



# Quantum circuits of CNOT gates

Marc Bataille

## ► To cite this version:

| Marc Bataille. Quantum circuits of CNOT gates. 2020. hal-02948598v1

**HAL Id: hal-02948598**

**<https://normandie-univ.hal.science/hal-02948598v1>**

Preprint submitted on 24 Sep 2020 (v1), last revised 29 Sep 2020 (v2)

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

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

# Quantum circuits of **CNOT** gates

Marc Bataille  
marc.bataille1@univ-rouen.fr

LITIS laboratory, Université Rouen-Normandie \*

## **Abstract**

We study in details the algebraic structure underlying quantum circuits generated by **CNOT** gates. Our results allow us to propose polynomial heuristics to reduce the number of gates used in a given **CNOT** gates circuit and we also give algorithms to optimize this type of circuits in some particular cases. Finally we show how to create some usefull entangled states using a **CNOT** gates circuit acting on a fully factorized state.

---

\*685 Avenue de l'Université, 76800 Saint-Étienne-du-Rouvray. France.

# 1 Introduction

The controlled Pauli-X gate, also called the **CNOT** gate, is a very common and useful gate in quantum circuits. This gate involves two qubits  $i$  and  $j$  in a  $n$ -qubit system. One of the two qubits (say qubit  $i$ ) is the target qubit whereas the other qubit plays the role of control. When the control qubit  $j$  is in the state  $|1\rangle$  then a Pauli-X gate (*i.e.* a NOT gate) is applied to the target qubit  $i$  which gets flipped. When qubit  $j$  is in the state  $|0\rangle$  nothing happens to qubit  $i$ .

Actually, CNOT gates are of crucial importance in the fields of quantum computation and quantum information. Indeed, it appears that single qubit unitary gates together with CNOT gates constitute an universal set for quantum computation : any arbitrary unitary operation on a  $n$ -qubit system can be implemented using only CNOT gates and single qubit unitary gates (see [29, Section 4.5.2] for a complete proof of this important result). As a consequence, many multiple-qubit gates are implemented in current experimental quantum machines using CNOT gates plus other single-qubit gates. In Figure 3 we give a few classical examples of such an implementation : a SWAP gate can be simulated using 3 CNOT gates, a controlled Pauli-Z gate can be implemented by means of 2 Hadamard single-qubit gates and one CNOT gate. These implementations are used for instance in the IBM superconducting transmon device ([www.ibm.com/quantum-computing/](http://www.ibm.com/quantum-computing/)).

From this universality result it is possible to show that any unitary operation can be approximated to arbitrary accuracy using CNOT gates together with Hadamard, Phase, and  $\pi/8$  gates (see Figure 2 for a definition of these gates and [29, Section 4.5.3] for a proof of this result). This discrete set of gates is often called the standard set of universal gates. Using a discrete set of gates brings a great advantage in terms of reliability because it is possible to apply these gates in an error-resistant way through the use of quantum error-correcting codes (again refer to [29, Chapter 10] for further information). Currently, important error rates in CNOT gates implemented on experimental quantum computers are one of the main causes of their unreliability (see [24, 35] and Table 1). So the ability to correct errors on quantum circuits is a key point for successfully building a functional and reliable quantum computer. A complementary approach to the Quantum Error-Correction is to improve reliability by minimizing the number of gates and particularly the number of two-qubit gates used in a given circuit. Our work takes place in this context : we show that a precise understanding of the algebraic structures underlying circuits of CNOT gates makes it possible to reduce and, in some special cases, to minimize the number of gates in these circuits.

In this paper we also study the emergence of entanglement in CNOT gates circuits and we show that these circuits are a convenient tool for creating many types of entangled states. These particular states of a quantum system were first mentioned by Einstein, Podolsky and Rosen in their famous EPR article of 1935 [9] and in Quantum Information Theory (QIT) they can be considered as a fundamental physical resource (see e.g. [22]). Entangled states turn out to be essential in many areas of QIT such as quantum error correcting codes [13], quantum key distribution [10] or quantum secret sharing [6]. Spectacular applications such as super-dense coding

[3] or quantum teleportation [32, 11, 30] are based on the use of classical entangled states. This significant role played by entanglement represents for us a good reason to understand how **CNOT** gates circuits can be used to create entangled states.

The paper is structured as follows. Section 2 is mainly a background section where we recall some classical notions in order to guide non-specialist readers. In Section 3 we investigate the algebraic structure of the group generated by **CNOT** gates. Section 4 will be dedicated to the optimization problem of **CNOT** gates circuits in the general case while in Section 5 we deal with optimization in particular subgroups of the group generated by **CNOT** gates. Finally in Section 6 we study how to use **CNOT** gates circuits to create certain usefull entangled states.

<b>CNOT</b> <sub>ij</sub>	0	1	2	3	4
0		$1.035 \times 10^{-2}$			
1	$1.035 \times 10^{-2}$		$9.658 \times 10^{-3}$		
2		$9.658 \times 10^{-3}$		$9.054 \times 10^{-3}$	
3			$9.054 \times 10^{-3}$		$8.838 \times 10^{-3}$
4				$8.838 \times 10^{-3}$	
<b>H</b> <sub>i</sub>	$2.656 \times 10^{-4}$	$3.675 \times 10^{-4}$	$2.581 \times 10^{-4}$	$3.572 \times 10^{-4}$	$2.831 \times 10^{-4}$




**Table 1:** Error rates for **CNOT** gates acting on qubits i and j and for Hadamard gates acting on qubit i, where  $i, j \in \{0, 1, 2, 3, 4\}$ . The data comes from ibmq\_rome 5-qubit quantum computer after a calibration on May 12, 2020 and is publicly available at [www.ibm.com/quantum-computing/](http://www.ibm.com/quantum-computing/).

## 2 Quantum circuits, CNOT and SWAP gates

We recall here some definitions and basic facts about quantum circuits and **CNOT** gates. We also introduce some notations used in this paper and we add some developments about **SWAP** gates circuits. For a comprehensive introduction to quantum circuits the reader may refer to [29, Chapter 4] or, for a shorter but self-contained introduction), to our last article [2].

In QIT, a qubit is a quantum state that represents the basic information storage unit. This state is described by a ket vector in the Dirac notation  $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$  where  $a_0$  and  $a_1$  are complex numbers such that  $|a_0|^2 + |a_1|^2 = 1$ . The value of  $|a_i|^2$  represents the probability that measurement produces the value  $i$ . The states  $|0\rangle$  and  $|1\rangle$  form a basis of the Hilbert space  $\mathcal{H} \simeq \mathbb{C}^2$  where a one qubit quantum system evolves.

Operations on qubits must preserve the norm and are therefore described by unitary operators. In quantum computation, these operations are represented by quantum gates and a quantum circuit is a conventional representation of the sequence of quantum gates applied to the qubit register over time. In Figure 1 we recall the definition of the Pauli gates : notice that the states  $|0\rangle$  and  $|1\rangle$  are eigenvectors of the Pauli-Z operator respectively associated to the eigenvalues 1 and -1, *i.e.*  $Z|0\rangle = |0\rangle$  and  $Z|1\rangle = -|1\rangle$ . Hence the computational standard basis ( $|0\rangle, |1\rangle$ ) is also called the Z-basis.

Pauli-X		=	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y		=	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z		=	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

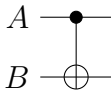



**Figure 1:** The Pauli gates

A quantum system of two qubits  $A$  and  $B$  (also called a two-qubit register) lives in a 4-dimensional Hilbert space  $\mathcal{H}_A \otimes \mathcal{H}_B$  and the computational basis of this space is :  $(|00\rangle = |0\rangle_A \otimes |0\rangle_B, |01\rangle = |0\rangle_A \otimes |1\rangle_B, |10\rangle = |1\rangle_A \otimes |0\rangle_B, |11\rangle = |1\rangle_A \otimes |1\rangle_B)$ . If  $U$  is any unitary operator acting on one qubit, a controlled- $U$  operator acts on the Hilbert space  $\mathcal{H}_A \otimes \mathcal{H}_B$  as follows. One of the two qubits (say qubit  $A$ ) is the control qubit whereas the other qubit is the target qubit. If the control qubit  $A$  is in the state  $|1\rangle$  then  $U$  is applied on the target qubit  $B$  and if qubit  $A$  is in the state  $|0\rangle$  nothing is done on qubit  $B$ . If  $U$  is the Pauli-X operator then **CNOT** is nothing more than the controlled-X operator (also denoted by  $c-X$ ) with control on qubit  $A$  and target on qubit  $B$ . So the action of **CNOT** on the two-qubit register is described by :  $\text{CNOT}|00\rangle = |00\rangle, \text{CNOT}|01\rangle = |01\rangle, \text{CNOT}|10\rangle = |11\rangle, \text{CNOT}|11\rangle = |10\rangle$  (the corresponding matrix is given in Figure 2). Notice that the action of the **CNOT** gate on the system can be sum up by the following simple formula :

$$\forall x, y \in \{0, 1\}, \text{CNOT}|xy\rangle = |x, x \oplus y\rangle \quad (1)$$

where  $\oplus$  denotes the XOR operator between two bits which is also the addition in  $\mathbb{F}_2$ . To emphasize that qubit  $A$  is the control and  $B$  is the target, **CNOT** is also denoted **CNOT<sub>AB</sub>**. So interchanging the roles played by  $A$  and  $B$  yields another operator denoted by **CNOT<sub>BA</sub>**.

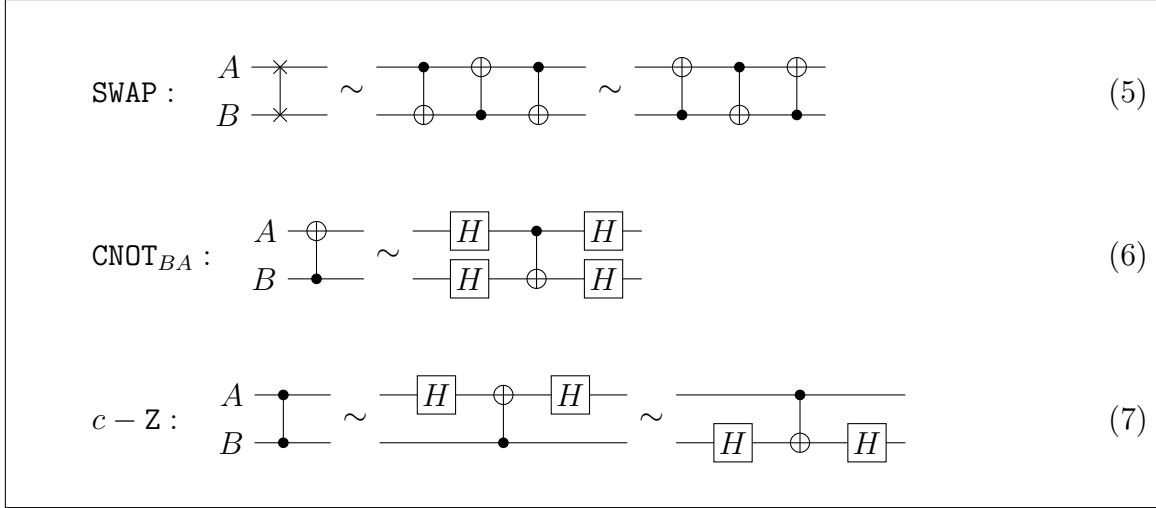
$$\forall x, y \in \{0, 1\}, \text{CNOT}_{BA}|xy\rangle = |x \oplus y, y\rangle \quad (2)$$

<b>CNOT :</b> 	<b>CNOT<sub>AB</sub></b> = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	<b>Phase :</b> 	$\mathbf{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
<b>Hadamard :</b> 	$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$\pi/8 :$ 	$\mathbf{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$

**Figure 2:** The standard set of universal gates : names, circuit symbols and matrices.

Another useful and common two-qubit quantum gate is the **SWAP** operator whose action on a basis state vector  $|xy\rangle$  is given by :  $\text{SWAP}|xy\rangle = |yx\rangle$ . The interesting point is that a **SWAP** gate can be simulated using 3 **CNOT** gates :

$$\text{SWAP} = \text{CNOT}_{AB}\text{CNOT}_{BA}\text{CNOT}_{AB} = \text{CNOT}_{BA}\text{CNOT}_{AB}\text{CNOT}_{BA} \quad (3)$$



**Figure 3:** Some classical equivalences of circuits involving CNOT gates.

This identity can be proved easily using equations (1) and (2).

The depth of a quantum circuit is the number of gates composing this circuit and we say that two circuits are *equivalent* if their action on the basis state vectors is the same *in theory*, *i.e.* the two circuits represents the same unitary operator. So Identity (3) is a proof of equivalence (5) in Figure 3. This equivalence can be used to implement a SWAP gate from 3 CNOT gates on an actual quantum machine. Two equivalent circuits generally do not have the same depth. We use the word *equivalent* instead of the word *equal* to emphasize the fact that, due to the errors rate on gates in all current implementations (see Figure 1), two equivalent circuits acting on two qubits registers in the same input state will probably not produce *in practice* the same output state. This experimental fact is an important technical problem and a good motivation to work on quantum circuits optimization.

Equivalence (6) in Figure 3 is usefull in practice because the CNOT<sub>BA</sub> gate may not be native in some implementations, so we need to simulate it : this can be done using the native gate CNOT<sub>AB</sub> plus 4 Hadamard gates. Finally another classical equivalence of quantum circuits involves the CNOT gate with the controlled Pauli-Z gate (also denoted by  $c - Z$ ) and the Hadamard gate (equivalence (7) in Figure 3). We already mentionned it in the introduction to emphasize the ubiquity of the CNOT gates in quantum circuits as well as the importance of the universality theorem. Using the definitions of the Pauli-Z gate (Figure 1) and of a controlled-U gate, it is easy to check that the action of the  $c - Z$  gate on a basis state vector is defined by

$$\forall x, y \in \{0, 1\}, c - Z |xy\rangle = (-1)^{xy} |xy\rangle \quad (4)$$

and that it is invariant by switching the control and the target qubits. Equivalence (7) can be proved using the definition of the Hadamard gate (Figure 1) and Relation (4).

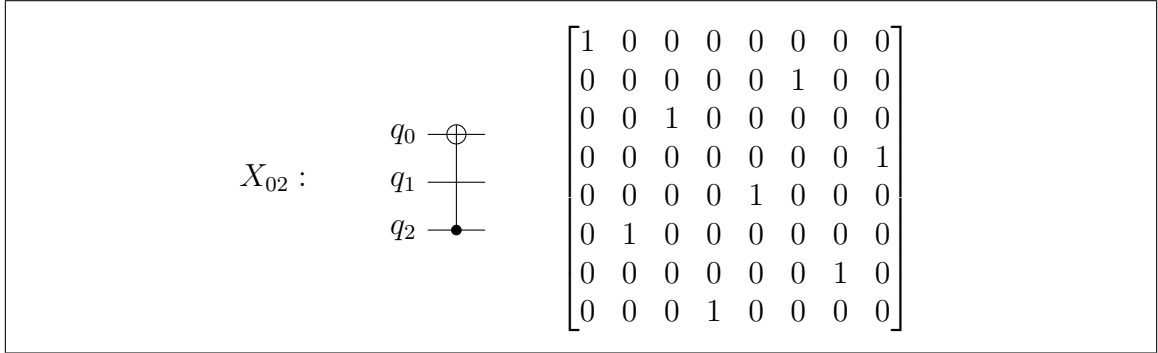
On a system of  $n$  qubits, we label each qubit from 0 to  $n - 1$  thus following the usual convention. For coherence we also number the lines and columns of a matrix of dimension  $n$  from 0 to  $n - 1$  and we consider that a permutation of the symmetric

group  $\mathfrak{S}_n$  is a bijection of  $\{0, \dots, n-1\}$ . The  $n$ -qubit system evolves over time in the Hilbert space  $\mathcal{H}_0 \otimes \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_{n-1}$  where  $\mathcal{H}_i$  is the Hilbert space of qubit  $i$ . Hence the Hilbert space of an  $n$ -qubit system is isomorphic to  $\mathbb{C}^{2^n}$ . In this space, a state vector of the standard computational basis is denoted by  $|b_0 b_1 \dots b_{n-1}\rangle$  with  $b_i \in \{0, 1\}$ . A **CNOT** gate with target on qubit  $i$  and control on qubit  $j$  will be denoted  $X_{ij}$ . The reader will pay attention to the fact that our convention is the opposite of the one generally used in the literature (and in the beginning of this section) where **CNOT** $_{ij}$  denotes a **CNOT** gate with control on qubit  $i$  and target on qubit  $j$ . The reason for this convention is explained in the proof of Theorem 4, Section 3. So, if  $i < j$ , the action of  $X_{ij}$  and  $X_{ji}$  on a basis state vector is given by :

$$X_{ij} |b_0 \dots b_i \dots b_j \dots b_{n-1}\rangle = |b_0 \dots b_i \oplus b_j \dots b_j \dots b_{n-1}\rangle, \quad (8)$$

$$X_{ji} |b_0 \dots b_i \dots b_j \dots b_{n-1}\rangle = |b_0 \dots b_i \dots b_j \oplus b_i \dots b_{n-1}\rangle. \quad (9)$$

Notice that the  $X_{i,j}$  gates are (represented by) matrices of size  $2^n \times 2^n$  in the orthogonal group  $\mathcal{O}_{2^n}(\mathbb{R})$  and that they are permutation matrices.



**Figure 4:** The gate  $X_{02}$  in a 3-qubit circuit and its matrix in the standard basis.

To represent a permutation of  $\mathfrak{S}_n$ , we use the 2-line notation as well as the cycle notation and the  $n \times n$  permutation matrix whose entry  $(i, j)$  is 1 if  $i = \sigma(j)$  and 0 otherwise. As an example, if  $\sigma \in \mathfrak{S}_6$  is the permutation defined by  $\sigma(0) = 4, \sigma(1) = 5, \sigma(2) = 0, \sigma(3) = 3, \sigma(4) = 2, \sigma(5) = 1$  then the 2-line notation is  $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 0 & 3 & 2 & 1 \end{pmatrix}$ , a cycle notation can be  $\sigma = (204)(15) = (51)(420)$  or  $\sigma = (204)(15)(3)$  if we want to write the one-cycle and the permutation matrix is

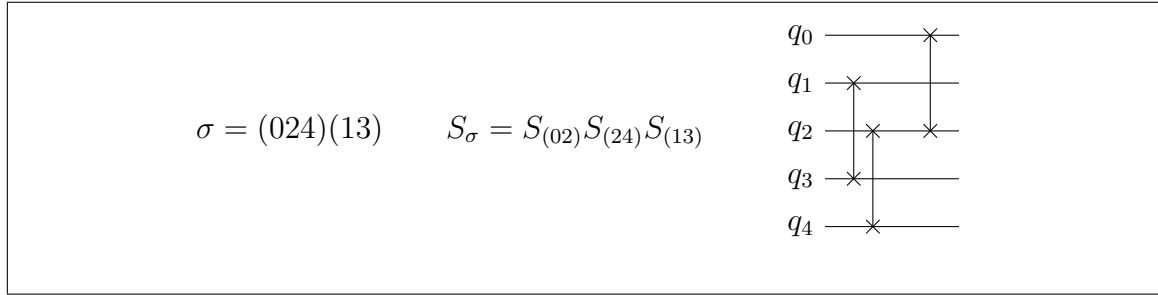
$$M_\sigma = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad \text{The } \textit{cycle type} \text{ of a permutation } \sigma \in \mathfrak{S}_n \text{ is the tuple}$$

$\lambda = (n_1, n_2, \dots, n_p)$  of positive integers such that  $n_1 \geq n_2 \geq \dots \geq n_p$ ,  $n = \sum_{i=1}^p n_i$  and  $\sigma$  is the commutative product of cycles of length  $n_i$  (including the cycles of length 1). This kind of tuple is called a decreasing *partition* of  $n$ . For instance  $\sigma = (204)(15)(3) = (204)(15)$  has cycle type  $\lambda = (3, 2, 1)$ . Notice that the cycle type of the identity is  $\lambda = (1, \dots, 1)$ . Two permutations have the same cycle type

iff they are in the same conjugacy class. For instance  $\sigma' = (350)(24)$  has the same cycle type as  $\sigma$  and  $\sigma' = \gamma\sigma\gamma^{-1}$  where  $\gamma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 0 & 4 \end{pmatrix}$ .

A **SWAP** gate between qubit  $i$  and qubit  $j$  is denoted by  $S_{(ij)}$  where  $(ij)$  is the cyclic notation for the transposition that exchange  $i$  and  $j$ . Since the symmetric group  $\mathfrak{S}_n$  is generated by the transpositions, it is straightforward to prove that the group generated by the  $S_{(ij)}$  is isomorphic to the symmetric group : each **SWAP** gate  $S_{(ij)}$  in a  $n$ -qubit circuit corresponds to the transposition  $(ij)$  in  $\mathfrak{S}_n$ . Notice that the cyclic notation of a transposition (*i.e.*  $(ij) = (ji)$ ) implies  $S_{(ij)} = S_{(ji)}$  which is coherent with the symmetry of a **SWAP** gate. More generally any circuit of **SWAP** gates maps to a permutation  $\sigma$  (examples in Figure 5 and Figure 13). If we denote by  $S_\sigma$  the unitary operator corresponding to that circuit one has :

$$S_\sigma |b_0 b_1 \cdots b_{n-1}\rangle = |b_{\sigma^{-1}(0)} b_{\sigma^{-1}(1)} \cdots b_{\sigma^{-1}(n-1)}\rangle \quad (10)$$

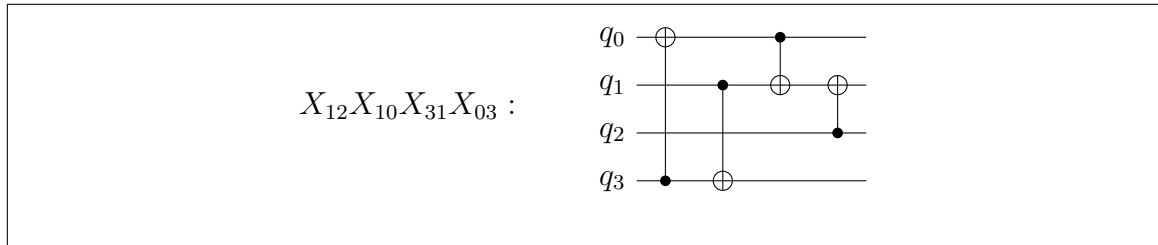


**Figure 5:** A 5-qubit quantum circuit of **SWAP** gates and the corresponding permutation

### 3 The group generated by the CNOT gates

We denote by  $c\mathcal{X}_n$  ( $n \geq 2$ ) the group generated by the  $n(n-1)$  gates (*i.e.* matrices)  $X_{ij}$ .

$$c\mathcal{X}_n := \langle X_{ij} \mid 0 \leq i, j < n, i \neq j \rangle \quad (11)$$



**Figure 6:** A circuit of  $c\mathcal{X}_4$  and the corresponding operator.



**Proposition 1.** *The following identities are satisfied by the generators of  $\text{c}\mathcal{X}_n$ .*

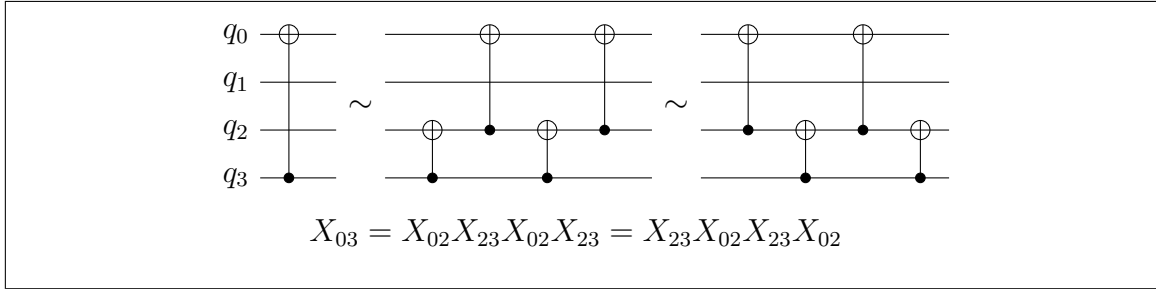
$$\text{Involution} : X_{ij}^2 = I \quad (12)$$

$$\text{Braid relation} : X_{ij}X_{ji}X_{ij} = X_{ji}X_{ij}X_{ji} = S_{(ij)} \quad (13)$$

$$\text{Commutation} : (X_{ij}X_{kl})^2 = I \quad \text{where } i \neq \ell, j \neq k \quad (14)$$

$$\text{Non-commutation} : (X_{ij}X_{jk})^2 = (X_{jk}X_{ij})^2 = X_{ik} \quad (15)$$

*Proof.* One checks each identity  $A = B$  by showing that the actions of gates  $A$  and  $B$  on a basis state vector  $|b_0 \cdots b_{n-1}\rangle$  are the same. Using identities 8 and 9, the results follow from direct computation let to the readers.  $\square$



**Figure 7:** Example of Identity (15) in a  $\text{c}\mathcal{X}_4$  circuit.

Using the identities from Proposition 1, one gets easily the conjugacy relations in  $\text{c}\mathcal{X}_n$  :

$$X_{ij}X_{jk}X_{ij} = X_{jk}X_{ik} \quad \text{and} \quad X_{ij}X_{ki}X_{ij} = X_{ki}X_{kj}. \quad (16)$$

Let us denote by  $\mathcal{S}_n$  the group generated by the  $S_{ij}$ ,

$$\mathcal{S}_n := \langle S_{(ij)} \mid 0 \leq i, j < n \rangle \quad (17)$$

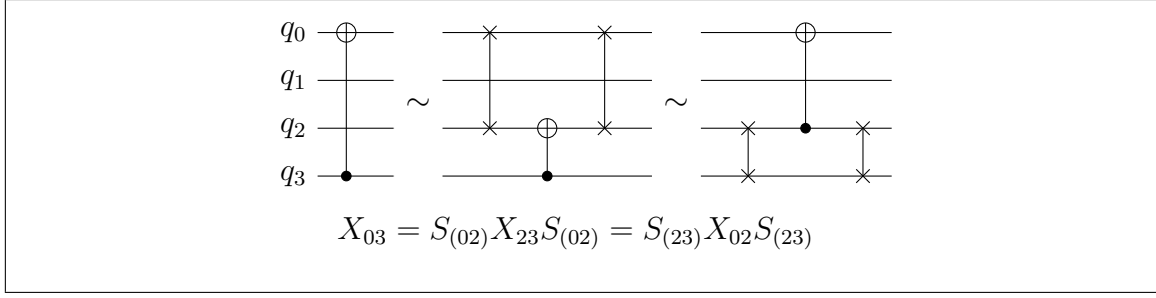
As explained at the end of Section 2,  $\mathcal{S}_n$  is isomorphic to the symmetric group  $\mathfrak{S}_n$  and Identity (13) implies that  $\mathcal{S}_n$  is a subgroup of  $\text{c}\mathcal{X}_n$ . The action of  $\mathcal{S}_n$  on  $\text{c}\mathcal{X}_n$  by conjugation is given by the following proposition :

**Proposition 2.** *For any permutation  $\sigma$  in  $\mathfrak{S}_n$  and any  $i \neq j$ , one has :*

$$S_\sigma X_{ij} S_{\sigma^{-1}} = X_{\sigma(i)\sigma(j)}. \quad (18)$$

*Proof.* Since the transpositions generate the symmetric group, it suffices to prove the result when  $\sigma$  is a transposition, i.e.  $S_\sigma = X_{kl}X_{\ell k}X_{kl}$  for some  $\ell \neq k$ . Hence, the result comes straightforwardly from equalities (12), (13), (14) and (16).  $\square$

We denote by  $\text{SL}_n(K)$  the special linear group on a field  $K$  and by  $T_{ij}(n)$  the matrix  $I_n + nE_{ij}$  where  $n \in K \setminus \{0\}$ ,  $i \neq j$  and  $E_{ij}$  is the matrix with 0 on all entries but the entry  $(i, j)$  which is equal to 1. Let  $(e_k)_{0 \leq k < n}$  be the canonical basis of the vector space  $K^n$  and  $(e_k^*)_{0 \leq k < n}$  its dual basis. Then the matrix  $T_{ij}(n)$  represents in the canonical basis the automorphism  $t_{ij}(n) : u \rightarrow u + ne_j^*(u)e_i$  of  $K^n$  which is



**Figure 8:** Example of Identity (18) in a  $c\mathcal{X}_4$  circuit.

a *transvection* fixing the hyperplane  $\langle e_k \mid k \neq j \rangle$  and directed by the line  $\langle e_i \rangle$ . So  $T_{ij}(n)$  is a *transvection matrix* and this is a well known fact in linear algebra that the transvection matrices generate  $\text{SL}_n(K)$ . A simple way to find a decomposition in transvection matrices of any matrix  $M$  in  $\text{SL}_n(K)$  is to use the Gauss-Jordan algorithm with  $M$  as input. This algorithm is generally used to compute an inverse of a matrix but it also yields a decomposition of  $M$  as a product of transvections (see Figure 11 in Section 4 for an example).

If  $K = \mathbb{F}_2$  then  $n = 1$  and the set  $\{T_{ij}(n) \mid n \in K\}$  is reduced to the  $n(n-1)$  transvection matrices  $T_{ij} := I_n + E_{ij}$ . Moreover, since any invertible matrix of  $\text{GL}_n(\mathbb{F}_2)$  has determinant 1, one has :

$$\text{GL}_n(\mathbb{F}_2) = \langle T_{ij} \mid 0 \leq i, j < n, i \neq j \rangle. \quad (19)$$

We recall that the Gauss-Jordan algorithm is based on the following observation :

**Proposition 3.** *Multiplying to the left (resp. the right) any  $\mathbb{F}_2$ -matrix  $M$  by a transvection matrix  $T_{ij}$  is equivalent to add the  $j$ th line (resp.  $i$ th column) to the  $i$ th line (resp.  $j$  column) in  $M$ .*

In particular, one has

$$T_{ij} \begin{bmatrix} b_0 \\ \vdots \\ b_i \\ \vdots \\ b_j \\ \vdots \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} b_0 \\ \vdots \\ b_i \oplus b_j \\ \vdots \\ b_j \\ \vdots \\ b_{n-1} \end{bmatrix}. \quad (20)$$

The notation  $|b_0 b_1 \cdots b_{n-1}\rangle$  used in QIT is a shorthand for the tensor product  $|b_0\rangle \otimes |b_1\rangle \otimes \cdots \otimes |b_{n-1}\rangle$  and it is convenient to identify the binary label  $b_0 b_1 \cdots b_{n-1}$  with the column vector  $u = [b_0, b_1, \cdots, b_{n-1}]^T$  of  $\mathbb{F}_2^n$  since the  $\oplus$  (XOR) operation between two bits corresponds to the addition in  $\mathbb{F}_2$ . So the computational basis of the Hilbert space  $\mathcal{H}_0 \otimes \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{n-1}$  is from now on denoted by  $(|u\rangle)_{u \in \mathbb{F}_2^n}$  and using Relation (20) we can rewrite Relation (8) in a much cleaner way as

$$X_{ij} |u\rangle = |T_{ij}u\rangle. \quad (21)$$

The above considerations lead quiet naturally to the following theorem :

**Theorem 4.** *The group  $c\mathcal{X}_n$  generated by the CNOT gates acting on  $n$  qubits is isomorphic to  $\text{GL}_n(\mathbb{F}_2)$ . The morphism  $\Phi$  sending each  $X_{ij}$  to  $T_{ij}$  is an explicit isomorphism.*

*Proof.* The surjectivity of  $\Phi$  is due to the fact that  $\text{GL}_n(\mathbb{F}_2)$  is generated by the transvections  $T_{ij}$ . Furthermore, due to Relation (21), a preimage  $N$  by  $\Phi$  of a matrix  $M$  in  $\text{GL}_n(\mathbb{F}_2)$  must satisfy the relation  $N|u\rangle = |Mu\rangle$  for any basis vector  $|u\rangle$  and there is only one matrix  $N$  satisfying this relation. So  $\Phi$  is also injective and the result is proved.  $\square$

Notice that the image by  $\Phi$  of a SWAP matrix  $S_{(ij)}$  is a transposition matrix  $P_{(ij)} := T_{ij}T_{ji}T_{ij} = T_{ji}T_{ij}T_{ji}$  in  $\text{GL}_n(\mathbb{F}_2)$  and more generally  $\Phi(S_\sigma)$  is the permutation matrix  $P_\sigma$  for any permutation  $\sigma$  in  $\mathfrak{S}_n$ . From now on we will denote by  $M^\sigma = P_\sigma M P_\sigma^{-1}$  the conjugate of a matrix  $M$  in  $\text{GL}_n(\mathbb{F}_2)$  by a permutation matrix  $P_\sigma$ . Using the isomorphism  $\Phi$ , Relation (18) leads to

$$T_{ij}^\sigma = P_\sigma T_{ij} P_\sigma^{-1} = T_{\sigma(i)\sigma(j)}. \quad (22)$$

The order  $\text{GL}_n(\mathbb{F}_2)$  is classically obtained by computing the number of different basis of  $\mathbb{F}_2^n$  and Theorem 4 implies

**Corollary 5.**

$$|c\mathcal{X}_n| = 2^{\frac{n(n-1)}{2}} \prod_{i=1}^n (2^i - 1). \quad (23)$$

In his "Lectures on Chevalley Group" [31, Chapter 6], Steinberg gives a presentation of the special linear group on a finite field  $K$  in dimension  $n \geq 3$ . The notation  $(a, b)$  stands here for the commutator of two elements  $a$  and  $b$  of a group (*i.e.*  $a^{-1}b^{-1}ab$ ) which is usually denoted by  $[a, b]$ .

**Theorem 6.** (*Steinberg*)

*If  $n \geq 3$  and  $K$  is a finite field, the symbols  $x_{ij}(t)$ , ( $1 \leq i, j \leq n$ ,  $i \neq j$ ,  $t \in K$ ) subject to the relations :*

$$(A) \quad x_{ij}(t)x_{ij}(u) = x_{ij}(t+u)$$

$$(B) \quad (x_{ij}(t), x_{jk}(u)) = x_{ik}(tu) \text{ if } i, j, k \text{ are distinct, } (x_{ij}(t), x_{k\ell}(u)) = 1 \\ \text{if } j \neq k, i \neq \ell$$

*define the group  $\text{SL}_n(K)$ .*

It is straightforward to adapt this presentation to the case  $K = \mathbb{F}_2$  and we get so a presentation for the group  $c\mathcal{X}_n$  for any  $n \geq 3$ .

**Corollary 7.** *If  $n \geq 3$ , a presentation of the group  $cX_n$  is  $\langle \mathcal{S} \mid \mathcal{R} \rangle$  where  $\mathcal{S}$  is the set of the  $n(n-1)$  symbols  $x_{ij}$  ( $0 \leq i, j \leq n-1$ ,  $i \neq j$ ) and  $\mathcal{R}$  is the set of the relations :*

$$x_{ij}^2 = 1, \quad (24)$$

$$(x_{ij}x_{jk})^2 = x_{ik}, \quad (25)$$

$$(x_{ij}x_{k\ell})^2 = 1 \quad \text{if } i \neq \ell, j \neq k. \quad (26)$$

We remark that all the identities given by Proposition 1 appear in this presentation but Identity (13). Of course the braid relation (13) can be deduced from the presentation relations but the calculation is tricky. First of all, using the above relations we obtain the conjugacy relation  $x_{ij}x_{jk}x_{ij} = x_{jk}x_{ik} = x_{ik}x_{jk}$  (as we did to obtain Relation (16)). Then we use many times this conjugacy relation to obtain the relation  $x_{ij}x_{ji}x_{ij}x_{ji}x_{ij} = x_{ji}$  and finally we get the braid relation  $x_{ij}x_{ji}x_{ij} = x_{ji}x_{ij}x_{ji}$  using Relation (24). The calculation is detailed in Figure 9.

$  \begin{aligned}  x_{ji}x_{ij}x_{ji} &= x_{ji}(x_{ik}x_{kj})^2x_{ji} \\  &= (x_{ji}x_{ik}x_{kj}x_{ji})^2 \\  &= (x_{ji}x_{ik}x_{ji}x_{ji}x_{kj}x_{ji})^2 \\  &= (x_{ik}x_{jk}x_{ki}x_{kj})^2  \end{aligned}  $	$  \begin{aligned}  x_{ij}x_{ji}x_{ij}x_{ji}x_{ij} &= x_{ij}(x_{ik}x_{jk}x_{ki}x_{kj})^2x_{ij} \\  &= (x_{ij}x_{ik}x_{jk}x_{ki}x_{kj}x_{ij})^2 \\  &= (x_{ik}x_{ij}x_{jk}x_{ki}x_{ij}x_{kj})^2 \\  &= (x_{ik}x_{ik}x_{jk}x_{ki}x_{kj}x_{kj})^2 \\  &= (x_{jk}x_{ki})^2 \\  &= x_{ji}  \end{aligned}  $
--	--

**Figure 9:** Getting the braid relation  $x_{ij}x_{ji}x_{ij} = x_{ji}x_{ij}x_{ji}$  from Corollary 7.

A classical result in Group Theory is that the projective special linear group  $\text{PSL}_n(K)$  is simple when  $n \geq 3$  (see *e.g.* [34, Chapter 3] for a proof). This group is defined as  $\text{SL}_n(K)/Z$  where  $Z$  is the subgroup of all scalar matrices with determinant 1, which appears to be the center of  $\text{SL}_n(K)$ . If  $K = \mathbb{F}_2$  the identity matrix is the only scalar matrix that has determinant 1 and the center of  $\text{SL}_n(\mathbb{F}_2)$  is reduced to the trivial group. Hence  $\text{SL}_n(\mathbb{F}_2) = \text{PSL}_n(\mathbb{F}_2)$  and the group  $c\mathcal{X}_n$  is simple when  $n \geq 3$ . If  $n = 2$ ,  $c\mathcal{X}_2$  has order 6 and is isomorphic to  $\mathfrak{S}_3$ , one possible isomorphism being  $X_{01} \simeq (01)$ ,  $X_{10} \simeq (12)$ ,  $X_{01}X_{10} \simeq (012)$ ,  $X_{10}X_{01} \simeq (021)$  and  $X_{01}X_{10}X_{01} \simeq (02)$ . So  $c\mathcal{X}_2$  is not a simple group since the alternating group is always a normal subgroup of  $\mathfrak{S}_n$ .

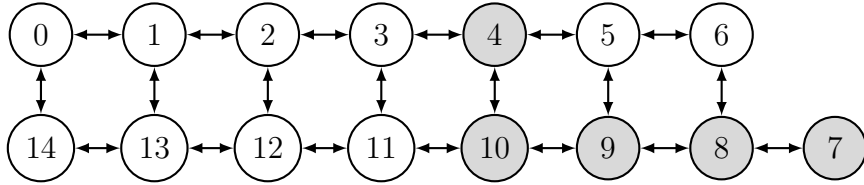
Identity (15) involves 3 distinct integers  $i, j, k$  and can be generalized by induction to an arbitrary number of distinct integers in the following way :

**Proposition 8.** *Let  $i_1, i_2, \dots, i_p$  be distinct integers ( $p \geq 3$ ) of  $\{0, 1, \dots, n-1\}$ , then :*

$$X_{i_1, i_p} = (X_{i_1, i_2}X_{i_2, i_3} \dots X_{i_{p-2}, i_{p-1}}X_{i_{p-1}, i_p}X_{i_{p-2}, i_{p-1}} \dots X_{i_2, i_3})^2 \quad (27)$$

Proposition 8 provides a simple way to adapt any CNOT gate to the topological constraints of a given quantum computer. These constraints can be represented by

a directed graph whose vertices are labelled by the qubits. There is an arrow from qubit  $i$  to qubit  $j$  when these two qubits can interact to perform an  $X_{ij}$  operation on the system. In a device with the complete graph topology, the full connectivity is achieved (see *e.g.* [24, 35]) and any  $X_{ij}$  operation can be performed directly (*i.e.* without involving other two-qubit operations on other qubits than  $i$  and  $j$ ). In contrast, the constraints in the LNN (Linear Nearest Neighbour) topology are strong as direct interaction is allowed only on consecutive qubits, *i.e.* only  $X_{i,i+1}$  or  $X_{i+1,i}$  [36]. Of course there are also many intermediate graph configurations as in the IBM superconducting transmon device ([www.ibm.com/quantum-computing/](http://www.ibm.com/quantum-computing/)). To implement a  $X_{ij}$  gate when there is no arrow between  $i$  and  $j$ , the usual method is to use **SWAP** gates together with allowed **CNOT** gates as we did in Figure 8. But, if **SWAP** gates are implemented on the device using 3 **CNOT** gates (circuit equivalence (5)), this implementation can be done in a more reliable fashion by using less gates : just find a shortest path ( $i_1 = i, \dots, i_p = j$ ) between  $i$  and  $j$  in the undirected graph, then apply formula (27). Notice that it can be important to take into account the error rate associated to each arrow  $(i, j)$  in the shortest path computation since it may vary from one gate to another (see Figure 1). Case of  $(i_k, i_{k+1})$  is not an arrow, use the classical equivalence 6 in Figure 3 to invert target and control. Of course this adds two single-qubit gates to the circuit but the impact on reliability is small since on current experimental quantum devices the fidelity of single qubit gates as the Hadamard gate is much higher than any two-qubit gate fidelity (*e.g.* Figure 1 again). In the example below, we implement a **CNOT** gate considering the topology of the 15-qubit `ibmq_16_melbourne` device :



Chosen path to implement  $X_{4,7}$  :  $(4, 10, 9, 8, 7)$

$$X_{4,7} = (X_{4,10}X_{10,9}X_{9,8}X_{8,7}X_{9,8}X_{10,9})^2$$

We end this section by remarking that  $\text{GL}_p(\mathbb{F}_2)$  can be regarded as a subgroup of  $\text{GL}_n(\mathbb{F}_2)$  if  $p < n$ . Indeed, let  $\varphi$  be the injective morphism from  $\text{GL}_p(\mathbb{F}_2)$  into  $\text{GL}_n(\mathbb{F}_2)$  defined by  $\varphi(M) = \begin{bmatrix} M & 0 \\ 0 & I_{n-p} \end{bmatrix}$ , one has  $\text{GL}_p(\mathbb{F}_2) \simeq \varphi(\text{GL}_p(\mathbb{F}_2))$ , so we will consider that  $\text{GL}_p(\mathbb{F}_2) \subset \text{GL}_n(\mathbb{F}_2)$  and no distinction will be made between matrices  $M$  and  $\varphi(M)$ .

## 4 Optimization of CNOT gates circuits

A **CNOT** circuit is *optimal* if there is not another equivalent **CNOT** circuit with less gates. In the same way a decomposition of a matrix  $M \in \text{GL}_n(\mathbb{F}_2)$  in product of transvections  $T_{i,j}$  is *optimal* if  $M$  cannot be written with less transvections. If the depth of a circuit  $C'$  is less than the depth of an equivalent circuit  $C$  we say that  $C'$

is a *reduction* of  $C$  (or that  $C$  has been *reduced* to  $C'$ ) and if  $C'$  is *optimal* we say that  $C'$  is an *optimization* of  $C$  (or that  $C$  has been *optimized* to  $C'$ ).

For a better readability we denote from now on the transvection matrix  $T_{ij}$  by  $[ij]$  and the permutation matrix  $P_\sigma$  by  $\sigma$ . As a consequence,  $(ij)$  denotes the transposition which exchanges  $i$  and  $j$  as well as the transposition matrix  $P_{(ij)}$ . Notice that  $(ij) = (ji)$  but  $[ij] = [ji]^T$  ( $[ij]$  is the transpose matrix of  $[ji]$ ). With these notations the braid relation (13) becomes  $(ij) = (ji) = [ij][ji][ij] = [ji][ij][ji]$  and Identity (22) becomes  $\sigma[ij]\sigma^{-1} = [ij]^\sigma = [\sigma(i)\sigma(j)]$ . In particular,  $(ij)[ij](ij) = [ij]^{(ij)} = [ji]$ .

From Section 3, any **CNOT** circuit can be optimized using the following rewriting rules.

**Proposition 9.** *Let  $0 \leq i, j, k, l \leq n - 1$  be distinct integers :*

$$[ij]^2 = 1 \quad (28)$$

$$[ij][jk][ik] = [ik][ij][jk] = [jk][ij] ; [ij][ki][kj] = [kj][ij][ki] = [ki][ij] \quad (29)$$

$$[ij][jk][ij] = [jk][ik] = [ik][jk] ; [ij][ki][ij] = [ki][kj] = [kj][ki] \quad (30)$$

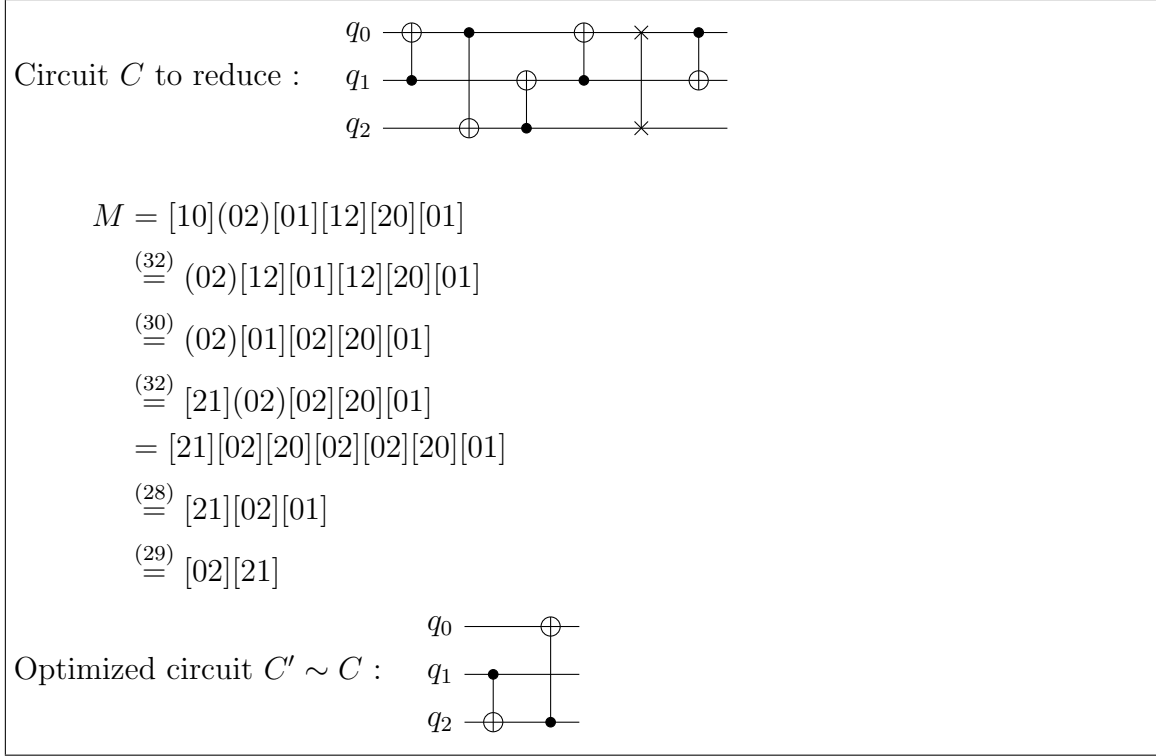
$$[ij][kl] = [kl][ij] ; [ij][ik] = [ik][ij] ; [ij][kj] = [kj][ij] \quad (31)$$

$$\sigma[ij] = [ij]^\sigma \sigma = [\sigma(i)\sigma(j)]\sigma ; [ij]\sigma = \sigma[ij]^{\sigma^{-1}} = \sigma[\sigma^{-1}(i)\sigma^{-1}(j)] \quad (32)$$

In practice one tries to find an *ad hoc* sequence of the above rules to reduce or to optimize a given circuit (see Figure 10 for an example) but the computation can be tricky even with a few qubits. So it is difficult to build a general reduction/optimization algorithm from Proposition 9.

To optimize a **CNOT** circuit of a few qubits we use a C ANSI program that builds the Cayley Graph of the group  $GL_n(\mathbb{F}_2)$  by Breadth-first search and then find in the graph the group element corresponding to that circuit. This program optimizes in a few seconds any **CNOT** circuit up to 5 qubits and the source code can be downloaded at <https://github.com/mbataille/cnot/optimization>. In the rest of this article we refer to it as "the computer optimization program". However, due to the exponential growth of the group order (for instance  $\text{Card}(c\mathcal{A}_6) = 20\,158\,709\,760$ ), the computer method fails from 6 qubits with a basic PC. In this context we remark that the Gauss Jordan algorithm mentionned in Section 3 can be used as a heuristic method to reduce a given **CNOT** gates circuit (see Figure 11 for a detailed example). It works as follows :

- Each  $X_{ij}$  gate of a given circuit  $C$  corresponds to a transvection matrix  $[ij]$ . Multiplying these transvection matrices yields a matrix  $M$  in  $GL_n(\mathbb{F}_2)$  that we call *the matrix of the circuit in dimension  $n$* .
- The Gauss-Jordan algorithm applied to the matrix  $M$  gives a decomposition of  $M$  under the form  $M = KU$  where  $U$  is an upper triangular matrix and  $K$  is a matrix that is a lower triangular matrix if and only if the element of  $\mathbb{F}_2$  that appears on the diagonal at each step of the algorithm is 1, so we can choose it as pivot. In this case the matrix  $M$  as a *LU (Lower Upper)* decomposition



**Figure 10:** Optimizing a CNOT circuit using an *ad hoc* sequence of reduction rules.

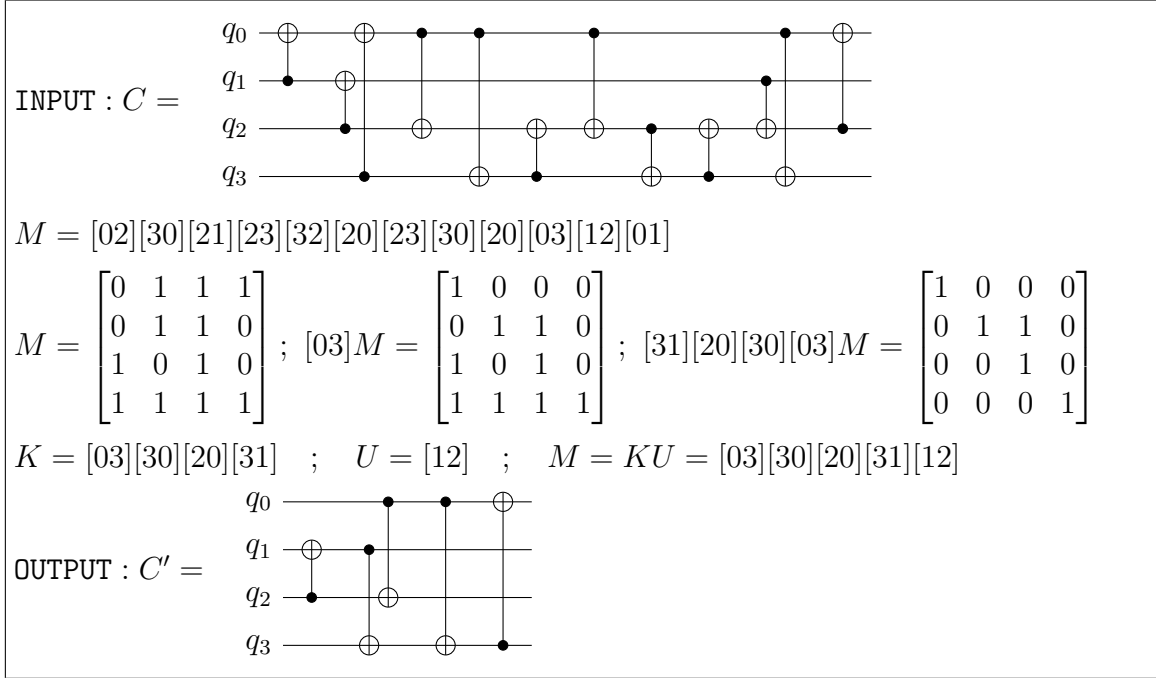
and this decomposition is unique. If at a given step the bit on the diagonal is 0 then we have to choose another pivot and the matrix  $K$  is not triangular anymore. Moreover the decomposition  $M = KU$  is not unique as the matrix  $K$  depends on the choice of the pivot at each step, so the algorithm is not deterministic in this case.

- A decomposition of  $K$  in product of transvections is directly obtained while executing the algorithm and a simple and direct decomposition of an upper triangular matrix  $U = (u_{ij})$  in  $\text{GL}_n(\mathbb{F}_2)$  is  $U = \prod_{j=n-1}^1 \prod_{i=j-1}^0 [ij]^{u_{ij}}$ . We call this decomposition the *canonical* decomposition of  $U$  and symmetrically the canonical decomposition of a lower triangular matrix is  $L = \prod_{j=0}^{n-2} \prod_{i=j+1}^{n-1} [ij]^{l_{ij}}$ .
- Replacing each transvection  $[ij]$  in the decomposition of  $M$  by the corresponding CNOT gate  $X_{ij}$ , we obtain a circuit  $C'$  equivalent to  $C$ . If the depth of  $C'$  is less than the depth of  $C$  then we have successfully reduced the circuit  $C$ . If not, the heuristic failed.

We note that the circuit  $C'$  obtained by this process is generally not optimal even for small values of  $n$ . However the Gauss-Jordan algorithm has the great advantage of providing an upper bound on the optimal number of CNOT gates in a circuit.

**Proposition 10.** *Any  $n$ -qubit circuit of CNOT gates is equivalent to a circuit composed of less than  $n^2$  gates.*

*Proof.* We apply the Gauss-Jordan elimination algorithm to get a decomposition of  $M \in \text{GL}_n(\mathbb{F}_2)$  in transvections. The first part of the algorithm consists in multiplying  $M$  to the left by a sequence of transvections in order to obtain an upper triangular matrix  $U$ . For  $k = 0, 1, \dots, n-1$ , we consider the column  $k$  and the entry of the matrix on the diagonal. If this entry is 1 we choose it as a pivot but if it is 0 we first need to put a 1 on the diagonal. This can be done by swapping row  $k$  with a row  $\ell$  whose entry  $(\ell, k)$  is 1. However, this will cost 3 transvections and it is more economical to add row  $\ell$  to row  $k$ , *i.e.* multiplying to the left by  $[k, \ell]$ . The number of left multiplications by transvections necessary to have a pivot equal to 1 on the diagonal at each step is bounded by  $n-1$  and the number of left multiplications necessary to eliminate the 1's below the pivot is bounded by  $n-1 + \dots + 1 = \frac{n(n-1)}{2}$ . Hence the number of transvections that appears in the first part of the algorithm is bounded by  $\frac{n(n+1)}{2} - 1$ . In the second part of the algorithm we just write the canonical decomposition of  $U$  which contains at most  $n-1 + n-2 + \dots + 1 = \frac{n(n-1)}{2}$  transvections. Finally we see that the number of transvections in the resulting decomposition of  $M$  is at most  $n^2 - 1$ .  $\square$



**Figure 11:** The Gauss-Jordan algorithm applied to a CNOT gates circuit.

The canonical decomposition of an upper or lower triangular matrix is generally not optimal, so we propose in what follows another algorithm to decompose a triangular matrix in transvections. Applying this algorithm to the matrix  $U$  when the decomposition of  $M$  is  $KU$  or to both matrices  $L$  and  $U$  when the decomposition of  $M$  is  $LU$  can often improve the decomposition given by the Gauss-Jordan heuristic, especially when the triangular matrix has a high density of 1's (See Figure 12 for an example). We describe below this algorithm for an upper triangular matrix (UTD algorithm) but it can be easily adapted to the case of a lower triangular matrix (LTD algorithm). We denote by  $|L_i|$  is the number of 1's in line  $i$  of a matrix.



**Algorithm 11.** *Upper Triangular Decomposition (UTD algorithm)*

INPUT : An upper triangular matrix  $U$  in  $\text{GL}_n(\mathbb{F}_2)$ .

OUTPUT : A sequence  $S = (t_0, t_1, \dots, t_{p-1})$  of transvections such that  $U = \prod_{j=0}^{p-1} t_j$ .

```

1   $S = ()$ ;  $j = 0$ ;
2  while  $U \neq I$  :
3    for  $i = 0$  to  $n - 2$  :
4      if  $|L_i| > 1$  :
5        Let  $E_i = \{k \mid i < k \leq n - 1 \text{ and } |L_i \oplus L_k| < |L_i|\}$ ;
6        if  $E_i \neq \emptyset$  :
7          Choose the smallest  $k \in E_i$  such that  $|L_i \oplus L_k|$  is minimal;
8           $U = [ik]U$ ;
9           $t_j = [ik]$  ;  $j = j + 1$ ;
10 return  $S$ ;
```

The algorithm ends because for each loop (for  $i = 0$  to  $n - 2$ ) the number of 1's in the matrix decreases of at least one. Indeed, there is always at least one couple  $(i, k)$  chosen during this loop, namely :  $i = \max\{j \mid |L_j| > 1\}$  and  $k = \max\{j \mid U_{ij} \neq 0\}$ . Furthermore, we notice that the number of transvections in the decomposition  $S$  is always less than or equal to the number of transvections in the canonical decomposition of the matrix  $U$  since each transvection in the canonical decomposition of  $U$  contributes to a decrease of exactly one in the initial number of 1's in the matrix  $U$  whereas each transvection in  $S$  contributes to a decrease of at least one in this initial number of 1's.

Again, the decomposition obtained by applying the Gauss-Jordan algorithm followed by the UTD or LTD algorithm is generally not optimal. In fact we conjecture the following result.

**Conjecture 12.** *Any  $n$ -qubit circuit of CNOT gates is equivalent to a circuit composed of at most  $3(n - 1)$  gates. The upper bound of  $3(n - 1)$  gates is reached only in the special case of SWAP gates circuits  $S_\sigma$  where  $\sigma$  is a cycle of length  $n$  in  $\mathfrak{S}_n$ .*

We checked this conjecture up to 5 qubits thanks to our computer optimization program (see the results summarized in Table 2).

## 5 Optimization in subgroups of $c\mathcal{X}_n$

In this section we describe the structure of some particular subgroups of  $c\mathcal{X}_n \simeq \text{GL}_n(\mathbb{F}_2)$  and we propose algorithms to optimize CNOT gates circuits of these subgroups. Starting from an input circuit  $C$ , we first compute the matrix  $M$  of the circuit in dimension  $n$ . In some specific cases the matrix  $M$  has a particular shape so we can propose an optimal decomposition in transvections for  $M$  and output an optimization  $C'$  of the circuit  $C$ . We describe 3 subgroups corresponding to 3 types of matrices with the objective of building step by step a kind of atlas of CNOT gates circuits with specific optimization algorithms.

optimal length	$n = 2$	$n=3$	$n = 4$	$n = 5$
$l = 0$	1	1	1	1
$l = 1$	2	6	12	20
$l = 2$	2	24	96	260
$l = 3$	<b>1</b>	51	542	2 570
$l = 4$		60	2 058	19 680
$l = 5$		24	5 316	117 860
$l = 6$		<b>2</b>	7 530	540 470
$l = 7$			4 058	1 769 710
$l = 8$			541	3 571 175
$l = 9$			<b>6</b>	3 225 310
$l = 10$				736 540
$l = 11$				15 740
$l = 12$				<b>24</b>
Order of $\text{c}\mathcal{X}_n$	6	168	20 160	9 999 360

**Table 2:** Number of elements of  $\text{c}\mathcal{X}_n$  having an optimal decomposition of length  $l$ . The numbers in bold correspond to the  $(n - 1)!$  cyclic permutations of length  $n$ .

## 5.1 Permutation matrices

The first case considered is when the matrix  $M \in \text{GL}_n(\mathbb{F}_2)$  of the circuit is a permutation matrix  $P_\sigma$ . In this case the circuit is equivalent to a **SWAP** gates circuit and we work in  $\mathcal{S}_n$ , the subgroup of  $\text{c}\mathcal{X}_n$  generated by the  $S_{(ij)}$  gates which is isomorphic to  $\mathfrak{S}_n$  (see example in Figure 13).

**Proposition 13.** *Any permutation matrix  $P_\sigma$  can be decomposed as a product of  $3(n - p)$  transvections where  $p$  is the number of cycles of the permutation  $\sigma$ .*

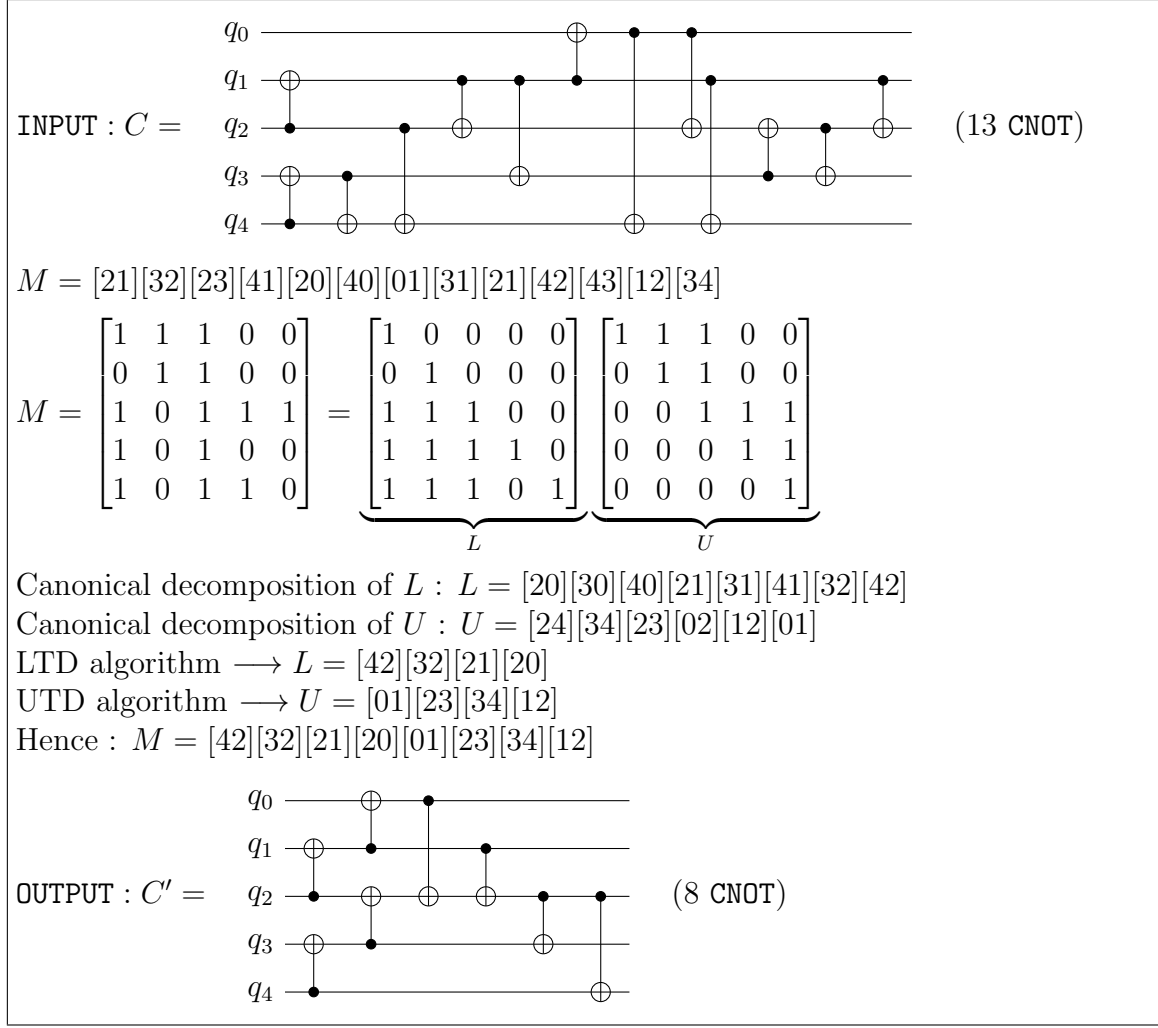
*Proof.* Let  $\lambda = (n_1, \dots, n_p)$  be the cycle type of  $\sigma$ . Any cycle of length  $n_i$  can be decomposed in the product of  $n_i - 1$  transpositions and each transposition can be decomposed in a product of 3 transvections, so the total number of transvections used in the decomposition of  $P_\sigma$  is  $3 \sum_{i=1}^p (n_i - 1) = 3(n - p)$ .  $\square$

The following conjecture has been checked up to 5 qubits using the computer optimization program.

**Conjecture 14.** *The decomposition in transvections of a permutation matrix  $P_\sigma$  given by Proposition 13 is optimal.*

## 5.2 Block diagonal matrices

In the second case, we consider that the matrix  $M$  of the circuit in dimension  $n$  is a block diagonal matrix or the conjugate of a diagonal block matrix by a permutation matrix. Let  $(n_1, \dots, n_p)$  be a tuple of  $p$  positive integers such that  $\sum_{i=1}^p n_i = n$  and



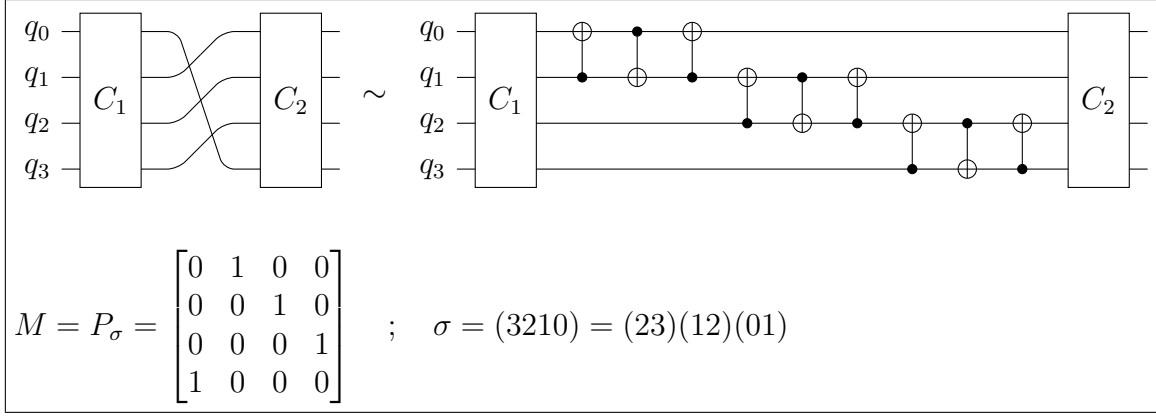
**Figure 12:** The UTD/LTD algorithms applied to a  $LU$  circuit of CNOT gates

consider the matrix  $M_S = \begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & A_p \end{bmatrix}$  where  $S = (A_1, \dots, A_p)$  is a tuple of

matrices  $A_i$  in  $\text{GL}_{n_i}(\mathbb{F}_2)$ . Here  $M_S$  is a block diagonal matrix and we shall see right after the case of the conjugate of a block diagonal matrix by a permutation matrix. Clearly  $\{M_S \mid S \in \text{GL}_{n_1}(\mathbb{F}_2) \times \dots \times \text{GL}_{n_p}(\mathbb{F}_2)\}$  is a group isomorphic to the direct group product  $\text{GL}_{n_1}(\mathbb{F}_2) \times \dots \times \text{GL}_{n_p}(\mathbb{F}_2)$  since

$$M_S = \begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & I_{n_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & I_{n_p} \end{bmatrix} \times \dots \times \begin{bmatrix} I_{n_1} & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & I_{n_{p-1}} & 0 \\ 0 & \dots & 0 & A_p \end{bmatrix} \text{ where } I_\alpha \text{ is the identity}$$

matrix in dimension  $\alpha$ . This equality can be written as  $M_S = \prod_{i=1}^p M_i$  where



**Figure 13:** A cyclic permutation of the qubits between two circuits  $C_1$  and  $C_2$

$M_i = \begin{bmatrix} I_{N_{i-1}} & 0 & 0 \\ 0 & A_i & 0 \\ 0 & 0 & I_{n-N_i} \end{bmatrix}$  and  $N_i = \sum_{k=1}^i n_k$ . We recall that the conjugation  $M^\sigma = P_\sigma M P_\sigma^{-1}$  of a square matrix  $M$  by a permutation matrix  $P_\sigma$  has the following effect on  $M$  : if we denote by  $L_i$  (resp.  $L'_i$ ) and  $C_i$  (resp.  $C'_i$ ) the lines and columns of matrix  $M$  (resp.  $M^\sigma$ ) then  $L'_i = L_{\sigma^{-1}(i)}$  and  $C'_i = C_{\sigma^{-1}(i)}$ , hence if  $M = (m_{ij})$  and  $M' = (m'_{ij})$  then  $m'_{ij} = m_{\sigma^{-1}(i)\sigma^{-1}(j)}$ . So, if we consider now a tuple of  $p$  permutations  $(\sigma_1, \dots, \sigma_p)$  verifying the conditions  $\sigma_i(n_1 + n_2 + \dots + n_{i-1}) = 0, \sigma_i(n_1 + n_2 + \dots + n_{i-1} + 1) = 1, \dots, \sigma_i(n_1 + n_2 + \dots + n_{i-1} + n_i - 1) = n_i - 1$  then  $M_S = \prod_{i=1}^p (M_i^{\sigma_i})^{\sigma_i^{-1}} = \prod_{i=1}^p (M'_i)^{\sigma_i^{-1}}$  where  $M'_i = \begin{bmatrix} A_i & 0 \\ 0 & I_{n-n_i} \end{bmatrix} \simeq A_i$ . Moreover, for Relation (22), the number of transvections in an optimal decomposition of any matrix  $M$  in  $\text{GL}_n(\mathbb{F}_2)$  is the same as the number of transvections in an optimal decomposition of  $M^\sigma$  for any permutation  $\sigma$ . As a consequence, the product of the conjugates by  $\sigma_i^{-1}$  of any optimal decomposition of the matrix  $A_i$  yields an optimal decomposition of the matrix  $M_S$  (see Figure 14 for an example).

The generalization of the previous situation to the case of a matrix  $M = M_S^\sigma$  where  $M_S$  is a block diagonal matrix and  $\sigma$  a permutation matrix is straightforward. Indeed, if we have an optimal decomposition of  $M_S$  in transvections, then we deduce an optimal decomposition for  $M_S^\sigma$  by conjugating by  $\sigma$  each transvection in the decomposition of  $M_S$ . This is due to the fact that the number of transvections in an optimal decomposition of any matrix  $M$  in  $\text{GL}_n(\mathbb{F}_2)$  is the same as the number of transvections in an optimal decomposition of  $M^\sigma$  (see Relation (22)). In fact the problem we adress here is rather the following : how can we efficiently recognize that the matrix  $M$  is of type  $M = M_S^\sigma$  ? To do that we interpret the matrix  $M$  of the circuit in dimension  $n$  as the adjacency matrix of the directed graph  $\mathcal{G}(M)$  whose set of vertices is  $V = \{0, 1, \dots, n-1\}$  and whose set of edges is  $E = \{(i, j) \mid m_{ij} = 1\}$ . We call  $\mathcal{G}(M)$  *the graph of the circuit*. The graph  $(\mathcal{G}(M))^\sigma$  defined by the set of vertices  $\sigma(V) = V$  and by the set of edges  $E_n^\sigma = \{(\sigma(i), \sigma(j)) \mid m_{ij} = 1\}$  is isomorphic to  $\mathcal{G}(M)$ . Besides,  $E_n^\sigma = \{(i, j) \mid m_{\sigma^{-1}(i)\sigma^{-1}(j)} = 1\}$  and  $M^\sigma = (m_{\sigma^{-1}(i)\sigma^{-1}(j)})$ , so  $(\mathcal{G}(M))^\sigma = \mathcal{G}(M^\sigma)$ . The graph  $\mathcal{G}(M_S)$  is a disconnected graph whose  $p$  connected components are  $V_1 = \{0, \dots, n_1 - 1\}, V_2 = \{n_1, \dots, n_1 + n_2 - 1\}, \dots, V_p =$

$$\begin{aligned}
\text{Let } M_{(A_1, A_2)} &= \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \text{ where } A_1 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \text{ and} \\
A_2 &= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}. \text{ Let } \sigma_1 = I_7 \text{ and } \sigma_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \end{pmatrix}, \text{ then :} \\
M_{(A_1, A_2)} &= \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}^{\sigma_2^{-1}} = M_1'^{\sigma_1^{-1}} M_2'^{\sigma_2^{-1}}.
\end{aligned}$$

Using the computer optimization program, one finds  
 $A_1 = [13][01][30][21][13][02][01]$ ,  $A_2 = [01][12][10][21][01]$ .  
Hence an optimal decomposition for  $M$  is  

$$\begin{aligned}
M_{(A_1, A_2)} &= [13][01][30][21][13][02][01]([01][12][10][21][01])^{\sigma_2^{-1}} \\
&= [13][01][30][21][13][02][01][45][56][54][65][45].
\end{aligned}$$

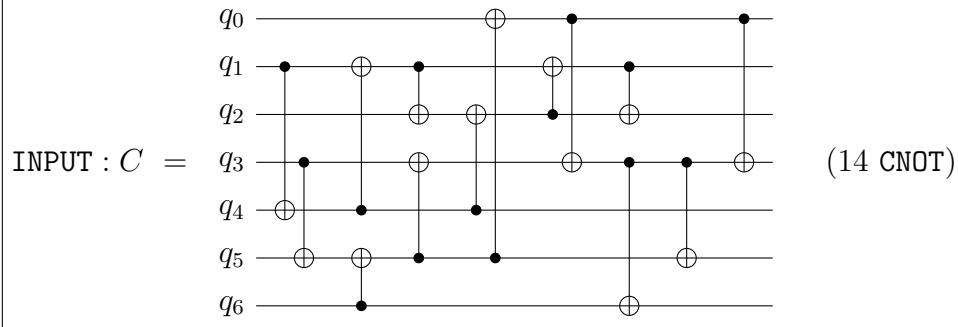
**Figure 14:** Decomposition of a matrix using cartesian product of subgroups.

$\{n_1 + \dots + n_{p-1}, \dots, n_1 + \dots + n_{p-1} + n_p - 1\}$ , so the graph  $\mathcal{G}(M_S^\sigma) = (\mathcal{G}(M_S))^\sigma$  is also a disconnected graph whose  $p$  connected components are  $\sigma(V_1), \dots, \sigma(V_p)$ .

By applying a Breadth-first search or a Depth-first search to the graph  $\mathcal{G}(M)$  of a given circuit, one can get the connected components of  $\mathcal{G}(M)$  in linear time (see [21] for a detailed description of the algorithm). Suppose that we find more than one connected component, say  $C_1, \dots, C_p$  and let  $n_i$  be the cardinal of  $C_i$  for  $1 \leq i \leq p$ . Let  $\sigma$  be any permutation verifying  $\sigma(C_1) = \{0, \dots, n_1 - 1\}$ ,  $\sigma(C_2) = \{n_1, \dots, n_1 + n_2 - 1\}$ ,  $\dots$ ,  $\sigma(C_p) = \{n_1 + \dots + n_{p-1}, \dots, n_1 + \dots + n_{p-1} + n_p - 1\}$ . Then the matrix  $M^\sigma$  is a block diagonal matrix  $M_S$  and we obtain an optimal decomposition of  $M^\sigma$  as explained before. Finally, we deduce an optimal decomposition of  $M = (M^\sigma)^{\sigma^{-1}}$  by conjugating by  $\sigma^{-1}$  this decomposition (see Figure 15 for an example). Since we can find an optimal decomposition of any matrix of  $\text{GL}_n(\mathbb{F}_2)$  for  $n \leq 5$  (using the computer optimization program), then we can optimize any CNOT circuit whose graph has connected components of size up to 5.

### 5.3 Bit reverse of permutation matrices

The third and last case we consider in this section is the case of a matrix  $M$  of type  $\bar{\sigma}$  where  $\bar{\sigma}$  denotes a permutation matrix in even dimension in which all the bits are



$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$C_1 = \{0, 3, 5, 6\}, \quad C_2 = \{1, 2, 4\}$$

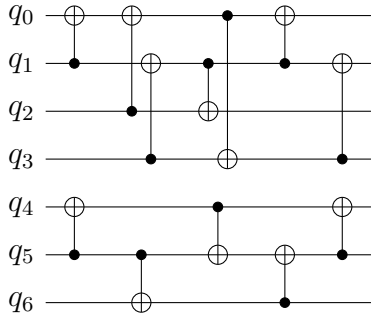
$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 1 & 6 & 0 & 2 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 0 & 2 & 1 & 4 \end{pmatrix}$$

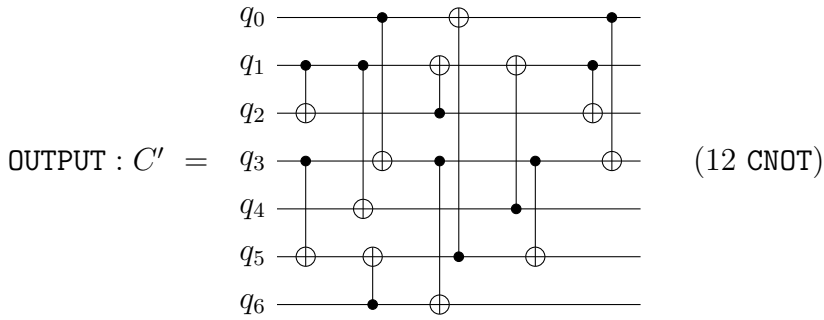
$$M^\sigma = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} = M_{(A_1, A_2)}$$

From example 14,  $M_{(A_1, A_2)} = [13][01][30][21][13][02][01][45][56][54][65][45]$ .

The corresponding circuit is :



$$M = M_{(A_1, A_2)}^{\sigma^{-1}} = [30][53][05][63][30][56][53][21][14][12][41][21]$$



**Figure 15:** Circuit optimization using a cartesian product of subgroups.

reversed. For instance  $\overline{(02)(13)} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$  and  $\overline{I_4} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ .

We check that  $\overline{\sigma} = \sigma \overline{I}$ . For instance  $\overline{(02)(13)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$ .

**Lemma 15.** *Let  $n \geq 2$  be an even integer.*

$$\overline{I_n} \in \text{GL}_n(\mathbb{F}_2) \text{ and } \overline{I_n}^2 = I_n. \quad (33)$$

$$\forall \sigma \in \mathfrak{S}_n, \sigma \overline{I_n} \sigma^{-1} = \overline{I_n}. \quad (34)$$

$$\forall \sigma, \gamma \in \mathfrak{S}_n, \overline{\sigma} \overline{\gamma} = \overline{\sigma \gamma}. \quad (35)$$

*Proof.* Let denote by  $1_n$  the matrix of dimension  $n$  whose elements are all equal to 1. One has  $\overline{I_n}^2 = (I_n \oplus 1_n)^2 = I_n^2 \oplus 1_n^2 = I_n \oplus 1_n^2$ . If  $n$  is even then  $1_n^2 = 0$ , hence  $\overline{I_n}^2 = I_n$ . Besides  $\sigma \overline{I_n} \sigma^{-1} = \sigma(I_n \oplus 1_n) \sigma^{-1} = \sigma I_n \sigma^{-1} \oplus \sigma 1_n \sigma^{-1} = I_n \oplus 1_n = \overline{I_n}$ . Finally  $\overline{\sigma} \overline{\gamma} = \sigma \overline{I_n} \gamma \overline{I_n} = \sigma \gamma \gamma^{-1} \overline{I_n} \gamma \overline{I_n} = \sigma \gamma \overline{I_n}^2 = \sigma \gamma$ .  $\square$

From Lemma 15 we directly deduce the structure of the group  $\langle \sigma, \overline{\sigma} \rangle$  :

**Proposition 16.** *The group generated by the permutation matrices and the matrix  $\overline{I_n}$  is isomorphic to the cartesian product  $\mathfrak{S}_n \times (\mathbb{F}_2, \oplus)$ .*

The following lemma gives a simple decomposition for the product of  $[ij][ki][jk]$  by a transposition matrix  $(ij)$ ,  $(ki)$  or  $(jk)$ . We use it in the proof of Proposition 19.

**Lemma 17.** *Let  $0 \leq i, j, k \leq n-1$  be distinct integers :*

$$R1 : [ij][ki][jk](\mathbf{jk}) = [ki][ij][jk] \quad (36)$$

$$L1 : (\mathbf{ij})[ij][ki][jk] = [ij][jk][ki] \quad (37)$$

$$R2 : [ij][ki][jk](\mathbf{ki}) = [jk][ij][ki][jk] \quad (38)$$

$$L2 : (\mathbf{ki})[ij][ki][jk] = [ij][ki][jk][ij] \quad (39)$$

$$R3 : [ij][ki][jk](\mathbf{ij}) = [ji][ik][kj] \quad (40)$$

$$L3 : (\mathbf{jk})[ij][ki][jk] = [ji][ik][kj] \quad (41)$$

*Proof.* We prove only (41), the other proofs being similar :

$$\begin{aligned} (\mathbf{jk})[ij][ki][jk] &= [ij]^{(jk)}[ki]^{(jk)}(\mathbf{jk})[jk] \\ &= [ik][ji](\mathbf{jk})[jk] \text{ (using (22))} \\ &= [ik][ji][jk][kj] \\ &= [ji][ik][kj] \text{ (using (29))} \end{aligned}$$

$\square$

One obtains similar rules for matrices of type  $[ij][jk][ki]$  by taking the inverse of each member of the identities of Lemma 17. For convenience we denote the product  $[ij][ki][jk]$  by  $[ijk]$ . With this notation one has  $[ij][jk][ki] = [kij]^{-1}$ .

**Proposition 18.** *Let  $n \geq 2$  be even and let  $n = 2q$ .*

*Let  $B_q = \prod_{i=0}^{q-2} [2i+1 \quad 2i+2 \quad 2i+3]$  if  $q > 1$  and  $B_1 = I_2$ . Then*

$$\overline{I_{2q}} = B_q^{-1}(01)B_q. \quad (42)$$

*Proof.* We prove the result by induction on  $q \geq 1$ .

The initial case follows from  $\overline{I_2} = (01)$ .

Induction step : suppose that  $q \geq 1$  and  $\overline{I_{2q}} = B_q^{-1}(01)B_q$ .

We use the morphism  $\varphi$  already mentioned in the final remark of Section 3 :  $\varphi$  is the injective morphism from  $\text{GL}_{2q}(\mathbb{F}_2)$  into  $\text{GL}_{2(q+1)}(\mathbb{F}_2)$  defined by  $\varphi(M) = \begin{bmatrix} M & 0 \\ 0 & I_2 \end{bmatrix}$  and we make no distinction between matrices  $M$  and  $\varphi(M)$ .

$$\text{So, one has : } \varphi(\overline{I_{2q}}) = \begin{bmatrix} \overline{I_{2q}} & 0 \\ 0 & I_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 & \dots & 1 & 0 & 0 \\ 1 & 0 & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 1 & \vdots & \vdots \\ 1 & \dots & 1 & 0 & 0 & \vdots \\ 0 & \dots & \dots & 0 & 1 & 0 \\ 0 & \dots & \dots & \dots & 0 & 1 \end{bmatrix} \text{ and } \varphi(\overline{I_{2q}}) = B_q^{-1}(01)B_q.$$

Due to the effect on lines and columns of a multiplication by a transvection matrix (Proposition 3), we check that :

$$[2q \quad 2q+1][2q+1 \quad 2q-1][2q-1 \quad 2q]\varphi(\overline{I_{2q}})[2q-1 \quad 2q][2q+1 \quad 2q-1][2q \quad 2q+1] = \overline{I_{2q+2}}.$$

Since  $[2q-1 \quad 2q][2q+1 \quad 2q-1][2q \quad 2q+1] = [2q-1 \quad 2q \quad 2q+1]$  one has :

$$\overline{I_{2q+2}} = [2q-1 \quad 2q \quad 2q+1]^{-1}\varphi(\overline{I_{2q}})[2q-1 \quad 2q \quad 2q+1].$$

$$\overline{I_{2q+2}} = [2q-1 \quad 2q \quad 2q+1]^{-1}B_q^{-1}(01)B_q[2q-1 \quad 2q \quad 2q+1].$$

$$\text{Hence : } \overline{I_{2q+2}} = B_{q+1}^{-1}(01)B_{q+1}. \quad \square$$

Formula (42) gives a decomposition of  $\overline{I_{2q}}$  in  $3(q-1) + 3 + 3(q-1) = 3(n-1)$  transvections (where  $n = 2q$ ). We remark that this decomposition is not optimal if  $q > 1$ . Indeed, it can be reduced as follows.

$$\text{Firstly } B_q = \prod_{i=0}^{q-2} [2i+1 \quad 2i+2 \quad 2i+3] = [12][31][23] \prod_{i=1}^{q-2} [2i+1 \quad 2i+2 \quad 2i+3].$$

$$\text{Thus } B_q = [12][31][23]B'_q, \text{ where } B'_q = \prod_{i=1}^{q-2} [2i+1 \quad 2i+2 \quad 2i+3]. \text{ Hence}$$

$$\overline{I_{2q}} = B_q^{-1}(01)B_q = (B'_q)^{-1}[23][31][12](01)[12][31][23]B'_q. \quad (43)$$

Then, one has :

$$\begin{aligned} [23][31][12](01)[12][31][23] &= [23][31][12][10][01][10][12][31][23] \\ &\stackrel{31}{=} [23][31][10][12][01][12][10][31][23] \\ &\stackrel{30}{=} [23][31][10][01][02][10][31][23]. \text{ (8 transvections)} \end{aligned}$$



So, from Equation (43), we now have a decomposition of  $\overline{I_{2q}}$  in  $3(q-2) + 8 + 3(q-2) = 3(n-1) - 1$  transvections. We remark that this result is coherent with Conjecture 12. Indeed, since  $\overline{I_{2q}}$  is not a cycle of length  $n$  in  $\text{GL}_n(\mathbb{F}_2)$ , it must have a decomposition in strictly less than  $3(n-1)$  transvections. We also conjecture that this decomposition of  $\overline{I_n}$  in  $3(n-1) - 1$  transvections is optimal and we checked this conjecture for  $n = 4$  using our computer optimization program.

Actually Proposition 18 is a special case of the following proposition.

**Proposition 19.** *Let  $n \geq 2$  be even and let  $n = 2q$ . For any permutation matrix  $\sigma$  of  $\text{GL}_n(\mathbb{F}_2)$  different from  $I_n$  there exists  $q-1$  matrices  $M_1, \dots, M_{q-1}$  of type  $[xyz]$ ,  $q-1$  integers  $\varepsilon_i \in \{1, -1\}$ ,  $q-1$  matrices  $M'_1, \dots, M'_{q-1}$  of type  $[xyz]$  and  $q-1$  integers  $\varepsilon'_i \in \{1, -1\}$  such that :*

$$\overline{I_n} = \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \sigma \prod_{i=1}^{q-1} M_i'^{\varepsilon'_i} \quad (44)$$

*Proof.* Let  $n \geq 2$  be an even integer. We denote by  $\mathcal{P}_n^*$  the set of decreasing partitions  $\lambda$  of  $n$  such that  $\lambda \neq (1, \dots, 1)$ . Any  $\lambda \in \mathcal{P}_n^*$  is the cycle type of a permutation different from the identity (see Section 2). If  $\lambda \in \mathcal{P}_n^*$ , we denote by  $\alpha_\lambda$  the permutation of  $\mathfrak{S}_n$  (or equivalently the permutation matrix of  $\text{GL}_n(\mathbb{F}_2)$ ) defined by :

$$\alpha_\lambda = \underbrace{(0 \dots n_1 - 1)}_{\text{cycle of length } n_1} \underbrace{(n_1 \dots n_1 + n_2 - 1)}_{\text{cycle of length } n_2} \dots \underbrace{\left( \sum_{i=1}^{p-1} n_i \dots \sum_{i=1}^p n_i - 1 \right)}_{\text{cycle of length } n_p}.$$

Notice that  $\alpha_\lambda$  has cycle type  $\lambda$  and is therefore different from the identity.

If  $n \geq 4$  and  $\lambda \in \mathcal{P}_n^*$ , we denote by  $\lambda_{-2}$  the element of  $\mathcal{P}_{n-2}^*$  obtained from  $\lambda$  as follows. To describe the operation we distinguish the general case ( $n_p > 2$ ) and three specific cases and we write each time the relation between  $\alpha_\lambda$  and  $\alpha_{\lambda_{-2}}$ . Notice that  $\alpha_{\lambda_{-2}}$  is a permutation in  $\mathfrak{S}_{n-2}$  or a permutation matrix in  $\text{GL}_{n-2}(\mathbb{F}_2)$  since  $\lambda \in \mathcal{P}_{n-2}^*$  but we can consider  $\alpha_{\lambda_{-2}}$  as a permutation in  $\mathfrak{S}_n$  (by setting  $\alpha_{\lambda_{-2}}(n-2) = n-2$  and  $\alpha_{\lambda_{-2}}(n-1) = n-1$ ) or as a permutation matrix of  $\text{GL}_n(\mathbb{F}_2)$  (using the injective morphism  $\varphi$  from  $\text{GL}_{n-2}(\mathbb{F}_2)$  into  $\text{GL}_n(\mathbb{F}_2)$ ).

In the general case,  $\lambda_{-2} := (n_1, \dots, n_p - 2)$ , so  $\alpha_{\lambda_{-2}} = \alpha_\lambda(n-2 \ n-1)(n-3 \ n-2)$ . If  $n_p = n_{p-1} = 1$  (first specific case),  $\lambda_{-2} := (n_1, \dots, n_{p-2})$ , hence  $\alpha_{\lambda_{-2}} = \alpha_\lambda$ . If  $n_p = 1$  and  $n_{p-1} > 1$  (second specific case),  $\lambda_{-2} := (n_1, \dots, n_{p-2}, n_{p-1} - 1)$ , hence  $\alpha_{\lambda_{-2}} = \alpha_\lambda(n-3 \ n-2)$ . If  $n_p = 2$  (third specific case),  $\lambda_{-2} := (n_1, \dots, n_{p-1})$ , hence  $\alpha_{\lambda_{-2}} = \alpha_\lambda(n-2 \ n-1)$ .

Without loss of generality we can prove Proposition 19 in the case of a permutation  $\sigma = \alpha_\lambda$  where  $\lambda \in \mathcal{P}_n^*$ . Indeed, if  $\sigma$  is any permutation (different from the identity) that has cycle type  $\lambda$ , then  $\sigma$  is in the same conjugacy class as  $\alpha_\lambda$  since they have the same cycle type and we build a permutation  $\gamma$  such that  $\sigma = \gamma \alpha_\lambda \gamma^{-1}$ . Since

$$\overline{I_n} = \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda \prod_{i=1}^{q-1} M_i'^{\varepsilon'_i} \text{ and } \overline{I_n} \stackrel{34}{=} (\overline{I_n})^\gamma, \text{ it follows that}$$

$$\overline{I_n} = \prod_{i=1}^{q-1} (M_i^{\varepsilon_i})^\gamma \sigma \prod_{i=1}^{q-1} (M_i'^{\varepsilon'_i})^\gamma. \quad (45)$$

To conclude it is sufficient to notice that  $([ijk]^\varepsilon)^\gamma = [\gamma(i)\gamma(j)\gamma(k)]^\varepsilon$  for any permutation  $\gamma$  and for  $\varepsilon \in \{-1, 1\}$ . So Equation (45) can easily be written under the form of Equation (44) and this proves Proposition 19 for the permutation  $\sigma$ .

We prove now Proposition 19 for a permutation  $\alpha_\lambda$ , by induction on  $n \geq 2$  even. The initial case is clear since there is only one partition of 2 different from  $(1, 1)$  namely  $\lambda = (2)$ . In this case  $\alpha_\lambda = (01) = \overline{I_2}$ .

Induction step : let  $n \geq 2$  be an even integer, let  $\lambda$  in  $\mathcal{P}_{n+2}^*$  and  $\alpha_\lambda$  in  $\mathfrak{S}_{n+2}$ . From Proposition 18, one has  $\overline{I_{n+2}} = [n-1 \quad n \quad n+1]^{-1} \overline{I_n} [n-1 \quad n \quad n+1]$ . We use the induction hypothesis on  $\alpha_{\lambda_{-2}} \in \mathfrak{S}_n$  :  $\overline{I_n} = \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_{\lambda_{-2}} \prod_{i=1}^{q-1} M_i^{\varepsilon'_i}$ , hence

$$\overline{I_{n+2}} = [n-1 \quad n \quad n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_{\lambda_{-2}} \prod_{i=1}^{q-1} M_i^{\varepsilon'_i} [n-1 \quad n \quad n+1]. \quad (46)$$

We consider now the different possible relations between  $\alpha_{\lambda_{-2}}$  and  $\alpha_\lambda$ , starting by the three specific cases and ending by the general case which is more technical.

In the first case  $\alpha_{\lambda_{-2}} = \alpha_\lambda$ , so Equation (46) becomes

$$\overline{I_{n+2}} = [n-1 \quad n \quad n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda \prod_{i=1}^{q-1} M_i^{\varepsilon'_i} [n-1 \quad n \quad n+1]$$

and we are done with the induction step.

In the second case  $\alpha_{\lambda_{-2}} = \alpha_\lambda(n-1 \quad n)$ , so Equation (46) becomes

$$\overline{I_{n+2}} = [n-1 \quad n \quad n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda(n-1 \quad n) \prod_{i=1}^{q-1} M_i^{\varepsilon'_i} [n-1 \quad n \quad n+1]. \quad (47)$$

Let  $M = (n-1 \quad n) \prod_{i=1}^{q-1} M_i^{\varepsilon'_i} [n-1 \quad n \quad n+1]$ . One has :

$$\begin{aligned} M &= \prod_{i=1}^{q-1} \left( M_i^{\varepsilon'_i} \right)^{(n-1 \quad n)} (n-1 \quad n) [n-1 \quad n] [n+1 \quad n-1] [n \quad n+1] \\ &\stackrel{37}{=} \prod_{i=1}^{q-1} \left( M_i^{\varepsilon'_i} \right)^{(n-1 \quad n)} [n-1 \quad n] [n \quad n+1] [n+1 \quad n-1] \\ &= \prod_{i=1}^{q-1} \left( M_i^{\varepsilon'_i} \right)^{(n-1 \quad n)} [n+1 \quad n-1 \quad n]^{-1}. \end{aligned}$$

Hence Equation (47) becomes

$$\overline{I_{n+2}} = [n-1 \quad n \quad n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda \prod_{i=1}^{q-1} \left( M_i^{\varepsilon'_i} \right)^{(n-1 \quad n)} [n+1 \quad n-1 \quad n]^{-1}$$

and we are done with the induction step since  $([xyz]^\varepsilon)^\sigma = [\sigma(x)\sigma(y)\sigma(z)]^\varepsilon$  where  $\sigma = (n-1 \quad n)$ .

In the third case  $\alpha_{\lambda_{-2}} = \alpha_\lambda(n \quad n+1)$ , so Equation (46) becomes

$$\overline{I_{n+2}} = [n-1 \quad n \quad n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda(n \quad n+1) \prod_{i=1}^{q-1} M_i^{\varepsilon'_i} [n-1 \quad n \quad n+1]. \quad (48)$$

Let  $M = (n \quad n+1) \prod_{i=1}^{q-1} M_i^{\prime \varepsilon'_i} [n-1 \quad n \quad n+1]$ . One has :

$$\begin{aligned} M &= \prod_{i=1}^{q-1} \left( M_i^{\prime \varepsilon'_i} \right)^{(n \quad n+1)} (n \quad n+1) [n-1 \quad n] [n+1 \quad n-1] [n \quad n+1] \\ &\stackrel{41}{=} \prod_{i=1}^{q-1} \left( M_i^{\prime \varepsilon'_i} \right)^{(n \quad n+1)} [n \quad n-1] [n-1 \quad n+1] [n+1 \quad n] \\ &= \prod_{i=1}^{q-1} \left( M_i^{\prime \varepsilon'_i} \right)^{(n \quad n+1)} [n+1 \quad n \quad n-1]^{-1}. \end{aligned}$$

Hence Equation (48) becomes

$$\overline{I_{n+2}} = [n-1 \quad n \quad n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda \prod_{i=1}^{q-1} \left( M_i^{\prime \varepsilon'_i} \right)^{(n \quad n+1)} [n+1 \quad n \quad n-1]^{-1}$$

and we are done with the induction step since  $([xyz]^\varepsilon)^\sigma = [\sigma(x)\sigma(y)\sigma(z)]^\varepsilon$  where  $\sigma = (n \quad n+1)$ .

In the general case, we start by conjugating each member of Equation (46) by  $(n \quad n+1)$ . Using the invariance of  $\overline{I_n}$  by conjugation (Identity (34)), we get :

$$\overline{I_{n+2}} = (n \quad n+1) [n-1 \quad n \quad n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_{\lambda_{-2}} \prod_{i=1}^{q-1} M_i^{\prime \varepsilon'_i} [n-1 \quad n \quad n+1] (n \quad n+1). \quad (49)$$

On one hand, we have :

$$\begin{aligned} (n \quad n+1) [n-1 \quad n \quad n+1]^{-1} &= (n \quad n+1) [n \quad n+1] [n+1 \quad n-1] [[n-1 \quad n] \\ &\stackrel{37}{=} [n \quad n+1] [[n-1 \quad n] [n+1 \quad n-1] \\ &= [n \quad n+1 \quad n-1] \end{aligned}$$

On the other hand we have :

$$\begin{aligned} [n-1 \quad n \quad n+1] (n \quad n+1) &= [n-1 \quad n] [n+1 \quad n-1] [n \quad n+1] (n \quad n+1). \\ &\stackrel{36}{=} [n+1 \quad n-1] [n-1 \quad n] [n \quad n+1]. \\ &= [n \quad n+1 \quad n-1]^{-1} \end{aligned}$$

So Equation (49) becomes :

$$\overline{I_{n+2}} = [n \quad n+1 \quad n-1] \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_{\lambda_{-2}} \prod_{i=1}^{q-1} M_i^{\prime \varepsilon'_i} [n \quad n+1 \quad n-1]^{-1}$$

In the general case, one has :

$$\alpha_{\lambda_{-2}} = \alpha_\lambda (n \quad n+1) (n-1 \quad n) = \alpha_\lambda (n-1 \quad n) (n+1 \quad n-1), \text{ hence}$$

$$\overline{I_{n+2}} = [n \quad n+1 \quad n-1] \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda (n-1 \quad n) (n+1 \quad n-1) \prod_{i=1}^{q-1} M_i^{\prime \varepsilon'_i} [n \quad n+1 \quad n-1]^{-1}. \quad (50)$$

Let  $M = (n-1 \quad n) (n+1 \quad n-1) \prod_{i=1}^{q-1} M_i^{\prime \varepsilon'_i} [n \quad n+1 \quad n-1]^{-1}$ . One has :

$$M = \prod_{i=1}^{q-1} \left( M_i^{\prime \varepsilon'_i} \right)^{(n-1 \quad n)(n+1 \quad n-1)} (n-1 \quad n) (n+1 \quad n-1) [n \quad n+1 \quad n-1]^{-1}$$

$$\begin{aligned}
&\stackrel{37}{=} \prod_{i=1}^{q-1} \left( M_i^{\varepsilon'_i} \right)^{(n-1 \ n)(n+1 \ n-1)} (n-1 \ n)[n+1 \ n-1][n \ n+1][n-1 \ n] \\
&\stackrel{41}{=} \prod_{i=1}^{q-1} \left( M_i^{\varepsilon'_i} \right)^{(n-1 \ n)(n+1 \ n-1)} [n-1 \ n+1][n+1 \ n][n \ n-1] \\
&= \prod_{i=1}^{q-1} \left( M_i^{\varepsilon'_i} \right)^{(n-1 \ n)(n+1 \ n-1)} [n \ n-1 \ n+1]^{-1}.
\end{aligned}$$

Hence Equation (50) becomes :

$$\overline{I_{n+2}} = [n \ n+1 \ n-1] \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda \prod_{i=1}^{q-1} \left( M_i^{\varepsilon'_i} \right)^{(n-1 \ n)(n+1 \ n-1)} [n \ n-1 \ n+1]^{-1}$$

and we are done with the induction step since  $([xyz]^\varepsilon)^\sigma = [\sigma(x)\sigma(y)\sigma(z)]^\varepsilon$  where  $\sigma = (n-1 \ n)(n+1 \ n-1)$ .  $\square$

Actually the main interest of Proposition 19 is to give a way to compute easily a decomposition of  $\bar{\sigma}$  in transvections, as described in the following proposition.

**Proposition 20.** *Let  $n \geq 2$  be an even integer. For any permutation matrix  $\sigma$  of  $\text{GL}_n(\mathbb{F}_2)$  different from  $I_n$  there exists  $n-2$  matrices  $M_1, \dots, M_{n-2}$  of type  $[xyz]$  and  $n-2$  integers  $\varepsilon_i \in \{1, -1\}$  such that :*

$$\bar{\sigma} = \prod_{i=1}^{n-2} M_i^{\varepsilon_i} \tag{51}$$

*Proof.* Let  $\sigma$  be a permutation matrix of  $\text{GL}_n(\mathbb{F}_2)$  different from  $I_n$ . Applying Proposition 19 to  $\sigma^{-1}$  one has  $\overline{I_n} = \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \sigma^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon'_i}$ . Hence  $\bar{\sigma} = \sigma \overline{I_n} =$

$$\prod_{i=1}^{q-1} (M_i^{\varepsilon_i})^\sigma \prod_{i=1}^{q-1} M_i^{\varepsilon'_i}. \tag{52}$$

$\square$

Since the proof of Proposition 19 is constructive, the method used in the proof of Proposition 20 gives an algorithm to decompose any matrix  $\bar{\sigma}$  different from  $\overline{I_n}$  in  $3(n-2)$  transvections (see Figure 16 for an example). We conjecture that this decomposition is optimal and we checked it for  $n = 4$ .

Let  $n = 6$  and  $\bar{\sigma} = \overline{(503)(142)} =$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

$\sigma^{-1} = (305)(241)$ . Let  $\lambda_6 = (3, 3)$  be the cycle type of  $\sigma^{-1}$ , then  $\alpha_{\lambda_6} = (012)(345)$ .  
Let  $\lambda_4 = (3, 1)$ , then  $\alpha_{\lambda_4} = (012)(3) = \alpha_{\lambda_6}(34)(53)$ .  
Let  $\lambda_2 = (2)$ , then  $\alpha_{\lambda_2} = (01) = \alpha_{\lambda_4}(12)$ .  
 $\bar{I}_2 = \alpha_{\lambda_2}$   
 $\bar{I}_4 = [123]^{-1}\bar{I}_2[123] = [123]^{-1}\alpha_{\lambda_2}[123] = [123]^{-1}\alpha_{\lambda_4}(12)[123]$   
 $\bar{I}_4 = [123]^{-1}\alpha_{\lambda_4}(12)[12][31][23] = [123]^{-1}\alpha_{\lambda_4}[12][23][31] = [123]^{-1}\alpha_{\lambda_4}[312]^{-1}$   
 $\bar{I}_6 = [345]^{-1}\bar{I}_4[345] = [345]^{-1}[123]^{-1}\alpha_{\lambda_4}[312]^{-1}[345]$   
 $\bar{I}_6 = [45][53][34][123]^{-1}\alpha_{\lambda_6}(34)(53)[312]^{-1}[34][53][45]$   
 $\bar{I}_6 = (45)[45][53][34][123]^{-1}\alpha_{\lambda_6}(34)(53)[312]^{-1}[34][53][45](45)$   
 $\bar{I}_6 = [45][34][53][123]^{-1}\alpha_{\lambda_6}(34)(53)[312]^{-1}[53][34][45]$   
 $\bar{I}_6 = [453][123]^{-1}\alpha_{\lambda_6}([312]^{-1})^{(34)(53)}(34)(53)[53][34][45]$   
 $\bar{I}_6 = [453][123]^{-1}\alpha_{\lambda_6}[512]^{-1}(34)[53][45][34]$   
 $\bar{I}_6 = [453][123]^{-1}\alpha_{\lambda_6}[512]^{-1}[35][54][43]$   
 $\bar{I}_6 = [453][123]^{-1}\alpha_{\lambda_6}[512]^{-1}[435]^{-1}$   
 $\sigma^{-1} = \alpha_{\lambda_6}^{\gamma}$  where  $\gamma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 0 & 5 & 2 & 4 & 1 \end{pmatrix}$ , hence :  
 $\bar{I}_6 = (\bar{I}_6)^{\gamma} = ([453][123]^{-1})^{\gamma}\sigma^{-1}([512]^{-1}[435]^{-1})^{\gamma} = [412][052]^{-1}\sigma^{-1}[105]^{-1}[421]^{-1}$   
 $\bar{\sigma} = \sigma\bar{I}_6 = ([412][052]^{-1})^{\sigma}[105]^{-1}[421]^{-1} = [241][301]^{-1}[105]^{-1}[421]^{-1}$   
 $\bar{\sigma} = [24][12][41][01][13][30][05][51][10][21][14][42]$

**Figure 16:** Decomposition in transvections of a matrix of type  $\bar{\sigma}$ .

## 6 Entanglement in CNOT gates circuits

The notion of entanglement is usually defined through the group of Stochastic Local Operations assisted by Classical Communication denoted by **SLOCC** which is assimilated to the cartesian group product  $\text{SL}_2(\mathbb{C})^{\times n}$  [27, 8]. Mathematically two states  $|\psi\rangle$  and  $|\varphi\rangle$  are **SLOCC**-equivalent if there exist  $n$  operators  $A_1, \dots, A_n$  in  $\text{SL}_2(\mathbb{C})$  such that  $A_1 \otimes \dots \otimes A_n |\psi\rangle = \lambda |\varphi\rangle$  for some complex number  $\lambda$ . In other words,  $|\psi\rangle$  and  $|\varphi\rangle$  are **SLOCC**-equivalent if they are in the same orbit of  $\text{GL}_2(\mathbb{C})^{\times n}$  acting on the Hilbert space  $\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$ . The **SLOCC**-equivalence of two states  $|\varphi\rangle$  and  $|\psi\rangle$  has a physical interpretation as explained in [8] :  $|\varphi\rangle$  and  $|\psi\rangle$  can be interconverted into each other with non zero probability by  $n$  parties being able to coordinate their action by classical communication, each party acting separately on one of the qubits. The **SLOCC**-equivalence of two states  $|\varphi\rangle$  and  $|\psi\rangle$  implies that both states can achieve the same tasks (for instance in a communication protocol) but with a probability of a success that may differ. In this sense the **SLOCC**-equivalence can be considered as a qualitative way of separating non equivalent quantum states.

Some states have a particular interest like the Greenberger-Horne-Zeilinger state [15]

$$|\text{GHZ}_n\rangle = \frac{1}{\sqrt{2}} \left( \overbrace{|0 \dots 0\rangle}^{\times n} + \overbrace{|1 \dots 1\rangle}^{\times n} \right) = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes n} + |1\rangle^{\otimes n}) \quad (n \geq 3) \quad (52)$$

and the W-state [8]

$$|\text{W}_n\rangle = \frac{1}{\sqrt{n}} (|10 \dots 0\rangle + |010 \dots 0\rangle + \dots + |0 \dots 01\rangle) \quad (n \geq 3). \quad (53)$$

These two states represent two non-equivalent kind of entanglements : they belong to distinct **SLOCC** orbits and thus cannot be interconverted into each other by local operations (even probabilistically). These states are particularly useful because they are required as a physical resource to realize many specific tasks. For instance, in an anonymous network where the processors share the W-state, the leader election problem can be solved by a simple protocol whereas the GHZ-state is the only shared state that allows solution of distributed consensus [7]. The GHZ-state is also used in many protocols in quantum cryptography, *e.g.* in secret sharing [17].

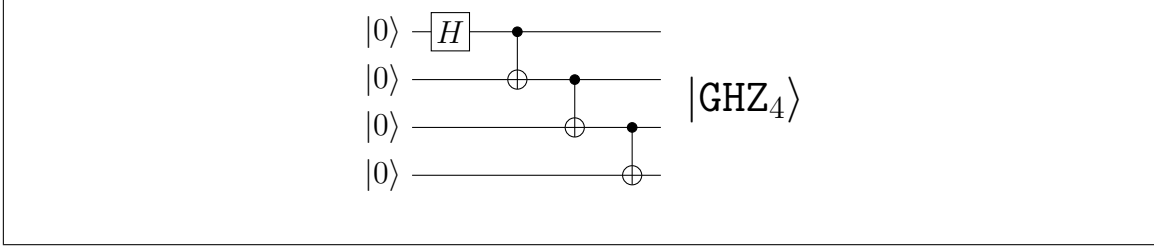
We denote by  $H_i$  the Hadamard gate (see Figure 2) applied on qubit  $i$ . For instance in a 3-qubit system,  $H_1 = \text{I} \otimes \text{H} \otimes \text{I}$  where  $\text{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  and  $\text{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ . In the following we study the emergence of entanglement when a CNOT gates circuit acts on a fully factorized state.

### 6.1 Creating a GHZ-state

The construction of the GHZ-state for  $n$  qubit is straightforward :

$$|\text{GHZ}_n\rangle = X_{n-1} X_{n-2} \dots X_{21} X_{10} H_0 |0\rangle^{\otimes n}. \quad (54)$$

A simple computation proves Equation (54). Indeed one has  $H_0 |0 \dots 0\rangle = \frac{1}{\sqrt{2}}(|0 \dots 0\rangle + |10 \dots 0\rangle)$  and  $X_{n-1} X_{n-2} \dots X_{21} X_{10} |10 \dots 0\rangle = |1 \dots 1\rangle$ . If  $n = 4$ , Equation (54) corresponds to the circuit in Figure 17.



**Figure 17:** Using a circuit of  $c\mathcal{K}_4$  to obtain  $|\text{GHZ}_4\rangle$ .

## 6.2 The group $c\mathcal{K}_3$ and entanglement of a 3-qubit system

We prove that the group  $c\mathcal{K}_3$  is powerful enough to generate any entanglement type from a completely factorized state. We use the method pioneered by Klyachko in [23] 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  $|\psi\rangle = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} |ijk\rangle$  be a 3-qubit state. The simplest covariant associated to  $|\psi\rangle$  is the trilinear form :

$$A = \sum_{i,j,k \in \{0,1\}} \alpha_{ijk} x_i y_j z_k. \quad (55)$$

From  $A$  one computes three quadratic forms :

$$B_x(x_0, x_1) = \begin{vmatrix} \frac{\partial^2 A}{\partial y_0 \partial z_0} & \frac{\partial^2 A}{\partial y_0 \partial z_1} \\ \frac{\partial^2 A}{\partial y_1 \partial z_0} & \frac{\partial^2 A}{\partial y_1 \partial z_1} \end{vmatrix}, \quad (56)$$

$$B_y(y_0, y_1) = \begin{vmatrix} \frac{\partial^2 A}{\partial x_0 \partial z_0} & \frac{\partial^2 A}{\partial x_0 \partial z_1} \\ \frac{\partial^2 A}{\partial x_1 \partial z_0} & \frac{\partial^2 A}{\partial x_1 \partial z_1} \end{vmatrix}, \quad (57)$$

$$B_z(z_0, z_1) = \begin{vmatrix} \frac{\partial^2 A}{\partial x_0 \partial y_0} & \frac{\partial^2 A}{\partial x_0 \partial y_1} \\ \frac{\partial^2 A}{\partial x_1 \partial y_0} & \frac{\partial^2 A}{\partial x_1 \partial y_1} \end{vmatrix}. \quad (58)$$

The catalecticant is a trilinear form obtained by computing any of the three Jacobians of  $A$  with one of the quadratic forms, which turns out to be the same,

$$C(x_0, x_1, y_0, y_1, z_0, z_1) = \begin{vmatrix} \frac{\partial A}{\partial x_0} & \frac{\partial A}{\partial x_1} \\ \frac{\partial B_x}{\partial x_0} & \frac{\partial B_x}{\partial x_1} \end{vmatrix}. \quad (59)$$

The three quadratic forms  $B_x$ ,  $B_y$  and  $B_z$  have the same discriminant  $\Delta$  which is the last covariant polynomial we need to characterize the SLOCC-orbits :

$$\Delta(|\psi\rangle) = (\alpha_{000}\alpha_{111} - \alpha_{001}\alpha_{110} - \alpha_{010}\alpha_{101} + \alpha_{011}\alpha_{100})^2 - 4(\alpha_{000}\alpha_{011} - \alpha_{001}\alpha_{010})(\alpha_{100}\alpha_{111} - \alpha_{101}\alpha_{110}). \quad (60)$$

The polynomial  $\Delta$  is the generator of the algebra of invariant polynomials under the action of SLOCC (*i.e.*  $\Delta(|\psi\rangle) = \Delta(M|\psi\rangle)$  for any  $M \in \text{SL}_2(\mathbb{C})^{\times 3}$ ). It is also the Cayley hyperdeterminant of the trilinear binary form  $A$  [4].

Let  $V := [B_x, B_y, B_z, C, \Delta]$  be a vector of covariants. We associate the binary vector  $V[|\psi\rangle] := [[B_x(|\psi\rangle)], [B_y(|\psi\rangle)], [B_z(|\psi\rangle)], [C(|\psi\rangle)], [\Delta(|\psi\rangle)]]$  to any state  $|\psi\rangle$ , where  $[P(|\psi\rangle)] = 0$  if  $P(|\psi\rangle) = 0$  and  $[P(|\psi\rangle)] = 1$  if  $P(|\psi\rangle) \neq 0$ . The value of  $V[|\psi\rangle]$  is sufficient to distinguish between the different orbits (see [18]). Results are summarized in Table 3.

Orbit Symbols	Representatives $ \psi\rangle$	$V[ \psi\rangle]$
$\mathcal{O}_{VI}$	$ \text{GHZ}_3\rangle$	$[1, 1, 1, 1, 1]$
$\mathcal{O}_V$	$ \text{W}_3\rangle$	$[1, 1, 1, 1, 0]$
$\mathcal{O}_{IV}$	$\frac{1}{\sqrt{2}}( 000\rangle +  110\rangle)$	$[0, 0, 1, 0, 0]$
$\mathcal{O}_{III}$	$\frac{1}{\sqrt{2}}( 000\rangle +  101\rangle)$	$[0, 1, 0, 0, 0]$
$\mathcal{O}_{II}$	$\frac{1}{\sqrt{2}}( 000\rangle +  011\rangle)$	$[1, 0, 0, 0, 0]$
$\mathcal{O}_I$	$ 000\rangle$	$[0, 0, 0, 0, 0]$

**Table 3:** The SLOCC orbits in a 3-qubit system.

For Equation (54) one has  $|\text{GHZ}_3\rangle = X_{21}X_{10}H_0|000\rangle$  (orbit  $\mathcal{O}_V$ ) and it is easy to check that  $\frac{1}{\sqrt{2}}(|000\rangle + |011\rangle) = X_{21}H_1|000\rangle$  (orbit  $\mathcal{O}_{II}$ ),  $\frac{1}{\sqrt{2}}(|000\rangle + |101\rangle) = X_{20}H_0|000\rangle$  (orbit  $\mathcal{O}_{III}$ ), and  $\frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) = X_{10}H_0|000\rangle$  (orbit  $\mathcal{O}_{IV}$ ).

In order to obtain a SLOCC-equivalent to  $|\text{W}_3\rangle$  we see from Table 3 that one has to construct a state  $\psi$  such that  $\Delta(|\psi\rangle) = 0$  and  $C(x_0, x_1, y_0, y_1, z_0, z_1) \neq 0$ . This can be done using only gates of the standard set of universal gates (Figure 2) as explained in Proposition 21 (see Figure 18 for an example of circuit). Note that the construction involves CNOT gates circuits that have matrices of type  $[ijk]$  (described in Subsection 5.3).

**Proposition 21.** *Let  $X_{[ijk]} = X_{ij}X_{ki}X_{jk}$  where  $i, j, k$  are distinct integers in  $\{0, 1, 2\}$  and  $k \neq 2$ . The state*

$$X_{[ijk]}(\text{T} \otimes \text{T} \otimes \text{S})\text{H}^{\otimes 3}|000\rangle \quad (61)$$

*is SLOCC-equivalent to  $|\text{W}_3\rangle$ .*

*Proof.* Let  $q = e^{\frac{i\pi}{4}}$  and let  $|\psi_{(k_0, k_1, \dots, k_7)}\rangle = \frac{1}{\sqrt{8}}(q^{k_0}|000\rangle + q^{k_1}|001\rangle + \dots + q^{k_7}|111\rangle)$  where  $k_i$  is an integer. A simple calculation shows that  $(\text{T} \otimes \text{T} \otimes \text{S})\text{H}^{\otimes 3}|000\rangle = |\psi_{(0, 2, 1, 3, 1, 3, 2, 4)}\rangle$ . Then we compute the values of polynomials  $\Delta$  (Formula (60)) and



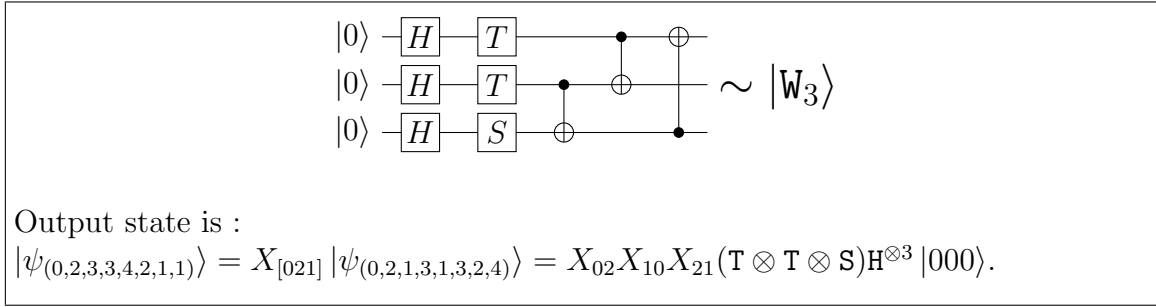
$C$  (Formula (59)) on the state  $|\psi'\rangle = X_{[ijk]} |\psi_{(0,2,1,3,1,3,2,4)}\rangle$  for  $i, j, k \in \{0, 1, 2\}$ . When  $k \neq 2$  we find that  $\Delta = 0$  and  $C \neq 0$  (see results in the table below).

$[ijk]$	$X_{[xyz]}  \psi_{(0,2,1,3,1,3,2,4)}\rangle$	$C(x_0, x_1, y_0, y_1, z_0, z_1)$
[021]	$ \psi_{(0,2,3,3,4,2,1,1)}\rangle$	$\frac{1}{8}((1+i)x_0y_0z_0 + (1+i)x_0y_0z_1 + (1-i)x_1y_0z_0 + (1-i)x_1y_0z_1)$
[120]	$ \psi_{(0,2,1,3,1,3,2,4)}\rangle$	$\frac{1}{8}((1+i)x_0y_0z_0 + (1+i)x_0y_0z_1 + (1-i)x_0y_1z_0 + (1-i)x_0y_1z_1)$
[201]	$ \psi_{(0,4,2,2,3,1,3,1)}\rangle$	$\frac{1}{8}((1+i)x_0y_0z_0 + (1-i)x_0y_0z_1 + (1+i)x_0y_1z_0 + (1-i)x_0y_1z_1)$
[210]	$ \psi_{(0,4,3,1,2,2,3,1)}\rangle$	$\frac{1}{8}((1+i)x_0y_0z_0 + (1-i)x_0y_0z_1 + (1+i)x_1y_0z_0 + (1-i)x_1y_0z_1)$

□

Computing  $\Delta$  and  $C$  for the state  $X_{[ijk]}(\mathbf{T} \otimes \mathbf{T} \otimes \mathbf{S})\mathbf{H}^{\otimes 3} |000\rangle$  when  $k = 2$ , one finds  $\Delta \neq 0$  and  $C \neq 0$ , thus the resulting state is SLOCC-equivalent to  $|\mathbf{GHZ}_3\rangle$ .

As the dimension of the Hilbert space  $\mathcal{H}^{\otimes 3}$  is small, namely  $2^3$ , one can compute three 2-dimensional matrices  $A, B, C$  of determinant 1 and a complex number  $k$  such that  $A \otimes B \otimes C |\psi_{(0,2,3,3,4,2,1,1)}\rangle = k |\mathbf{W}_3\rangle$ . This can be done by solving an eight algebraic equations system. We check that the values  $A = \begin{bmatrix} 3i & 1 \\ \frac{1}{2} & -\frac{1}{2}i \end{bmatrix}$ ,  $B = 2^{\frac{1}{4}} \begin{bmatrix} -i\sqrt{2} & 2 \\ 0 & \frac{1}{2}i \end{bmatrix}$ ,  $C = \begin{bmatrix} i & i \\ \frac{1}{2}i & -\frac{1}{2}i \end{bmatrix}$  and  $k = 2^{\frac{1}{4}} \frac{\sqrt{3}}{\sqrt{2}} e^{\frac{i\pi}{4}}$  are solutions.



**Figure 18:** A circuit of  $c\mathcal{X}_3$  producing a SLOCC-equivalent to  $|\mathbf{W}_3\rangle$ .

### 6.3 The group $c\mathcal{X}_4$ and entanglement of a 4-qubit system

The situation of 4-qubits systems is more complex than for 3-qubits systems. The corresponding Hilbert space  $\mathcal{H}^{\otimes 4}$  has infinitely many orbits under the action of  $\text{SLOCC} = \text{SL}_2(\mathbb{C})^{\times 4}$ . These orbits have been classified by Verstraete *et al.* [33] into 9 families (6 families are described with parameters). Among these 9 families only one is generic : any state in the more general situation belongs to the family

$$G_{abcd} = \frac{a+d}{2} (|0000\rangle + |1111\rangle) + \frac{a-d}{2} (|0011\rangle + |1100\rangle) + \frac{b+c}{2} (|0101\rangle + |1010\rangle) + \frac{b-c}{2} (|0110\rangle + |1001\rangle), \quad (62)$$

for independent parameters  $a, b, c$ , and  $d$  [33, 19].

More precisely, a generic state of 4 qubits is SLOCC-equivalent, up to permutations of the qubits, to 192 Verstraete states of the  $G_{abcd}$  family [20].

To determine the Verstraete family to which a given state belongs, one can use an algorithm described in a previous paper [20]. As is the case of 3 qubits, this

algorithm is based on the evaluation of some covariants polynomials (see Appendix A). We do not recall the algorithm since it is not usefull to understand the present paper.

Let  $|\psi\rangle = \sum_{i,j,k,\ell \in \{0,1\}} \alpha_{ijkl} |ijkl\rangle$  be a 4-qubit state. The algebra of **SL0CC**-invariant polynomials is freely generated by the four following polynomials [25]:

- The smallest degree invariant

$$B := \sum_{0 \leq i_1, i_2, i_3 \leq 1} (-1)^{i_1+i_2+i_3} \alpha_{0i_1i_2i_3} \alpha_{1(1-i_1)(1-i_2)(1-i_3)}, \quad (63)$$

- Two polynomials of degree 4

$$L := \begin{vmatrix} \alpha_{0000} & \alpha_{0010} & \alpha_{0001} & \alpha_{0011} \\ \alpha_{1000} & \alpha_{1010} & \alpha_{1001} & \alpha_{1011} \\ \alpha_{0100} & \alpha_{0110} & \alpha_{0101} & \alpha_{0111} \\ \alpha_{1100} & \alpha_{1110} & \alpha_{1101} & \alpha_{1111} \end{vmatrix} \quad (64)$$

and

$$M := \begin{vmatrix} \alpha_{0000} & \alpha_{0001} & \alpha_{0100} & \alpha_{0101} \\ \alpha_{1000} & \alpha_{1001} & \alpha_{1100} & \alpha_{1101} \\ \alpha_{0010} & \alpha_{0011} & \alpha_{0110} & \alpha_{0111} \\ \alpha_{1010} & \alpha_{1011} & \alpha_{1110} & \alpha_{1111} \end{vmatrix}. \quad (65)$$

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

$$[x_0^2, x_0x_1, x_1^2] B_{xy} \begin{bmatrix} y_0^2 \\ y_0y_1 \\ y_1^2 \end{bmatrix} = \det \left( \frac{\partial^2}{\partial z_i \partial t_j} A \right) \quad (66)$$

with  $A = \sum_{i,j,k,\ell \in \{0,1\}} \alpha_{ijkl} x_i y_j z_k t_\ell$  being the quadrilinear binary form associated to the state  $|\psi\rangle$ .

Using the generators  $B, L, M$  and  $D_{xy}$ , one can build  $\Delta$ , an invariant polynomial of degree 24 that plays an important role in the quantitative and qualitative study of entanglement [28, 26]. As described in [19] and [25],  $\Delta$  is the discriminant of any of the quartics

$$Q_1 = x^4 - 2Bx^3y + (B^2 + 2L + 4M)x^2y^2 + 4(D_{xy} - B(M + \frac{1}{2}L))xy^3 + L^2y^4, \quad (67)$$

$$Q_2 = x^4 - 2Bx^3y + (B^2 - 4L - 2M)x^2y^2 + (4D_{xy} - 2MB)xy^3 + M^2y^4, \quad (68)$$

and

$$Q_3 = x^4 - 2Bx^3y + (B^2 + 2L - 2M)x^2y^2 - (2(L + M)B - 4D_{xy})xy^3 + N^2y^4. \quad (69)$$

We recall that, for a quartic  $Q = \alpha x^4 - 4\beta x^3y + 6\gamma x^2y^2 - 4\delta xy^3 + \omega y^4$ , the discriminant can be computed as

$$\Delta = I_2^3 - 27I_3^2 \quad (70)$$

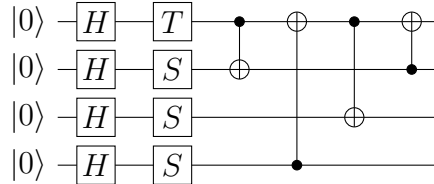
where  $I_2 = \alpha\omega - 4\beta\delta + 3\gamma^2$  and  $I_3 = \alpha\gamma\omega - \alpha\delta^2 - \omega\beta^2 - \gamma^3 + 2\beta\gamma\delta$ .

It appears that  $\Delta$  is the Cayley hyperdeterminant (in the sense of Gelfand *et al.* [12]) of  $A$  [25]. In [26], Miyake showed that the more generic entanglement holds only for the states  $|\psi\rangle$  such that  $\Delta(|\psi\rangle) \neq 0$ . Moreover any generically entangled state is equivalent to a state of the Verstraete  $G_{abcd}$  family [25, Appendix A]. So one can consider  $\Delta$  as a qualitative measure of entanglement : an entangled state (*i.e.* not factorized state) is generically entangled if  $\Delta \neq 0$ .

In the case of 3 qubits,  $\Delta(|\text{GHZ}_3\rangle) \neq 0$  (see Table 3). Using (60) one checks easily that  $\Delta(|\text{GHZ}_3\rangle) = \frac{1}{4}$ . So the state  $|\text{GHZ}_3\rangle$  is generically entangled. In the 4 qubits case one computes  $\Delta(|\text{GHZ}_4\rangle) = 0$  using (70). Hence, suprisingly,  $|\text{GHZ}_4\rangle$  is not generically entangled and this result can be generalized : in [2] Appendix C we proved that, for any  $k > 3$ ,  $\Delta(|\text{GHZ}_k\rangle) = 0$ .

In this context we ask ourselves if it is possible to find a 4-qubit CNOT gates circuit that takes as input a completely factorized state and output a generically entangled state. The following statement answers the question.

**Theorem 22.** *The state  $|BL\rangle := X_{01}X_{20}X_{03}X_{10}(\text{T} \otimes \text{S} \otimes \text{S} \otimes \text{S})\text{H}^{\otimes 4}|0000\rangle$  is generically entangled. It is produced by the circuit :*



*Proof.* Using formula (70) one computes  $\Delta(|BL\rangle) = -\frac{1}{2^{24}} \simeq -5,96 \times 10^{-8}$ .  $\square$

According to Miyake [28], the value of  $|\Delta|$  can be considered as a measure of entanglement. So a state with the most amount of generic entanglement can be defined as a state that maximize  $|\Delta|$ . In the 4-qubits case the maximal value of  $|\Delta|$  is  $\frac{1}{2^{839}} \simeq 1,98 \times 10^{-7}$  [5] and the mean is around  $1.32 \times 10^{-9}$  (value based on 10000 random states [1]). So the amount of generic entanglement in the state  $|BL\rangle$  is not maximal, although much higher than the mean.

A few states are known to maximize  $|\Delta|$  :  $|L\rangle$  [16, 14, 5],  $|HD\rangle$  [1] and  $|M_{2222}\rangle$  (Jaffali, phd thesis). Figure 19 gives the definition of these states. It seems interesting to know if it is possible, starting from a fully factorized state, to reach one of these 3 states by a 4-qubit CNOT gates circuit. To answer this question we proceed as follows. We start from a fully factorized state

$$|F(u)\rangle := (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) \otimes (c_0|0\rangle + c_1|1\rangle) \otimes (d_0|0\rangle + d_1|1\rangle) \quad (71)$$

where  $u := [a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1]$  is a vector of complex numbers. Then, for each circuit  $C$  in  $\mathcal{cX}_4$ , we compute  $C|F(u)\rangle$  and we check that the equation  $C|F(u)\rangle = |\psi\rangle$  where  $|\psi\rangle \in \{|L\rangle, |HD\rangle, |M_{2222}\rangle\}$  has no solution. This can be done in a few seconds using Maple 2020 (X86 64 LINUX). The corresponding script can be downloaded at <https://github.com/mbataille/cnot/entanglement>. Hence the answer to our question is negative.

Note that the question whether a state different from  $|L\rangle$ ,  $|HD\rangle$ , or  $|M_{2222}\rangle$  that has maximal generic entanglement can be produced under the same constraints (*i.e.* factorized state plus 4-qubit **CNOT** gates circuit) remains open, however.

$$|L\rangle = \frac{1}{\sqrt{3}}(|u_0\rangle + \omega |u_1\rangle + \omega^2 |u_2\rangle) \quad (72)$$

with:  $|u_0\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$   
 $|u_1\rangle = \frac{1}{2}(|0000\rangle - |0011\rangle - |1100\rangle + |1111\rangle)$   
 $|u_2\rangle = \frac{1}{2}(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle)$   
 $\omega = e^{\frac{2i\pi}{3}}$

$$|HD\rangle = \frac{1}{\sqrt{6}}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle + \sqrt{2}|1111\rangle). \quad (73)$$

$$|M_{2222}\rangle = \frac{1}{\sqrt{6}}|v_1\rangle + \frac{\sqrt{6}}{4}|v_1\rangle + \frac{1}{\sqrt{2}}|v_3\rangle \quad (74)$$

with:  $|v_1\rangle = \frac{1}{\sqrt{6}}(|0000\rangle + |0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle + |1111\rangle)$   
 $|v_2\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$   
 $|v_3\rangle = \frac{1}{\sqrt{2}}(-|0001\rangle + |0010\rangle - |0100\rangle + |0111\rangle + |1000\rangle - |1011\rangle + |1101\rangle - |1110\rangle)$

**Figure 19:** 4-qubits states for which  $|\Delta|$  is maximal.

We examine now whether it is possible to obtain a **SLOCC**-equivalent to  $|W_4\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$  when a **CNOT** gates circuit acts on a fully factorized state. The **SLOCC**-orbit of  $|W_4\rangle$  belongs to the null cone, which is the algebraic variety defined by the vanishing of all invariants (*i.e.*  $B(|\psi\rangle) = L(|\psi\rangle) = M(|\psi\rangle) = D_{xy}(|\psi\rangle) = 0$ ). The null cone contains 31 **SLOCC**-orbits and the orbit of  $|W_4\rangle$  is characterized, inside the null cone, by the evaluation of a vector of 8 polynomial covariants  $A, P_B, P_C^1, P_C^2, P_D^1, P_D^2, P_F, P_L$  whose definitions have been related to Appendix A (see [19, Section III] for more details). More precisely, one has the following criterion :

**Proposition 23.** *Let  $V_1 := [B, L, M, D_{xy}]$  and  $V_2 := [A, P_B, P_C^1, P_C^2, P_D^1, P_D^2, P_F, P_L]$  then  $|\psi\rangle$  is in the **SLOCC**-orbit of  $|W_4\rangle$  if and only if  $V_1[|\psi\rangle] = [0, 0, 0, 0]$  and  $V_2[|\psi\rangle] = [1, 1, 1, 1, 0, 0, 0, 0]$ .*

The use of this criterion makes it possible to answer our initial question :

**Theorem 24.** *The SLOCC-orbit of  $|W_4\rangle$  cannot be reached when  $c\mathcal{X}_4$  acts on a fully factorized state  $|F(u)\rangle$ .*

*Proof.* We prove that, for any circuit  $C \in c\mathcal{X}_4$ , the state  $|\psi(u)\rangle = C|F(u)\rangle$  cannot be in the SLOCC-orbit of  $|W_4\rangle$ . The algorithm is the following. For each  $C$  in  $c\mathcal{X}_4$  we solve the system  $B(|\psi(u)\rangle) = L(|\psi(u)\rangle) = M(|\psi(u)\rangle) = D_{xy}(|\psi(u)\rangle) = 0$ . The solutions are parametrized vectors  $|\psi_1(u)\rangle, \dots, |\psi_n(u)\rangle$ . Then for each solution  $|\psi_i(u)\rangle$  we solve the system  $P_D^1(|\psi_i(u)\rangle) = P_D^2(|\psi_i(u)\rangle) = P_F(|\psi_i(u)\rangle) = P_L(|\psi_i(u)\rangle) = 0$  and for each solution  $|\psi_{ij}(u)\rangle$  we compute  $P_C^2$ : we check that the polynomial  $P_C^2(|\psi_{ij}(u)\rangle)$  is null for any  $u, C, i, j$ . We deduce from Proposition 23 that  $|\psi(u)\rangle$  is not SLOCC-equivalent to  $|W_4\rangle$ . The Maple script that implements this algorithm can be downloaded at <https://github.com/mbataille/cnot/entanglement> and needs a few hours to be executed. □

## 7 Conclusion and perspectives

The omnipresence and great significance of CNOT gates in quantum computation was our main motivation to better understand the quantum circuits build with these gates. First we described the link between CNOT gates circuits of  $n$  qubits and a classical group, namely  $GL_n(\mathbb{F}_2) = SL_n(\mathbb{F}_2)$ . From there we deduced some simplification rules and applied our results to optimization and reduction problems. In Section 4 we proposed some polynomial heuristics to reduce circuits in the general case and in Section 5 we described a few algorithms to optimize circuits in some special cases. Finally we studied some issues about entanglement and proposed simple constructions to produce some usefull entangled states. Optimization and entanglement are indeed two central topics in QIT since they are related to some important issues on the way to a reliable and functional quantum machine : optimization of circuits for scalable quantum computing and production of entanglement as a physical resource in quantum communication protocols.

As far as we know, a complete study of CNOT gates circuits does not exist yet in the litterature and we hope the results and conjectures contained in this paper will contribute to fill a part of this gap. We believe that the subject is rich and deserves certainly further investigations. In what follows we try to sketch some directions that future works on this subject could take.

Regarding to the optimization problem of CNOT gates circuits, it seems to us that the diversity of situations and methods described in Section 5 tends to show that a polynomial optimization algorithm for the general case, if it ever exists, will be hard to find out. In our opinion, a more realistic and feasible approach should be a mix of heuristics for the general case (as the Gauss-Jordan algorithm or the UTD algorithm described in Section 4) combined with a rich atlas of various methods to optimize or to reduce circuits in special cases (as the atlas we started to built in Section 5). Concerning heuristics in the general case, it is clear that the bound of  $n^2$  gates resulting from the Gauss-Jordan algorithm (Proposition 10) has to be improved by the use of another algorithm, since it is still far from the (probably) optimal linear

bound of  $3(n-1)$  gates given by Conjecture 12. Certainly, a constructive proof of this conjecture would be a big step towards a better understanding of the optimization problem. We will continue to investigate technics of reduction in future works.

The study of the emergence of entanglement in **CNOT** gates circuits done in Section 6 highlights the interest and utility of this tool especially in the case of 3 or 4 qubits systems. When the number of qubits is greater than 4, it would be interesting to know whether it is possible to create generic entanglement as in the 4 qubits case (Theorem 22). Unfortunately, from 5 qubits the hyperdeterminant is too huge to be computed in a suitable form. However its nullity can be tested thanks to its interpretation in terms of solution of a system of equations [12, p. 445] : if

$$A = \sum_{0 \leq i,j,k,l,n \leq 1} \alpha_{ijkln} x_i y_j z_k t_l s_n \text{ is the ground form associated to the five qubits state } |\varphi\rangle = \sum_{0 \leq i,j,k,l,n \leq 1} \alpha_{ijkln} |ijkln\rangle, \text{ the condition } \Delta(|\varphi\rangle) = 0 \text{ means that the system}$$

$$S_\varphi := \{A = \frac{d}{dx_0} A = \frac{d}{dx_1} A = \frac{d}{dy_0} A = \frac{d}{dy_1} A = \dots = \frac{d}{ds_0} A = \frac{d}{ds_1} A = 0\} \quad (75)$$

has a solution  $\hat{x}_0, \hat{x}_1, \hat{y}_0, \hat{y}_1, \dots, \hat{s}_0, \hat{s}_1$  in the variables  $x_0, x_1, y_0, y_1, \dots, s_0, s_1$  such that  $(\hat{x}_0, \hat{x}_1), (\hat{y}_0, \hat{y}_1), \dots, (\hat{s}_0, \hat{s}_1) \neq (0, 0)$ . Such a solution is called non trivial. Hence a possible approach to show that a state  $|\psi\rangle$  is generically entangled when  $n > 4$  is to prove that the corresponding system has no solution apart from the trivial solutions.

## References

- [1] Daniel Alsina. Phd thesis: Multipartite entanglement and quantum algorithms, 2017.
- [2] Marc Bataille and Jean-Gabriel Luque. Quantum circuits of cZ and SWAP gates: optimization and entanglement. *Journal of Physics A: Mathematical and Theoretical*, 52(32):325302, jul 2019.
- [3] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992.
- [4] Arthur Cayley. Mémoire sur les hyperdéterminants. *Journal für die reine und angewandte Mathematik*, 30:1–37, 1846.
- [5] Lin Chen and Dragomir . okovi. Proof of the Gour-Wallach conjecture. *Physical Review A*, 88(4), oct 2013.
- [6] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Physical Review Letters*, 83(3):648651, Jul 1999.
- [7] Ellie D’Hondt and Prakash Panangaden. The computational power of the W and GHZ states, 2004.

- [8] Wolfgang Dür, Guifre Vidal, and Cirac J. Ignacio. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62:062314, 2000.
- [9] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete ? *Physical Review*, Vol. 47, 1935.
- [10] Ekert. Quantum cryptography based on Bell’s theorem. *Physical review letters*, 67 6:661–663, 1991.
- [11] Akira Furusawa, Jens Lykke Sorensen, Samuel L. Braunstein, Christopher A Fuchs, H. Jeff Kimble, and Eugene S. Polzik. Unconditional Quantum Teleportation. *Science*, 282:706, October 1998.
- [12] Israel M Gelfand, Mikhail M. Kapranov, and Zelevinsky Andrei V. *Discriminants, Resultants and Multidimensional Determinant*. Birkhäuser, 1992.
- [13] Gilad Gour and Nolan R. Wallach. Entanglement of subspaces and error-correcting codes. *Physical Review A*, 76(4), Oct 2007.
- [14] Gilad Gour and Nolan R. Wallach. On symmetric SL-invariant polynomials in four qubits, 2012.
- [15] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Bell’s theorem without inequalities. *American Journal of Physics*, 58 (12):1131, 1990.
- [16] A. Higuchi and A. Sudbery. How entangled can two couples get? *Physics Letters A*, 273(4):213 – 217, 2000.
- [17] Mark Hillery, Vladimr Buek, and Andr Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):18291834, Mar 1999.
- [18] 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.
- [19] 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.
- [20] 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.
- [21] John Hopcroft and Robert Tarjan. Algorithm 447: Efficient algorithms for graph manipulation. *Commun. ACM*, 16(6):372378, June 1973.
- [22] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009.
- [23] Alexander Klyachko. Coherent states, entanglement, and geometric invariant theory. arXiv:quant-ph/0206012v1.

- [24] Norbert M. Linke, Dmitri Maslov, Martin Roetteler, Shantanu Debnath, Caroline Figgatt, Kevin A. Landsman, Kenneth Wright, and Monroe Christopher. Experimental comparison of two quantum computing architectures. *Proceedings of the National Academy of Sciences of the United States of America*, 114 (13):3305–3310, March 2017.
- [25] Jean-Gabriel Luque and Jean-Yves Thibon. The polynomial invariants of four qubits. *Phys. Rev. A*, 67:042303, 2003.
- [26] Akimasa Miyake. Classification of multipartite entangled states by multidimensional determinant. *Phys. Rev. A*, 67:012108, 2003.
- [27] Akimasa Miyake. Multipartite entanglement under stochastic local operations and classical communication, 2004.
- [28] Akimasa Miyake and Miki Wadati. Multipartite entanglement and hyperdeterminants. *Quantum Information and Computation*, 2:540–555, 2002.
- [29] 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.
- [30] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel L. Braunstein. Advances in quantum teleportation. *Nature Photonics*, 9:641–652, October 2015.
- [31] Robert Steinberg. *Lectures on Chevalley Groups*. University Lecture Series 66. American Mathematical Society, 2016.
- [32] Lev Vaidman. Teleportation of quantum states. *Physical Review A*, 49:1473–1476, February 1994.
- [33] 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.
- [34] Robert Wilson. *The Finite Simple Groups*. Springer London Ltd, 2009.
- [35] K. Wright, K. M. Beck, S. Debnath, J. M. Amini, Y. Nam, N. Grzesiak, J.-S. Chen, N. C. Pienti, M. Chmielewski, C. Collins, and et al. Benchmarking an 11-qubit quantum computer. *Nature Communications*, 10(1), Nov 2019.
- [36] D. M. Zajac, T. M. Hazard, X. Mi, E. Nielsen, and J. R. Petta. Scalable gate architecture for a one-dimensional array of semiconductor spin qubits. *Phys. Rev. Applied*, 6:054013, Nov 2016.



## A 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 SLOCC-orbit of  $|W_4\rangle$  inside the null cone (Section 6.3). We shall first recall the definition of the transvection of two multi-binary forms on the binary variables  $x^{(1)} = (x_0^{(1)}, x_1^{(1)}), \dots, x^{(p)} = (x_0^{(p)}, x_1^{(p)})$

$$(f, g)_{i_1, \dots, i_p} = \text{tr} \Omega_{x^{(1)}}^{i_1} \dots \Omega_{x^{(p)}}^{i_p} f(x'^{(1)}, \dots, x'^{(p)}) g(x''^{(1)}, \dots, x''^{(p)}), \quad (76)$$

where  $\Omega$  is the Cayley operator

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

and  $\text{tr}$  sends each variables  $x', x''$  on  $x$  (erases ' and "). In [18], 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

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

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

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

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

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

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
$H_{4200}$	$(A, G_{5111})^{1011}$
$H_{4020}$	$(A, G_{5111})^{1101}$
$H_{4002}$	$(A, G_{5111})^{1110}$
$H_{0420}$	$(A, G_{1511})^{1101}$
$H_{0402}$	$(A, G_{1511})^{1110}$
$H_{0042}$	$(A, G_{1151})^{1110}$
$H_{2400}$	$(A, G_{1511}^1)^{0111}$
$H_{2040}$	$(A, G_{1151})^{0111}$
$H_{2004}$	$(A, G_{1115}^1)^{0111}$
$H_{0240}$	$(A, G_{1151})^{1011}$
$H_{0204}$	$(A, G_{1115})^{1011}$
$H_{0024}$	$(A, G_{1115}^1)^{1101}$

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

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

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

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 characterize the  $|\mathbb{W}_4\rangle$  SLOCC-orbit:

$$P_B := B_{2200} + B_{2020} + B_{2002} + B_{0220} + B_{0202} + B_{0022},$$

$$P_C^1 := C_{3111} + C_{1311} + C_{1131} + C_{1113},$$

$$P_C^2 := C_{3111}C_{1311}C_{1131}C_{1113},$$

$$P_D^1 := D_{4000} + D_{0400} + D_{0040} + D_{0004},$$

$$P_D^2 := D_{2200} + D_{2020} + D_{2002} + D_{0220} + D_{0202} + D_{0022},$$

$$P_F := F_{2220}^1 + F_{2202}^1 + F_{2022}^1 + F_{0222}^1,$$

$$P_L := L_{6000} + L_{0600} + L_{0060} + L_{0006}.$$