# Quantum circuits of c – Z and SWAP gates optimization and entanglement

Marc Bataille, Jean-Gabriel Luque

# Quantum circuits of $c-\mathtt{Z}$ and SWAP gates: optimization and entanglement

**Marc Bataille**

E-mail: marc.bataille@ac-rouen.fr

**Jean-Gabriel Luque**

E-mail: Jean-Gabriel.Luque@univ-rouen.fr
LITIS laboratory, Université Rouen-Normandie, 685 Avenue de l'Université, 76800 Saint-Étienne-du-Rouvray. France.

**Abstract.** We have studied the algebraic structure underlying the quantum circuits composed by $c-\mathtt{Z}$ and SWAP gates. Our results are applied to optimize the circuits and to understand the emergence of entanglement when a circuit acts on a fully factorized state.

PACS numbers: 03.67.-a,03.65.Aa,03.65.Fd,03.65.Ud,03.67.Bg,

## 1. Introduction

Back to basics: Computer Science is the science of using the laws of physics to perform calculations. It is a multidisciplinary field in which physics, mathematics and engineering interact. The computers we are currently handling are based on a ( *classical* ) mechanistic vision of the calculations: at first, the calculations were thought of as the result of a series of actions on gears or ribbons before being implemented on electronic devices that will give them their flexibility of use and the performances we know them to have today. Since the pioneers' works, many algorithms adapted both to the representation of the information in the proposed physical devices as well as to the logic underlying them have been developed and intensively studied. Nevertheless, many important problems (e.g. integer factorization and discrete logarithms) are known to be difficult to solve by computer. The only hope of breakthrough is to develop a computer science based on other physical laws. A fairly natural and promising way is to extend information theory to the quantum world in order to use phenomena such as state superposition and entanglement to improve performances. The idea dates back to the early 1980s [1, 2, 3]. The theories of Quantum Information and Quantum Computation have been extensively developed from this (see e.g. [4]) and some spectacular algorithms have been exhibited (e.g. [5, 6, 7]). But building an efficient quantum computer remains one of the greatest challenge of modern physic and one of its main difficulties is to manage with the instability of superposition. Several devices have been already experimented: optical quantum computers (e.g [8]), cavity -QED technique (e.g. [9] ), trapped ions (e.g.[10]), nuclear spins (e.g.[11, 12]). One of the main drawbacks of these devices is that quantum gates can not be applied without errors. Many strategies exist to solve this problem. The first one is to find more stable devices. As an example, Topological Quantum Computers [13] are good candidates but at the present time they are only theoretical machines manipulating quasi-particles named non-abelian anyons that have not been discovered yet. The second strategy consists in elaborating a theory of Quantum Error-Correction [14]. Finally, parallel to the latter, it is possible to optimize the circuits, for instance, by minimizing the number of multiqubit gates that generate many errors. Our work is situated in this context. More specifically, we are interested in the interactions between `SWAP` and $c-\mathtt{Z}$ (controlled Pauli-`Z` ) gates that allow simplifications. After recalling background on quantum circuits, we'll prove that circuits generated by these two gates form a finite group. Investigating its structure, we'll find algebraic and combinatorial properties that allow us to propose a very simple algorithm of simplification. Then, we'll ask the question of the emergence of entanglement: can we move from one entanglement level to another using only $c-\mathtt{Z}$ and `SWAP` gates together with `SLOCC` operations ?

## 2. Qubit systems, quantum gates and quantum circuits

The material contained in this section is rather classical in Quantum Information Theory. We mainly recall notations and results that the reader can find in [4, 15].
In Quantum Information a qubit is a quantum state that represents the basic information storage unit. For our purpose, we consider that the states are pure, i.e. states that are described by a single ket vector in the Dirac notation $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$ with $|a_0|^2+|a_1|^2 = 1$. The value of $|a_i|^2$ represents the probability that measurement produces the value $i$. Such a superposed state is often written as

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right). \tag{1}$$

The factor $e^{i\gamma}$ being ignored because having no observable effects, a single qubit depends only on two parameters and so defines a point on the unit three-dimensional sphere (the so called Bloch sphere)

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{2}$$

Operations on qubits must preserve the norm. So they act on qubits as $2\times 2$ unitary matrices act on two dimensional vectors. In Quantum Computation, they are represented by quantum gates. See figure 1 for a non exhaustive list of most used gates. The behavior of multiple qubit systems with respect to the action of its dynamic group is very rich and complicated to describe in the general case. A $k$-qubit system is seen as a superposition:

$$|\psi\rangle = \sum_{0\leq i_1,\ldots,i_k\leq 1} a_{i_1\cdots i_k}|i_1\cdots i_k\rangle, \tag{3}$$

with $\sum |a_{i_1\cdots i_k}|^2 = 1$. Some states have a particular interest like the Greenberger-Horne-Zeilinger state[16]

$$|\mathtt{GHZ}_k\rangle = \frac{1}{\sqrt{2}}\left(|\overbrace{0\cdots 0}^{\times k}\rangle + |\overbrace{1\cdots 1}^{\times k}\rangle\right) \tag{4}$$

and the `W`-states[17]

$$|\mathtt{W}_k\rangle = \frac{1}{\sqrt{k}}\left(|10\cdots 0\rangle + |010\cdots 0\rangle + \cdots + |0\cdots 01\rangle\right). \tag{5}$$

These two states represent two non-equivalent entanglements for a $k$-particles system (among a multitude of other non-equivalent ones).
Again operations on $k$-qubits must preserve the norm and are assimilated to $2^k\times 2^k$ matrices. For simplicity, we consider the rows and the column of the matrices encoding operations on qubits are indexed by integers in $\{0,\ldots,2^k-1\}$ written in the binary representations; the index $\alpha_{k-1}\cdots\alpha_0$ (i.e. binary representation of $\alpha_{k-1}2^{k-1}+\cdots+\alpha_0 2^0$) corresponds to the wave function $|\alpha_{k-1}\cdots\alpha_0\rangle$ (see figure 2 for some examples of 2-qubit gates). Notice that the $c-\mathtt{Not}$ and $c-\mathtt{Z}$ gates are special cases of controlled gates based on Pauli-`X` and Pauli-`Z` matrices. Notice also that for the $c-\mathtt{Z}$ gates the two

Hadamard $-\boxed{H}- \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

Pauli-`X` $-\boxed{X}- \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Pauli-`Y` $-\boxed{Y}- \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Pauli-`Z` $-\boxed{Z}- \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Rotation about the $x$ axis $-\boxed{R_x(\theta)}- \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$

Rotation about the $y$ axis $-\boxed{R_y(\theta)}- \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$

Rotation about the $z$ axis $-\boxed{R_z(\theta)}- \begin{bmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix}$

**Figure 1.** Some single qubit gates

`SWAP`  $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

$c-$ `Not`  $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

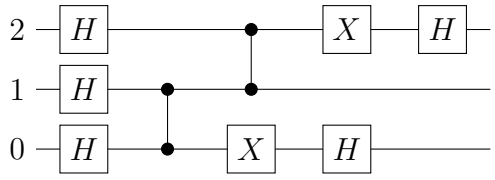
$c-$ `Z`  $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$

**Figure 2.** Some 2-qubit gates

qubits play the same role, hence the symmetrical representation of the gate. The gates can be combined in series or in parallel to form *Quantum Circuits* that represent new operators. Composing quantum gates in series allows to act on the same number of qubits and results in a multiplication of matrices read from the right to the left on the circuit‡. Composing quantum gates in parallel makes it possible to act on larger systems

‡ The reader must pay attention to the following fact: the circuits act to the right of the wave functions presented to their left but the associated operators act to the left of the ket, i.e. $O|\psi\rangle$.

and results in a Kronecker product of the matrices read from the top to the bottom on the circuit. See figure 3 for an example of quantum circuit and figure 4 for its action on a qubit system.



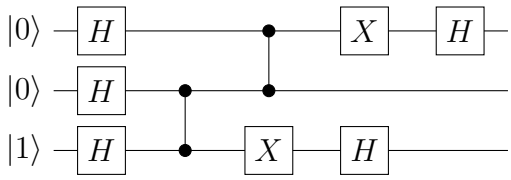

$$
\begin{aligned}
C &= (H \otimes I_4) \cdot (X \otimes I_2 \otimes H) \cdot (c-\mathtt{Z} \otimes X) \cdot (I_2 \otimes c-\mathtt{Z}) \cdot (H \otimes H \otimes H) \\
&= \frac{1}{\sqrt{2}} \begin{bmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\
0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\end{aligned}
$$

**Figure 3.** Example of Quantum Circuit together with its associated matrix ($I_k$ stands for the identity $k \times k$ matrix).

Using `SWAP` gates it is always possible to simulate gates acting on separate qubits on the circuits (see figure 5 as an example). From a purely algebraic point of view, the circuit compositions as well as the manipulations of the associated matrices fit in the context of the PRO theory (*product categories*) [18, 19]. PRO are algebraic structures that allow to abstract behaviors of operators with several inputs and several outputs. The link between compositions of gates and manipulations of matrices fits in a representation theory of PRO [20]. This remark has no impact on the rest of the paper, but it shows that the problem takes place within a much broader framework that connect many domains in Mathematics, Physics and Computer Science.

## 3. The group generated by $c-\mathtt{Z}$ and `SWAP` gates

For a computational point of view, 2-qubits gates are known to be universal [21], i.e. any quantum circuit admits an equivalent one composed only with single qubit and 2-qubits gates. More precisely, one can simulate any quantum system by using only single qubits




$$C|001\rangle \sim C \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = -\frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \sim -\frac{1}{\sqrt{2}} \left(|001\rangle + |110\rangle\right)$$

**Figure 4.** Example of the action of a Quantum circuit on a qubit system. $C$ denotes the operator associated to the circuit of figure 3.

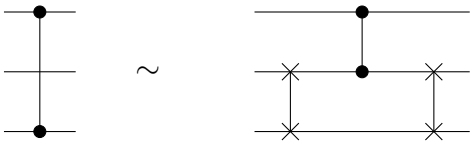
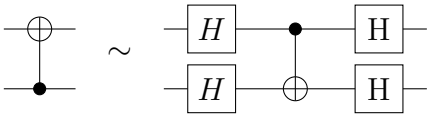


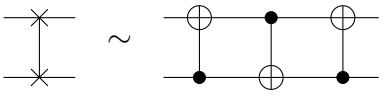
**Figure 5.** A $c-$ `Z` gate acting on two separated qubits simulated with `SWAP` gates

gates together with $c-$ `Not` gates. In particular, we have



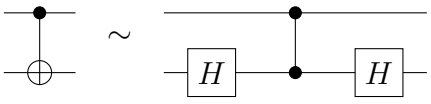

(6)

and



(7)

We notice also that the $c-$ `Z` has the same property of universality as $c-$ `Not` because we have




(8)

In general, two qubits quantum gates implementations are unreliable and may cause many execution errors (see appendix Appendix A). It is therefore of crucial importance to study the algebraic nature of the circuits in order to know how to use as few two-qubits gates as possible. In that context, we study the group $\mathtt{cZS}_k$ generated by the $c-\mathtt{Z}$ and `SWAP` gates acting on $k$-qubits. The motivation for studying such a (toy) model is that experimentally the order of the group is $k!2^{\binom{k}{2}}$, which suggests that it has interesting algebraic and combinatorial structures that can be exploited to simplify circuits.

### *3.1. The group* $\mathtt{cZS}_k$ *as a semi-direct product*

Let us prove the formula for the order of $\mathtt{cZS}_k$ and, at the same time, we exhibit the algebraic structure of this group. The $\mathtt{cZS}_k$ group is not the only interesting finite subgroup of the unitary transform of $k$-qubit systems. Let us denote by $S_i$ the `SWAP` gate acting simultaneously on the qubits $i$ and $i+1$ of the system. The group $\mathcal{S}_k$ generated by the $S_i$'s is straightforwardly isomorphic to the symmetric group $\mathfrak{S}_k$, i.e. $\mathcal{S}_k$ is a faithful (but non irreducible) representation of $\mathfrak{S}_k$. In literature, a permutation is usually a bijection of $\{1,\dots,k\}$ but to make it compatible with our notations, we instead consider that a permutation acts on $\{0,\dots,k-1\}$. This changes nothing to the theory of symmetric group (except a shift $-1$ for the notations). A `SWAP` gate is nothing but a transposition. We have seen that there is a one to one correspondence between the permutations of $\mathfrak{S}_k$ and the matrices of $\mathcal{S}_k$. To each permutation $\sigma$, we associate its corresponding matrix $S_\sigma$.

Similarly, denote by $Z_{ij}$ the matrix corresponding to the $c-\mathtt{Z}$ gates acting on the qubits $i$ and $j$. We notice that

$$Z_{ij}=Z_{ji},\ Z_{ij}^{-1}=Z_{ij}, \text{and } Z_{ij}Z_{i'j'}=Z_{i'j'}Z_{ij}. \tag{9}$$

Indeed, $Z_{ij}$ is a diagonal matrix where the entry $(\alpha,\alpha)$ equals $-1$ if both the bit $i$ of $\alpha$ and the bit $j$ of $\alpha$ equal 1, and 1 otherwise. We deduce that the group $\mathcal{P}_k$ generated by the $Z_{ij}$'s is isomorphic to the group $\mathfrak{P}_k$ whose elements are the subsets of $\{\{i,j\}\mid 0\leq i,j\leq k-1\}$ and the product is the symmetric difference $\oplus$. For any $E\subset\{\{i,j\}\mid 0\leq i,j\leq k-1\}$, we denote by $Z_E$ the preimage of $E$ by this isomorphism. Each matrix $Z_E$ is diagonal with only entries 1 and $-1$ on the diagonal. More precisely, the set $E$ is completely encoded in the diagonal of $Z_E$ since the entry of coordinates $(\alpha_{k-1}\cdots\alpha_0,\alpha_{k-1}\cdots\alpha_0)$ equals $(-1)^{\mathtt{card}\{\{i,j\}\in E\mid\alpha_i=\alpha_j=1\}}$. As an example,

$$Z_{\{\{0,1\},\{0,2\}\}}=\mathtt{diag}(1,1,1,-1,1,-1,1,1), \tag{10}$$

where $\mathtt{diag}(e_1,\dots,e_k)$ stands for the diagonal matrix with diagonal entries $e_1,\dots,e_k$. So, the product is easy to describe as

$$Z_EZ_{E'}=Z_{E\oplus E'}. \tag{11}$$

For instance, consider the following elements of $\mathcal{P}_3$:

$$Z_{\{\{0,1\},\{0,2\}\}}=Z_{01}Z_{02}=\mathtt{diag}(1,1,1,-1,1,-1,1,1), \tag{12}$$

$$Z_{\{\{0,1\},\{1,2\}\}} = \mathtt{diag}(1,1,1,-1,1,1,-1,1), \tag{13}$$

and

$$\begin{array}{rcl} Z_{\{\{0,1\},\{0,2\}\}}Z_{\{\{0,1\},\{1,2\}\}} & = & \mathtt{diag}(1,1,1,1,1,-1,-1,1) \\ & = & Z_{\{\{0,2\},\{1,2\}\}}. \end{array} \tag{14}$$

The group $\mathcal{P}_k$ is abelian with order $2^{\binom{k}{2}}$. The group $\mathtt{cZS}_k$ is the smallest group containing both $\mathcal{S}_k$ and $\mathcal{P}_k$ as subgroups. The conjectured order suggests that the underlying set of $\mathtt{cZS}_k$ is in bijection with the cartesian product $\mathfrak{S}_k \times \mathfrak{P}_k$. We remark also that the orbit of $Z_{01}$ for conjugation by the elements of $\mathcal{S}_k$ is the set $\{Z_{ij} \mid 0 \leq i,j \leq k-1\}$ (see figure 16 for an example with $k=6$). To be more precise, we have

$$S_\sigma Z_{ij} S_\sigma^{-1} = Z_{\sigma(i),\sigma(j)}. \tag{15}$$

This extends to any element of $\mathcal{P}_k$ by

$$S_\sigma Z_E S_\sigma^{-1} = S_\sigma \prod_{\{i,j\}\in E} Z_{ij} S_\sigma^{-1} = \prod_{\{i,j\}\in E} S_\sigma Z_{ij} S_\sigma^{-1} = Z_{\sigma(E)}. \tag{16}$$

From equality (16), we deduce that any $G \in \mathtt{cZS}_k$ admits a unique decomposition $G = PS$ with $P \in \mathcal{P}_k$ and $S \in \mathcal{S}$. Indeed, such a decomposition exists since if $Z_E, Z_{E'} \in \mathcal{P}_k$ and $S_\sigma, S_{\sigma'} \in \mathcal{S}_k$ we have

$$Z_E S_\sigma Z_{E'} S_{\sigma'} = Z_E S_\sigma Z_{E'} S_\sigma^{-1} S_\sigma S_{\sigma'} = Z_{E\oplus\sigma(E')} S_{\sigma\sigma'}. \tag{17}$$

The decomposition is unique because if $PS = P'S'$ with $P, P' \in \mathcal{P}_k$ and $S, S' \in \mathcal{S}_k$ then $SS'^{-1} = P^{-1}P \in \mathcal{P}_k \cap \mathcal{S}_k = \{I_{2^k}\}$, and so $S = S'$ and $P = P'$.

The results of this section are summarized in the following statement.

**Theorem 1** *The group* $\mathtt{cZS}_k$ *is a finite group of order* $k!2^{\binom{k}{2}}$. *It is isomorphic to the semi-direct product* $\mathfrak{P}_k \rtimes \mathfrak{S}_k$. *We recall that the underlying set of* $\mathfrak{P}_k \rtimes \mathfrak{S}_k$ *is the cartesian product* $\mathfrak{P}_k \times \mathfrak{S}_k$ *and its product is defined by* $(E,\sigma)(E',\sigma') = (E \oplus \sigma(E'), \sigma\sigma')$.

### *3.2. The group* $\mathtt{cZS}_k$ *as the quotient of a Coxeter group*

We give a few expressions of the group $\mathtt{cZS}_k$ as the quotient of some Coxeter groups. We recall that a Coxeter group (see eg [22]) is generated by a set of elements $g_0, g_1, \ldots$ satisfying $(g_i g_j)^{m_{ij}} = 1$ where $m_{ij} \in \mathbb{N} \cup \{\infty\} \setminus \{0,1\}$ and $m_{ij} = 1$ if and only if $i = j$; the condition $m_{ij} = \infty$ means that there is no relation of the form $(g_i g_j)^m = 1$. The relations are encoded in a Coxeter matrix $M = (m_{ij})_{ij}$ or, equivalently, in a Coxeter-Dynkin diagram which is the graph of the matrix $M$ where the edges $\{i,j\}$ where $m_{ij} \leq 2$ are removed and the edges where $m_{ij} = 3$ are unlabeled.

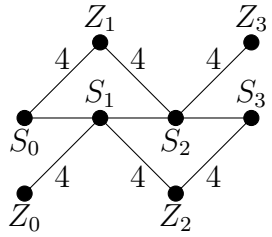
**Theorem 2** *Let us denote by* $\mathcal{W}_k$ *the Coxeter group generated by* $2(k-1)$ *elements* $g_0, g_1, \ldots, g_{2(k-2)+1}$ *submitted to the relations given by the Coxeter matrix*

$$M_k = \begin{bmatrix} D & A & B & \cdots & B \\ A & \ddots & \ddots & \ddots & \vdots \\ B & \ddots & \ddots & \ddots & B \\ \vdots & \ddots & \ddots & \ddots & A \\ B & \cdots & B & A & D \end{bmatrix} \tag{18}$$

*where* $A = \begin{bmatrix} 2 & 4 \\ 4 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$, *and* $D = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$.
*The group* $\mathtt{cZS}_k$ *is isomorphic to the quotient* $\mathcal{W}_k/_{\mathcal{R}_k}$ *of* $\mathcal{W}_k$ *by the relations* $\mathcal{R}_k := \{g_{2i+1}g_{2i+3}g_{2i}g_{2i+3}g_{2i+1}g_{2i+2} = 1 \mid 0 \leq i \leq k-3\}$. *The explicit isomorphism sends* $Z_i$ *to* $g_{2i}$ *and* $S_i$ *to* $g_{2i+1}$.

Although the proof is not very difficult, it is relatively long and technical. In order not to distract the reader, it has been relegated in Appendix B.

**Example 3** For $k = 5$, the elements of the group $\mathtt{cZS}_5$ submitted to the relations $S_i^2 = Z_i^2 = 1$, $(S_0S_1)^3 = (S_1S_2)^3 = (S_2S_3)^3 = 1$, $(S_0S_2)^2 = (S_0S_3)^2 = (S_1S_3)^2 = 1$, $(Z_0S_1)^4 = (Z_1S_0)^4 = (Z_1S_2)^4 = (Z_2S_1)^4 = (Z_2S_3)^4 = 1$, $(Z_0S_0)^2 = (Z_0S_2)^2 = (Z_0S_3)^2 = (Z_1S_1)^2 = (Z_1S_3)^2 = (Z_2S_0)^2 = (Z_2S_2)^2 = (Z_3S_0)^2 = (Z_3S_1)^2 = (Z_3S_3)^2$, and $S_0S_1Z_0S_1S_0Z_1 = S_1S_2Z_1S_2S_1Z_2 = S_2S_3Z_2S_3S_2Z_3 = 1$. The group $\mathtt{cZS}_5$ is the quotient of the Coxeter group $\mathcal{W}_5$ with Coxeter diagram




by the relations $S_0S_1Z_0S_1S_0Z_1 = S_1S_2Z_1S_2S_1Z_2 = S_2S_3Z_2S_3S_2Z_3 = 1$.

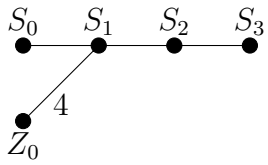
There exists other ways to write $\mathtt{cZS}_k$ as the quotient of a Coxeter group. As an example, consider the following result that proves that it is isomorphic to the quotient of a Coxeter group generated by $k$ elements by a single relation.

**Theorem 4** *Let us denote by* $\mathcal{C}_k$ *the Coxeter group generated by* $k$ *elements* $g_0, g_1, \ldots, g_{k-1}$ *submitted to the relations encoded in the Coxeter matrix*

$$N_k = \begin{bmatrix} 1 & 2 & 4 & 2 & \cdots & 2 \\ 2 & 1 & 3 & 2 & & \vdots \\ 4 & 3 & 1 & 3 & \ddots & \vdots \\ 2 & 2 & 3 & 1 & \ddots & 2 \\ \vdots & & \ddots & \ddots & \ddots & 3 \\ 2 & \cdots & \cdots & 2 & 3 & 1 \end{bmatrix}. \tag{19}$$

*The group* $\mathtt{cZS}_k$ *is isomorphic to the quotient* $\mathcal{C}_k/_{(g_0g_2g_3g_1g_2)^4}$. *The explicit isomorphism sends* $Z_0$ *to* $g_0$ *and each* $S_i$ *to* $g_{i+1}$

**Example 5** The group $\mathtt{cZS}_5$ is isomorphic to the quotient of the Coxeter group $\mathcal{C}_5$ with Coxeter diagram




by the relation $(Z_0S_1S_2S_0S_1)^4$.

## 4. Optimization of circuits of $c-\mathtt{Z}$ and `SWAP` gates

We apply the result of the previous section in order to exhibit algorithms for simplifying circuits. When we manipulate more than 2 qubits, the network structure of the qubits must be taken into account. Indeed, if some connections are missing, then it is necessary to simulate some gates from the others and this can increase dramatically the size of the circuit. For our purpose, we consider only two cases: the complete graph topology and the line topology.

### *4.1. Optimization in circuits of* `SWAP` *gates*

In order to illustrate the fact that the algebraic structure allows us to find efficient algorithm, let us investigate the simplest examples of circuits: those constituted only of `SWAP` gates. Indeed, the group $\mathcal{S}_k$, generated by the gates $S_i$, is isomorphic to the symmetric group $\S_k$ and so is the simplest example of a finite subgroup of $\mathtt{cZS}_k$ for which the mechanism of simplification can be completely described. In the case of the complete graph topology, the process to find a minimal decomposition of a permutation into transpositions is well known. It suffices to first decompose the permutation into cycles and hence decompose each cycle $(i_1,\dots,i_\ell)$ of length $\ell$ into $\ell-1$ transpositions

$$(i_1,\dots,i_\ell)=(i_1i_2)\cdot(i_2,i_3)\cdots(i_{\ell-1},i_\ell). \tag{20}$$

In the case of the line topology, the algorithm is a bit more subtle but also is well known. The minimal number of `SWAP` gates necessary to obtain a given permutation $\sigma\in\mathfrak{S}_k$ is known to be the length $\ell(\sigma)$ of $\sigma$ and such a decomposition of $\sigma$ is called *reduced*. One can compute a reduced decomposition of $\sigma$ by constructing its *Rothe diagram* (see e.g. [23] pp.14-15). The construction being very classical, we will recall it briefly. The Rothe diagram of a permutation $\sigma\in\mathfrak{S}_k$ is a $k\times k$ square matrix, whose rows and columns are indexed by integers in $\{0,\dots,k-1\}$, such that the only non-empty entries have coordinates $(r,c)$ ($r$ stands for the row number and $c$ for the column number) such that $(r,\sigma^{-1}(c))$ is an inversion in $\sigma$. The non-empty entries in the same column in the Rothe diagram are labeled with increasing successive integers from the top to

the bottom; the highest entry in a column being labeled with the column number. A reduced decomposition is found by reading the entries from the right to the left and the top to the bottom (see figure 6 for an example).

$$\mathtt{Rothe}((0,3)(2,4)) = \begin{bmatrix} 0 & 1 & 2 & \\ 1 & & & \\ 2 & & 3 & \\ & & & \\ & & & \end{bmatrix}$$

$$(0,3)(2,4) = S_2S_1S_0S_1S_3S_2$$

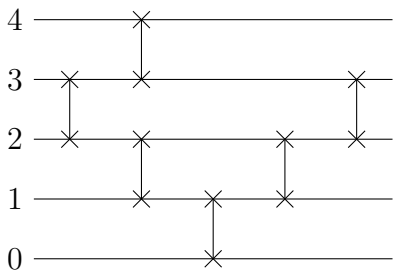



**Figure 6.** A permutation, its Rothe diagram, a reduced decomposition and the associated quantum circuit. In this figure, a permutation (acting on the set $\{0,\dots,k-1\}$) is represented by its decomposition into cycles. The symbol $S_i$ denotes the elementary transposition $(i,i+1)$.

### *4.2. Optimization of circuits in* $\mathtt{cZS}_k$ *for the complete graph topology*

The main application of Theorem 1 is that it allows us to exhibit an algorithm for simplifying circuits constituted of SWAP and $c-\mathtt{Z}$ gates. The principle is very simple: first we write the circuit as a product of many elements $PS$ with $P \in \mathcal{P}_k$ and $S \in \mathcal{S}_k$, then we use successively many times formula (17) in order to get only one element $PS$ and finally we use formula (20) in order to write the permutation $S$ using SWAP. More precisely, as a direct consequence of Theorem 1 and formula (17), the following algorithm allows us to give a reduced expression of an element of $\mathtt{cZS}_k$ in terms of the generators $Z_{\{i,j\}}$ and $S_{\{i,j\}}$ $(0 \le i < j \le k-1)$.

**Algorithm 6** CtoZS

**Input***: A circuit described as a sequence of gates $C = Z_{E_0}(S_{\sigma_1}Z_{E_1})\cdots(S_{\sigma_{\ell-1}}Z_{E_{\ell-1}})S_{\sigma_\ell}$ with $E_0,\dots,E_{\ell-1} \subset \{\{i,j\}|0 \le i < j \le k-1\}$ and $\sigma_1,\dots,\sigma_\ell \in \mathfrak{S}_k$.*

**Ouput***: An equivalent description of the circuits under the form $Z_E S_\sigma$.*

*(i) Compute $\sigma'_i = \sigma_1\cdots\sigma_i$, for $i = 1\dots\ell$.*

*(ii) Compute $E'_i = E_0 \oplus \sigma'_1(E_1) \oplus \cdots \sigma'_i(E_i)$, for $i = 0\dots\ell-1$.*

*(iii) Return* $Z_{E'_{\ell-1}}S_{\sigma'_\ell}$.

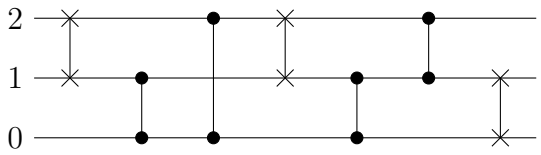



**Figure 7.** Circuits corresponding to the operator $A := S_0Z_{12}Z_{01}S_1Z_{02}Z_{01}S_1$

As an example, consider the circuit given in figure 7. We apply our algorithm on the associated operator,

$$\begin{aligned} A &= Z_\emptyset S_{(0,1)} \cdot Z_{\{\{0,1\},\{1,2\},\}}S_{(1,2)} \cdot Z_{\{0,1\},\{0,2\}\}}S_{(1,2)} \\ &= Z_{\{\{0,1\},\{0,2\}\}}S_{(0,1,2)} \cdot Z_{\{0,1\},\{0,2\}\}}S_{(1,2)} \\ &= Z_{\{\{0,1\},\{0,2\}\}\oplus\{\{0,1\},\{1,2\}\}}S_{(0,1,2)}S_{(1,2)} \\ &= Z_{02}Z_{12}S_{(0,1)}, \end{aligned} \tag{21}$$

and we obtain the reduced circuit drawn in figure 8.

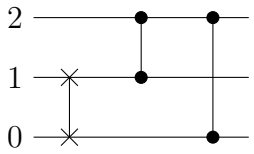



**Figure 8.** Simplification of the circuit of figure 7.

### *4.3. Simplification of circuits in* $\mathtt{cZS}_k$ *for the line topology*

Algorithm `CtoZS` is therefore suitable for complete graphs. For technical reasons, current machines impose more restrictive conditions on the qubits network. Let us consider machines in which only gates acting on two adjacent qubits are allowed. More precisely, we address the following problem: given a $cZS_k$ circuit written only with $Z_i$ and $S_i$ gates for $0 \leq i \leq k-2$, find an efficient algorithm (i.e. having a reasonable polynomial complexity) optimizing this circuit or, if it is not possible to obtain a minimal equivalent circuit in a polynomial time, at least giving a way to improve it.

First of all, it should be noted that there is a fairly obvious algorithm for finding the reduced decomposition. It consists in constructing the Cayley graph of the group according to the generators $Z_i$ and $S_i$ and hence deducing a reduced form by appliying a shorted path algorithm. Of course, such an algorithm has exponential time and space complexities with respect to the number of qubits, and is not practicable as soon as we exceed 6 or 7 qubits.

Another strategy consists in using the presentation of the group in order to reduce

expressions. In that context, one of the main tools is the Dehn algorithm [24]. Let us recall the principle. The starting point is a finite presentation of the group $G \sim \langle \mathcal{S}|\mathcal{R}\rangle$. Denote by $\tilde{\mathcal{R}}$ the closure of $\mathcal{R}$ under cyclic permutation of the symbols and inverse. We consider a reduced word $w$ in the free group $\mathbb{F}_{\mathcal{S}}$ generated by $\mathcal{S}$. The Dehn algorithm allows us to construct a sequence of word $w_0 = w$, $w_1, w_2, \ldots$, through the following process. It stops if $w_i$ is the empty word. Otherwise, if it exists a factor $u$ in $w_i$ which is the prefix of a word $r = uv$ in $\tilde{\mathcal{R}}$ with $|u| > |v|$, then the factor $u$ in $w_i$ is replaced by $v^{-1}$ and $w_{i+1}$ is the reduced word (in the free group) of this word. If such a word does not exist the algorithm stops. Obviously, we observe that the length of the words is strictly decreasing as the algorithm goes along. Hence, the Dehn algorithm allows us to compute a reduced (but not minimal) expression in a finite number of steps. In our special case, the Coxeter structure helps to improve the method. It suffices to apply successively many times the computation of a (minimal) reduced words in the Coxeter group $\mathcal{W}_k$ (see e.g. [22]) followed by the Dehn algorithm applied to the remaining relations.

**Example 7** For instance, consider the circuit that implements the transform $C = Z_0Z_3S_1S_0Z_1Z_3S_0$. This circuit is not minimal in $\mathcal{W}_5$, since by using successively the relations $(Z_3Z_1)^2$, $(Z_3S_0)^2$, $(Z_3S_1)^2$, and $Z_3^2$ it reduces to $C = Z_0S_1S_0Z_1S_0$. Hence, we use the Dehn algorithm, remarking that $Z_0S_1S_0Z_1S_0$ is a prefix of the additional relation $Z_0S_1S_0Z_1S_0S_1$ (obtained from $S_0S_1Z_0S_1S_0Z_1$ by applying a cyclic permutation), and we deduce that $C$ reduces to $S_1$.

Nevertheless, this is often not sufficient to obtain a minimal circuit as shown by the following example.

**Example 8** The circuit describing the composition $C = S_3S_2Z_1S_2S_3S_2Z_1S_2$ is minimal in $\mathcal{W}_5$. The minimality is checked by using classical algorithms of reduction for Coxeter groups (See e.g. [22]).

The only relations that could be used in the Dehn algorithm are $(S_2S_3)^3$, $(Z_1S_2)^4$, $(S_2Z_1)^4$ and $S_1S_2Z_1S_2S_1Z_2$. But no subword of $S_3S_2Z_1S_2S_3S_2Z_1S_2$ is a prefix of a relation $r = uv$ with $|u| > |v|$, so the circuit cannot be reduced using Dehn algorithm and the strategy which consists to apply successively a reduction in the Coxeter group and the Dehn algorithm fails to compute a shorter equivalent circuit. Nevertheless, from $S_2Z_1S_2 = S_1Z_2S_1$, one obtains $C = S_2S_1Z_2S_1S_3S_1Z_2S_1$ and it reduces to $C = S_2S_1Z_2S_3Z_2S_1$ from $(S_1S_3)^2$ and $S_1^2$.

We will continue to investigate technics of reduction in future works.

## 5. $c-\mathtt{Z}$ gates and entanglement

Local unitary operations ($\mathtt{LU} = U(2)^{\otimes k}$) can be implemented on quantum circuits. They transform states into others without changing their entanglement properties. The notion of LU-equivalence appears to be the finest allowing to distinguish two states but it does not take into account more subtle communication protocols. The notion of entanglement is usually defined through the group of stochastic local operations assisted

by classical communication (SLOCC). This group of operations allows to locally change the amplitude of a state for instance, by applying unitary operations on bigger Hilbert spaces obtained by adding ancillary particles. Mathematically, two states $|\psi\rangle$ and $|\phi\rangle$ are SLOCC-equivalent if there exist $k$ operators $A_1, \ldots, A_k$ such that $A_1 \otimes \cdots \otimes A_k |\psi\rangle = \lambda |\phi\rangle$ for some complex number $\lambda$. In other words, $|\psi\rangle$ and $|\phi\rangle$ are SLOCC-equivalent if they are in the same orbit of $GL(2)^{\otimes k}$ acting on the Hilbert space $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$. Since the relevant states belong to the unit sphere, one has only to consider the action of $SL(2)^{\otimes k}$ on the projective space $\mathbb{P}(\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2)$. Each orbit is a set of states which are entangled in the same way. Let us conclude this introductory paragraph by noting that the naive definition of entanglement as it can be naturally generalized from 2-qubit systems (the measurement of one component of the system determines the measurement of the other components) cannot be applied to systems of 3 qubits and more. For instance, the state $|\mathtt{GHZ}_3\rangle$ is SLOCC-equivalent (and also LU-equivalent) to the state $|\mathtt{GHZ}'_3\rangle := \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$ through the map $|i\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + (-1)^i|1\rangle)$, i.e. $|\mathtt{GHZ}'_3\rangle = H^{\otimes 3}|\mathtt{GHZ}_3\rangle$. In $|\mathtt{GHZ}'_3\rangle$, the value of the first qubit does not determine the values of the others but the property of entanglement can be seen when the state is rewritten as $|\mathtt{GHZ}'_3\rangle = \frac{1}{\sqrt{2}}\left(\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes 3} + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)^{\otimes 3}\right)$. In fact, entanglement is not a property that depends only on one of the observables but on the whole space of observables. Choosing an observable is equivalent to modifying the base of the Hilbert space by acting with an element of the Lie group associated to the Lie algebra of observables. Hence, entanglement is a SLOCC (or LU, depending on the problem you're considering) invariant property.

### *5.1.* LU*-equivalence to* $|\mathtt{GHZ}_k\rangle$

Although the group $\mathtt{cZS}_k$ does not contain all quantum gates, it is still powerful enough to generate a state equivalent to $|\mathtt{GHZ}_k\rangle$. Remark that SWAP gates can be avoided as they do not generate any entanglement. More precisely, let us show the following result.

**Proposition 9** *The state*

$$\frac{1}{\sqrt{2^k}} Z_{\{\{0,1\},\{0,2\},\cdots,\{0,k-1\}\}} \left(|0\rangle + |1\rangle\right)^{\otimes k} \tag{22}$$

*is* LU*-equivalent to* $|\mathtt{GHZ}_k\rangle$.

A fast computation shows

$$|\Psi_E\rangle := \frac{1}{\sqrt{2^k}} Z_E \left(|0\rangle + |1\rangle\right)^{\otimes k} = \frac{1}{\sqrt{2^k}} \sum_{0 \le i_0, \ldots, i_{k-1} \le 1} (-1)^{\sum_{\{\alpha,\beta\} \in E} i_\alpha i_\beta} |i_{k-1} \cdots i_0\rangle. \tag{23}$$

In particular

$$|\Psi_{\{\{0,1\},\{0,2\},\cdots,\{0,k-1\}\}}\rangle = \frac{1}{\sqrt{2^k}} \sum_{0 \le i_0, \ldots, i_{k-1} \le 1} (-1)^{i_0(i_1 + \cdots + i_{k-1})} |i_{k-1} \cdots i_0\rangle. \tag{24}$$

Since it is not factorizing, it is entangled. However, it is not completely obvious to see that such a state is LU-equivalent to $|\mathtt{GHZ}_k\rangle$. Acting by $H$ on the qubit $\ell > 0$, one obtains

$$\begin{aligned}&(I_{2^{k-\ell-1}} \otimes H \otimes I_{2^\ell})\,|\Psi_{\{\{0,1\},\{0,2\},\cdots,\{0,k-1\}\}}\rangle \\ &= \frac{1}{\sqrt{2^{k-1}}} \sum_{0\leq i_1,\ldots,i_{\ell-1},i_{\ell+1}\ldots i_{k-1}\leq 1} (|i_{k-1}\cdots i_{\ell-1}0 i_{\ell+1}\cdots i_1 0\rangle \\ &+(-1)^{i_1+\cdots+i_{\ell-1}+i_{\ell+1}+\cdots+i_{k-1}}|i_{k-1}\cdots i_{\ell-1}1 i_{\ell+1}\cdots i_1 1\rangle)\,.\end{aligned} \tag{25}$$

By iterating on all the qubits but the qubit 0, one finds

$$\left(H^{\otimes k-1}\otimes I_2\right)|\Psi_{\{\{0,1\},\{0,2\},\cdots,\{0,k-1\}\}}\rangle = |\mathtt{GHZ}_k\rangle. \tag{26}$$

Since the action on a single qubit does not change the entanglement properties, equation (26) shows that the state (22) is LU-equivalent to $|\mathtt{GHZ}_k\rangle$. Figure 9 contains an example of such a circuit for $k = 5$. Notice that $|\mathtt{GHZ}_k\rangle$ is a generic entangled state in the sense

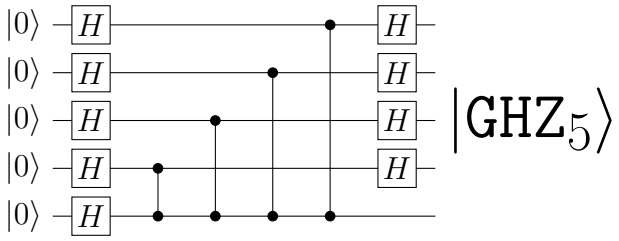



**Figure 9.** The entangled state $|\mathtt{GHZ}_5\rangle$ created from the completely factorized state $|00000\rangle$. The first five $H$ gates are used to create superposition and generate the state $\frac{1}{4\sqrt{2}}(|0\rangle+|1\rangle)^5$ from $|00000\rangle$.

of Miyake [25] only for $k \leq 3$ (see appendix Appendix C). In the rest of the section, we prove that the group $\mathtt{cZS}_k$ does not generate all entanglement types from a completely factorized state and in general, it is not possible to compute a generic entangled state by using only these operations.

### *5.2.* SLOCC*-equivalence to* $|\mathtt{W}_3\rangle$

We shall prove that the group $\mathtt{cZS}_k$ is not powerful enough to generate any entanglement type from a completely factorized state. More precisely, we shall find a counter-example for $k = 3$ qubits: it is not possible to generates a state which is SLOCC-equivalent to $|\mathtt{W}_3\rangle$. We use the method pioneered by Klyachko in [26] wherein he promoted the use of Algebraic Theory of Invariant. The states of a SLOCC-orbit are characterized by their values on covariant polynomials. Let $|\psi\rangle = \sum_{i,j,k}\alpha_{ijk}|ijk\rangle$. For our purpose we consider only two polynomials:

$$\begin{aligned}\Delta(|\psi\rangle) &= (\alpha_{000}\alpha_{111}-\alpha_{001}\alpha_{110}-\alpha_{010}\alpha_{101}+\alpha_{011}\alpha_{100})^2 \\ &\quad -4\,(\alpha_{000}\alpha_{011}-\alpha_{001}\alpha_{010})\,(\alpha_{100}\alpha_{111}-\alpha_{101}\alpha_{110})\end{aligned} \tag{27}$$

and the catalecticant

$$C(x_0,x_1,y_0,y_1,z_0,z_1) = \begin{bmatrix} \frac{\partial A}{\partial x_0} & \frac{\partial A}{\partial x_1} \\ \frac{\partial B_x}{\partial x_0} & \frac{\partial B_x}{\partial x_1} \end{bmatrix}, \tag{28}$$

with $A=\sum_{ijk}\alpha_{ijk}x_iy_jz_k$ and

$$B_x(x_0,x_1)=\begin{bmatrix}\frac{\partial^2 A}{\partial y_0\partial z_0} & \frac{\partial^2 A}{\partial y_0\partial z_1}\\ \frac{\partial^2 A}{\partial y_1\partial z_0} & \frac{\partial^2 A}{\partial y_1\partial z_1}\end{bmatrix}. \tag{29}$$

The states which are SLOCC-equivalent to $|\mathtt{GHZ}_3\rangle$ are characterized by $\Delta\neq 0$ while the states which are SLOCC-equivalent to $|W_3\rangle$ are characterized by $C\neq 0$ and $\Delta=0$ [27]. For the other states, we have $\Delta=C=0$.
We remark that

$$Z_E=\mathtt{diag}(1,1,1,\epsilon_{\{0,1\}},1,\epsilon_{\{0,2\}},\epsilon_{\{1,2\}},\epsilon_{\{0,1\}}\epsilon_{\{0,2\}}\epsilon_{\{1,2\}}) \tag{30}$$

where $\epsilon_{\{0,1\}},\epsilon_{\{0,2\}}$, and $\epsilon_{\{1,2\}}\in\{-1,1\}$ and we consider the states

$$|\phi_E\rangle:=Z_E\sum_{ijk}a_ib_jc_k|ijk\rangle=Z_E(a_0|0\rangle+a_1|1\rangle)(b_0|0\rangle+b_1|1\rangle)(c_0|0\rangle+c_1|1\rangle). \tag{31}$$

We have

$$C(|\phi_E\rangle)=a_0b_0c_0a_1b_1c_1(2-\epsilon_{\{0,1\}}-\epsilon_{\{0,2\}}-\epsilon_{\{1,2\}}+\epsilon_{\{0,1\}}\epsilon_{\{0,2\}}\epsilon_{\{1,2\}})P \tag{32}$$

where $P=\sum_{i_0i_1i_2}a_{i_2}b_{i_1}c_{i_0}(-1)^{\mathrm{card}\{j|i_j=1\}}\left(\prod_{\{j,k\}|i_j+i_k>0}\epsilon_{\{j,k\}}\right)x_{i_2}y_{i_1}z_{i_0}$ is a non zero trilinear form, and

$$\Delta(|\phi_E\rangle)=4(a_0b_0c_0a_1b_1c_1)\epsilon_{01}\epsilon_{02}\epsilon_{12}(2-\epsilon_{01}-\epsilon_{02}-\epsilon_{12}+\epsilon_{01}\epsilon_{02}\epsilon_{12}). \tag{33}$$

So if $\Delta$ vanishes then $C$ also vanishes. This implies the following result

**Proposition 10** *The state* $|\phi_E\rangle$ *is not* SLOCC*-equivalent to* $|W_3\rangle$.

However, it is interesting to note that it is possible to join a state of the LU-orbit of $|\mathtt{GHZ}_3\rangle$ to a state of the SLOCC-orbit of $|\mathtt{W}_3\rangle$. Consider the state

$$|\phi_1\rangle:=\left(R_y(\frac{\pi}{4})HX\otimes R_y(\frac{\pi}{4})\otimes HX\right)Z_{01}Z_{12}(|0\rangle+|1\rangle)^3$$

The state $|\phi_1\rangle$ is in the LU-orbit of $|GHZ\rangle$ since

$$\left(R_y(\frac{\pi}{4})^{-1}\otimes R_y(\frac{\pi}{4})^{-1}\otimes I\right)|\phi_1\rangle=|\mathtt{GHZ}_3\rangle. \tag{34}$$

A fast computation shows

$$\Delta\left(Z_{12}|\phi_1\rangle\right)=0 \text{ and } C\left(Z_{12}|\phi_1\rangle\right)\neq 0, \tag{35}$$

equivalently $Z_{12}|\phi_1\rangle$ is in the SLOCC-orbit of $|\mathtt{W}_3\rangle$.

### *5.3. Four qubits systems*

The situation of 4-qubits systems is more complex than for 3-qubits systems. Nevertheless, there still is a classification of entanglement as well as related mathematical tools. We refer to the classification of Verstraete et al [28] which assigns any 4-qubit

state to one of 9 families. Any state in the more general situation (in the sense of Zarisky topology) is SLOCC-equivalent to 192 Verstraete states of the family

$$\begin{array}{rcl} G_{abcd} & = & \frac{a+d}{2}\left(|0000\rangle+|1111\rangle\right)+\frac{a-d}{2}\left(|0011\rangle+|1100\rangle\right) \\ & & +\frac{b+c}{2}\left(|0101\rangle+|1010\rangle\right)+\frac{b-c}{2}\left(|0110\rangle+|1001\rangle\right). \end{array} \tag{36}$$

for independent parameters $a, b, c$, and $d$ [28, 29, 30]. To determine the Verstraete family to which a state belongs, we use an algorithm described in a previous paper [30]. This algorithm is based on the evaluation of some covariants. Recall that the algebra of (relative) SLOCC-invariant is freely generated by the four following polynomials [31]:

- The smallest degree invariant

$$B := \sum_{0\leq i_1,i_2,i_3\leq 1} (-1)^{i_1+i_2+i_3}\alpha_{0i_1i_2i_3}\alpha_{1(1-i_1)(1-i_2)(1-i_3)}, \tag{37}$$

- Two polynomials of degree 4

$$L := \begin{vmatrix} \alpha_{0000} & \alpha_{0010} & \alpha_{0001} & \alpha_{0011} \\ \alpha_{1000} & \alpha_{1010} & \alpha_{1001} & \alpha_{1011} \\ \alpha_{0100} & \alpha_{0110} & \alpha_{0101} & \alpha_{0111} \\ \alpha_{1100} & \alpha_{1110} & \alpha_{1101} & \alpha_{1111} \end{vmatrix} \tag{38}$$

  and

$$M := \begin{vmatrix} \alpha_{0000} & \alpha_{0001} & \alpha_{0100} & \alpha_{0101} \\ \alpha_{1000} & \alpha_{1001} & \alpha_{1100} & \alpha_{1101} \\ \alpha_{0010} & \alpha_{0011} & \alpha_{0110} & \alpha_{0111} \\ \alpha_{1010} & \alpha_{1011} & \alpha_{1110} & \alpha_{1111} \end{vmatrix}. \tag{39}$$

- and a polynomial of degree 6 defined by $D_{xy} = -\det(B_{xy})$ where $B_{xy}$ is the $3\times 3$ matrix satisfying

$$\left[x_0^2, x_0x_1, x_1^2\right] B_{xy} \begin{bmatrix} y_0^2 \\ y_0y_1 \\ y_1^2 \end{bmatrix} = \det\left(\frac{\partial^2}{\partial z_i \partial t_j} A\right) \tag{40}$$

  with $A = \sum_{ijkl} \alpha_{ijkl} x_i y_j z_k t_l$.

For our purpose we define also

$$N = -L - M = \begin{vmatrix} \alpha_{0000} & \alpha_{1000} & \alpha_{0001} & \alpha_{1001} \\ \alpha_{0100} & \alpha_{1100} & \alpha_{0101} & \alpha_{1101} \\ \alpha_{0010} & \alpha_{1010} & \alpha_{0011} & \alpha_{1011} \\ \alpha_{0110} & \alpha_{1110} & \alpha_{0111} & \alpha_{1111} \end{vmatrix}. \tag{41}$$

We need also the covariant polynomials $\overline{\mathcal{G}}$, $\mathcal{G}$, $\mathcal{H}$, $\mathcal{K}_3$, and $\mathcal{L}$ defined in [30] and those complete definition is relegated to appendix. We recall the principle of the algorithm as described in [30]. A first coarser classification is obtained by investigating the roots of the three quartics

$$Q_1 = x^4 - 2Bx^3y + (B^2 + 2L + 4M)x^2y^2 + 4(D_{xy} - B(M + \frac{1}{2}L))xy^3 + L^2y^4, \tag{42}$$

$$Q_2 = x^4 - 2Bx^3y + (B^2 - 4L - 2M)x^2y^2 + (4D_{xy} - 2MB)xy^3 + M^2y^4, \quad (43)$$

and

$$Q_3 = x^4 - 2Bx^{3y} + (B^2 + 2L - 2M)x^2y^2 - (2(L+M)B - 4D_{xy})xy^3 + N^2y^4. \quad (44)$$

We determine the roots configuration of a quartic $Q = \alpha x^4 - 4\beta x^3y + 6\gamma x^2y^2 - 4\delta xy^3 + \omega y^4$ by examining the vanishing of the five covariants

$$I_2 = \alpha\omega - 4\beta\delta + 3\gamma^2, \quad (45)$$

$$I_3 = \alpha\gamma\omega - \alpha\delta^2 - \omega\beta^2 - \gamma^3 + 2\beta\gamma\delta, \quad (46)$$

$$\Delta = I_2^3 - 27I_3^2, \quad (47)$$

$$Hess = \begin{vmatrix} \frac{\partial^2}{\partial x^2}Q & \frac{\partial^2}{\partial x \partial y}Q \\ \frac{\partial^2}{\partial x \partial y}Q & \frac{\partial^2}{\partial y^2}Q \end{vmatrix}, \quad (48)$$

and

$$T = \begin{vmatrix} \frac{\partial}{\partial x}Q & \frac{\partial}{\partial y}Q \\ \frac{\partial}{\partial x}Hess(Q) & \frac{\partial}{\partial y}Hess(Q) \end{vmatrix}. \quad (49)$$

The interpretation of the values of the covariants in terms of roots is summarized in table 1 (see eg [32]). Notice that the values of the invariant polynomials $I_2$, $I_3$ and $\Delta$

| *covariants* | *Interpretation* |
|---|---|
| $\Delta \neq 0$ | Four distinct roots |
| $\Delta = 0$ and $T \neq 0$ | Exactly one double root |
| $T = 0$ and $I_2 \neq 0$ | Two distinct double roots |
| $I_2 = I_3 = 0$ and $Hess \neq 0$ | A triple root |
| $Hess = 0$ | a quadruple root |

**Table 1.** Roots of a quartic

are the same for the three quartics. These invariants are also invariant polynomials of the binary quadrilinear form $A$. Furthermore, $\Delta$ is nothing but the hyperdeterminant, in the sense of Gelfand et al. [33], of $A$ [30]. Remark also that

$$Q_1(G_{abcd}) = (x - a^2)(x - b^2)(x - c^2)(x - d^2). \quad (50)$$

Once the configuration of the roots has been identified, we can refine our result by looking at the values of the other covariants and refer to the classification described in [30] p32.

We have to investigate the 64 possible values of $E$.

(i) If $E = \emptyset$ then $|\Phi_E\rangle$ is completely factorized.

(ii) If $E = \{\{i, j\}\}$ for some $i, j = 0, \ldots, 3$, $i \neq j$ (6 cases), then $|\Phi_E\rangle$ belongs to the nilpotent cone and so each quartic equals $x^4$. The state $|\Phi_E\rangle$ is partially factorized as a state which is `SLOCC`-equivalent to an EPR pair on the qubits $i, j$ together with two independent particles.

(iii) If $E = \{\{i,j\},\{i,k\}\}$ for some $i,j,k$ distinct (12 cases), then each quartic equals $x^4$. The state $|\Phi_E\rangle$ factorizes as a state which is SLOCC-equivalent to $|\mathtt{GHZ}_3\rangle$ on the qubits $i,j,k$ together with an independent qubit.

(iv) If $E = \{\{i,j\},\{k,l\}\}$ with $\{i,j\}\cap\{k,l\} = \emptyset$ (3 cases) then one of the quartic equals $x^3(x - 4\exp\{i\diamond\}y)$ and the two others equal $(x - \frac{1}{4}\exp\{i\diamond\}y)^4$ with $a_0b_0c_0d_0a_1b_1c_1d_1 = \frac{1}{16}\exp\{i\diamond\}$. For generic values of the parameters we have $\diamond \neq 0$ and this implies that $|\Phi_E\rangle$ factorizes as a two 2-qubits state which are SLOCC-equivalent to two EPR pairs. Let us examine only the case where $E = \{\{1,2\},\{3,4\}\}$, the other cases are obtained symmetrically. In this case, we have $Q_1 = x^3(x-4\exp\{i\diamond\}y)$ and $\mathcal{C} = \mathcal{D} = \mathcal{K}_5 = \mathcal{L} = 0$. From [30], this implies that it is in the same orbit as $G_{a000}$ with $a = \frac{1}{2}\exp\{\frac{1}{2}i\diamond\}$.

(v) If $E = \{\{i,j\},\{j,k\},\{i,k\}\}$ with $i,j,k$ distinct (4 cases) then each quartic equals $x^4$. The state $|\Phi_E\rangle$ factorizes as a state which is SLOCC-equivalent to $|\mathtt{GHZ}_3\rangle$ on the qubits $i,j,k$ together with a single independent qubit.

(vi) If $E = \{\{i,j\},\{j,k\},\{k,l\}\}$ with $\{i,j,k,l\} = \{0,1,2,3\}$ (12 cases) then one of the quartics equals $x^2(x^2 + \frac{1}{4}\exp\{2i\diamond\}y^2)$ and the two others equal $(x^2 - \frac{1}{16}\exp\{2i\diamond\})^2$. For generic values of the parameters, one quartic has a double zero root together with two simple roots and the two other quartics have two double roots. Let us examine only the case $E = \{\{1,2\},\{2,3\},\{3,4\}\}$ for which $Q_1 = x^2(x^2 + \frac{1}{4}\exp\{2i\diamond\}y^2)$. Following the algorithm described in [30], we have to compute the values of the $\mathcal{K}_3$ and $\mathcal{L}$. The two covariants being zero, we deduce that $|\Phi_E\rangle$ is in the SLOCC-orbit of a degenerated $G_{abcd}$. More precisely, following the value of $E$, $|\Phi_E\rangle$ is equivalent to $G_{ab00}$ with $a = \frac{1}{\sqrt{2}}\exp\{\frac{1}{2}(\diamond + \frac{\pi}{2})\}$ and $b = \frac{1}{\sqrt{2}}\exp\{\frac{1}{2}(\diamond - \frac{\pi}{2})\}$.

(vii) If $E = \{\{i,j\},\{i,k\},\{i,l\}\}$ with $\{i,j,k,l\} = \{0,1,2,3\}$ (4 cases) then the three quartics are equal to $x^2(x+\frac{1}{2}\exp\{i\diamond\})^2$. Following [30], the Verstraete type of $|\Phi_E\rangle$ is determined by evaluating $\mathcal{K}_3$ and $\mathcal{L}$. Since the two covariants vanish, we deduce that $|\Phi_E\rangle$ is in the SLOCC-orbit of $G_{aa00}$ with $a = \frac{1}{\sqrt{2}}\exp\{\frac{1}{2}i(\diamond + \frac{\pi}{2})\}$. We are in the case where $L = M = B = 0$. From [27], there is only one dense SLOCC-orbit in that variety.

(viii) If $E = \{\{i,j\},\{i,k\},\{i,l\},\{j,k\}\}$ with $\{i,j,k,l\} = \{0,1,2,3\}$ (12 cases) then one of the quartics equals $x^2(x-\frac{1}{2}y\diamond)(x+\frac{1}{2}y\diamond)$ and the two others equal $(x^2+\frac{1}{16}y^2\diamond^2)^2$. We only investigate the case $E = \{\{1,2\},\{1,3\},\{1,4\},\{3,4\}\}$, since one can easily deduce the others by symmetry. From [30], one has to compute the values of $\mathcal{K}_3$ and $\mathcal{L}$. Both covariants vanish and we deduce that $|\Phi_E\rangle$ is SLOCC-equivalent to $G_{ab00}$ with $a = \frac{1}{2}\exp\{\frac{1}{2}i\diamond\}$ et $b = \frac{1}{2}\exp\{\frac{1}{2}i(\diamond + \pi)\}$. Furthermore, it belongs to the variety defined by $L = 0$.

(ix) If $E = \{\{i,j\},\{j,k\},\{k,l\},\{l,i\}\}$ with $\{i,j,k,l\} = \{0,1,2,3\}$ (3 cases) then we find that one of the quartics equals $x^2(x^2 + \frac{1}{16}y^2\exp\{2i\diamond\})$ and the others equal $(x^2 - \frac{1}{16}y^2\diamond^2)^2$. Let us only examine the case $E = \{\{1,3\},\{2,3\},\{2,4\},\{1,4\}\}$. From [30], one has to compute the values of $\mathcal{K}_3$ and $\mathcal{L}$. Both covariants vanish and we deduce that $|\Phi_E\rangle$ is SLOCC-equivalent to $G_{ab00}$ with $a = \frac{1}{2}\exp\{\frac{1}{2}i(\diamond + \frac{\pi}{2})\}$ et

$b = \frac{1}{2}\exp\{\frac{1}{2}i(\diamond - \frac{\pi}{2})\}$. Furthermore, it belongs to the variety defined by $L = 0$.

(x) If $E = \{\{i,j\} \mid 0 \leq i < j \leq 3\} \setminus \{k,l\}\}$ for some $k \neq l$ (6 cases) then one of the quartics equal $x^2(x^2 - \frac{1}{4}\exp\{2i\diamond\}y^2)$ while the two others equal $(x^2 + \frac{1}{16}\exp\{2i\diamond\}y^2)^2$. Without loss of generalities one supposes that $E = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}$; the other cases being obtained by symmetry. We have $Q_1 = x^2(x^2 - \frac{1}{4}\exp\{2i\diamond\}y^2)$. Following [30], we have computed $\mathcal{K}_3$ and $\mathcal{L}$. Since the two invariants vanish, we have deduced that $|\Phi_E\rangle$ is equivalent to a degenerated $G_{abcd}$. More precisely, following the value of $E$, it is equivalent to $G_{ab00}$ with $a = \sqrt{2}\exp\{\frac{1}{2}i\diamond\}$ and $b = \sqrt{2}\exp\{\frac{1}{2}i(\diamond - \pi)\}$.

(xi) If $E = \{\{i,j\} \mid 0 \leq i < j \leq 3\}$ then the two quartics are equal to $x^2(x - \frac{1}{2}\exp\{i\diamond\}y)^2$. Following [30], we have computed the values of the four covariants $\overline{\mathcal{G}}$, $\mathcal{G}$, $\mathcal{H}$, and $\mathcal{L}$. Since they all vanish, we have deduced that $|\Phi_E\rangle$ is equivalent to a degenerated $G_{abcd}$. More precisely, $|\Phi_E\rangle$ is SLOCC-equivalent to $G_{aa00}$ with $a = \frac{1}{\sqrt{2}}\exp\{\frac{1}{2}i\diamond\}$.

Viewing $E$ as the set of the edges of a 4 vertices graph, the cases (i) to (v) above correspond to disconnected graphs and factorized states. The other ones correspond to connected graphs and degenerated $G_{abcd}$ states. Notice that some degenerated $G_{abcd}$ factorize.

Miyake [25] has shown that the more generic entanglement holds for $\Delta \neq 0$. So we have,

**Proposition 11** *The states* $|\Phi_E\rangle$ *are not generically entangled.*

We can be more precise by noticing that the invariant polynomial $LMN$ vanishes for any state $|\Phi_E\rangle$. In terms of (projective) geometry, this means that $|\Phi_E\rangle$ corresponds to a point of the secant variety of one of the three Segre embedding $\sigma(Seg_{ij}(\mathbb{P}^3 \times \mathbb{P}^3))$ (see [30] p18-21), $\{i,j\} \in \{\{0,1\},\{0,2\},\{0,3\}\}$. The three Segre varieties $Seg_{ij}(\mathbb{P}^3 \times \mathbb{P}^3)$ are isomorphic and are the image of one of the three Segre bilinear map $Seg_{ij} : \mathbb{P}^3 \times \mathbb{P}^3 \to \mathbb{P}^{15} = \mathbb{P}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2)$, defined by

$$Seg_{01}([v_0 \otimes v_1],[w_0 \otimes w_1]) = [v_0 \otimes v_1 \otimes w_0 \otimes w_1], \tag{51}$$

$$Seg_{02}([v_0 \otimes v_1],[w_0 \otimes w_1]) = [v_0 \otimes w_0 \otimes v_1 \otimes w_1], \text{ and} \tag{52}$$

$$Seg_{03}([v_0 \otimes v_1],[w_0 \otimes w_1]) = [v_0 \otimes w_0 \otimes w_1 \otimes v_1]. \tag{53}$$

Alternatively, the Segre varieties are the zero locus of the $2 \times 2$-minors of one of the matrices involved in the definition of $L$, $M$ and $N$. The secant variety of a projective variety $Y$ is the algebraic closure of the union of secant lines $\mathbb{P}^1_{xy}$, $x, y \in Y$. The variety $\sigma(Seg_{ij}(\mathbb{P}^3 \times \mathbb{P}^3))$ corresponds to the zero locus the $3 \times 3$-minors of one of the matrices involved in the definition of $L$, $M$, and $N$.

From [30] and the vanishing of $LMN$, we deduce that all the $|\Phi_E\rangle$ belong to one of the third secant variety

$$\sigma_3(Seq_{ij}(\mathbb{P}^3 \times \mathbb{P}^3)) := \overline{\bigcup_{x_1,x_2,x_3} \mathbb{P}^2_{x_1x_2x_3}}, \tag{54}$$

where $\overline{Y}$ denotes the algebraic closure of $Y$ and $P^2_{x_1x_2x_3}$ is the only projective plane containing the point $x_1$, $x_2$, and $x_3$. The computation of corresponding Verstraete forms allows us to refine this result by exhibiting for each state a strictly included variety to which it belongs. For all the cases but (iii) and (v), the corresponding varieties are

| $Varieties$ | $Cases$ |
|---|---|
| $\sigma(Seg_{ij}(\mathbb{P}^3\times\mathbb{P}^3))$ | $(i),(ii),(iv),(vi),(vii),(viii),(ix),(x),(xi)$ |
| $\sigma(\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1)=\bigcap_{ij}\sigma(Seg_{ij}(\mathbb{P}^3\times\mathbb{P}^3)$ | $(i),(vi),(xi)$ |
| $Seg_{ij}(\mathbb{P}^3\times\mathbb{P}^3)$ | $(i),(ii),(iv)$ |
| $Seg_{ij}(\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^3)$ | $(i),(ii)$ |
| $\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1$ | $(i)$ |

**Table 2.** Varieties associated to cases (i), (ii), (iv), (vi), (vii), (viii), (ix), (x), (xi)

summarized in table 2. The 16 remaining cases, corresponding to (iii) and (v), belong to one of the four Segre varieties $\mathbb{P}^1\times\mathbb{P}^7\to\mathbb{P}^{15}$.

Notice also that $|\mathtt{GHZ}_4\rangle$ is SLOCC-equivalent to a $G_{aa00}$ state [30] as case (vii) above. Moreover when $a_i=b_i=c_i=d_i=\frac{1}{\sqrt{2}}$ for $i=0,1$, it is possible to create a state which is LU-equivalent to $|\mathtt{GHZ}_4\rangle$ (see proposition 9).
The state $|\mathtt{W}_4\rangle=|1000\rangle+|0100\rangle+|0010\rangle+|0001\rangle$ belongs to the null cone (ie, all the invariant polynomials vanish). Since all the $|\Phi_E\rangle$ belonging to the null cone factorize and the factorization properties is a SLOCC-invariant property, we deduce that no $|\Phi_E\rangle$ is SLOCC-equivalent to $|\mathtt{W}_4\rangle$, as in the case of 3-qubit systems.

### *5.4. Five qubits and beyond*

For more five qubits and more, the number of tools is much smaller. Indeed, the description of the algebra of covariant polynomials is out of reach and even some important invariant polynomial, such that the hyperdeterminant, are too huge to be computed in a suitable form. We recall that the importance of the hyperdeterminant is due to the fact that it vanishes when the system is not generically entangled [25]. Although this polynomial is very difficult to calculate, its nullity can be tested thanks to its interpretation in terms of solution to a system of equations, e.g. [33] p445. For instance , if $A=\sum_{0\leq i,j,k,l,n\leq 1}\alpha_{ijkln}x_iy_jz_kt_ls_n$ is the ground form associated to the five qubits state $|\phi\rangle=\sum_{0\leq i,j,k,l,n\leq 1}\alpha_{ijkln}|ijkln\rangle$, the condition $\Delta(|\phi\rangle)=0$ means that the system

$$S_\phi:=\{A=\frac{d}{dx_0}A=\frac{d}{dx_1}A=\frac{d}{dy_0}A=\frac{d}{dy_1}A=\cdots=\frac{d}{ds_0}A=\frac{d}{ds_1}A=0\}(55)$$

has a solution $\hat{x}_0,\hat{x}_1,\hat{y}_0,\hat{y}_1,\ldots,\hat{s}_0,\hat{s}_1$ in the variables $x_0,x_1,y_0,y_1,\ldots,s_0,s_1$ such that $(\hat{x}_0,\hat{x}_1),(\hat{y}_0,\hat{y}_1),\ldots,(\hat{s}_0,\hat{s}_1)\neq(0,0)$. Such a solution is called non trivial. We process

exhaustively by exhibiting a non trivial solution for each of the 1024 systems $S_{\Phi_E}$ where

$$|\Phi_E\rangle = Z_E(a_0|0\rangle+a_1|0\rangle)(b_0|0\rangle+b_1|0\rangle)(c_0|0\rangle+c_1|0\rangle)(d_0|0\rangle+d_1|0\rangle)(e_0|0\rangle+e_1|0\rangle). \quad (56)$$

Since permutations of the qubits let the value of the hyperdeterminant $\Delta$ unchanged, the set of systems $S_{\Phi_E}$ splits into 34 classes corresponding to undirected unlabeled graphs. For each of these classes, we find a non trivial solution with $x_1 = y_1 = z_1 = t_1 = s_1 = 1$ for a given representative element. The solutions are summarized in tables 3, 4 and 5 with the notations $\triangle_1 := \sum_{i,j,k}(-1)^{j(i+1)+ik}a_ib_jc_k$, $\triangle_2 := \sum_{i,j,k}(-1)^{i(j+k)}a_ib_jc_k$, $\triangle_3 = \sum_{i,j,k}(-1)^{k(1+j)+ij}a_ib_jc_k$, $\triangle_4 := \sum_{i,j,k}(-1)^{j(i+k)}a_ib_jc_k$, $\triangle_5 := \sum_{ijk}(-1)^{k+j(k+i)}a_ib_jc_k$, and $\triangle_6 := \sum_{ijk}(-1)^{j(i+k)}a_ib_jc_k$.

So we deduce

| *Classes* | *Representative elements* | *Cardinals* | *Solutions* $[x_0, y_0, z_0, t_0, s_0]$ |
|---|---|---|---|
| $\{\}$ | $\{\}$ | 1 | $[1, -\frac{b_1}{b_0}, -\frac{c_1}{c_0}, 1, 1]$ |
| $\{\{i,j\}\}$ | $\{\{0,1\}\}$ | 10 | $[1, 1, 1, -\frac{d_1}{d_0}, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\}\}$ | $\{\{0,1\},\{0,2\}\}$ | 30 | $[1, 1, 1, -\frac{d_1}{d_0}, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{k,l\}\}$ | $\{\{0,1\},\{2,3\}\}$ | 15 | $[1, 1, 1, -\frac{d_1(c_0-c_1}{d_0(c_0+c_1)}, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{i,l\}\}$ | $\{\{0,1\},\{0,2\},\{0,3\}\}$ | 20 | $[1, \frac{b_1}{b_0}, -\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{j,k\},\{i,k\}\}$ | $\{\{0,1\},\{1,2\},\{0,2\}\}$ | 10 | $[1, 1, 1, -\frac{d_1}{d_0}, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{j,l\}\}$ | $\{\{0,1\},\{0,2\},\{1,3\}\}$ | 60 | $[1, 1, 1, -\frac{d_1\triangle_1}{d_0\triangle_2}, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{l,n\}\}$ | $\{\{0,1\},\{0,2\},\{3,4\}\}$ | 30 | $[1, 1, 1, -\frac{d_1}{d_0}, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{i,l\},\{i,n\}\}$ | $\{\{0,1\},\{0,2\},\{0,3\},\{0,4\}\}$ | 5 | $[1, \frac{b_1}{b_0}, -\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{i,l\},\{j,n\}\}$ | $\{\{0,1\},\{0,2\},\{0,3\},\{1,4\}\}$ | 60 | $[1, \frac{b_1}{b_0}, -\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{j,k\},\{i,k\},\{i,l\}\}$ | $\{\{0,1\},\{1,2\},\{0,2\},\{0,3\}\}$ | 60 | $[1, -\frac{(i-1)b_1}{(i+1)b_0}, (i+1)\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{j,k\},\{k,l\},\{i,l\}\}$ | $\{\{0,1\},\{1,2\},\{2,3\},\{0,3\}\}$ | 15 | $[\frac{a_1}{a_0}, \frac{b_1}{b_0}, -\frac{c_1}{c_0}, \frac{d_1}{d_0}, 1]$ |
| $\{\{i,j\},\{k,l\},\{l,n\},\{k,n\}\}$ | $\{\{0,1\},\{2,3\},\{3,4\},\{2,4\}\}$ | 10 | $[1, 1, 1, -\frac{d_1(c_0-c_1)}{d_1(c_0+c_1)}, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{j,k\},\{k,l\},\{l,n\}\}$ | $\{\{0,1\},\{1,2\},\{2,3\},\{3,4\}\}$ | 60 | $[1, 1, 1, -\frac{d_1\triangle_3}{d_0\triangle_4}, \frac{e_1}{e_0}]$ |

**Table 3.** Non trivial solutions of $S_{\Phi_E}$ for $\mathtt{card}(E) < 5$

**Proposition 12** *For five qubit systems, the states* $|\Phi_E\rangle$ *are not generically entangled.*

In principle the same strategy can be applied for more than five qubits and we conjecture that the property is still true.

| *Classes* | *Representative elements* | *Cardinals* | *Solutions* $[x_0, y_0, z_0, t_0, s_0]$ |
|---|---|---|---|
| $\{\{i,j\},\{j,k\},\{k,l\},$ $\{l,n\},\{i,n\}\}$ | $\{\{0,1\},\{1,2\},\{2,3\},$ $\{3,4\},\{0,4\}\}$ | 12 | $[1,1,1,\frac{-d_1\triangle_5}{d_0\triangle_6},-\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{i,l\},$ $\{i,n\},\{j,k\}\}$ | $\{\{0,1\},\{0,2\},\{0,3\},$ $\{0,4\},\{1,2\}\}$ | 30 | $[1,-\frac{b_1(i-1)}{b_0(i+1)},(i+1)\frac{c_1}{c_0},1,-\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{i,l\},$ $\{j,n\},\{j,k\}\}$ | $\{\{0,1\},\{0,2\},\{0,3\},$ $\{1,4\},\{1,2\}\}$ | 60 | $[1,-\frac{b_1(i-1)}{b_0(i+1)},(i+1)\frac{c_1}{c_0},1,-\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{i,l\},$ $\{j,k\},\{k,l\}\}$ | $\{\{0,1\},\{0,2\},\{0,3\},$ $\{1,2\},\{1,3\}\}$ | 30 | $[-i\frac{a_1}{a_0},i\frac{b_1(i-1)}{b_0(i+1)},\frac{c_1}{c_0},\frac{d_1}{d_0},1]$ |
| $\{\{i,j\},\{j,k\},\{k,l\},$ $\{i,l\},\{j,n\}\}$ | $\{\{0,1\},\{1,2\},\{2,3\},$ $\{0,3\},\{1,4\}\}$ | 60 | $[\frac{a_1(i-1)(b_0-b_1)}{a_0(i+1)(b_0+b_1)},1,\frac{c_1}{c_0}i,1,1]$ |
| $\{\{i,j\},\{j,k\},\{i,k\},$ $\{i,l\},\{l,n\}\}$ | $\{\{0,1\},\{1,2\},\{0,2\},$ $\{0,3\},\{3,4\}\}$ | 60 | $[1,-\frac{b_1(i-1)}{b_0(i+1)},i\frac{c_1}{c_0},1,-\frac{e_1}{e_0}]$ |

**Table 4.** Non trivial solutions of $S_{\Phi_E}$ for $\mathtt{card}(E)=5$

## 6. Conclusion and perspectives

We have investigated some properties of the controlled-$Z$ gates. In particular, we have described combinatorially and algebraically the group generated by controlled-$Z$ and swap gates and we have studied its action with respect to the entanglement (`SLOCC`-equivalence). In terms of algebra, this group is isomorphic to the semi-direct product of two well known groups and this property allows us to propose algorithms for simplifying circuits. About entanglement, we have shown that the group is powerful enough to generate the states $|\mathtt{GHZ}_k\rangle$ from a completely factorized state but not to generate a representative element for every `SLOCC`-classes. In particular, we have shown that for four and five qubits, it is not possible to produce a generically entangled state (in the sense of Miyake [25]). Furthermore, by adding unitary single qubit operations, all the unitary operations can be encoded and the associated circuits can be implemented on actual quantum machines without too many adjustments. So we have here an interesting toy model for the study of quantum circuits with many connections with algebra, combinatorics and geometry. Nevertheless, there are still many interesting questions to explore. Let us list some of them.

### *6.1. On the network structure of the qubits*

It would be interesting to design circuit simplification algorithms that work regardless of the configuration of the network of the qubits. Since the controlled-$Z$ operations are symmetrical, we have only to investigate networks which are undirected graphs. If the network is organized as a line (the bit 0 is connected to the bit 1, the bit 1 is connected to the bit 2 etc.) then one has to manage with generators which are

| *Classes* $\{\{i,j\} \mid 0 \le i < j \le 4\} \setminus E'$ *with* $E' =$ | *Representative elements* $E' =$ | *Cardinals* | *Solutions* $[x_0, y_0, z_0, t_0, s_0]$ |
|---|---|---|---|
| $\{\}$ | $\{\}$ | 1 | $[\frac{a_1}{a_0}, -\frac{b_1}{b_0}, -\frac{c_1}{c_0}, \frac{d_1}{d_0}, 1]$ |
| $\{\{i,j\}\}$ | $\{\{0,1\}\}$ | 10 | $[\frac{a_1}{a_0}, -\frac{b_1}{b_0}, -\frac{c_1}{c_0}, \frac{d_1}{d_0}, 1]$ |
| $\{\{i,j\},\{i,k\}\}$ | $\{\{0,1\},\{0,2\}\}$ | 30 | $[1, -\frac{b_1(i-1)}{b_0(i+1)}, i\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{k,l\}\}$ | $\{\{0,1\},\{2,3\}\}$ | 15 | $[\frac{a_1}{a_0}, -\frac{b_1(i-1)}{b_0(i+1)}, i\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{i,l\}\}$ | $\{\{0,1\},\{0,2\},\{0,3\}\}$ | 20 | $[-\frac{a_1}{a_0}, -\frac{b_1(i-1)}{b_0(i+1)}, i\frac{c_1}{c_0}, 1, 1]$ |
| $\{\{i,j\},\{j,k\},\{i,k\}\}$ | $\{\{0,1\},\{1,2\},\{0,2\}\}$ | 10 | $[1, \frac{b_1}{b_0}, -\frac{c_0}{c_1}, 1, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{j,l\}\}$ | $\{\{0,1\},\{0,2\},\{1,3\}\}$ | 60 | $[\frac{a_1}{a_0}, 1, -\frac{b_1(c_0-c_1)}{b_0(c_0+c_1)}, 1, 1, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{l,n\}\}$ | $\{\{0,1\},\{0,2\},\{3,4\}\}$ | 30 | $[1, -\frac{b_1(i-1)}{b_0(i+1)}, i\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$ |
| $\{\{i,j\},\{i,k\},\{i,l\},\{i,n\}\}$ | $\{\{0,1\},\{0,2\},\{0,3\},\{0,4\}\}$ | 5 | $[-\frac{a_1}{a_0}, -\frac{b_1(i-1)}{b_0(i+1)}, i\frac{c_1}{c_0}, 1, 1]$ |
| $\{\{i,j\},\{i,k\},\{i,l\},\{j,n\}\}$ | $\{\{0,1\},\{0,2\},\{0,3\},\{1,4\}\}$ | 60 | $[-\frac{a_1}{a_0}, -\frac{b_1(i-1)}{b_0(i+1)}, i\frac{c_1}{c_0}, 1, 1]$ |
| $\{\{i,j\},\{j,k\},\{i,k\},\{i,l\}\}$ | $\{\{0,1\},\{1,2\},\{0,2\},\{0,3\}\}$ | 60 | $[-\frac{a_1}{a_0}, \frac{b_1}{b_0}, -\frac{c_1}{c_0}, 1, 1]$ |
| $\{\{i,j\},\{j,k\},\{k,l\},\{i,l\}\}$ | $\{\{0,1\},\{1,2\},\{2,3\},\{0,3\}\}$ | 15 | $[-\frac{a_1(c_0-c_1)}{a_0(c_0+c_1)}, 1, 1, -\frac{d_1(b_0-b_1)}{d_0(b_0+b_1)}, 1]$ |
| $\{\{i,j\},\{k,l\},\{l,n\},\{k,n\}\}$ | $\{\{0,1\},\{2,3\},\{3,4\},\{2,4\}\}$ | 10 | $[\frac{a_1}{a_0}, -\frac{b_1}{b_0}, -\frac{c_1}{c_0}, \frac{d_1}{d_1}, 1]$ |
| $\{\{i,j\},\{j,k\},\{k,l\},\{l,n\}\}$ | $\{\{0,1\},\{1,2\},\{2,3\},\{3,4\}\}$ | 60 | $[\frac{a_0(c_0-c_1)}{a_1(c_0+c_1)}, -\frac{b_1}{b_0}, 1, 1, -\frac{e_1}{e_0}]$ |

**Table 5.** Non trivial solutions of $S_{\Phi_E}$ for $\mathtt{card}(E) > 5$

elementary transpositions $S_i$, $i = 0 \ldots k-2$, that permute the values of $i$ and $i+1$, together with the controlled-$Z$: $Z_i := Z_{i,i+1}$. Minimizing the number of elementary transposition in a permutation is a well known exercise in combinatorics. This is important for quantum computing, because transpositions are often implemented from 3 quantum 2-qubit gates, see equality (7), and so are particularly unreliable. Finding an optimal algorithm for reduction requires a deeper knowledge of the algebraic and combinatorial structure of the group $\mathtt{cZS}_k$ and will be the topic of future works.

### *6.2. Algebraic structure*

Beyond applications in quantum information, the groups $\mathtt{cZS}_k$ deserve to be studied for themselves. First, as for symmetric group, we have a tower of groups $\mathtt{cZS}_2 \subset \mathtt{cZS}_3 \subset \cdots \subset \mathtt{cZS}_k \subset \cdots$. This suggests connections with combinatorial Hopf algebras. In particular, the conjugacy classes and the representation theory of these groups must be studied in details. One of the underlying question is: Is there a polynomial

representation whose base would be indexed by combinatorial objects and which could be provided with a co-product giving it a Hopf algebra structure?
Representations as matrices are also highly relevant in our context. Indeed, any circuit composed of controlled-$Z$ and `SWAP` gates is nothing but the image of an element of the abstract group $\mathtt{cZS}_k$ through a certain representation. This representation has the particularity that it is also a linear representation of a free PRO [20]. So it is not irreducible and it would be interesting to understand its decomposition into irreducible representations.

### *6.3. Generalizations of* $\mathtt{cZS}_k$ *and entanglement*

Even if we investigated a few properties of $\mathtt{cZS}_k$ with respect to entanglement, a detailed and complete study remains to be done for any number of qubits. In particular, we focused on `SLOCC`-equivalence but `LU`-equivalence is also highly relevant in that context. Gühne at al. [34] investigated `LU`-equivalence with respect to more general operations indexed by hypergraphs (instead of simple graphs in our paper). They proved that some generically entangled states, like

$$\begin{array}{rcl} V_3 & := & \frac{1}{\sqrt{8}}\left(|0011\rangle+|0101\rangle+|1001\rangle+|0110\rangle+|1010\rangle+|1100\rangle\right. \\ & & \left.+|0000\rangle-|1111\rangle\right), \\ V_9 & := & \frac{1}{2}\left(|0000\rangle-|1111\rangle\right)+\frac{1}{4}\left(|0100\rangle+|0101\rangle-0110\rangle+|0111\rangle\right. \\ & & \left.+|1000\rangle-|1001\rangle+|1010\rangle+|1011\rangle\right) \\ V_{14} & = & \frac{1}{\sqrt{8}}\left(|0011\rangle+|0101\rangle+|1001\rangle+|0110\rangle+|1010\rangle+|1100\rangle\right. \\ & & \left.+|0001\rangle-|1110\rangle\right). \end{array} \tag{57}$$

can be obtained from $|0000\rangle$. Remark that even if these states are generically entangled in the sense of [25], ie. $\Delta \neq 0$, they have , however, some specificities. For instance $V_3$ and $V_{14}$ belongs to the third secant variety $\sigma_3(\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1)$, ie. $L=M=N=0$ [30]. For the state $V_{14}$, we have $Q_1(V_{14})=Q_2(V_{14})=Q_3(V_{14})=-x(x-\frac{1}{4}y)(x^2-\frac{3}{4}xy+\frac{1}{16}x^2)$. The state $V_9$ is in a certain sense more general than $V_3$ and $V_{14}$ because only the invariant $L$ vanishes but this means that it belongs to the third secant variety $\sigma_3(\mathbb{P}^3\times\mathbb{P}^3)$. It would be interesting to know if one can generate more general entanglement types such that $L, M, N \neq 0$.

**Acknowledgement** We acknowledge Irina Yakimenko and Frédéric Holweck the fruitful discussions. We thank Ammar Husain for suggesting us the possibility of using Dehn's algorithm for simplifying quantum circuits.
This work is partially supported by the projects MOUSTIC (ERDF/GRR) and ARTIQ (ERDF/RIN).

[1] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22:563–591, May 1980.

[2] Yuri Ivanovitch Manin. *Computable and Noncomputable (in Russian)*. Sovetskoye Radio, Moscow, 1980.

[3] Richard P. Feynman. Simulating Physics with Computers. *International Journal of Theoretical Physics*, 21:467–488, June 1982.

[4] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[5] David Deutsch and Jozsa Richard. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 439(1907):553–558, 1992.

[6] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.

[7] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.

[8] Isaak Chuang and Yoshihisa Yamamoto. Simple quantum computer. *Physical review. A*, 52:3489–3496, 12 1995.

[9] Quentin A. Turchette. *Quantum optics with single atoms and single photons*. PhD thesis, California Institute of Technology, 01 1997.

[10] Juan I. Cirac and P Zoller. Quantum computer with cold trapped ions. *Physical Review Letters*, 74:4091, 1995.

[11] David G. Cory, Amr F. Fahmy, and Havel Timothy F. Two-bit gates are universal for computation. *Physical Review A*, 51(2):1015–1022, 1995.

[12] Neil Gershenfeld and Isaak I. Chuang. Bulk spin resonance quantum computation. *Science*, 275:350, 1997.

[13] Michael H. Freedman, Kitaev Alexei, Michael J. Larsen, and Zhenghan Wang. Topological quantum computation. *Bulletin of American Mathematical Society*, 40:31–38, 2004.

[14] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493, 1995.

[15] Irina Yakimenko. *Lecture notes on quantum computers*. Linköping University, 2018.

[16] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58 (12):1131, 1990.

[17] Wolfgang Dür, Guifre Vidal, and Cirac J. Ignacio. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62:062314, 2000.

[18] Saunders MacLane. Categorical algebra. *Bulletin of the American Mathematical Society*, 71:40–106, 1965.

[19] Tom Leinster. *Higher Operads, Higher Categories*. Cambridge University Press, 2004.

[20] Eric Laugerotte, Jean-Gabriel Luque, Ludovic Mignot, and Florent Nicart. Multilinear representations of free pros. arXiv:1803.00228.

[21] David P. DiVincenzo. Two-bit gates are universal for computation. *Physical Review A*, 51(2):1015–1022, 1995.

[22] Anders Björner and Francesco Brenti. *Combinatorics of Coxeter Groups, Graduate Texts in Mathematics, 231*. Springer, 2005.

[23] Donald E. Knuth. *The Art of Computer Programming, Volume 3: Sorting and Searching, Reading*. Mass.: Addison-Wesley, 1973.

[24] I.G. Lysënok. Some algorithmic properties of hyperbolic groups. *Izv. Akad. Nauk SSSR Ser. Mat*, 53(4):814832, 1989.

[25] Akimasa Miyake. Classification of multipartite entangled state s by multidimensional determinant. *Phys. Rev. A*, 67:012108, 2003.

[26] Alexander Klyachko. Coherent states, entanglement, and geometric invariant theory. arXiv:quant-ph/0206012v1.

[27] Frédéric Holweck, Jean-Gabriel Luque, and Thibon Jean-Yves. Geometric descriptions of

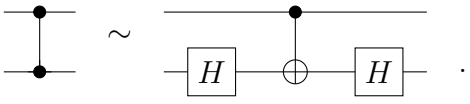
entangled states by auxiliary varieties. *Journal of Mathematical Physics*, 53 (10):102203, 2012.
[28] Frank Verstraete, Jeronen Dehaene, Bart De Moor, and Henri Verschelde. Four qubits can be entangled in nine different ways. *Phys. Rev. A*, 65:052112, 2002.
[29] Frédéric Holweck, Jean-Gabriel Luque, and Thibon Jean-Yves. Entanglement of four qubit systems: A geometric atlas with polynomial compass i (the finite world). *Journal of Mathematical Physics*, 55 (1):012202, 2014.
[30] Frédéric Holweck, Jean-Gabriel Luque, and Thibon Jean-Yves. Entanglement of four-qubit systems: a geometric atlas with polynomial compass ii (the tame world). *Journal of Mathematical Physics*, 58 (2):022201, 2017.
[31] Jean-Gabriel Luque and Jean-Yves Thibon. The polynomial invariants of four qubits. *Phys. Rev. A*, 67:042303, 2003.
[32] Peter Olver. *Classical Invariant Theory.* Cambridge University Press, Cambridge UK, 1999.
[33] Israel M Gelfand, Mikhail M. Kapranov, and Zelevisnky Andrei V. *Discriminants, Resultants and Multidimensional Determinant.* Birkhäuser, 1992.
[34] Otfried Gühne, Marti Cuquet, Frank E. S. Steinhoff, Tobias Moroder, Matteo Rossi, Dagmar Bruß, Barbara Kraus, and Chiara Macchiavello. Entanglement and nonclassical properties of hypergraph states. *Journal of Physics A: Mathematical and Theoretical*, 47(33):335303, 2014.
[35] D.L. Johnson. *Presentation of groups, London Math. Soc. Lecture Note series 22.* Cambridge University Press, 1976.

## Appendix A. Quantum circuits on actual quantum computers

Although the model we have investigated is a toy model, the calculations can be performed on actual quantum machines and illustrate the importance of using the less of 2-qubit gates as possible. To perform our computations, we use the `IBM` Q experience. On its website `https://quantumexperience.ng.bluemix.net/qx/experience`, `IBM` offers a free online access to three quantum computers. Two of these computers have 5 qubits and the third has 16 qubits. We used them to test our quantum circuits. The 5 qubits computers are not organized as a complete graph since there are only 6 connections implemented. There are several differences between the circuits that can be realized on these machines and those presented in the paper:

- The network is not a complete graph.
- The only 2-qubit gates that can be used are $c-\mathtt{X}$. The others must be obtained by combining gates.
- The uses of the gates induce a probability of error, with a very significant probability of error for 2-qubit gates.

The $c-\mathtt{Z}$ gates are implementable since we have




(A.1)

Elementary transpositions are obtained by using (7). Nevertheless, they used three 2-qubit gates and then are very unreliable. Despite all this, we can test some of our circuits in real situations and check some of their properties. For instance, consider the circuit of figure A1 computed on the IBM Q 5 Tenerife machine. The result of the

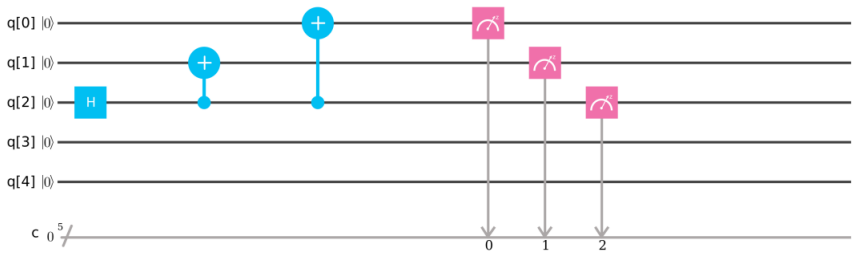



**Figure A1.** Circuit producing a $|\mathtt{GHZ}_3\rangle$ state on the IBM Q 5 Tenerife machine

experiment is in figure A2. It is interesting to note that although theoretically only the states $|00000\rangle$ and $|00111\rangle$ can be reached, the other states have a low but not zero probability of being obtained after the measure. Consider the circuit pictured in figure

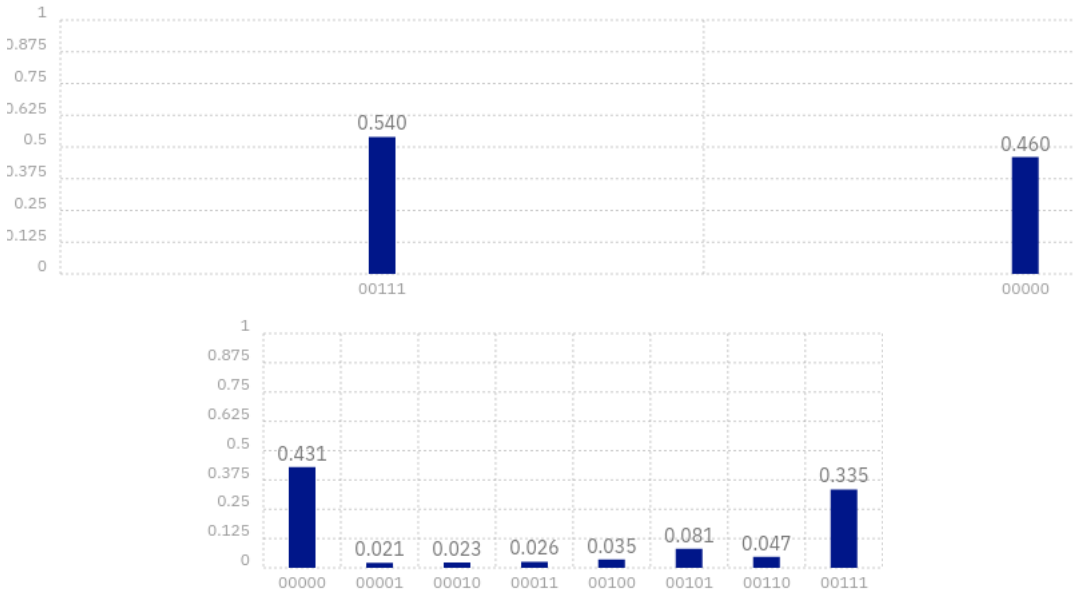



**Figure A2.** Execution of the circuit of figure A1. The top graphic is a simulation while the graphic on the bottom is obtained after 1024 executions on the IBM Q 5 Tenerife machine. Both graphics have been produced through the IBM website.

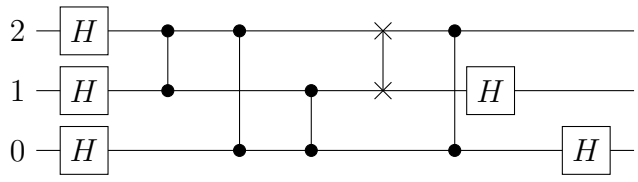



**Figure A3.** Circuit equivalent to those of figure A1 but with more 2-qubit gates.

A3. Applying the results of section 4 we find that it is equivalent to those of figure A1. This circuit has been implemented on the IBM Q 5 Tenerife machine (see figure

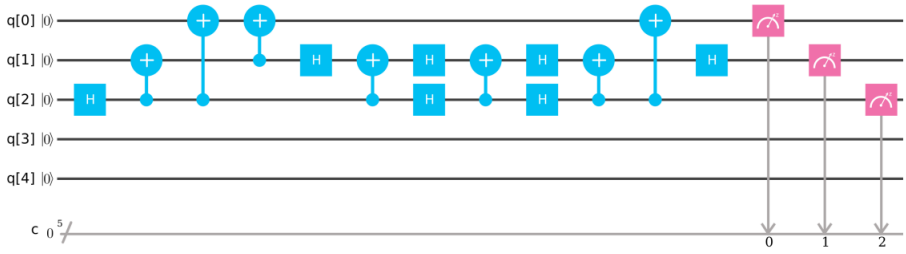



**Figure A4.** Circuit of A3 implemented on the IBM Q 5 Tenerife machine.

A4). After 1024 executions, we observe that reliability is less good than for the circuit of figure A1. This is due to the fact that more 2-qubit gates were used.

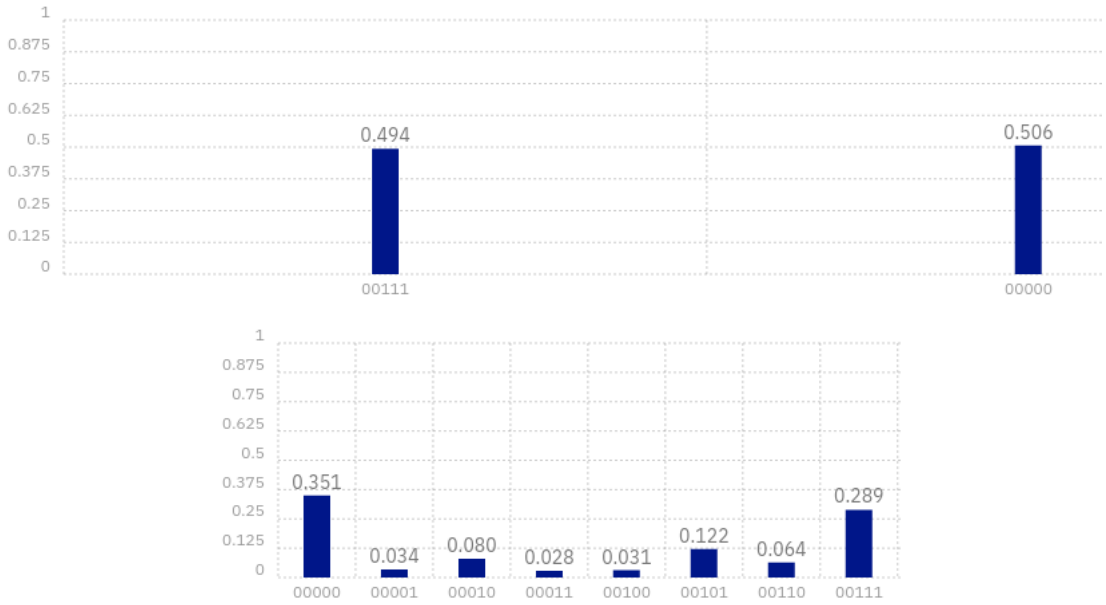



**Figure A5.** Execution of the circuit of figure A4. The top graphic is a simulation while the graphic on the bottom is obtained after 1024 executions on the IBM Q 5 Tenerife machine. Both graphics have been produced through the IBM website.

## Appendix B. Proofs of Theorems 2 and 4

The proofs are based on two well known facts about group presentations.

**Claim 13** *(See eg. [35])*
*Let* $G_1 = \langle \mathcal{S}_1 | \mathcal{R}_1 \rangle$ *and* $G_2 = \langle \mathcal{S}_2 | \mathcal{R}_2 \rangle$ *be two groups given by presentation. The semidirect*

*product* $G_1 \rtimes_\Phi G_2$ *is isomorphic to*

$$\langle \mathcal{S}_1 \cup \mathcal{S}_2 | \mathcal{R}_1 \cup \mathcal{R}_2 \cup \{ g_2 g_1 g_2^{-1} \left(\Phi(g_2)(g_1)\right)^{-1} \mid g_1 \in \mathcal{S}_1, g_2 \in \mathcal{S}_2 \} \rangle. \tag{B.1}$$

**Claim 14** *Let* $G = \langle \mathcal{S} | \mathcal{R} \rangle$. *We suppose that* $\mathcal{S}$ *splits into two subsets* $\mathcal{S}_1$ *and* $\mathcal{S}_2$ *such that* $\mathcal{S}_2$ *is include to the subgroup of* $G$ *generted by* $\mathcal{S}_1$. *Let* $\mathcal{R}_1$ *denote the set of relations in* $\mathcal{R}$ *that involves at least an element of* $\mathcal{S}_2$ *and* $\mathcal{R}_2 = \mathcal{R} \setminus \mathcal{R}_1$. *We construct a set* $\mathcal{R}'_2$ *by replacing in* $\mathcal{R}_2$ *each occurrence of an element of* $\mathcal{S}_2$ *by an equivalent product of elements of* $\mathcal{S}_1$. *Obviously, one obtains that* $G$ *is isomorphic to* $\langle G | \mathcal{R}_1 \cup \mathcal{R}'_2 \rangle$.

**Example 15** Let us illustrate our purpose by giving a presentation of $\mathtt{cZS}_3$. First we remark that $\mathfrak{P}_3$ is isomorphic to $\langle z_0, z_1, z_{02} | z_0^2, z_1^2, z_{02}^2, (z_0 z_{02})^2, (z_0 z_1)^2, (z_0 z_{02})^2 \rangle$ and $\mathfrak{S}_3$ is isomorhic to $\langle s_0, s_1 | s_0^2, s_1^2, (s_0 s_1)^3 \rangle$. One applies Claim 13 from Theorem 1 and obtains that $\mathtt{cZS}_3$ is isomorphic to $\langle z_0, z_1, z_{02}, s_0, s_1 | \mathcal{R} \rangle$, where

$$\mathcal{R} = \{ z_0^2, z_1^2, z_{02}^2, (z_0 z_{02})^2, (z_0 z_1)^2, (z_0 z_{02})^2, (z_1 z_{02})^2, s_0^2, s_1^2, (s_0 s_1)^3, (z_0 s_0)^2, (z_1 s_1)^2, s_1 z_0 s_1 z_{02}, s_0 z_1 s_0 z_{02} \}.$$

We apply Claim 14 with $\mathcal{S}_1 = \{ z_0, z_1, s_0, s_1 \}$ and $\mathcal{S}_2 = \{ z_{02} \}$. Indeed we note that $z_{02} = s_1 z_0 s_1$. Hence

$$\mathcal{R}_1 = \{ z_0^2, z_1^2, (z_0 z_1)^2, s_0^2, s_1^2, (s_0 s_1)^3, (z_0 s_0)^2, (z_1 s_1)^2 \}$$

and

$$\mathcal{R}_2 = \{ z_{02}^2, (z_1 z_{02})^2, (z_0 z_{02})^2, s_1 z_0 s_1 z_{02}, s_0 z_1 s_0 z_{02} \},$$

and so

$$\mathcal{R}'_2 = \{ (s_1 z_0 s_1)^2, (z_1 s_1 z_0 s_1)^2, (z_0 s_1 z_0 s_1)^2, s_1 z_0 s_1 s_1 z_0 s_1, s_0 z_1 s_0 s_1 z_0 s_1 \}.$$

Since, $s_1^2 = z_0^2 = 1$ we can remove the relation $s_1 z_0 s_1 s_1 z_0 s_1$ from $\mathcal{R}'_2$. Furthermore, $s_0 z_1 s_0 s_1 z_0 s_1 = 1$ implies $(z_1 s_1 z_0 s_1)^2 = (z_1 s_0)^4$. Hence, $\mathtt{cZS}_3$ is isomorphic to

$$\langle z_0, z_1, s_0, s_1 | z_0^2, z_1^2, s_0^2, s_1^2, (s_0 s_1)^3, (z_0 z_1)^2, (z_0 s_0)^2, (z_1 s_1)^2, (z_0 s_1)^4, (z_1 s_0)^4, s_0 s_1 z_0 s_1 s_0 z_1 \rangle.$$

Assuming that $s_0 s_1 z_0 s_1 s_0 z_1 = (z_0 s_0)^2 = (z_0 s_1)^4 = s_0^2 = s_1^1 = 1$, one finds

$$(z_1 s_1)^2 = s_0 s_1 (z_0 s_0)^2 s_1 s_0 = 1,$$

$$(z_0 z_1)^2 = s_0 (z_0 s_1)^4 s_0 = 1,$$

$$(z_1 s_0)^4 = s_1 (z_0 z_1)^2 s_1 = 1.$$

Then we simplify the presentation of $\mathtt{cZS}_3$ as

$$\langle z_0, z_1, s_0, s_1 | z_0^2, z_1^2, s_0^2, s_1^2, (s_0 s_1)^3, (z_0 s_0)^2, (z_0 s_1)^4, s_0 s_1 z_0 s_1 s_0 z_1 \rangle.$$

Reformulated in terms of presentation Theorem 2 reads:

**Theorem 16** *Suppose* $k \geq 2$. *The group* $\mathtt{cZS}_k$ *is isomorphic to the presentation* $\langle z_0, \ldots, z_{k-2}, s_0, \ldots, s_{k-2} | \mathcal{R} \rangle$ *where* $\mathcal{R}$ *is the following set of relations*

*(i) for any* $0 \leq i \leq k-2$, $z_i^2 = s_i^2 = 1$,
*(ii) for any* $0 \leq i < j \leq k-2$ *such that* $j-i > 1$, $(s_i s_j)^2 = 1$,
*(iii) for any* $0 \leq i \leq k-3$, $(s_i s_{i+1})^3 = 1$,
*(iv) for any* $0 \leq i < j \leq k-2$, $(z_i z_j)^2 = 1$,
*(v) for any* $0 \leq i, j \leq k-2$ *such that* $|i-j| \neq 1$, $(z_i s_j)^2 = 1$,
*(vi) for any* $0 \leq i, j \leq k-2$ *such that* $|i-j| = 1$, $(z_i s_j)^4 = 1$,
*(vii) for any* $0 \leq i \leq k-3$, $s_i s_{i+1} z_i s_{i+1} s_i z_{i+1} = 1$.

**Proof** If $k = 2$ the result is straightforward from the definition. Now we assume $k \geq 3$. We apply Claim 13 and find a presentation of $\mathtt{cZS}_k$ as $\langle \mathcal{S} | \mathcal{R} \rangle$ with

$$\mathcal{S} = \mathcal{T} \cup \mathcal{Z}$$

and

$$\mathcal{R} = \mathcal{RS} \cup \mathcal{RZ} \cup \mathcal{RC},$$

where $\mathcal{T} = \{s_i \mid 0 \leq i \leq k-2\}$, $\mathcal{Z} = \{z_{\{i,j\}} \mid 0 \leq i \leq j-1 \leq k-2\}$, $\mathcal{RS} = \{s_i^2 \mid 0 \leq i \leq k-3\} \cup \{(s_i s_j)^2 \mid 0 \leq i < j-1 \leq k-3\} \cup \{(s_i s_{i+1})^3 \mid 0 \leq i \leq k-3\}$, $\mathcal{RZ} = \{z_{\{i,j\}}^2 \mid 0 \leq i < j \leq k-1\} \cup \{(z_{\{i,j\}} z_{\{p,q\}})^2 \mid 0 \leq i \leq j-1 \leq k-2, 0 \leq p \leq q-1 \leq k-2\}$, and $\mathcal{RC} = \{s_p z_{\{i,j\}} s_p z_{\{s_p(i), s_p(j)\}} | 0 \leq i < j \leq k-1, 0 \leq p \leq k-2\}$.The set $\mathcal{RS}$ means that the subgroup $G_S = \langle T | \mathcal{RS} \rangle$ is isomorphic to the symmetric group $\mathfrak{S}_k$. The set $\mathcal{RZ}$ means that the subgroup $G_Z = \langle \mathcal{Z} | \mathcal{RZ} \rangle$ is isomorphic to $\mathbb{Z}_2^{\binom{k}{2}}$. The set $\mathcal{R}C$ encodes the conjugacy of an element of $\mathcal{Z}$ by an element of $G_S$. More precisely, if $\sigma$ is a permutation of $\mathfrak{S}_k$ and $w_\sigma$ denotes the image of $\sigma$ in $G_S$ then the relations of $\mathcal{R}S$ and $\mathcal{R}C$ implies

$$w_\sigma z_{\{i,j\}} w_\sigma^{-1} = z_{\{\sigma(i), \sigma(j)\}}. \tag{B.2}$$

For simplicity, in the rest of the proof we set $z_{ij} := z_{\{i,j\}}$ and $z_i := z_{ii+1}$. The relation $z_{ij}^2 = 1$ can be recovered from $z_i^2 = 1$ and the relations of $\mathcal{RS} \cup \mathcal{RC}$. Indeed it suffices to consider a permutation $\sigma$ sending $\{i, j\}$ to $\{i, i+1\}$ and write $z_{ij}^2 = (w_\sigma^{-1} z_i w_\sigma)^2 = w_\sigma^{-1} z_i^2 w_\sigma = 1$. In the same way, if $\sigma$ is a permutation sending $\{i, j\}$ to $\{i_1, i_1{+}1\}$ and $\{p, q\}$ to $\{i_2, i_2{+}1\}$ for some $0 \leq i < j \leq k{-}1$, $0 \leq p < q \leq k{-}1$, $i \neq p$, $j \neq q$ and $0 \leq i_1, i_2 \leq k-2$ we have $(z_{ij} z_{pq})^2 = (w_\sigma^{-1} z_{i_1} w_\sigma w_\sigma^{-1} z_{i_2} w_\sigma)^2 = w_\sigma^{-1} (z_{i_1} z_{i_2})^2 w_\sigma$. So the relation $(z_{ij} z_{pq})^2 = 1$ can be recovered from $(z_{i_1} z_{i_2})^2 = 1$ and the relations of $\mathcal{RS} \cup \mathcal{RC}$. If ($i = p$ and $j \neq q$) or ($i \neq p$ and $j = q$), there exists no permutation sending $\{i, j\}$ to $\{i_1, i_1 + 1\}$ and $\{p, q\}$ to $\{i_2, i_2 + 1\}$ for some $0 \leq i_1, i_2 \leq k-2$. We introduce the set of relations $\mathcal{RSZ} := \{(z_i s_j)^4 | 0 \leq i, j \leq k-2, |i-j| = 1\}$. These relations can be recovered from $\mathcal{R}$ since $(z_i s_{i+1})^4 = (z_i z_{ii+2})^2$ and $(z_i s_{i-1})^4 = (z_i z_{i-1i+1})^2$. If ($i = p$ and $j \neq q$) or ($i \neq p$ and $j = q$) then there exists a permutation $\sigma$ sending $\{i, j\}$ to $\{i_1, i_1 + 1\}$ and $\{p, q\}$ to $\{i_1, i_1 + 2\}$ for some $0 \leq i_1 \leq k-3$. Hence, $(z_{ij} z_{pq})^2 = (w_\sigma^{-1} z_{i_1} z_{i_1 i_1+2} w_\sigma)^2 = w_\sigma^{-1} (z_{i_1} z_{i_1 i_1+2})^2 w_\sigma = w_\sigma^{-1} (z_{i_1} s_{i_1+1})^4 w_\sigma$.
As a conclusion, we deduce that $\langle \mathcal{S} | \mathcal{R} \rangle = \langle \mathcal{S} | \mathcal{R}' \rangle$ with $\mathcal{R}' = \mathcal{RS} \cup \mathcal{RZ}' \cup \mathcal{RC} \cup \mathcal{RSZ}$ and $\mathcal{RZ}' = \{z_i^2 \mid 0 \leq i \leq k-2\} \cup \{(z_i z_p)^2 \mid 0 \leq i, p \leq k-2\}$.

Now let us remove redundancies in $\mathcal{RC}$ and proves that it can be replaced by $\mathcal{RC}' := \{(s_jz_i)^2 \mid |i-j| \neq 1\} \cup \{s_is_{i+1}z_is_{i+1}s_iz_{i+1} \mid 0 \leq i \leq k-3\} \cup \{s_{j-1}z_{ij}s_{j-1}z_{ij-1} \mid 0 \leq i \leq j-2 \leq k-3\}$ in the presentation. The first and the last sets of the definition of $\mathcal{RC}'$ are include in $\mathcal{RC}$. Furthermore, in $\langle \mathcal{S}|\mathcal{R}'\rangle$, we have $s_is_{i+1}z_is_{i+1}s_iz_{i+1} = s_iz_{ii+2}s_iz_{i+1} \in \mathcal{RC}$. Conversely, we set $\mathcal{R}'' := \mathcal{RS} \cup \mathcal{RZ}' \cup \mathcal{RC}' \cup \mathcal{RSZ}$ and we prove that for any $w \in \mathcal{RC}$, we have $w = 1$ in $\langle S|\mathcal{R}''\rangle$. Indeed, we have $\mathcal{RC} \setminus \mathcal{RC}' \subset \{s_pz_{ij}s_pz_{ij}|p \notin \{i-1, i, j-1, j\} \cup \{s_jz_{ij}s_jz_{ij+1} \mid 0 \leq i \leq j-1 \leq k-3\} \cup \{s_{i-1}z_{ij}s_{i-1}z_{i-1j} \mid 1 \leq i < j \leq k-1\} \cup \{s_iz_{ij}s_iz_{i+1j} \mid 0 \leq i \leq j-2 \leq k-3\}$. So we have to consider 4 cases:

(i) Consider the element $s_jz_{ij}s_jz_{ij+1}$ with $0 \leq i \leq j-1 \leq k-3$. We have $s_jz_{ij}s_jz_{ij+1} = (z_{ij+1}s_jz_{ij}s_j)^{-1} = s_j(s_jz_{ij+1}s_jz_{ij})^{-1}s_j = s_j^2 = 1$ in $\langle \mathcal{S} \mid \mathcal{R}''\rangle$.

(ii) Consider the element $s_{i-1}z_{ij}s_{i-1}z_{i-1j}$ with $1 \leq i < j \leq k-1$. If $i = j-1$ then, using the second and third sets of the definition of $\mathcal{RC}'$ one obtains $s_{i-1}z_{ii+1}s_{i-1}z_{i-1i+1} = s_{i-1}z_is_{i-1}s_iz_{i-1}s_i = s_{i-1}z_iz_is_{i-1} = 1$ in $\langle \mathcal{S} \mid \mathcal{R}''\rangle$. If $i < j-1$ then $s_{i-1}z_{ij}s_{i-1}z_{i-1j} = s_{i-1}s_{j-1}z_{ij-1}s_{j-1}s_{i-1}s_{j-1}z_{i-1j-1}s_{j-1} = s_{j-1}s_{i-1}z_{ij-1}s_{i-1}z_{i-1j-1}s_{j-1}$ and, using an induction on $|i-j|$ one finds $s_{j-1}s_{i-1}z_{ij-1}s_{i-1}z_{i-1j-1}s_{j-1} = s_{j-1}^2 = 1$ in $\langle \mathcal{S} \mid \mathcal{R}''\rangle$.

(iii) Consider the element $s_iz_{ij}s_iz_{i+1j}$ for $0 \leq i < j-2 \leq k-3$. We have $s_iz_{ij}s_iz_{i+1j} = s_i(s_iz_{i+1j}s_iz_{ij})^{-1}s_i = 1$ from the previous case.

(iv) Suppose $p \notin \{i-1, i, j-1, j\}$. We proceed by induction on $|i-j|$. If $j = i+1$ then the result is directly obtains from the first set of the definition of $\mathcal{RC}'$. If $p = i+1 = j-2$ then we use the previous cases and obtains $s_{i+1}z_{ii+3}s_{i+1}z_{ii+3} = s_{i+1}s_{i+2}s_{i+1}z_is_{i+1}s_{i+2}s_{i+1}s_{i+2}s_{i+1}z_is_{i+1}s_{i+2}$. Hence using the fact that $z_i$ and $s_{i+2}$ commute in $\langle \mathcal{S} \mid \mathcal{R}''\rangle$ together with the braid relations, one obtains $s_{i+1}s_{i+2}s_{i+1}z_is_{i+1}s_{i+2}s_{i+1}s_{i+2}s_{i+1}z_is_{i+1}s_{i+2} = s_{i+2}s_{i+1}s_{i+2}z_is_{i+2}z_is_{i+1}s_{i+2} = 1$.
If $p \neq j-2$ then $s_pz_{ij}s_pz_{ij} = s_ps_{j-1}z_{ij-1}s_{j-1}s_ps_{j-1}z_{ij-1}s_{j-1} = s_{j-1}s_pz_{ij-1}s_pz_{ij-1}s_{j-1} = 1$ using the induction hypothesis. Finally, if $p \neq i+1$ then $s_pz_{ij}s_pz_{ij} = s_ps_iz_{i+1j}s_is_ps_iz_{i+1j}s_i = s_is_pz_{i+1j}s_pz_{i+1j}s_i = 1$ using the induction hypothesis.

So we have proved that $\langle S \mid \mathcal{R}\rangle = \langle S \mid \mathcal{R}''\rangle$. Now we apply Claim 14 with $\mathcal{S}_1 = \{z_i \mid 0 \leq i \leq k-2\} \cup \{s_i \mid 0 \leq i \leq k-2\}$ and $\mathcal{S}_2 = \{z_{ij} \mid 0 \leq i \leq j-2 \leq k-3\}$. We obtain $\mathcal{R}'' = \mathcal{R}_1 \cup \mathcal{R}_2$ with $\mathcal{R}_1 = \mathcal{RS} \cup \mathcal{RZ}' \cup \mathcal{RSZ} \cup \{(z_is_j)^2 \mid |i-j| \neq 1\} \cup \{s_is_{i+1}z_is_{i+1}s_iz_{i+1} \mid 0 \leq i \leq k-3\}$ and $\mathcal{R}_2 = \{s_{j-1}z_{ij}s_{j-1}z_{ij-1} \mid 0 \leq i \leq j-2 \leq k-3\}$. To obtain $\mathcal{R}_2'$, we substitute each occurrence of $z_{ij}$ in $\mathcal{R}_2$ by $s_{j-1}s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-2}s_{j-1}$. In other words,

$$\mathcal{R}_2' = \{s_{j-1}\cdot s_{j-1}s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-1}\cdot s_{j-1}\cdot s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-2} \mid 0 \leq i \leq j-2 \leq k-3\}.$$

But each $s_{j-1}\cdot s_{j-1}s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-1}\cdot s_{j-1}\cdot s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-2}$ reduces to 1 by using rules of $\mathcal{RS}$ and $\mathcal{RZ}'$. Hence we deduce that $\langle \mathcal{S}|\mathcal{R}\rangle = \langle \mathcal{S}_1|\mathcal{R}_1\rangle$, as expected. □

Theorem 4 is restated as

**Theorem 17** *For* $k \geq 2$, *the group* $\mathtt{cZS}_k$ *is isomorphic to the group* $\langle g_0, g_1, g_2, \ldots, g_{k-1} | \mathcal{R}_k \rangle$, *where* $\mathcal{R}_k$ *is the set of the following relations:*

*(i)* *For any* $0 \leq i \leq k-1$, $g_i^2 = 1$,

*(ii)* *For any* $1 \leq i < j \leq k-1$ *such that* $|i-j| > 1$, $(g_i g_j)^2 = 1$,

*(iii)* *For any* $1 \leq i \leq k-2$, $(g_i g_{i+1})^3 = 1$,

*(iv)* *For any* $i = 1, 3, \ldots k-1$, $(g_0 g_i)^2 = 1$,

*(v)* $(g_0 g_2)^4 = 1$,

*(vi)* $(g_0 g_2 g_3 g_1 g_2)^4 = 1$.

*The explicit isomorphism sends* $Z_0$ *to* $g_0$ *and each* $S_i$ *to* $g_{i+1}$.

**Proof** We find several redundancies in the presentation of Theorem 16. First we compute

$$\begin{array}{rcl} (z_i s_{i-1})^4 & \overset{(vii),(i)}{=} & (s_{i-1} s_i z_{i-1} s_i)^4 \\ & \overset{(iii),(v)}{=} & (s_{i-1} s_i z_{i-1} s_{i-1} s_i z_{i-1} s_{i-1} s_i)^2 \\ & \overset{(iii),(i)}{=} & s_i s_{i-1} (s_i z_{i-1})^4 s_{i-1} s_i. \end{array} \tag{B.3}$$

The overscripted numbers correspond to the rules of Theorem 16 used to obtain each equality. Assuming $(z_{i-1} s_i)^4 = 1$ and applying the rule $(i)$, we show that $(z_i s_{i-1})^4 = 1$. So this relation can be removed from the presentation.
Now let us consider the relations $\{(z_i z_j)^2 = 1 \mid 0 \leq i < j \leq k-2\}$ of point $(iv)$ of Theorem 16. If $j = i+1$ we have :

$$\begin{array}{rcl} (z_i z_{i+1})^2 & \overset{(vii)}{=} & (z_i s_i s_{i+1} z_i s_{i+1} s_i)^2 \\ & \overset{(v)}{=} & (s_i z_i s_{i+1} z_i s_{i+1} s_i)^2 \\ & \overset{(i)}{=} & s_i (z_i s_{i+1})^4 s_i. \end{array}$$

Assuming $(z_i s_{i+1})^4 = 1$ and applying the rule $(i)$ we have $(z_i z_{i+1})^2 = 1$ so this relation can also be removed from the presentation.

If $j = i+2$ then we have

$$\begin{array}{rcl} (z_i z_{i+2})^2 & \overset{(vii)}{=} & (s_{i-1} s_i z_{i-1} s_i s_{i-1} z_{i+2})^2 \\ & \overset{(v)}{=} & (s_{i-1} s_i z_{i-1} z_{i+2} s_i s_{i-1})^2 \\ & \overset{(i)}{=} & s_{i-1} s_i (z_{i-1} z_{i+2})^2 s_i s_{i-1} \\ & \overset{(vii)}{=} & s_{i-1} s_i (z_{i-1} s_{i+1} s_{i+2} z_{i+1} s_{i+2} s_{i+1})^2 s_i s_{i-1} \\ & \overset{(v)}{=} & s_{i-1} s_i (s_{i+1} s_{i+2} z_{i-1} z_{i+1} s_{i+2} s_{i+1})^2 s_i s_{i-1} \\ & \overset{(i)}{=} & s_{i-1} s_i s_{i+1} s_{i+2} (z_{i-1} z_{i+1})^2 s_{i+2} s_{i+1} s_i s_{i-1}. \end{array}$$

Hence by induction on $i$, assuming that $(z_0 z_2)^2 = 1$, we show that $(z_i z_{i+2})^2 = 1$.

If $j > i+2$, then we have

$$\begin{array}{rcl}(z_iz_j)^2 & \overset{(vii)}{=} & (z_is_{j-1}s_jz_{j-1}s_js_{j-1})^2 \\ & \overset{(v)}{=} & (s_{j-1}s_jz_iz_{j-1}s_js_{j-1})^2 \\ & \overset{(i)}{=} & s_{j-1}s_j(z_iz_{j-1})^2s_js_{j-1}\end{array}.$$

Hence by induction on $j$, assuming that $(z_iz_{i+2})^2 = 1$, we show that $(z_iz_j)^2 = 1$.

To summarize we have shown that, assuming points $(vii), (vi), (v), (i)$ of Theorem 16, all the relations of point $(iv)$ (i.e $\{(z_iz_j)^2 = 1 \mid 0 \leq i < j \leq k-2\}$) are redundancies except one : $(z_0z_2)^2 = 1$. We also notice that $(z_0z_2)^2 = (z_0s_1s_2s_0s_1z_0s_1s_0s_2s_1)^2 = (z_0s_1s_2s_0s_1)^4$

Now we apply Claim 14 by setting $\mathcal{S}_1 = \{z_0, s_0, \ldots, s_{k-2}\}$ and $\mathcal{S}_2 = \{z_1, \ldots, z_{k-2}\}$ since

$$z_i = (s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1}). \tag{B.4}$$

We have

$$\mathcal{R}_1 = \mathcal{RS} \cup \{z_0^2 = 1, (z_0s_1)^4 = 1, (z_0s_1s_2s_0s_1)^4 = 1\} \cup \{(z_0s_j)^2 = 1 \mid j \neq 1\}$$

and

$$\begin{array}{rcl}\mathcal{R}_2 & = & \{z_i^2 = 1 \mid 1 \leq i \leq k-2\} \cup \{(z_is_{i+1})^4 = 1 \mid 1 \leq i \leq k-3\} \\ & & \cup\{(z_is_j)^2 = 1 \mid 1 \leq i, j \leq k-2, j \notin \{i-1, i+1\} \\ & & \cup\{s_is_{i+1}z_is_{i+1}s_iz_{i+1} = 1 \mid 0 \leq i \leq k-3\}\end{array}$$

So we have $\mathcal{R}_2' = \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{T}_3 \cup \mathcal{T}_4$ with

$$\mathcal{T}_1 = \{((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1}))^2 = 1 \mid 1 \leq i \leq k-2\}$$

$$\mathcal{T}_2 = \{((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1})^4 = 1 \mid 1 \leq i \leq k-3\}$$

$$\mathcal{T}_3 = \{((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_j)^2 = 1 \mid 1 \leq i, j \leq k-2, j \notin \{i-1, i+1\}$$

$$\mathcal{T}_4 = \{s_is_{i+1}(s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1}s_i(s_is_{i+1})\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_{i+1}s_i) = 1 \mid 0 \leq i \leq k-3\}.$$

Remarking that $((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1}))^2 \overset{\mathcal{R}_1}{=} 1$ we can remove the relation of $\mathcal{T}_1$ from $\mathcal{R}_2'$.

In order to remove the relations of $\mathcal{T}_3$ from $\mathcal{R}_2'$ we distinguish three cases :

(i) If $j > i+1$ then

$$\begin{array}{rcl}((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_j)^2 & \overset{\mathcal{R}_1}{=} & ((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1}))^2s_j^2 \\ & \overset{\mathcal{R}_1}{=} & 1.\end{array}$$

(ii) If $j = i$ then we use the the braid relations and obtain

$$(s_1 s_0)\cdots(s_i s_{i-1})s_i \overset{braid}{=} s_0(s_1 s_0)\cdots(s_i s_{i-1}). \tag{B.5}$$

Hence,

$$\begin{aligned}((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_i)^2 &\overset{braid}{=} ((s_{i-1}s_i)\cdots(s_0s_1)z_0s_0(s_1s_0)\cdots(s_is_{i-1}))^2\\ &\overset{\mathcal{R}_1}{=} (s_{i-1}s_i)\cdots(s_0s_1)(z_0s_0)^2(s_1s_0)\cdots(s_is_{i-1})\\ &\overset{\mathcal{R}_1}{=} 1.\end{aligned}$$

(iii) If $j < i-1$ then we have

$$\begin{aligned}((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_j)^2 &\overset{\mathcal{R}_1}{=} ((s_{i-1}s_i)\cdots(s_js_{j+1})(s_{j-1}s_j)\cdots(s_0s_1)z_0\\ &\quad\cdot(s_1s_0)\cdots(s_js_{j-1})(s_{j+1}s_j)(s_{j+2}s_{j+1})s_j\cdots(s_is_{i-1}))^2\\ &\overset{\mathcal{R}_1}{=} ((s_{i-1}s_i)\cdots(s_js_{j+1})(s_{j-1}s_j)\cdots(s_0s_1)z_0\\ &\quad\cdot(s_1s_0)\cdots(s_js_{j-1})(s_{j+1}s_{j+2})(s_js_{j+1}s_j)\cdots(s_is_{i-1}))^2\\ &\overset{\mathcal{R}_1}{=} ((s_{i-1}s_i)\cdots(s_js_{j+1})(s_{j-1}s_j)\cdots(s_0s_1)z_0\\ &\quad\cdot(s_1s_0)\cdots(s_js_{j-1})(s_{j+1}s_{j+2})(s_{j+1}s_js_{j+1})\cdots(s_is_{i-1}))^2\\ &\overset{\mathcal{R}_1}{=} ((s_{i-1}s_i)\cdots(s_js_{j+1})(s_{j-1}s_j)\cdots(s_0s_1)z_0\\ &\quad\cdot(s_1s_0)\cdots(s_js_{j-1})s_{j+2}(s_{j+1}s_j)(s_{j+2}s_{j+1})\cdots(s_is_{i-1}))^2\\ &\overset{\mathcal{R}_1}{=} (s_{i-1}s_i)\cdots(s_js_{j+1})((s_{j-1}s_j)\cdots(s_0s_1)z_0\\ &\quad\cdot(s_1s_0)\cdots(s_js_{j-1})s_{j+2})^2(s_{j+1}s_j)(s_{j+2}s_{j+1})\cdots(s_is_{i-1})\\ &\overset{\mathcal{R}_1}{=} 1 \text{ (using the first case)}\end{aligned}$$

So we can remove the relations of $\mathcal{T}_3$ from $\mathcal{R}'_2$.
Also, using the relation of the symmetric group, one finds

$$(s_1s_0)\cdots(s_is_{i-1})s_{i+1}(s_{i-1}s_i)\cdots(s_0s_1) \overset{\mathcal{R}_1}{=} s_{i+1}s_i\cdots s_2s_1s_2\cdots s_is_{i+1}. \tag{B.6}$$

Hence,

$$\begin{aligned}((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1})^4 &\overset{\mathcal{R}_1}{=} (s_{i-1}s_i)\cdots(s_0s_1)\\ &\quad\cdot(z_0s_{i+1}s_i\cdots s_2s_1s_2\cdots s_is_{i+1})^3\\ &\quad\cdot z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1}\\ &\overset{\mathcal{R}_1}{=} (s_{i-1}s_i)\cdots(s_0s_1)s_{i+1}s_i\cdots s_2\\ &\quad\cdot(z_0s_1)^3z_0s_2\cdots s_is_{i+1}(s_1s_0)\cdots(s_is_{i-1})s_{i+1}\\ &\overset{\mathcal{R}_1}{=} (s_{i-1}s_i)\cdots(s_0s_1)s_{i+1}s_i\cdots s_2\\ &\quad\cdot(z_0s_1)^4s_2\cdots s_is_{i+1}(s_1s_0)\cdots(s_is_{i-1})\\ &\overset{\mathcal{R}_1}{=} 1.\end{aligned}$$

We deduce that we can remove the relation of $\mathcal{T}_2$. Finally the relation $s_is_{i+1}(s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1}s_i(s_is_{i+1})\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_{i+1}s_i)$ reduces to 1 using only $s_i^2 = z_0^2 = 1$. The relations of $\mathcal{T}_4$ are redundancies. Hence, the group $\mathtt{cZS}_k$ is isomorphic to $\langle\mathcal{S}_1|\mathcal{R}_1\rangle$ and we recover the statement of Theorem 17 by sending $z_0$ to $g_0$ and each $s_i$ to $g_{i+1}$. □

## Appendix C. Entanglement of $|\mathtt{GHZ}_k\rangle$

In this section, we prove that the state $|\mathtt{GHZ}_k\rangle$ is not generically entangled. We start with a result of Miyake [25] stating that a state is generically entangled if and only if its hyperdeterminant $\Delta$ does not vanish. The hyperdeterminant is a high degree invariant polynomial impossible to compute in practice but its interpretation in terms of solutions to a system of equations allows us to test its nullity, see e.g. [33] p445. Let us recall briefly how to process. First we consider $k$ binary variables $\mathbf{x}^{(i)} = (x_0^{(i)}, x_1^{(i)})$, $i = 1..k$. To each state $|\phi\rangle = \sum \alpha_{i_1\dots i_k}|i_1\cdots i_k\rangle$, we associate the binary multilinear form

$$f_\phi := \sum_{0\leq i_1,\dots,i_k\leq 1} \alpha_{i_1,\dots,i_k} x_{i_1}^{(1)}\cdots x_{i_k}^{(k)}. \tag{C.1}$$

The hyperdeterminant vanishes if and only if the system

$$\{f_\phi = 0\} \cup \{\frac{d}{dx_i^{(j)}} f_\phi = 0 \mid 0\leq i\leq 1, 1\leq j\leq k\} \tag{C.2}$$

has a non trivial solution $\hat{\mathbf{x}}^{(1)},\dots,\hat{\mathbf{x}}^{(k)}$, ie such that there exists $1\leq j\leq k$ with $\hat{\mathbf{x}}^{(j)}\neq(0,0)$. For $|\mathtt{GHZ}_k\rangle$ the system is

$$\begin{array}{l} x_0^{(1)}\cdots x_0^{(k)} + x_1^{(1)}\cdots x_1^{(k)} = x_0^{(2)}\cdots x_0^{(k)} = x_1^{(2)}\cdots x_1^{(k)} = x_0^{(1)}x_0^{(3)}\cdots x_0^{(k)} \\ = x_1^{(1)}x_1^{(3)}\cdots x_1^{(k)} = \cdots = x_0^{(1)}\cdots x_0^{(k-1)} = x_1^{(1)}\cdots x_1^{(k-1)} = 0. \end{array} \tag{C.3}$$

We check that for $k>3$, $x_0^{(1)} = x_0^{(2)} = x_1^{(3)} = x_1^{(4)} = 0$ implies (C.3). So for $k>3$, $|\mathtt{GHZ}_k\rangle$ is not generically entangled. Remark that, when $k = 2, 3$, all the solutions of (C.3) are trivial and so $|\mathtt{GHZ}_k\rangle$ is generically entangled.

## Appendix D. Some covariant polynomials associated to 4 qubit systems

In this section, we shall explain how to compute the polynomials which are used to determine the entanglement type of the systems in section 5.3.We shall first recall the definition of the transvection of two multi-binary forms on the binary variables $x^{(1)} = (x_0^{(1)}, x_1^{(1)}),\dots, x^{(p)} = (x_0^{(p)}, x_1^{(p)})$

$$(f,g)_{i_1,\dots,i_p} = \mathrm{tr}\Omega_{x^{(1)}}^{i_1}\dots\Omega_{x^{(p)}}^{i_p} f(x'^{(1)},\dots,x'^{(p)}) g(x''^{(1)},\dots,x''^{(p)}), \tag{D.1}$$

where $\Omega$ is the Cayley operator

$$\Omega_x = \begin{vmatrix} \frac{\partial}{\partial x'_0} & \frac{\partial}{\partial x''_0} \\ \partial x'_1 & \frac{\partial}{\partial x''_1} \end{vmatrix}$$

and tr sends each variables $x', x''$ on $x$ (erases $'$ and $''$). In [27], we give a list of generators of the algebra of covariant polynomials for 4 qubits systems which are obtained by transvection from the ground form

$$A = \sum_{i,j,k,\ell} \alpha_{i,j,k,l} x_i y_j z_k t_\ell.$$

Here we give formulas for some of the polynomials which are used in the paper.

| Symbol | Transvectant |
|---|---|
| $B_{2200}$ | $\frac{1}{2}(A,A)^{0011}$ |
| $B_{2020}$ | $\frac{1}{2}(A,A)^{0101}$ |
| $B_{2002}$ | $\frac{1}{2}(A,A)^{0110}$ |
| $B_{0220}$ | $\frac{1}{2}(A,A)^{1001}$ |
| $B_{0202}$ | $\frac{1}{2}(A,A)^{1010}$ |
| $B_{0022}$ | $\frac{1}{2}(A,A)^{1100}$ |

| Symbol | Transvectant |
|---|---|
| $C^1_{1111}$ | $(A,B_{2200})^{1100}+(A,B_{0022})^{0011}$ |
| $C_{3111}$ | $\frac{1}{3}\left((A,B_{2200})^{0100}+(A,B_{2020})^{0010}+(A,B_{2002})^{0001}\right)$ |
| $C_{1311}$ | $\frac{1}{3}\left((A,B_{2200})^{1000}+(A,B_{0220})^{0010}+(A,B_{0202})^{0001}\right)$ |
| $C_{1131}$ | $\frac{1}{3}\left((A,B_{2020})^{1000}+(A,B_{0220})^{0100}+(A,B_{0022})^{0001}\right)$ |
| $C_{1113}$ | $\frac{1}{3}\left((A,B_{2002})^{1000}+(A,B_{0202})^{0100}+(A,B_{0022})^{0010}\right)$ |

| Symbol | Transvectant |
|---|---|
| $D_{2200}$ | $(A,C^1_{1111})^{0011}$ |
| $D_{2020}$ | $(A,C^1_{1111})^{0101}$ |
| $D_{2002}$ | $(A,C^1_{1111})^{0110}$ |
| $D_{0220}$ | $(A,C^1_{1111})^{1001}$ |
| $D_{0202}$ | $(A,C^1_{1111})^{1010}$ |
| $D_{0022}$ | $(A,C_{1111})^{1100}$ |
| $D_{4000}$ | $(A,C_{3111})^{0111}$ |
| $D_{0400}$ | $(A,C_{1311})^{1011}$ |
| $D_{0040}$ | $(A,C_{1131})^{1101}$ |
| $D_{0004}$ | $(A,C_{1113})^{1110}$ |

| Symbol | Transvectant |
|---|---|
| $F_{4200}$ | $(A,E^1_{3111})^{0011}$ |
| $F_{4020}$ | $(A,E^1_{3111})^{0101}$ |
| $F_{4002}$ | $(A,E^1_{3111})^{0110}$ |
| $F_{0420}$ | $(A,E^1_{1311})^{1001}$ |
| $F_{0402}$ | $(A,E^1_{1311})^{1010}$ |
| $F_{0042}$ | $(A,E^1_{1131})^{1100}$ |
| $F_{2400}$ | $(A,E^1_{1311})^{0011}$ |
| $F_{2040}$ | $(A,E^1_{1131})^{0101}$ |
| $F_{2004}$ | $(A,E^1_{1113})^{0110}$ |
| $F_{0240}$ | $(A,E^1_{1131})^{1001}$ |
| $F_{0204}$ | $(A,E^1_{1113})^{1010}$ |
| $F_{0024}$ | $(A,E^1_{1113})^{1100}$ |

| Symbol | Transvectant |
|---|---|
| $E^1_{3111}$ | $(A,D_{2200})^{0100}+(A,D_{2020})^{0010}+(A,D_{2002})^{0001}$ |
| $E^1_{1311}$ | $(A,D_{2200})^{1000}+(A,D_{0220})^{0010}+(A,D_{0202})^{0001}$ |
| $E^1_{1131}$ | $(A,D_{2020})^{1000}+(A,D_{0220})^{0100}+(A,D_{0022})^{0001}$ |
| $E^1_{1113}$ | $(A,D_{2002})^{1000}+(A,D_{0202})^{0100}+(A,D_{0022})^{0010}$ |

| Symbol | Transvectant |
|---|---|
| $G^1_{3111}$ | $(A,F_{4200})^{1100}$ |
| $G^2_{3111}$ | $(A,F_{4020})^{1010}$ |
| $G^1_{1311}$ | $(A,F_{2400})^{110}$ |
| $G^2_{1311}$ | $(A,F_{0420})^{0110}$ |
| $G^1_{1131}$ | $(A,F_{2040})^{1010}$ |
| $G^2_{1131}$ | $(A,F_{0240})^{0110}$ |
| $G^1_{1113}$ | $(A,F_{2004})^{1001}$ |
| $G^2_{1113}$ | $(A,F_{0204})^{0101}$ |

| Symbol | Transvectant |
|---|---|
| $G_{5111}$ | $(A,F_{4002})^{0001}+(A,F_{4020})^{0010}+(A,F_{4200})^{0100}$ |
| $G_{1511}$ | $(A,F_{0402})^{0001}+(A,F_{0420})^{0010}+(A,F_{2400})^{1000}$ |
| $G_{1151}$ | $(A,F_{0042})^{0001}+(A,F_{0240})^{0100}+(A,F_{2040})^{1000}$ |
| $G_{1115}$ | $(A,F_{0204})^{0100}+(A,F_{0024})^{0010}+(A,F_{2004})^{1000}$ |

| Symbol | Transvectant |
|---|---|
| $H_{4200}$ | $(A, G_{5111})^{1011}$ |
| $H_{4020}$ | $(A, G_{5111})^{1101}$ |
| $H_{4002}$ | $(A, G_{5111})^{1110}$ |
| $H_{0420}$ | $(A, G_{1511})^{1101}$ |
| $H_{0402}$ | $(A, G_{1511})^{1110}$ |
| $H_{0042}$ | $(A, G_{1151})^{1110}$ |
| $H_{2400}$ | $(A, G^1_{1511})^{0111}$ |
| $H_{2040}$ | $(A, G_{1151})^{0111}$ |
| $H_{2004}$ | $(A, G^1_{1115})^{0111}$ |
| $H_{0240}$ | $(A, G_{1151})^{1011}$ |
| $H_{0204}$ | $(A, G_{1115})^{1011}$ |
| $H_{0024}$ | $(A, G^1_{1115})^{1101}$ |
| $H^1_{2220}$ | $(A, G^1_{1311})^{0101} + (A, G^1_{3111})^{1001} + (A, G^1_{1131})^{0011}$ |
| $H^2_{2220}$ | $(A, G^2_{1311})^{0101} + (A, G^2_{3111})^{1001} + (A, G^2_{1131})^{0011}$ |
| $H^1_{2202}$ | $(A, G^1_{1311})^{0110} + (A, G^1_{3111})^{1010} + (A, G^1_{1113})^{0011}$ |
| $H^1_{2022}$ | $(A, G^1_{3111})^{1100} + (A, G^1_{1131})^{0110} + (A, G^1_{1113})^{0101}$ |
| $H^1_{0222}$ | $(A, G^1_{1311})^{1100} + (A, G^1_{1131})^{1010} + (A, G^1_{1113})^{1001}$ |

| Symbol | Transvectant |
|---|---|
| $I^1_{5111}$ | $(A, H_{4020})^{0010} + (A, H_{4200})^{0100} + (A, H_{4002})^{0001}$ |
| $I^1_{1511}$ | $(A, H_{0420})^{0010} + (A, H_{2400})^{1000} + (A, H_{4002})^{0001}$ |
| $I^1_{1151}$ | $(A, H_{0240})^{0100} + (A, H_{2040})^{1000} + (A, H_{0042})^{0001}$ |
| $I^1_{1115}$ | $(A, H_{0204})^{0100} + (A, H_{2004})^{1000} + (A, H_{0024})^{0010}$ |

| Symbol | Transvectant |
|---|---|
| $J_{4200}$ | $(A, I^1_{5111})^{1011}$ |
| $J_{4020}$ | $(A, I^1_{5111})^{1101}$ |
| $J_{4002}$ | $(A, I^1_{5111})^{1110}$ |
| $J_{0420}$ | $(A, I^1_{1511})^{1101}$ |
| $J_{0402}$ | $(A, I^1_{1511})^{1110}$ |
| $J_{0042}$ | $(A, I^1_{1151})^{1110}$ |
| $J_{2400}$ | $(A, I^1_{1511})^{0111}$ |
| $J_{2040}$ | $(A, I^1_{1151})^{0111}$ |
| $J_{2004}$ | $(A, I^1_{1115})^{0111}$ |
| $J_{0240}$ | $(A, I^1_{1151})^{1011}$ |
| $J_{0204}$ | $(A, I^1_{1115})^{1011}$ |
| $J_{0024}$ | $(A, I^1_{1115})^{1101}$ |

| Symbol | Transvectant |
|---|---|
| $K_{3311}$ | $= (A, J_{4200})^{1000} - (A, J_{2400})^{0100}$ |
| $K_{3131}$ | $= (A, J_{4020})^{1000} - (A, J_{2040})^{0010}$ |
| $K_{3113}$ | $= (A, J_{4002})^{1000} - (A, J_{2004})^{0001}$ |
| $K_{1331}$ | $= (A, J_{0420})^{0100} - (A, J_{0240})^{0010}$ |
| $K_{1313}$ | $= (A, J_{0402})^{0100} - (A, J_{0204})^{0001}$ |
| $K_{1133}$ | $= (A, J_{0042})^{0010} - (A, J_{0024})^{0001}$ |
| $K_{5111}$ | $= (A, J_{4200})^{0100} - (A, J_{4020})^{0010} + (A, J_{4002})^{0001}$ |
| $K_{1511}$ | $= (A, J_{2400})^{1000} - (A, J_{0420})^{0010} + (A, J_{0402})^{0001}$ |
| $K_{1151}$ | $= (A, J_{2040})^{1000} - (A, J_{0240})^{0100} + (A, J_{0042})^{0001}$ |
| $K_{1115}$ | $= (A, J_{2004})^{1000} - (A, J_{0204})^{0110} + (A, J_{0024})^{0010}$ |

| Symbol | Transvectant |
|---|---|
| $L_{6000}$ | $= (A, K_{5111})^{0111}$ |
| $L_{0600}$ | $= (A, K_{1511})^{1011}$ |
| $L_{0060}$ | $= (A, K_{1151})^{1101}$ |
| $L_{0006}$ | $= (A, K_{1115})^{1110}$ |

We use the following polynomials in order to determine the entanglement level of a sys-

tem:

$$\mathcal{L} = L_{6000} + L_{0600} + L_{0060} + L_{0006}$$

$$\mathcal{K}_3 = K_{3311} + K_{3131} + K_{3113} + K_{1331} + K_{1313} + K_{1133},$$

$$\overline{\mathcal{G}} = G^1_{3111}G^1_{1311}G^1_{1131}G^1_{1113},\ \mathcal{G} = G^2_{3111} + G^2_{1311} + G^2_{1131} + G^2_{1113},$$

$$\mathcal{H} = H^1_{2220} + H^1_{2202} + H^1_{2022} + H^1_{0222},$$

$$\mathcal{D} = D_{4000} + D_{0400} + D_{0040} + D_{0004},$$

and $\mathcal{C} = (A, B_{2200})^{0110} + (A, B_{2002})^{1001}$.