which doesn't appear in x, and hence it appears exactly once in $x + D^r_{\underline{\varepsilon}}$. It follows that $x + D^r_{\underline{\varepsilon}}$ survives in homology for the same reason as $D^r_{\underline{\varepsilon}}$. But $\dim\big(\mathrm{Kh}^r(D)\big) = 1$, so $[x] = [D^r_{\underline{\varepsilon}}]$ and $[x + D^r_{\underline{\varepsilon}}] = 0$. This concludes the proof for $r \in [\![2, \ell]\!]$. □

Remark 5.1. Defining a representative of the non trivial homology class for every $(\varepsilon_1, \cdots, \varepsilon_{\ell-1}) \in S$ is obviously redundant since the simpliest case, when all circles are labelled by $-$, would have been sufficient. However, all these $D^r_{\underline{\varepsilon}}$ will be helpful in the proof of the next proposition.

Proposition 5.3. *For $r \in [\![0, \ell-2]\!]$, $d^r_{D^{\mathrm{tl}}_\ell!} = 2^{\ell-r-1}$ and $d^\ell_{D^{\mathrm{tl}}_\ell!} = 1$.*

Proof. Since the homology is non trivial in degree ℓ, the assertion on $d^\ell_{D^{\mathrm{tl}}_\ell!}$ is also trivial.

The map β_ℓ from section 5.1 is an isomorphism and the map underlying β_ℓ at the chain complexes level is a generator-preserving isomorphism. Since it follows from Prop. 2.11 that $d^0_{U_{\ell-1}} = 2^{\ell-1}$, Prop. 2.10 implies that $d^0_{D^{\mathrm{tl}}_\ell!} = 2^{\ell-1}$. Then, inductive use of maps α^r_ℓ, for $r \in [\![1, \ell-2]\!]$, shows that $d^r_{D^{\mathrm{tl}}_\ell!} \leq 2^{\ell-r-1}$.

Reciprocally, we consider an element $x \in \mathrm{Ker}(\partial_{D^{\mathrm{tl}}_\ell!}) \cap C^r(D^{\mathrm{tl}}_\ell!)$ such that $|x| < 2^{\ell-r-1}$. Up to the reversing of all signs, x can be seen as an element $x^\vee$ of the dual of $C^{\ell-r}(D^{\mathrm{tl}}_\ell!)$. Using the notation of the previous proof, our goal is now to prove that there exists some $\underline{\varepsilon} \in S$ such that $x^\vee(D^r_{\underline{\varepsilon}}) = 0$. It will follow from lemma 1.1 and the fact that $\dim\big(C^{\ell-r}(D^{\mathrm{tl}}_\ell)\big) = 1$, that $x^\vee$ is null in cohomology. Let x_0 be a generator of $C^{\ell-r}(D^{\mathrm{tl}}_\ell!)$ and $x_0^\vee$ its dual element under the map m of Prop. 2.5. For $x_0^\vee(D^r_{\underline{\varepsilon}}) = 0$ to hold, it is sufficient that x_0 doesn't appear in $D^r_{\underline{\varepsilon}}$. The generator x_0 is determined by its labelling $(\eta_1, \cdots, \eta_{\ell-r-1}) \in \{+, -\}^{\ell-r-1}$ read from left to right and its r crossings c which are 0–resolved. It is easily checked that for each such crossing, ∂_c^{-1}(any generator) contains exactly two elements. It follows that there are only 2^r elements $\underline{\varepsilon} \in S$ so that $x_0^\vee(D^r_{\underline{\varepsilon}}) \neq 0$. As a consequence, there is at most $2^r|x| < 2^{\ell-1} = \#S$ elements $\underline{\varepsilon} \in S$ so that $x^\vee(D^r_{\underline{\varepsilon}}) \neq 0$. There is thus room for at least one $\underline{\varepsilon} \in S$ such that $x^\vee(D^r_{\underline{\varepsilon}}) = 0$. This concludes the proof. □

Corollary 5.4. $d_{\ell,r} = \min\left\{\binom{\ell}{r}, 2^{r-1}\right\}$.

5.4. **Summary.**

r	0	1	2	$r \in [\![3, \ell-1]\!]$	ℓ
$\dim\left(C^r(D^{\mathrm{tl}}_\ell)\right)$	2	ℓ	$\ell(\ell+1)$	$2^{r-1}\binom{\ell}{r}$	$2^{\ell-1}$
$\dim\left(\mathrm{Kh}^r(D^{\mathrm{tl}}_\ell)\right)$	1	0	1	1	1
$d^r_{D^{\mathrm{tl}}_\ell}$	2	∞	$\frac{\ell(\ell+1)}{2}$	$\binom{\ell}{r}$	1
$d^{\ell-r}_{D^{\mathrm{tl}}_\ell!}$	1	∞	2	2^{r-1}	$2^{\ell-1}$

5.5. **Extraction of a subfamily.** Since the minimum distance $d_{\ell,r}$ is a minimum involving $\binom{\ell}{r}$, it collapses for extremal values of r. However, for $r \approx \frac{\ell}{2}$, we have, for large ℓ, $\binom{\ell}{\frac{\ell}{2}} \sim \frac{2^{\ell+\frac{1}{2}}}{\sqrt{\pi\ell}}$ which is greater than $2^{\frac{\ell}{2}-1}$. So one can expect to find a "best" value r_ℓ such that $\binom{\ell}{r_\ell} \approx 2^{r_\ell-1}$. As a matter of fact, for every $\ell \in \mathbb{N}^*$, we define $r_\ell := \mathrm{round}\big(\alpha_0\ell - \beta_0\ln(\ell) + \gamma_0\big)$ with round(.) any rounding function to the nearest integer, α_0 the unique zero in $(0,1)$ of the function $\big(x \mapsto (2x)^x(1-x)^{1-x} - 1\big)$, $\beta_0 := \frac{1}{2\ln\left(\frac{2\alpha_0}{1-\alpha_0}\right)}$ and $\gamma_0 := \beta_0 \ln\left(\frac{2}{\pi\alpha_0(1-\alpha_0)}\right)$.

Proposition 5.5. *The family of $(\ell, r_\ell)^{th}$ $(2,\ell)$–torus link codes has asymptotical parameter $[\![n; 1; d_n]\!]$ with $d_n > \frac{\sqrt{n}}{1{,}62}$.*

Proof. This is a consequence of Prop. A.3 □

Question 5.2. Computations suggests that the sequence $(2\varepsilon_\ell)_{\ell\in\mathbb{N}^*}$ is dense in $[-1,1]$. If true, or at least if there is a subsequence $(\varepsilon_{\ell_s})_{s\in\mathbb{N}}$ converging to 0, then the subfamily of $(\ell_s, r_{\ell_s})^{\text{th}}$ $(2,\ell)$–torus link codes would have an asymptotical parameter $[\![n; 1; \sqrt{n}]\!]$ similar to Kitaev code one.

5.6. **Sparseness.**

Proposition 5.6. *If $(r_\ell)_{\ell\in\mathbb{N}}$ is any sequence satisfying $\alpha\ell \le r_\ell \le \beta\ell$ for every $\ell \in \mathbb{N}$ and some given $\alpha, \beta \in (0,1)$, then the weight of each row in the $(\ell, r_\ell)^{th}$ $(2,\ell)$–torus link code is $O\big(\ln(n_{\ell,r_\ell})\big)$ as ℓ increases.*

Proof. By construction, the rows of one matrix have exactly $2(\ell - r_\ell)$ non trivial entries and the rows of the other matrix exactly r_ℓ. So the weight of each row is bounded below by $\min\big(\alpha, 2(1-\beta)\big)\ell$ and above by $\max\big(\beta, 2(1-\alpha)\big)\ell$. But according Prop. 5.1, the length is $2^{r_\ell-1}\binom{\ell}{r_\ell} \ge 2^{r_\ell-1} \ge \frac{(2^\alpha)^\ell}{2}$. □

Remark 5.3. The subfamily dicussed in the previous section satisfies such bounds for r_ℓ.

Appendix A. Technical proofs

For the sake of clarity, we gather in this appendix some analytical proofs which would have weight down the core of the text.

Proposition A.1. *For any $x \in \mathbb{R}_+^*$, $\sum_{r=0}^{\ell}\left[\binom{\ell}{r}x^r\right]^2 \sim \frac{(1+x)^{2\ell+1}}{2\sqrt{x\pi\ell}}$ as ℓ tends to infinity.*

Proof. For every $\ell \in \mathbb{N}$, we define $f_\ell\colon \mathbb{R} \longrightarrow \mathbb{C}$ by $f_\ell(t) = (1 + xe^{2it})^\ell = \sum_{r=0}^{\ell}\binom{\ell}{r}x^r e^{2irt}$. Then, since f_ℓ is clearly π–periodic and L^2, Parseval's identity gives

$$\sum_{r=0}^{\ell}\left[\binom{\ell}{r}x^r\right]^2 = \frac{1}{\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}|1+xe^{2it}|^{2\ell}dt = \frac{1}{\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}(1+2x\cos(2t)+x^2)^\ell dt = \int_I \frac{1}{\pi}e^{\ell f_x(t)}$$

with $I = \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ and $f_x(t) = \ln\big(1 + 2x\cos(2t) + x^2\big)$. Now, f_x is smooth with $f_x'(t) = \frac{-4x\sin(2t)}{1+2x\cos(2t)+x^2}$ and $f_x''(t) = \sin(2t) \times \text{something} - \frac{8x\cos(2t)}{1+2x\cos(2t)+x^2}$, so 0 is the unique maximum of f_x on I and it is non degenerate. It follows from the method of steepest descent that $\sum_{r=0}^{\ell}\left[\binom{\ell}{r}x^r\right]^2 \sim \frac{1}{\pi}\sqrt{\frac{2\pi}{\ell}}e^{\ell\ln(1+2x+x^2)}\frac{1}{\sqrt{\frac{8x}{1+2x+x^2}}} = \frac{(1+x)^{2\ell+1}}{2\sqrt{x\pi\ell}}$.

□

Proposition A.2. $2^\ell \sum_{r=0}^{\ell} \frac{\binom{\ell}{r}\binom{2r}{r}}{2^r} \sim \sqrt{\frac{3}{2\pi\ell}} 6^\ell$ *as* ℓ *tends to infinity.*

Proof. We consider the power series $f(x) = \sum_{\ell\geq 0} T_\ell x^\ell$ with $T_\ell := 2^\ell \sum_{r=0}^{\ell} \frac{\binom{\ell}{r}\binom{2r}{r}}{2^r}$. This is well defined in a neighrborhood of 0 since T_ℓ is clearly bounded above by $\left((t^{-1}+4+t)^\ell\right)_{t=1} = 6^\ell$. Then, for x sufficiently small, we have

$$f(x) = \sum_{\ell\geq 0}\sum_{r=0}^{\ell} 2^\ell \frac{\binom{\ell}{r}\binom{2r}{r}}{2^r} x^\ell = \sum_{r\geq 0}\sum_{\ell\geq r} \frac{\binom{2r}{r}}{2^r}\binom{\ell}{r}(2x)^\ell.$$

It is standard to check that $\frac{1}{\sqrt{1-4z}} = \sum_{r\geq 0}\binom{2r}{r} z^r$ and, for any $r\in\mathbb{N}$, $\frac{z^r}{(1-z)^{r+1}} = \sum_{\ell\geq r}\binom{\ell}{r} z^\ell$. So, we can deduce

$$f(x) = \sum_{r\geq 0} \frac{\binom{2r}{r}}{2^r} \frac{(2x)^r}{(1-2x)^{r+1}} = \frac{1}{1-2x}\sum_{r\geq 0}\binom{2r}{r}\left(\frac{x}{1-2x}\right)^r = \frac{1}{(1-2x)\sqrt{1-4\frac{2x}{1-2x}}} = \frac{1}{\sqrt{1-8x+12x^2}}$$

But since it is known (see *e.g.* [AS64], formula 22.9.1 for $\alpha=\beta=0$, p. 783) that $\frac{1}{\sqrt{1-2xt+t^2}} = \sum_{\ell\geq 0} P_\ell(x) t^\ell$ where P_ℓ is the ℓ^{th} Legendre polynomial. It follows that $T_\ell = \left(2\sqrt{3}\right)^\ell P_\ell\left(\frac{2}{\sqrt{3}}\right)$. On the other hand, it is also known (see *e.g.* [AS64], formula 22.3.1 for $\alpha=\beta=0$, p. 775) that $P_\ell(x) = \frac{1}{2^\ell}\sum_{r=0}^{\ell}\binom{\ell}{r}^2 (x-1)^{n-r}(x+1)^r$, so

$$x_0^\ell T_\ell = \sum_{r=0}^{\ell}\left[\binom{\ell}{r} x_0^r\right]^2$$

with $x_0 = \frac{1}{2-\sqrt{3}}$. Using Prop. A.1 for $x = x_0$, we obtain the desired $T_\ell \sim \sqrt{\frac{3}{2\pi\ell}} 6^\ell$. □

Proposition A.3. *If, for every* $\ell\in\mathbb{N}^*$, $r_\ell := \text{round}\left(\alpha_0\ell - \beta_0\ln(\ell) + \gamma_0\right)$ *with* α_0 *the unique zero in* $(0,1)$ *of the function* $\left(x\mapsto (2x)^x(1-x)^{1-x}-1\right)$, $\beta_0 := \frac{1}{2\ln\left(\frac{2\alpha_0}{1-\alpha_0}\right)}$ *and* $\gamma_0 := \beta_0\ln\left(\frac{2}{\pi\alpha_0(1-\alpha_0)}\right)$, *then, for every sufficiently large integer* ℓ, $\min\left\{\binom{\ell}{r_\ell}, 2^{r_\ell-1}\right\} > \frac{\sqrt{2^{r_\ell-1}\binom{\ell}{r_\ell}}}{1{,}62}$.

Proof. First we note that $\frac{1}{2} + \beta_0\ln\left(\frac{1-\alpha_0}{2\alpha_0}\right) = 0$ and that $\left(\frac{2\alpha_0}{1-\alpha_0}\right)^{\gamma_0} = \sqrt{\frac{2}{\pi\alpha_0(1-\alpha_0)}}$.

Now, we write $r_\ell = \alpha_0\ell - \beta_0\ln(\ell) + \gamma_0 + \varepsilon_\ell$ with $|\varepsilon_\ell|\leq\frac{1}{2}$ and $\gamma_\ell := \gamma_0 + \varepsilon_\ell$. Stirling's approximation applied to $\ell!$, $r_\ell!$ and $(n-r_\ell)!$ gives

$$\begin{aligned}\frac{2^{r_\ell-1}}{\binom{\ell}{r_\ell}} &= \sqrt{\frac{\ell\pi}{2}}\sqrt{\frac{r_\ell}{\ell}\left(1-\frac{r_\ell}{\ell}\right)}\left(\frac{2r_\ell}{\ell}\right)^{r_\ell}\left(1-\frac{r_\ell}{\ell}\right)^{\ell-r_\ell}\left(1+o(1)\right)\\ &= \sqrt{\frac{\ell\pi\alpha_0(1-\alpha_0)}{2}}\underbrace{\left(\frac{2r_\ell}{\ell}\right)^{r_\ell}\left(1-\frac{r_\ell}{\ell}\right)^{\ell-r_\ell}}_{A_\ell}\left(1+o(1)\right).\end{aligned}$$

Then

$$\begin{aligned}A_\ell &= 2^{\alpha_0-\beta_0\ln(\ell)+\gamma_\ell}\left(\alpha_0 - \beta_0\frac{\ln(\ell)}{\ell} + \frac{\gamma_\ell}{\ell}\right)^{\alpha_0\ell-\beta_0\ln(\ell)+\gamma_\ell}\left(1-\alpha_0+\beta_0\frac{\ln(\ell)}{\ell}-\frac{\gamma_\ell}{\ell}\right)^{(1-\alpha_0)\ell+\beta_0\ln(\ell)-\gamma_\ell}\\ &= \left((2\alpha_0)^{\alpha_0}(1-\alpha_0)^{1-\alpha_0}\right)^\ell \frac{2^{\gamma_\ell}}{2^{\beta_0\ln(\ell)}} B_\ell C_\ell D_\ell \;=\; \frac{2^{\gamma_\ell}}{\ell^{\beta_0\ln 2}} B_\ell C_\ell D_\ell\end{aligned}$$

with

$$B_\ell := \left(1-\beta_0\frac{\ln(\ell)}{\alpha_0\ell}+\frac{\gamma_\ell}{\alpha_0\ell}\right)^{\alpha_0\ell} \qquad C_\ell := \left(1+\beta_0\frac{\ln(\ell)}{(1-\alpha_0)\ell}-\frac{\gamma_\ell}{(1-\alpha_0)\ell}\right)^{(1-\alpha_0)\ell} \qquad D_\ell := \left(\frac{1-\alpha_0+\beta_0\frac{\ln(\ell)}{\ell}-\frac{\gamma_\ell}{\ell}}{\alpha_0-\beta_0\frac{\ln(\ell)}{\ell}+\frac{\gamma_\ell}{\ell}}\right)^{\beta_0\ln(\ell)-\gamma_\ell}.$$

But

$$B_\ell = e^{\alpha_0\ell\ln\left(1-\beta_0\frac{\ln(\ell)}{\alpha_0\ell}+\frac{\gamma_\ell}{\alpha_0\ell}\right)} = e^{\alpha_0\ell\left(-\beta_0\frac{\ln(\ell)}{\alpha_0\ell}+\frac{\gamma_\ell}{\alpha_0\ell}+o\left(\frac{1}{\ell}\right)\right)} = e^{-\beta_0\ln(\ell)+\gamma_\ell+o(1)} = \ell^{-\beta_0}e^{\gamma_\ell}\big(1+o(1)\big),$$

and similarly $C_\ell = \ell^{\beta_0}e^{-\gamma_\ell}\big(1+o(1)\big)$. Concerning D_ℓ, we have

$$\begin{aligned} D_\ell &= e^{(\beta_0\ln(\ell)-\gamma_\ell)\left(\ln\left(\frac{1-\alpha_0}{\alpha_0}\right)+\ln\left(1+\beta_0\frac{\ln(\ell)}{(1-\alpha_0)\ell}-\frac{\gamma_\ell}{(1-\alpha_0)\ell}\right)+\ln\left(1-\beta_0\frac{\ln(\ell)}{\alpha_0\ell}+\frac{\gamma_\ell}{\alpha_0\ell}\right)\right)} = e^{(\beta_0\ln(\ell)-\gamma_\ell)\left(\ln\left(\frac{1-\alpha_0}{\alpha_0}\right)+o\left(\frac{\ln(\ell)}{\ell}\right)\right)} \\ &= e^{\beta_0\ln\left(\frac{1-\alpha_0}{\alpha_0}\right)\ln(\ell)-\gamma_\ell\ln\left(\frac{1-\alpha_0}{\alpha_0}\right)+o(1)} = \ell^{\beta_0\ln\left(\frac{1-\alpha_0}{\alpha_0}\right)}\left(\frac{\alpha_0}{1-\alpha_0}\right)^{\gamma_\ell}\big(1+o(1)\big). \end{aligned}$$

Finally, we get $A_\ell = \frac{2^{\gamma_\ell}}{\ell^{\beta_0\ln(2)}}\ell^{\beta_0\ln\left(\frac{1-\alpha_0}{\alpha_0}\right)}\left(\frac{\alpha_0}{1-\alpha_0}\right)^{\gamma_\ell}\big(1+o(1)\big) = \left(\frac{2\alpha_0}{1-\alpha_0}\right)^{\gamma_\ell}\ell^{\beta_0\ln\left(\frac{1-\alpha_0}{2\alpha_0}\right)}\big(1+o(1)\big)$ and hence

$$\begin{aligned} \frac{2^{r_\ell-1}}{\binom{\ell}{r_\ell}} &= \sqrt{\frac{\pi\alpha_0(1-\alpha_0)}{2}}\left(\frac{2\alpha_0}{1-\alpha_0}\right)^{\gamma_\ell}\ell^{\frac{1}{2}+\beta_0\ln\left(\frac{1-\alpha_0}{2\alpha_0}\right)}\big(1+o(1)\big) \\ &= \left(\frac{2\alpha_0}{1-\alpha_0}\right)^{\varepsilon_\ell}\sqrt{\frac{\pi\alpha_0(1-\alpha_0)}{2}}\left(\frac{2\alpha_0}{1-\alpha_0}\right)^{\gamma_0}\big(1+o(1)\big) = \left(\frac{2\alpha_0}{1-\alpha_0}\right)^{\varepsilon_\ell}+o(1). \end{aligned}$$

Now, computations show that $\delta_0 := 2.61 > \sqrt{\frac{2\alpha_0}{1-\alpha_0}} \geq \left(\frac{2\alpha_0}{1-\alpha_0}\right)^{\varepsilon_\ell} \geq \sqrt{\frac{1-\alpha_0}{2\alpha_0}} > \delta_0^{-1}$. So, for ℓ sufficiently large, we have $\delta_0^{-1}\binom{\ell}{r_\ell} < 2^{r_\ell-1} < \delta_0\binom{\ell}{r_\ell}$. For symmetry reason, we may assume that $2^{r_\ell-1} \leq \binom{\ell}{r_\ell}$. Then $(2^{r_\ell-1})^2 > \frac{2^{r_\ell-1}\binom{\ell}{r_\ell}}{\delta_0}$ and the results follow since $\sqrt{\delta_0} < 1.62$. □

References

[AS64] Milton Abramowitz and Irene A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, National Bureau of Standards Applied Mathematics Series, vol. 55, For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964.

[BMD06] H. Bombin and M. A. Martin-Delgado, *Topological quantum distillation*, Phys. Rev. Let. **97** (2006), no. 5, 180501.

[BMD07] ———, *Homological error correction: classical and quantum codes*, J. Math. Phys. **48** (2007), no. 5, 052105, 35.

[BPT10] S. Bravyi, D. Poulin, and B. Terhal, *Tradeoffs for reliable quantum information storage in 2d systems*, Phys. Rev. Lett. **104** (2010), 050503.

[CDZ12] Alain Couvreur, Nicolas Delfosse, and Gilles Zémor, *A construction of quantum LDPC codes from Cayley graphs*, arXiv:1206.2656, to appear in IEEE Transaction On Information Theory, 2012.

[CS96] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist*, Phys. Rev. A **54:1098** (1996).

[Del12] Nicolas Delfosse, *Constructions et performances de codes LDPC quantiques*, Ph.D. thesis, University of Bordeaux, 2012.

[Del13] ———, *Tradeoffs for reliable quantum information storage in surface codes and color codes*, arXiv:1301.6588, 2013.

[Fet12] Ethan Fetaya, *Bounding the distance of quantum surface codes*, J. Math. Phys. **53** (2012), no. 6, 062202, 12.

[FML02] Michael H. Freedman, David A. Meyer, and Feng Luo, *Z_2-systolic freedom and quantum codes*, Mathematics of quantum computation, Comput. Math. Ser., Chapman & Hall/CRC, Boca Raton, FL, 2002, pp. 287–320.

[Gal62] Robert G. Gallager, *Low density parity check codes*, Ph.D. thesis, Massachussetts Institute of Technology, 1962.

[HS97] P. J. Hilton and U. Stammbach, *A course in homological algebra*, second ed., Graduate Texts in Mathematics, vol. 4, Springer-Verlag, New York, 1997.

[Ito11] Noboru Ito, *Chain homotopy maps for Khovanov homology*, J. Knot Theory Ramifications **20** (2011), no. 1, 127–139.

[Kau87] Louis H. Kauffman, *On knots*, Annals of Mathematics Studies, vol. 115, Princeton University Press, Princeton, NJ, 1987.

[Kho00] Mikhail Khovanov, *A categorification of the Jones polynomial*, Duke Math. J. **101** (2000), no. 3, 359–426.

[Kho03] ———, *Patterns in knot cohomology. I*, Experiment. Math. **12** (2003), no. 3, 365–374.

[Kit03] A. Yu. Kitaev, *Fault-tolerant quantum computation by anyons*, Ann. Physics **303** (2003), no. 1, 2–30.

[Lan02] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[Lic97] W. B. Raymond Lickorish, *An introduction to knot theory*, Graduate Texts in Mathematics, vol. 175, Springer-Verlag, New York, 1997.

[ML95] Saunders Mac Lane, *Homology*, Classics in Mathematics, Springer-Verlag, Berlin, 1995, Reprint of the 1975 edition.

[NC10] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, 10th anniversary editions ed., Cambridge University Press. xxxi, Cambridge, 2010.

[Pre] John Preskill, *Quantum information and computation*, `http://www.theory.caltech.edu/people/preskill/ph229/`.

[Rei72] Kurt Reidemeister, *Einführung in die kombinatorische Topologie*, Wissenschaftliche Buchgesellschaft, Darmstadt, 1972, Unveränderter reprografischer Nachdruck der Ausgabe Braunschweig 1951.

[Shu11] Alexander N. Shumakovitch, *Patterns in odd Khovanov homology*, J. Knot Theory Ramifications **20** (2011), no. 1, 203–222.

[Ste96] A. Steane, *Multiple particle interference and quantum error correction*, Proc. Roy. Soc. Lond. A **452:2551** (1996), 2551–2577.

[TZ09] Jean-Pierre Tillich and Gilles Zémor, *Quantum LDPC codes with positive rate and minimum distance proportional to $n^{\frac{1}{2}}$*, arXiv:0903.0566, 2009.

[Vir04] Oleg Viro, *Khovanov homology, its definitions and ramifications*, Fund. Math. **184** (2004), 317–342.
[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.

CMI, Aix-Marseille Université, 39 rue Frédéric Joliot Curie 13453 Marseille Cedex 13 France
E-mail address: benjamin.audoux@univ-amu.fr