Quantum Information Processing (2019) 18:133
https://doi.org/10.1007/s11128-019-2249-y

Quantum entanglement involved in Grover's and Shor's algorithms: the four-qubit case

Hamza Jaffali[1] · Frédéric Holweck[2]

Received: 4 December 2018 / Accepted: 11 March 2019

Abstract
In this paper, we study the nature of entanglement in quantum Grover's and Shor's algorithms. So far, the authors who have been interested in this problem have approached the question quantitatively by introducing entanglement measures (numerical ones most of the time). One can ask a different question: What about a qualitative measure of entanglement? In other words, we try to find what are the different entanglement SLOCC classes that can be generated by these two algorithms. We treat in this article the case of pure four-qubit systems.

Keywords Entanglement · Four-qubit systems · Gover's algorithm · Shor's algorithm · Quantum Fourier transform · Periodic states

1 Introduction

Nowadays, quantum computation and quantum information theory are considered as valuable candidates for the future of computer science and information processing. The existence in the literature of quantum algorithms, quantum communication protocols and quantum cryptographic schemes, that outclass their classical counterparts, leads naturally to asking the question of what makes quantum computation so efficient.

One of the possible answers is to look at quantum entanglement. Quantum entanglement is considered as one of the most important resources in quantum computation and quantum information processing. It has been proved that for quantum algorithms, entanglement is necessary to provide speedup [1,2]. The problem of understanding entanglement has interested many scientists over the last 80 years with a scientific

✉ Hamza Jaffali
hamza.jaffali@utbm.fr

Frédéric Holweck
frederic.holweck@utbm.fr

[1] FEMTO-ST/UTBM, Université Bourgogne Franche-Comté, 90010 Belfort Cedex, France

[2] ICB/UTBM, Université Bourgogne Franche-Comté, 90010 Belfort Cedex, France

Published online: 22 March 2019

production going from theoretical interpretation to experimental manipulation of entanglement. Today with the recent development of quantum technologies, it is still an open problem to understand how quantum entanglement appears and evolves in quantum computation.

So far, the authors who have been interested in this problem have most of the time approached the question quantitatively by using entanglement measures [3] (numerical ones most of the time). Majorization theory was also applied to study quantum algorithms [4–6], showing that there is a majorization principle underlying the way quantum algorithms operate (even for every step of the quantum Fourier transform).

In this paper, we investigate quantum entanglement, using tools from algebraic geometry and invariant theory, to give a qualitative description of the quantum states involved in two well-known algorithms. Studying what types of entanglement do or do not appear during the algorithm, and how these types evolve, can be helpful to understand more precisely the role and nature of entanglement in quantum computation.

In our study, we focus on the entanglement of four-qubit states in Grover's and Shor's algorithms. The four-qubit case is interesting because it contains an infinite number of SLOCC orbits, but there is still a classification in terms of families of normal forms. Moreover, with the development of small quantum devices (IBM Quantum Experience), it is nowadays possible to implement famous quantum algorithms, such as Grover's and Shor's, with a limited number of qubits.

The paper is organized as follows. In Sect. 2, we recall the four-qubit classification and related developed tools for classification purposes. In Sect. 3, we focus on Grover's algorithm and present our results for the four-qubit case. In Sect. 4, we study entanglement of periodic states appearing in Shor's algorithm, before and after the application of quantum Fourier transform. In the same section, we also briefly study the influence of QFT on the entanglement of general quantum states. Finally, we discuss our results and present a conclusion in Sect. 5. The main observation raised by our study is that not all SLOCC classes appear and it is reasonable to wonder why some states, like the $|W\rangle$ state, never show up in those examples.

2 Entanglement of four qubits

2.1 Verstraete et al. classification

The Hilbert space of four qubits $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ contains an infinite number of orbits under the action of the SLOCC group $G = \mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C}) \times \mathrm{GL}_2(\mathbb{C})$.

In 2002, Verstraete et al. [7] used an original approach by studying the action of the group $\mathrm{SO}(4) \times \mathrm{SO}(4)$ as a subgroup of $\mathrm{SO}(8)$ and generalizing the singular-value decomposition in matrix analysis to complex orthogonal equivalence classes. They proposed a list of nine normal forms depending on parameters, which, up to permutation of the qubits, permit the parameterization of all SLOCC orbits. This list was corrected in 2006 by Chterental and Djokovic [8], and this one was used for our work (see Table 1).

Table 1 The nine (corrected) Verstraete et al. forms

$G_{abcd} = \frac{a+d}{2}\big(\lvert 0000\rangle+\lvert 1111\rangle\big)+\frac{a-d}{2}\big(\lvert 0011\rangle+\lvert 1100\rangle\big)+\frac{b+c}{2}\big(\lvert 0101\rangle+\lvert 1010\rangle\big)+\frac{b-c}{2}\big(\lvert 0110\rangle+\lvert 1001\rangle\big)$
$L_{abc_2} = \frac{a+b}{2}\big(\lvert 0000\rangle + \lvert 1111\rangle\big) + \frac{a-b}{2}\big(\lvert 0011\rangle + \lvert 1100\rangle\big) + c\big(\lvert 0101\rangle + \lvert 1010\rangle\big) + \lvert 0110\rangle$
$L_{a_2b_2} = a\big(\lvert 0000\rangle + \lvert 1111\rangle\big) + b\big(\lvert 0101\rangle + \lvert 1010\rangle\big) + \lvert 0011\rangle + \lvert 0110\rangle$
$L_{ab_3} = a\big(\lvert 0000\rangle + \lvert 1111\rangle\big) + \frac{a+b}{2}\big(\lvert 0101\rangle + \lvert 1010\rangle\big) + \frac{a-b}{2}\big(\lvert 0110\rangle + \lvert 1001\rangle\big) + \frac{i}{\sqrt{2}}\big(\lvert 0001\rangle + \lvert 0010\rangle - \lvert 0111\rangle - \lvert 1011\rangle\big)$
$L_{a_4} = a\big(\lvert 0000\rangle + \lvert 0101\rangle + \lvert 1010\rangle + \lvert 1111\rangle\big) + i\lvert 0001\rangle + \lvert 0110\rangle - i\lvert 1011\rangle$
$L_{a_2 0_{3\oplus\bar{1}}} = a\big(\lvert 0000\rangle + \lvert 1111\rangle\big) + \lvert 0011\rangle + \lvert 0101\rangle + \lvert 0110\rangle$
$L_{0_{5\oplus\bar{3}}} = \lvert 0000\rangle + \lvert 0101\rangle + \lvert 1000\rangle + \lvert 1110\rangle$
$L_{0_{7\oplus\bar{1}}} = \lvert 0000\rangle + \lvert 1011\rangle + \lvert 1101\rangle + \lvert 1110\rangle$
$L_{0_{3\oplus\bar{1}}0_{3\oplus\bar{1}}} = \lvert 0000\rangle + \lvert 0111\rangle$

2.2 Algebraic geometry and entanglement

Let us denote by $|j_1\rangle \otimes |j_2\rangle \otimes |j_3\rangle \otimes |j_4\rangle$ the standard basis, with $j_i \in [\![0, 1]\!]$, of $\mathcal{H}$. By shortening the basis notation to $|j_1 j_2 j_3 j_4\rangle$, we can write a four-qubit state $|\Psi\rangle$ as:

$$|\Psi\rangle = \sum_{j_1,j_2,j_3,j_4\in[\![0,1]\!]} a_{j_1 j_2 j_3 j_4}\ |j_1 j_2 j_3 j_4\rangle, \tag{1}$$

with $a_{j_1 j_2 j_3 j_4} \in \mathbb{C}$ and $\sum_{j_1,j_2,j_3,j_4} |a_{j_1 j_2 j_3 j_4}|^2 = 1$.

Nonzero scalar multiplication has no incidence on the entanglement nature of $|\Psi\rangle \in \mathcal{H}$. Therefore, we can consider quantum states as points in the projective space $\mathbb{P}(\mathcal{H}) = \mathbb{P}^{15}$. The set of separable states correspond to the set of factorized tensors, i.e., states that can be written $\left|\Psi_{Sep}\right\rangle = |v_1\rangle \otimes |v_2\rangle \otimes |v_3\rangle \otimes |v_4\rangle$, with $v_i = \alpha_i|0\rangle + \beta_i|1\rangle \in \mathbb{C}^2$.

If we look at the projectivization of the set of separable states, we retrieve an algebraic variety called the Segre embedding of the product of four projective lines $\mathbb{P}(\mathbb{C}^2) = \mathbb{P}^1$, defined as the image of the Segre map:

$$Seg : \begin{cases} \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{15} = \mathbb{P}(\mathcal{H}) \\ ([v_1], [v_2], [v_3], [v_4]) \mapsto [v_1 \otimes v_2 \otimes v_3 \otimes v_4] \end{cases}, \tag{2}$$

where $[v_i]$ refers to the projectivization of the vector v_i. When we work over $\mathbb{P}(\mathcal{H})$, the group SLOCC corresponds to $G = \mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})$. The variety of separable states also corresponds to the orbit of highest weight vector, which can be chosen to be $|0000\rangle$, and will be denoted by X such that

$$X = Seg(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1) = \mathbb{P}(G \cdot |0000\rangle)\ . \tag{3}$$

Because X is a G-orbit, auxiliary varieties, built from the knowledge of X, can be used to stratify the ambient space by G-invariant varieties. This idea of using algebraic geometry to describe entanglement classes has been investigated several

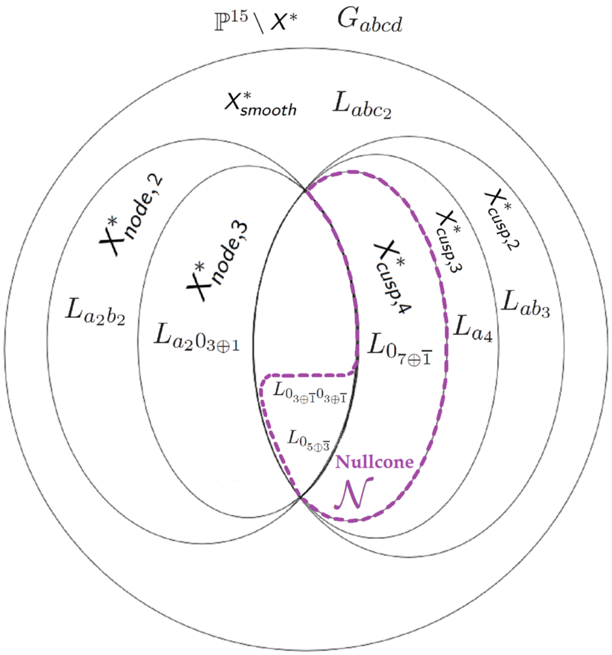

Fig. 1 Onion-like structure of the entanglement in the four-qubit case: The G_{abcd} states do not belong to the dual variety X^* for a, b, c, d generic while states of type L_{abc_2} corresponds to smooth point of X^* for a, b, c generic. The other states are points of the singular locus of X^*. The node components refer to states that corresponds to hyperplane with several points of tangency while the cusp components correspond to states/hyperplanes with one point of tangency of higher order [10]

times in the past 15 years [9–11,15–19]. For instance in [20–22], the dual variety of X was introduced to separate different classes of entanglement. Let us recall the definition of the dual of X,

$$X^* = \overline{\{H \in \mathbb{P}(\mathcal{H}^*), \exists x \in X, T_x X \subset H\}}, \tag{4}$$

where $T_x X$ denotes the tangent space to X at x. The dual variety parameterizes the hyperplanes tangent to X. In the four-qubit case, the defining equation of the dual of X is nothing but the so-called $2 \times 2 \times 2 \times 2$ Cayley Hyperdeterminant [14]. In [10], the correspondence between the singular loci of the $2 \times 2 \times 2 \times 2$ hyperdeterminant and the Verstraete et al.'s normal form was established (Fig. 1). In the next section, we explain the algorithm that we will use to identify the normal form of a given four-qubit state. Geometrically this algorithm allows one to know to which strata of the singular locus of the hyperdeterminant a given state $|\Psi\rangle$ belongs. We also reproduced (Fig. 2) the orbit stratification of the three-qubit classification as we will give illustrative examples regarding this case in Sect. 4.6 and "Appendix B." As pointed out by Miyake [20], the stratification of the orbits in the three-qubit case can also be described in terms of singularities of the $2 \times 2 \times 2$ Cayley hyperdeterminant.

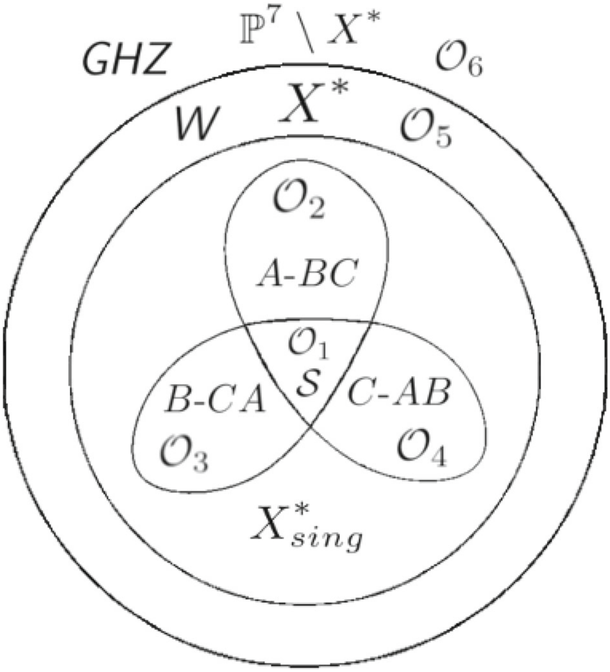

Fig. 2 Onion-like structure of the 3-qubit classification: The number of orbits is finite $\mathcal{O}_1, \ldots, \mathcal{O}_6$ and the closures of each define algebraic varieties. For instance $\overline{\mathcal{O}_6} = \mathbb{P}^7$ and $\overline{\mathcal{O}_5} = X^*$ (see [11])

Remark 2.1 Other auxiliary varieties can be built from the knowledge of $X = Seg(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1)$ that are meaningful in terms of entanglement. Let us mention the secant variety of X, $\sigma(X) = \overline{\cup_{x,y\in X}\mathbb{P}^1_{xy}}$ and the tangential variety $\tau(X) = \cup_{x\in X} T_x X$. When $X = Seg(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1)$, one has $\sigma(X) = \mathbb{P}(\overline{\text{SLOCC}.|\text{GHZ}\rangle_4})$ and $\tau(X) = \mathbb{P}(\overline{\text{SLOCC}.|W_4\rangle})$ where the overline denotes the Zariski closure. See [9–11] for more details about geometric constructions based on auxiliary varieties to describe entanglement.

2.3 Algorithms based on invariants

We now introduce two algorithms based on a family of invariants and covariants that have been proposed in [9,10] to discriminate both the Verstraete et al. families and the states that belong to the nullcone (states that vanish all SLOCC invariant polynomials). These algorithms have also been used recently in [12,13]. Recall that one can associate to each four-qubit state $|\Psi\rangle$ a quadrilinear form A:

$$|\Psi\rangle = \sum_{i,j,k,l\in[\![0,1]\!]} a_{ijkl}\ |ijkl\rangle, \tag{5}$$

$$A = \sum_{i,j,k,l\in[\![0,1]\!]} a_{ijkl} \cdot x_i y_j z_k t_l\ . \tag{6}$$

The ring of invariant polynomials for four qubits can be generated thanks to the four polynomial invariants H, L, M and D_{xy} [14], defined as

$$\begin{aligned}
H &= a_{0000}a_{1111} - a_{1110}a_{0001} - a_{0010}a_{1101} + a_{1100}a_{0011} - a_{0100}a_{1011} \\
&\quad + a_{1010}a_{0101} + a_{0110}a_{1001} - a_{1000}a_{0111}, && (7)\\
L &= \begin{vmatrix} a_{0000} & a_{0010} & a_{0001} & a_{0011} \\ a_{1000} & a_{1010} & a_{1001} & a_{1011} \\ a_{0100} & a_{0110} & a_{0101} & a_{0111} \\ a_{1100} & a_{1110} & a_{1101} & a_{1111} \end{vmatrix}, && (8)\\
M &= \begin{vmatrix} a_{0000} & a_{0001} & a_{0100} & a_{0101} \\ a_{1000} & a_{1001} & a_{1100} & a_{1101} \\ a_{0010} & a_{0011} & a_{0110} & a_{0111} \\ a_{1010} & a_{1011} & a_{1110} & a_{1111} \end{vmatrix}, && (9)\\
N &= -L - M, && (10)\\
b_{xy} &= \det\left(\frac{\partial^2 A}{\partial z_i \partial t_j}\right)_{i,j\in[\![0,1]\!]} = [x_0^2, x_0x_1, x_1^2]\; B_{xy} \begin{bmatrix} y_0^2 \\ y_0y_1 \\ y_1^2 \end{bmatrix}. && (11)
\end{aligned}$$

We determine the 3×3 matrix B_{xy} by retrieving the coefficients in front of the terms $x_ix_jy_ky_l$ with $i, j, k, l \in [\![0, 1]\!]$ in the quadratic form b_{xy}.

$$D_{xy} = -\det(B_{xy}). \tag{12}$$

One also needs to define three quartics, which coefficients are defined using the four-qubit invariants:

$$\begin{aligned}
Q_1(|\Psi\rangle) &= x^4 - 2H \cdot x^3y + (H^2 + 2L + 4M) \cdot x^2y^2 \\
&\quad + (4D_{xy} - 4H(M + \frac{1}{2}L)) \cdot xy^3 + L^2 \cdot y^4, && (13)\\
Q_2(|\Psi\rangle) &= x^4 - 2H \cdot x^3y + (H^2 - 4L - 2M) \cdot x^2y^2 \\
&\quad + (-2MH + 4D_{xy}) \cdot xy^3 + M^2 \cdot y^4, && (14)\\
Q_3(|\Psi\rangle) &= x^4 - 2H \cdot x^3y + (H^2 + 2L - 2M) \cdot x^2y^2 \\
&\quad - (2LH + 2MH - 4D_{xy}) \cdot xy^3 + N^2 \cdot y^4\ . && (15)
\end{aligned}$$

We define also two invariant polynomials of the quartics, I_2 and I_3, as follows:

$$\begin{aligned}
I_2(Q_1) = I_2(Q_2) = I_2(Q_3) &= \frac{4}{3}L^2 - \frac{4}{3}H^2M + \frac{4}{3}LM + \frac{4}{3}M^2 \\
&\quad + 2HD_{xy} + \frac{1}{12}H^4 - \frac{2}{3}H^2L, && (16)\\
I_3(Q_1) = I_3(Q_2) = I_3(Q_3) &= \frac{8}{27}L^3 - \frac{1}{216}H^6 - \frac{8}{27}M^3 - \frac{1}{6}DxyH^3
\end{aligned}$$

$$
\begin{aligned}
&+\frac{4}{3}HMDxy-\frac{5}{9}H^2ML+\frac{2}{3}HLDxy\\
&-\frac{2}{9}H^2L^2-\frac{5}{9}H^2M^2-{D_{xy}}^2+\frac{4}{9}L^2M+\frac{1}{18}H^4L+\frac{1}{9}H^4M-\frac{4}{9}LM^2.
\end{aligned}
\tag{17}
$$

The hyperdeterminant of a four-qubit state $|\Psi\rangle$ can be seen as the discriminant of one of the quartic $\mathrm{Det}_{2222}=\Delta(\mathcal{Q}_i)$, which is equal also to $\mathrm{Det}_{2222}={I_2}^3-27{I_3}^2$. If we want to investigate the nature and multiplicity of the roots of the quartics, we have to use two other covariant polynomials, the Hessian and the Jacobian of the Hessian, defined as follows:

$$
Hess(Q)=\begin{vmatrix}\frac{\partial^2 Q}{\partial x^2} & \frac{\partial^2 Q}{\partial x\partial y}\\ \frac{\partial^2 Q}{\partial y\partial x} & \frac{\partial^2 Q}{\partial y^2}\end{vmatrix}, \tag{18}
$$

$$
T(Q)=\begin{vmatrix}\frac{\partial Q}{\partial x} & \frac{\partial Q}{\partial y}\\ \frac{\partial Hess(Q)}{\partial x} & \frac{\partial Hess(Q)}{\partial y}\end{vmatrix}. \tag{19}
$$

The algorithms presented in [9,10] consider two main cases. The first case is when the state $|\Psi\rangle$ belongs to the nullcone. The nullcone is defined as the set of states which annihilate all invariant polynomials. In practice, we can define the projectivization $\mathcal{N}$ of the nullcone as

$$
\mathcal{N}=\{|\Psi\rangle\in\mathbb{P}(\mathcal{H})\ /\ H(|\Psi\rangle)=L(|\Psi\rangle)=M(|\Psi\rangle)=D_{xy}(|\Psi\rangle)=0\}\,. \tag{20}
$$

The nullcone contains 31 SLOCC orbits. If one allows permutations of the four qubits by the symmetric group $\mathcal{S}_4$, those 31 orbits can be grouped in eight non-equivalent strata of orbits $\mathrm{Gr}_1,\mathrm{Gr}_2,\ldots,\mathrm{Gr}_8$ forming a nested sequence (the orbit closures of the strata Gr_{i+1} containing orbits of Gr_i). In particular, Gr_1 only contains the orbit of separable states.

To distinguish between the different strata of the nullcone, we will use these polynomials defined as the sum or product of covariants:

$$
\begin{aligned}
P_B &= B_{2200}+B_{2020}+B_{2002}+B_{0220}+B_{0202}+B_{0022}, &(21)\\
P_C^1 &= C_{3111}+C_{1311}+C_{1131}+C_{1113}, &(22)\\
P_C^2 &= C_{3111}\cdot C_{1311}\cdot C_{1131}\cdot C_{1113}, &(23)\\
P_D^1 &= D_{4000}+D_{0400}+D_{0040}+D_{0004}, &(24)\\
P_D^2 &= D_{2200}+D_{2020}+D_{2002}+D_{0220}+D_{0202}+D_{0022}, &(25)\\
P_F &= F^1_{2220}+F^1_{2202}+F^1_{2022}+F^1_{0222}, &(26)\\
P_L &= L_{6000}+L_{0600}+L_{0060}+L_{0006}\ . &(27)
\end{aligned}
$$

We can in fact decide to which strata a given form belongs by evaluating the vector V defined in Eq. (28). When the evaluated value is nonzero, we replace the value by ‘1’. The elements in the vector V will thus only take binary values.

$$V = [A, P_B, P_C^1, P_C^2, P_D^1, P_D^2, P_F, P_L]. \tag{28}$$

In Algorithm 1, we reproduce [9] a procedure that takes in input a four-qubit state and the return the corresponding strata in the nullcone, or an error if the state is not nilpotent.

Algorithm 1 NilpotentType [9]

```
Require: $Y$ an array of size 16, the four-qubit state
Ensure: The nullcone type $\mathcal{N}$ of $Y$

if isInNullcone($Y$) then
    vectCov ← $[A, P_B, P_C^1, P_C^2, P_D^1, P_D^2, P_F, P_L]$
    eval ← evaluate(vectCov,$Y$)
    if eval = $[0, 0, 0, 0, 0, 0, 0, 0]$ then
        return $\mathrm{Gr}_0$
    else if eval = $[1, 0, 0, 0, 0, 0, 0, 0]$ then
        return $\mathrm{Gr}_1$
    else if eval = $[1, 1, 0, 0, 0, 0, 0, 0]$ then
        return $\mathrm{Gr}_2$
    else if eval = $[1, 1, 1, 0, 0, 0, 0, 0]$ then
        return $\mathrm{Gr}_3$
    else if eval = $[1, 1, 1, 0, 1, 0, 0, 0]$ then
        return $\mathrm{Gr}_4$
    else if eval = $[1, 1, 1, 1, 0, 0, 0, 0]$ then
        return $\mathrm{Gr}_5$
    else if eval = $[1, 1, 1, 1, 1, 1, 0, 0]$ then
        return $\mathrm{Gr}_6$
    else if eval = $[1, 1, 1, 1, 1, 1, 1, 0]$ then
        return $\mathrm{Gr}_7$
    else if eval = $[1, 1, 1, 1, 1, 1, 1, 1]$ then
        return $\mathrm{Gr}_8$
    end if
else
    return "Y does not belong to the nullcone"
end if
```

If the form is not nilpotent (does not belong to the nullcone), one needs to use other covariants computed in [9] to distinguish the different families. With the notations of [9], these are:

$$\mathcal{L} = L_{6000} + L_{0600} + L_{0060} + L_{0006}, \tag{29}$$

$$\mathcal{K}_5 = K_{5111} + K_{1511} + K_{1151} + K_{1115}, \tag{30}$$

$$\mathcal{K}_3 = K_{3311} + K_{3131} + K_{3113} + K_{1331} + K_{1313} + K_{1133}, \tag{31}$$

$$\mathcal{G} = G^2_{3111} + G^2_{1311} + G^2_{1131} + G^2_{1113}, \tag{32}$$

$$\overline{\mathcal{G}} = G^1_{3111} G^1_{1311} G^1_{1131} G^1_{1113}, \tag{33}$$

$$\mathcal{D} = D_{4000} + D_{0400} + D_{0040} + D_{0004}, \tag{34}$$

$$\mathcal{H} = H_{2220} + H_{2202} + H_{2022} + H_{0222}, \tag{35}$$

$$\mathcal{C} = G^2_{1111}\ . \tag{36}$$

In order to determine the Verstraete et al. type or family of a given state, we will use Algorithm 2 reproduced in "Appendix C." It is based on the roots of the three quartics and their multiplicities and also based on the evaluation of the covariants on the form defined by the state.

3 Entanglement in Grover's algorithm

3.1 Grover's algorithm

In 1996, Lov Grover discovered a quantum algorithm for searching elements in a large and non-ordered database [23] with a complexity of $\mathcal{O}(\sqrt{N})$ request, instead of the classical $\mathcal{O}(\frac{N}{2})$, with N being the database size.

There are four main steps in this algorithm, and they correspond to the following operations : Initialization, Oracle operator, Diffusion operator, Measurement. Depending on the number $|S|$ of searched elements and the size N of the database, the Oracle and Diffusion operators should be repeated several times.

The first register of n-qubits is initialized in the superposed state $|+\rangle^{\otimes n}$; then, depending on the searched elements, the Oracle gate (denoted by $\mathcal{O}$ in Fig. 3) will mark these elements (with a minus sign) and thus modify the state of the first register. Then, we will apply the Diffusion gate, in order to amplify the module of the amplitudes of the searched elements.

In our work, we focus on the different entanglement classes that can be generated by Grover's algorithm, in the four-qubit case. In other words, we want to know what are the different Verstraete et al. families that can be reached, starting from the state $|+\rangle^{\otimes n}$ and applying Oracle/Diffusion gates by varying the number and indices of searched elements in Grover's algorithm.

3.2 Previous work

Grover's algorithm is one of the most famous quantum algorithms in the literature, because it provides better performances for searching elements in a database than what is done in the classical case. It has been proved that entanglement is involved during the steps of the algorithm, but his role and his nature have not yet been fully understood. In fact, Braunstein and Pati was the first to prove in 2000 the presence and the necessity of entanglement in Grover's algorithm [24].

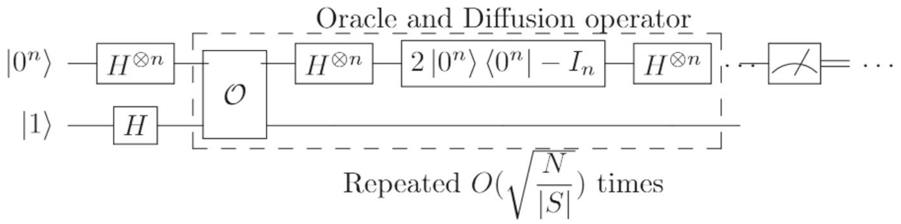
Oracle and Diffusion operator
$|0^n\rangle$
$|1\rangle$
$H^{\otimes n}$
H
$\mathcal{O}$
$H^{\otimes n}$
$2\,|0^n\rangle\langle 0^n| - I_n$
$H^{\otimes n}$
· · ·
Repeated $O(\sqrt{\frac{N}{|S|}})$ times

Fig. 3 Grover's algorithm as a quantum circuit

In 2002, Biham, Nielsen and Osborne [25] introduced an entanglement monotone derived from Grover's algorithm. Given as input a pure quantum state, the authors study the maximization of $P_{\max}$ the probability that the algorithm succeeds, and this, under local unitary operations. This defines an entanglement monotone, and in fact, it defines the well-known Groverian measure of entanglement.

The same year, Forcer et al. [26] examined the roles played by superposition and entanglement in quantum computing. The analysis is illustrated by a discussion on a classical implementation of Grover's algorithm. The absence of multi-particle entanglement leads to exponentially rising resources for implementing such quantum algorithms. They conclude that multi-particle entanglement is the key property of quantum systems that provides the remarkable power of quantum computers.

Biham et al. [27] have analyzed the dynamics of Grover's algorithm while initializing the algorithm with an arbitrary $|\Psi\rangle$ pure state, instead of the $|0\rangle$. The authors showed that the optimal measurement time is the same with both initial states, in the case of the same number of marked elements. Biham et al. generalized the Groverian entanglement measure to the case of several marked elements, previously limited to a single marked state. According to the authors, as long as $r << N$, with r the number of marked elements and N the size of the database, the Groverian measure is independent of r.

In 2004, Orus and Latorre [28] investigated the scaling of entanglement in adiabatic version of Grover's algorithm, precising that the Von Neumann entropy remains a bounded quantity regardless of the size of the system, even at they called the critical point. More precisely, ”the maximum of entropy approaches 1 as a square root in the size of the system, which is the typical Grover scaling factor.”

In 2005, Fang et al. [29] studied the degree of entanglement present in a multi-qubit register during the algorithm process, under the formalism of density matrices. The authors analyzed the variations of the concurrence and Von Neumann entropy for the one- and two-qubit reduced density matrix from an n-qubit register, in terms of the number of iterations, and this for one element marked. With the computed concurrence, they found that it can be related to the probability of success. Besides, they observed that the concurrence reaches a maximum value at approximately half of the optimal number of iterations.

In 2008, Iwai et al. [30] published an article dealing with the measure of entanglement with respect to bipartite partition of n-qubits, defined and studied from the viewpoint of Riemann geometry in a previous work of the first author [31]. This previous work permits to establish the distance between the maximally entangled states and the separable ones. In this work, the authors determine the set of maximally entangled states nearest to a separable state as we can encounter at the beginning of Grover's algorithm. They confirmed the fact that while the initial and the marked elements are separable the algorithm generates a sequence of entangled states.

In 2012, Wen and Cao [32] explored the behaviors of multipartite entanglement in Grover's algorithm by looking at the adiabatic version of the quantum search algorithm. The authors calculated the Von Neumann entropy of all possible bipartite divisions of the system. This led to a new measure of multipartite entanglement, generalizing the measure introduced by Meyer and Wallach in [33]. They showed the existence and the evolution of multipartite entanglement during the process. Besides, similar scaling behaviors were observed in both bipartite and multipartite case (beginning from zero to a maximum value at a critical point, then back to zero again). The symmetry behavior of the entanglement during the adiabatic evolution is also shown.

Rossi et al. [34] studied the scale invariance of entanglement dynamics in Grover's algorithm. They calculated the amount of entanglement of the quantum states generated by Grover's algorithm, through the computational steps. They used for that a numerical measure of entanglement named GME (geometric measure of entanglement). They showed that multipartite entanglement is always present during the algorithm, and studied it in function of the number of iterations of the algorithm, for a fixed number of qubits. They found the maximum of entanglement to be at some remarkable position, using the GME, and this, for specific values of marked elements.

The same year, Chakraborty et al. published a work [35] in the same philosophy as the work of Rossi et al. [34]. The geometric measure of entanglement has been used to quantify and analyze entanglement across iterations of the algorithm. The authors investigated how entanglement varies when the number of qubits and marked elements increases. The first result is that the behavior of the maximum value of entanglement is monotonous with the number of qubits. The second main result is that, for a given number of qubits, a change in marked elements alters the amount of entanglement.

One year later, Rossi et al. came back with another work involving Grover states and hypergraphs [36]. Numerical computation of the GME as a function of the number of qubit was made, when they only considered the first iteration of the algorithm. For different cases under consideration, the curves for one and two marked elements show the same behavior, i.e., an exponential decay. A link between the initial states of the algorithm and hypergraphs is established, giving a more pictorial representation and permitting to highlight some entanglement properties of these states, such as biseparability and the presence of genuine multipartite entanglement.

In 2015, Qu et al. [37] investigated multipartite entanglement by using separable degree as a qualitative measure. On the other hand, they also used a quantitative measure of entanglement introduced by Vidal [43], namely the Schmidt number. These qualitative and quantitative tools permitted to study the entanglement dynamics of Grover's search algorithm. The results, depending on the step in the algorithm, confirm that after first iterations fully entangled states appear in the algorithm.

Recently, in 2016, Ye et al. [38] published a work dealing with the influence of static imperfections on quantum entanglement and quantum discord. They used concurrence to investigate the behavior of entanglement. Static imperfections can break quantum correlations, according to the authors. In fact, for every weak imperfections, the quantum entanglement exhibits periodic behavior, while the periodicity will be destroyed with stronger imperfections. They confirmed therefore the periodic property of entanglement involved in Grover's algorithm.

The same year, in 2016, the authors of the present work, with Ismael Nounouh, investigated the entanglement nature of quantum states generated of Grover's algorithm by means of algebraic geometry [39]. The authors established a link between entanglement of states generated by the algorithm and auxiliary algebraic varieties built from the set of separable states. We were able to propose a qualitative interpretation of the earlier results, such as the work of Rossi et al. [34,36]. Some examples were investigated, such as the three-qubit case.

In 2017, Pan et al. [40] also studied the GME scale invariant property. Starting from the work of Rossi et al. [34], the authors showed that the entanglement dynamics in Grover's algorithm is not always scale invariant. They showed that after the turning point, the GME is not necessarily scale invariant, and then depend on the number n of qubits and the marked elements. Some examples, when the searched elements form separable states, GHZ or W states, were investigated to confirm the proposed results.

In this work, we continue in the same direction as our previous work [39], trying to bring explanation to behaviors observed by the different authors in the domain. More precisely, we study the example of four-qubit case, detailing what types of entanglement can be generated by Grover's algorithm in function of the marked elements and recovering some results established in our previous paper.

3.3 The four-qubit case

We investigate entanglement nature of states involved in Grover's algorithm by varying the marked elements and by determining the corresponding Verstraete et al. family or the nullcone strata. We list below all Verstraete et al. normal forms and the strata of the nullcone reached. $|\mathcal{S}|$ denotes the number of marked elements.

- **Standard regime** ($|\mathcal{S}| < \frac{N}{4}$)**:**
  - For $|\mathcal{S}| = 1$, we always reach the G_{00cc} orbit, as expected.
  - For $|\mathcal{S}| = 2$, the states generated by Grover's algorithm belong to G_{abc0}, L_{00c_2}, L_{ab0_2}, Gr_8 and Gr_4.
  - For $|\mathcal{S}| = 3$, we can obtain the orbits G_{abc0}, L_{00c_2}, L_{aa0_2}, $L_{0_2b_2}$ and $L_{a_20_{3\oplus\bar{1}}}$.
- **Critical case** ($|\mathcal{S}| = \frac{N}{4}$)**:** For $|\mathcal{S}| = 4$, which is the critical case (all amplitudes, except the marked one, are sent to zero, and the algorithm converges after one iteration), we can reach all the states that can be written as a sum of four basis states: G_{00cc}, G_{a000}, G_{ab00}, L_{00c_2}, L_{aa0_2}, L_{a00_2}, $L_{0_2b_2}$, and from Gr_8 to Gr_1.
- **Exceptional case** ($|\mathcal{S}| > \frac{N}{4}$, this is a not the standard case of application of Grover because the number of marked elements is not small compared to N)**:**
  - For $|\mathcal{S}| = 5$, the orbits G_{abc0}, G_{ab00}, L_{00c_2}, L_{aa0_2}, L_{ab0_2}, $L_{a_2b_2}$, $L_{0_2b_2}$ and $L_{a_20_{3\oplus\bar{1}}}$ can be obtained.
  - For $|\mathcal{S}| = 6$, Grover's algorithm can generate states that belong to G_{abcd}, G_{abc0}, G_{ab00}, L_{00c_2}, L_{aa0_2}, L_{ab0_2}, $L_{a_2b_2}$, $L_{0_2b_2}$, L_{a_4}, $L_{a_20_{3\oplus\bar{1}}}$, Gr_8 and Gr_4.
  - For $|\mathcal{S}| = 7$, one can reach the following orbits: G_{abcd}, G_{abc0}, G_{00cc}, G_{ab00}, L_{00c_2}, L_{aa0_2}, L_{ab0_2}, $L_{a_2b_2}$, $L_{0_2b_2}$, $L_{a_20_{3\oplus\bar{1}}}$.
  - For $|\mathcal{S}| = 8$, the generated states belong to G_{abc0}, G_{00cc}, G_{ab00}, L_{00c_2}, L_{aa0_2}, $L_{a_2b_2}$, $L_{0_2b_2}$, $L_{a_20_{3\oplus\bar{1}}}$, Gr_8, Gr_7, Gr_4, Gr_2 and Gr_1.

In the case of one marked element, we always belong to the secant variety $\sigma_2(X)$, which is the equivalence class of the $|GHZ_4\rangle$ state, also know as the set of tensors of rank 2, as it was demonstrated by the authors in [39].

We want to point out that, as it was mentioned in [39], the state $|W_4\rangle$ (which belongs to the Gr_5 orbit) is not reached by the states generated by Grover's algorithm, except in the critical case. The other orbits that are not reached, except in the critical case,

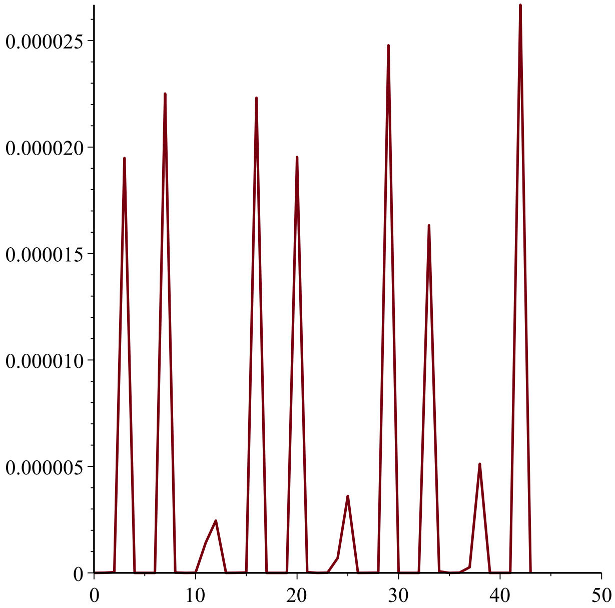

Fig. 4 Evolution of the absolute value of the hyperdeterminant of four qubits in function of the number of iteration of Grover's algorithm, for the set of marked elements $S = \{|0000\rangle, |1111\rangle\}$ (states in G_{abc0})

are Gr_6 and Gr_3. Moreover, we remark that the generic families L_{abc_2} and L_{ab_3} are not reached by states generated by Grover's algorithm, for four qubits. We present in "Appendix A" examples of marked elements generating a given family or orbit.

Besides, if we plot the variation, as a function of k (number of iterations), of the absolute value of the four-qubit hyperdeterminant evaluated on the state $|\Psi_k\rangle$ (the state generated by Grover's algorithm at the kth iteration), one obtains two different curves illustrating the periodicity of the algorithm (Figs. 4, 5). Since this $2 \times 2 \times 2 \times 2$ hyperdeterminant vanishes for states in the dual variety, plotting is only relevant for (sub-)families like G_{abcd} and G_{abc0}.

4 Entanglement in Shor's algorithm

4.1 Shor's algorithm

In 1995, Peter Shor revealed a new quantum algorithm for integer factorization [41]. The particularity of Shor's algorithm is that on a quantum computer, to factor an integer M, it runs in polynomial time. Thus, it can be used to break public-key cryptography schemes such as the widely used RSA scheme.

The algorithm is composed of several steps (pre-processing, order-finding, post-processing), but the only quantum part of the algorithm concerns the order-finding algorithm, so we will only focus on this part.

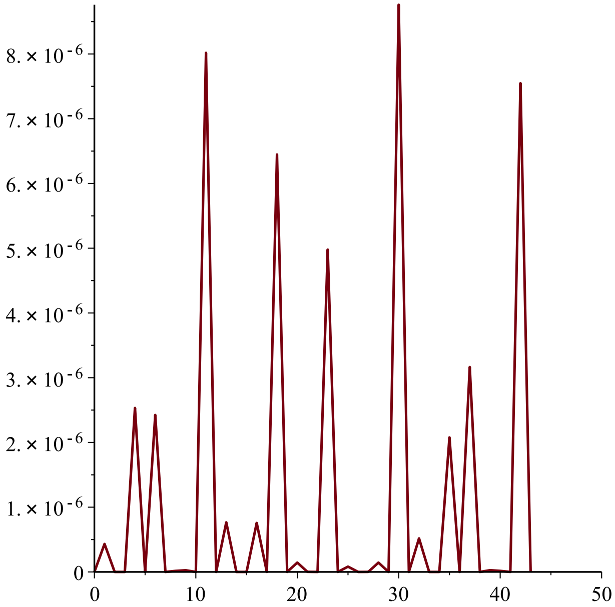

Fig. 5 Evolution of the absolute value of the hyperdeterminant of four qubits in function of the number of iteration of Grover's algorithm, for the set of marked elements $S = \{|0000\rangle, |0001\rangle, |0010\rangle, |0101\rangle, |1010\rangle, |1111\rangle\}$ (states in G_{abcd})

We define a function $f : \mathcal{H}_N \rightarrow \mathcal{H}_N$ with $\mathcal{H}_N = \{|x\rangle / x \in \mathbb{N}, x < N\}$. We say f is periodic of period $r < N$, when :

$$\forall x \in [\![0, N - r - 1]\!], \quad f(|x + r\rangle) = f(|x\rangle). \tag{37}$$

For the period-finding problem, one defines the periodic function f as, $f(|x\rangle) = |a^x \mod M\rangle$, which takes the state $|x\rangle$ in parameter and returns the state $|a^x$ modulo $M\rangle$. One also defines the related quantum gate $U_f : (x, y) \rightarrow (x, y \oplus f(x))$, with x called the data register.

The order-finding algorithm, which can be represented by a quantum circuit (see Fig. 6), is used to determine the order r of a modulo M, i.e., the smallest integer $r \in \mathbb{N}^*$ such as $a^r \equiv 1\ [M]$.

We start by initializing the first register to the parallelized state $|+\rangle^{\otimes n}$ and the second register to the qubit $|0\rangle$. Then, we apply the U_f gate and we make a measure on the second register. By knowing that the function f is periodic, we will retrieve a periodic state for the first register. Finally, we apply the quantum Fourier transform to the first register, in order to extract some information about the period r, and we make a measurement on the first register.

In our work, we focused on the nature of entanglement for the state obtained after applying the U_f gate and measuring the second register (which give us a periodic state), and after applying the quantum Fourier transform to the previous periodic state.

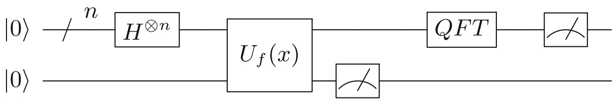

Fig. 6 Quantum circuit of order-finding algorithm

4.2 Previous work

Shor's algorithm is a quantum algorithm that offers an exponential speedup over its classical counterparts.

At the beginning of the 2000s, Jozsa et al. suggested that quantum entanglement is playing a major role in quantum computational efficiency [1,2]. It has been proven in fact that quantum entanglement is involved in Shor's algorithm, theoretically [2,42, 44,45,48] and experimentally [46,47].

Most of the studies related to entanglement, in this algorithm, focused on the entanglement between the two quantum registers. In 2001, Parker and Planio [42] looked at the average bipartite entanglement by using the logarithmic negativity, as a measure of the entanglement, at each stage of the algorithm. The states of the algorithm are defined by the controlled-U_α operations (composing the modulo exponentiation). They proved that entanglement exists in the algorithm and that the amount of entanglement increases toward the end of the algorithm. They also showed that if one tries to reduce the entanglement by introducing more mixing into the control qubit, one reduces the efficiency of the computation.

Two years later, Jozsa and Linden published an article dealing with the role of entanglement in quantum computational speedup [2]. They discussed the difference between classical and quantum computation, and when a quantum computation can be efficiently classically simulated. In particular, it has been proposed that if we cannot efficiently classically simulate a quantum algorithm in polynomial time, then quantum entanglement is involved in this quantum algorithm. It is the case of Shor's algorithm, and the presence of entanglement is proved by considering ”arithmetic progression” states (equivalent to periodic states) and the fact that they are not p-blocked.

In 2004, Orus and Latorre [28] studied the scaling of entanglement in Shor's algorithm, proving analytically that it makes use of an exponentially large amount of entanglement between the two registers after the modular exponentiation step. This implies the impossibility of an efficient classical simulation using the protocol proposed by Vidal in [43].

In 2005, Shimoni et al. used the Groverian measure of entanglement to characterize the quantum states generated by Shor's algorithm [44]. At each step of the QFT process (after each controlled-phase gates, Hadamard gate does not affect entanglement), they evaluate the Groverian measure of entanglement, and this for general quantum states and for periodic states of Shor's algorithm. For random product states, they showed that entanglement remains the same during most of the steps, but for particular controlled-phase gate the amount of entanglement measured by the Groverian measure increases significantly. For periodic states, it was found that the Groverian measure of entanglement does not change essentially, and the changes that we can encounter for small number n of qubits vanish exponentially with n.

Kendon and Munro published in 2006 an article ”Entanglement and its role in Shor’s algorithm” [45] where they investigate the entanglement involved in Shor’s algorithm by decomposing the U_f gate and considering the QFT^{-1} as a single gate. They focused first on the entanglement between the first and second register and then studied the entanglement involved in the first register. A quantitative study of entanglement is done in this paper, and some measures of entanglement like entropy of subsystems (between the two registers), negativity and entanglement of formation (within the first register) are used. According to the authors, after the modular exponentiation, the entanglement between the two registers cannot decrease during the QFT^{-1}. Furthermore, ”entanglement within the upper register can only be generated or shifted around, not decreased.” The authors also pointed out that the closer the period r is to a power of 2, the smaller the value of the difference in the average entropy ΔE_1 before and after the QFT^{-1}. When r is a power of 2, the QFT^{-1} is exact giving $\Delta E_1 = 0$ in all cases.

In 2007, some experimentations of Shor’s algorithm were implemented. Lanyon et al. [46] implemented a compiled version of Shor’s algorithm by using a photonic system. They proved the existence of entanglement within the algorithm via quantum state and process tomography, and that entanglement is involved in the arithmetic calculations. The same year, Lu et al. [47] implemented Shor’s factoring algorithm also using photonic qubits. The experimentation was made with four photonic qubits, and they detected genuine multi-particle entanglement during the algorithm (between the first and second register).

Three years later, Most, Shimoni and Biham published a work [48] related to entanglement of periodic states, the quantum Fourier transform and Shor’s algorithm. They pointed out the importance and role of the periodic states during the algorithm. They also analyzed the entanglement of periodic states, involved in Shor’s algorithm, and they looked at how these states are affected by the quantum Fourier transform. Some approximations were used in order to evaluate the Groverian measure of entangled periodic states. According to the authors, the QFT does not change the entanglement of periodic states, for a sufficiently large number of qubits.

All these studies have investigated the entanglement by using entanglement measure, and more precisely a quantitative analysis of the entanglement. It permitted to give a first idea about how entanglement can evaluate during the algorithm. Here, we focus on the periodic states and states after QFT.

4.3 Entanglement of periodic states

In Shor’s algorithm, the periodic states $\left|\Psi^n_{l,r}\right\rangle$ of n-qubits, with shift l and period r, that we can encounter after measuring the upper register, can be written as:

$$\left|\Psi^n_{l,r}\right\rangle = \frac{1}{\sqrt{A}} \sum_{i=0}^{A-1} |l + ir\rangle, \quad \text{with } A = \left\lceil \frac{N-l}{r} \right\rceil, \quad N = 2^n. \tag{38}$$

For example, for the periodic three-qubit states, with shift $l = 3$ and period $r = 2$, we have $A = \lceil \frac{8-3}{2} \rceil = 3$ basis elements, so :

$$\left|\Psi^3_{3,2}\right\rangle = \frac{1}{\sqrt{3}}\big(|3\rangle + |5\rangle + |7\rangle\big) = \frac{1}{\sqrt{3}}\big(|011\rangle + |101\rangle + |111\rangle\big)\,. \tag{39}$$

For every $(l, r) \in [\![0, 15]\!] \times [\![1, 15]\!]$, we write the periodic state and compute the corresponding Verstraete family. All the results are given in Table 2.

From the results presented in this table, we can extract the following properties for four-qubit periodic states:

- When $l = 0$ and the period take the values $r = 1$, $r = 2$, $r = 4$ and $r = 8$, the state is a separable state,
- When $r = 8$, the state always belongs to the Gr_1 orbit (separable),
- All the states on the anti-diagonal starting from $\{l = 1, r = 15\}$ to $\{l = 15, r = 1\}$, and all at the bottom right (under) this anti-diagonal belong to the Gr_1 orbit (separable),
- If the period takes the values $r = 1$, $r = 2$, $r = 4$ and $r = 8$, and if the shift $0 \leq l \leq r - 1$ or $\frac{N}{2} \leq l \leq \frac{N}{2} + r - 1$, then the state is a separable state,
- When $\{l = 1, r = 1\}$, $\{l = 7, r = 1\}$, and when $\{l = 0, r = 15\}$, $\{l = 1, r = 13\}$, $\{l = 2, r = 11\}$, $\{l = 3, r = 9\}$ and $\{l = 4, r = 7\}$ (almost half of an anti-diagonal) the periodic states belong to the G_{00cc} orbit, which is the orbit of $|GHZ_4\rangle$.

These observations lead us to try a generalization of these properties for any n-qubit periodic state.

Proposition 4.1 *Let $\left|\Psi^n_{l,r}\right\rangle$ be a n-qubit periodic state. If the shift $l = 0$ and the period $r = 2^s$ divide $N = 2^n$, then $\left|\Psi^n_{0,r}\right\rangle$ is a separable state, and it can be written $\left|\Psi^n_{0,r}\right\rangle = |+\rangle^{\otimes(n-s)} \otimes |0\rangle^{\otimes s}$.*

Proof Let $\left|\Psi^n_{l,r}\right\rangle$ be a n-qubit periodic state, and let $N = 2^n$. We suppose that the shift $l = 0$ and the period divide N. So there exist p such that $r \times p = N$, and thus, there exist $(s, q) \in \mathbb{N}^2$ such that $r = 2^s$ and $p = 2^q$. We recall that $\left|\Psi^n_{0,r}\right\rangle$ can be expressed as:

$$\left|\Psi^n_{0,r}\right\rangle = \frac{1}{\sqrt{A}}\sum_{i=0}^{A-1}|0 + ir\rangle, \quad \text{with } A = \left\lceil \frac{N-0}{r} \right\rceil = p, \tag{40}$$

so

$$\left|\Psi^n_{0,r}\right\rangle = \frac{1}{\sqrt{p}}\big(|0\rangle + |r\rangle + |2r\rangle + \cdots + |(p-1)r\rangle\big). \tag{41}$$

When the period r is equal to N, we have $A = \lceil \frac{N-0}{r} \rceil = 1$ basis state in the writing of $\left|\Psi^n_{0,r}\right\rangle$, which is $|0\ldots0\rangle$ in the binary notation. So the state is separable and we have $\left|\Psi^n_{0,r}\right\rangle = |+\rangle^{\otimes(n-n)} \otimes |0\rangle^{\otimes n} = |0\rangle^{\otimes n}$. Besides, if the period r is equal to one, then we have all the $A = \lceil \frac{N-0}{r} \rceil = N$ basis states in the decomposition of the periodic state, so we get in fact the fully superposed state as expected : $\left|\Psi^n_{0,r}\right\rangle = |+\rangle^{\otimes(n-0)} \otimes |0\rangle^{\otimes 0} = |+\rangle^{\otimes n}$.

Table 2 Verstraete et al. families of periodic states depending on their shift l and period r

r	l															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Gr_1	G_{00cc}	Gr_4	L_{00c_2}	Gr_2	L_{00c_2}	Gr_4	G_{00cc}	Gr_1	Gr_4	Gr_2	Gr_4	Gr_1	Gr_2	Gr_1	Gr_1
2	Gr_1	Gr_1	Gr_4	Gr_4	Gr_2	Gr_2	Gr_4	Gr_4	Gr_1	Gr_1	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1
3	$G_{aa(-2a)0}$	G_{abc0}	G_{abc0}	L_{a00_2}	Gr_8	Gr_8	L_{aa0_2}	Gr_6	Gr_3	Gr_3	Gr_4	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1
4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
5	G_{a000}	Gr_6	Gr_6	Gr_6	Gr_6	L_{aa0_2}	Gr_4	Gr_4	Gr_2	Gr_4	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
6	Gr_3	Gr_3	Gr_3	Gr_3	Gr_4	Gr_4	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
7	Gr_6	Gr_6	Gr_4	Gr_2	G_{00cc}	Gr_2	Gr_4	Gr_2	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
8	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
9	Gr_2	Gr_4	Gr_2	G_{00cc}	Gr_2	Gr_4	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
10	Gr_2	Gr_2	Gr_4	Gr_4	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
11	Gr_4	Gr_4	G_{00cc}	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
12	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
13	Gr_4	G_{00cc}	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
14	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
15	G_{00cc}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1

Now we consider the case when $1 < r < N$, i.e., when $2 \leq r \leq \frac{N}{2}$. The periodic state is a sum of p basis state, and p is even, so we can always split the periodic state into two parts :

$$\left|\Psi^n_{0,r}\right\rangle = \frac{1}{\sqrt{p}}\big(\underbrace{|0\rangle + |r\rangle + |2r\rangle + \cdots + \left|(\tfrac{p}{2}-1)r\right\rangle}_{\frac{p}{2}\text{ terms}} + \underbrace{\left|\tfrac{p}{2}r\right\rangle + \cdots + |(p-1)r\rangle}_{\frac{p}{2}\text{ terms}}\big)\,. \tag{42}$$

We can easily see that we always have the $|0\rangle$ and $\left|\frac{p}{2}r\right\rangle = \left|\frac{N}{2}\right\rangle$ states in the parts of the periodic state, and these basis states can be written in binary notation $|00\ldots0\rangle$ and $|10\ldots0\rangle$. Then, depending on the period r we will have other terms or not in each part, but we can always rewrite the periodic state as follows:

$$\begin{aligned}\left|\Psi^n_{0,r}\right\rangle = \frac{1}{\sqrt{p}}\big(&\underbrace{|0\rangle + |r\rangle + |2r\rangle + \cdots + \left|(\tfrac{p}{2}-1)r\right\rangle}_{\frac{p}{2}\text{ terms}} \\ &+ \underbrace{\left|\frac{N}{2}+0\right\rangle + \left|\frac{N}{2}+r\right\rangle + \left|\frac{N}{2}+2r\right\rangle + \cdots + \left|\frac{N}{2}+(\tfrac{p}{2}-1)r\right\rangle}_{\frac{p}{2}\text{ terms}}\big)\,.\end{aligned} \tag{43}$$

Therefore, the periodic state can be expressed as:

$$\left|\Psi^n_{0,r}\right\rangle = |+\rangle \otimes \frac{1}{\sqrt{2^{q-1}}}\Big(|0\rangle + |r\rangle + |2r\rangle + \cdots + \left|(\tfrac{p}{2}-1)r\right\rangle\Big) = |+\rangle \otimes \left|\Psi^{n-1}_{0,r}\right\rangle. \tag{44}$$

Now if we consider the state $\left|\Psi^{n-1}_{0,r}\right\rangle$, we can repeat the same process until it remains only one state in the sum decomposition of the periodic state. This happens when $A = 1$, so when the number of qubit of the periodic state considered (at the right side of the tensor product in Eq. (44)) is equal to s. So this process is repeated $q = n - s$ times, and at the end, we retrieve a separable state:

$$\left|\Psi^n_{0,r}\right\rangle = |+\rangle^{\otimes(n-s)} \otimes |0\rangle^{\otimes s}\,. \tag{45}$$

□

Proposition 4.2 *Let $\left|\Psi^n_{l,r}\right\rangle$ be a n-qubit periodic state. If the period r is equal to $\frac{N}{2} = 2^{n-1}$, then, for all possible values of the shift l, $\left|\Psi^n_{l,r}\right\rangle$ is a separable state.*

Proof Let $\left|\Psi^n_{l,r}\right\rangle$ be a n-qubit periodic state, and let $N = 2^n$. We suppose that the period r is equal to $\frac{N}{2}$. The periodic state will contain only $A = \left\lceil \frac{N-l}{\frac{N}{2}} \right\rceil$ basis states. If the shift satisfies $0 \leq l < \frac{N}{2}$, then we will have $A = 2$ elements; otherwise, if $\frac{N}{2} \leq l < N$, then we will only have $A = 1$.

In the second case, the only element in the periodic state will be $|l\rangle$ and then it is clear that the periodic state is a separable state. In the first case, we can rewrite the periodic state as:

$$\left|\Psi^n_{l,\frac{N}{2}}\right\rangle = \frac{1}{\sqrt{2}}\left(|l\rangle + \left|l + \frac{N}{2}\right\rangle\right) = |+\rangle \otimes |l\rangle, \tag{46}$$

which is also a separable state. □

Proposition 4.3 *Let $\left|\Psi^n_{l,r}\right\rangle$ be a n-qubit periodic state with shift l and period r, and let $N = 2^n$. If $l + r \geq N$, then $\left|\Psi^n_{l,r}\right\rangle$ is separable.*

Proof Because $l + r \geq N \iff 1 \geq \frac{N-l}{r}$, one knows that the number of basis states to express $\left|\Psi^n_{l,r}\right\rangle$ will be equal to $A = \lceil \frac{N-l}{r} \rceil = 1$, and thus, the state is separable.

Proposition 4.4 *Let $\left|\Psi^n_{l,r}\right\rangle$ be a n-qubit periodic state. If the period $r = 2^s$ divides $N = 2^n$, then for all values of the shift respectively $l \in [\![0, 2^s - 1]\!]$ or $l \in [\![\frac{N}{2}, \frac{N}{2} + 2^s - 1]\!]$, the state $\left|\Psi^n_{l,2^s}\right\rangle$ is a separable state, and it can be written, respectively, $\left|\Psi^n_{l,2^s}\right\rangle = |+\rangle^{\otimes(n-s)} \otimes |l\rangle^{[s]}$ or $\left|\Psi^n_{l,2^s}\right\rangle = |1\rangle \otimes |+\rangle^{\otimes(n-s-1)} \otimes |l\rangle^{[s]}$ (with $|l\rangle^{[s]}$ the state $|l\rangle$ written in binary notation with s bits).*

Proof Let $\left|\Psi^n_{l,r}\right\rangle$ be a n-qubit periodic state, and let $N = 2^n$. We suppose that the period divides N. So there exists p such that $r \times p = N$, and thus, there exists $(s, q) \in \mathbb{N}^2$ such that $r = 2^s$ and $p = 2^q$, and so r is a power of 2.

Therefore, the binary writing of r is composed by a unique digit '1' and $n-1$ digits '0.' We know that $r = 2^s$ that this '1' is at the sth position. Then, all multiples of r, which are sum of the same binary number r, can be written with '0' and '1' at the left of the sth bit and with only '0' bits at the right of the sth bit (if we assume that the most significant bit is at the left).

We focus first on the case $l \in [\![0, 2^s - 1]\!]$. By assuming that the shift satisfies $0 \leq l < r = 2^s$, one can determine that the number of terms in the writing of $\left|\Psi^n_{l,r}\right\rangle$ is always $A = \lceil \frac{N-l}{r} \rceil = p = 2^q$, and the periodic state can be written:

$$\left|\Psi^n_{l,r}\right\rangle = \frac{1}{\sqrt{p}}\left(|l\rangle + |l + r\rangle + |l + 2r\rangle + \cdots + |l + (p-1)r\rangle\right). \tag{47}$$

By knowing that $l < r$, and that r and all its multiples contain only '0' bits at the right of sth bit '1' in the binary notation of r, we know that we can factorize, by the binary notation of l in s bits, the sum of basis states defining $\left|\Psi^n_{l,r}\right\rangle$. Then, it will remove the s less significant bits in the binary writing of r and its multiples, and this leads us to the following expression:

$$\left|\Psi_{l,r}^{n}\right\rangle = \frac{1}{\sqrt{p}}\big(|0\rangle + |1\rangle + |2\rangle + \cdots + |(p-1)\rangle\big)^{[n-s]} \otimes |l\rangle^{[s]}. \tag{48}$$

The left factor of this tensor product is in fact the $|+\rangle^{\otimes(n-s)}$ state, and we can conclude that if r divides N, and $l \in [\![0, 2^s - 1]\!]$, then we retrieve a separable state of the form:

$$\left|\Psi_{l,r}^{n}\right\rangle = |+\rangle^{\otimes(n-s)} \otimes |l\rangle^{[s]} . \tag{49}$$

We focus now on the second case, i.e., when $l \in [\![\frac{N}{2}, \frac{N}{2} + 2^s - 1]\!]$, which is similar to the first one, except that we add $\frac{N}{2}$ to the shift. However, we know that $\frac{N}{2}$ is also a power of 2, and in our case, it corresponds to the state $|10\ldots0\rangle$ in binary notation, when we work with n bits. So this '1' bit will be present in every basis state composing the periodic state, and then, we can define $l' = l - \frac{N}{2}$:

$$\left|\Psi_{l,r}^{n}\right\rangle = \frac{1}{\sqrt{\frac{p}{2}}}\Big(|l\rangle + |l+r\rangle + |l+2r\rangle + \cdots + \Big|l + \big(\tfrac{p}{2} - 1\big)r\Big\rangle\Big), \tag{50}$$

$$\left|\Psi_{l,r}^{n}\right\rangle = \frac{1}{\sqrt{\frac{p}{2}}}\ |1\rangle \otimes \Big(\big|l'\big\rangle + \big|l'+r\big\rangle + \big|l'+2r\big\rangle + \cdots + \Big|l' + \big(\tfrac{p}{2} - 1\big)r\Big\rangle\Big). \tag{51}$$

The right factor of the tensor product, with the normalization factor $\frac{1}{\sqrt{\frac{p}{2}}}$, is in fact a periodic state with shift $l' \in [\![0, 2^s - 1]\!]$, and a period $r = 2^s$ for $(n-1)$-qubits. So by using results of the first case, we conclude that the state is separable, and we can express the whole state $\left|\Psi_{l,r}^{n}\right\rangle$ as:

$$\left|\Psi_{l,r}^{n}\right\rangle = |1\rangle \otimes |+\rangle^{\otimes(n-s-1)} \otimes \left|l - \frac{N}{2}\right\rangle^{[s]} . \tag{52}$$

□

Proposition 4.5 *Let $\left|\Psi_{l,r}^{n}\right\rangle$ be a n-qubit periodic state with shift l and period r, and let $N = 2^n$. Then, there is at least $\left\lfloor \frac{N-2}{3} \right\rfloor + 3$ pairs (l, r) that define periodic states SLOCC equivalents to $|GHZ_n\rangle$, and we can separate the following three cases:*

- *the case $l = 1$ and $r = 1$,*
- *the case $l = \frac{N}{2} - 1$ and $r = 1$,*
- *and the $\left\lfloor \frac{N-2}{3} \right\rfloor + 1$ other cases in the anti-diagonal defined by the relation $2l + r = N - 1$.*

Proof Let $\left|\Psi_{l,r}^{n}\right\rangle$ be a n-qubit periodic state, and let $N = 2^n$.

In the first case, if the shift is $l = 1$, and the period $r = 1$, we obtain the periodic state:

$$\left|\Psi_{1,1}^{n}\right\rangle = \frac{1}{\sqrt{N-1}} \sum_{x=1}^{N-1} |x\rangle = \frac{\sqrt{N}}{\sqrt{N-1}} |+\rangle^{\otimes n} - \frac{1}{\sqrt{N-1}} |0\rangle^{\otimes n} . \tag{53}$$

This state is a (generic) rank 2 tensor, which belongs to the smooth points of the secant variety, and in particular is SLOCC equivalent to $|GHZ_n\rangle$.

In the second case, if the shift is $l = \frac{N}{2} - 1$, and the period $r = 1$, by remarking that $\left|\frac{N}{2}\right\rangle = |10\ldots0\rangle$ and then $\left|\frac{N}{2} - 1\right\rangle = |01\ldots1\rangle$, we obtain the periodic state

$$\left|\Psi_{\frac{N}{2}-1,1}^{n}\right\rangle = \frac{1}{\sqrt{\frac{N}{2}+1}} \sum_{x=\frac{N}{2}-1}^{N-1} |x\rangle = \frac{1}{\sqrt{\frac{N}{2}+1}} \Big(|011\ldots1\rangle + |100\ldots0\rangle + |10\ldots01\rangle + \cdots + |111\ldots1\rangle\Big), \tag{54}$$

that can be also expressed as

$$\left|\Psi_{\frac{N}{2}-1,1}^{n}\right\rangle = \frac{1}{\sqrt{\frac{N}{2}+1}} \left(|011\ldots1\rangle + \sqrt{\frac{N}{2}} |1\rangle \otimes |+\rangle^{\otimes n-1}\right), \tag{55}$$

and this state is a also SLOCC equivalent to $|GHZ_n\rangle$.

For the third case, we should focus on the particular anti-diagonal starting from the "point" $\{l = 0, r = N-1\}$ and then moving to the top right, by adding one to l and removing two to r. This anti-diagonal is then defined by the following equations

$$\begin{cases} l = k \\ r = N - 1 - 2k \end{cases} \quad \text{with } k \in \left[\!\left[0, \frac{N}{2} - 1 \right]\!\right] . \tag{56}$$

We proved that the top-right point of the anti-diagonal $\{l = \frac{N}{2} - 1, r = 1\}$ is SLOCC equivalent to $|GHZ_n\rangle$, and we can easily prove that the bottom-left point of the anti-diagonal $\{l = 0, r = N - 1\}$ is in fact the definition of the generalized $|GHZ_n\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\big)$ state. The interesting part is to determine what is happening in the middle of the anti-diagonal.

In fact, we can deduce from the anti-diagonal equations that $2l + r = N - 1$. Besides, we know that the bottom-left point $\{l = 0, r = N - 1\}$ has only two basis states in its writing. Thus, we can remark that if a periodic state has only two basis states in its writing and if it satisfies the anti-diagonal condition $2l + r = N - 1$, then state is SLOCC equivalent to the $|GHZ_n\rangle$ state. In fact, this periodic state, let us call it $|\Psi\rangle$, that has only two basis states will be expressed as

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|l\rangle + |l + r\rangle\big). \tag{57}$$

But we also know that the shift l and the period r of this state satisfy the condition $2l + r = l + (l + r) = N - 1$. So if we work with binary notations, and by knowing that $N - 1 = 2^n - 1$ is always written with only '1' digits in its binary notation, we can conclude that the two binary numbers l and $l + r$ are complementary with respect to $N = 2^n$. Consequently, the state $|\Psi\rangle$ is by definition an equivalent state of $|GHZ_n\rangle$.

How many states are satisfying these conditions for periodic states? In order to determine that, we focus on the condition regarding the number of basis states in the periodic states. So we need that $A = \left\lceil \frac{N-l}{r} \right\rceil = 2$, so it is equivalent to the in equation

$$1 < \frac{N-l}{r} \leq 2. \tag{58}$$

If we substitute now l and r by the equations defining the anti-diagonal, we have

$$1 < \frac{N-k}{N-1-2k} \leq 2. \tag{59}$$

If we solve this in equation in k and forget about the ceiling operation, we retrieve the result

$$-1 < k \leq \frac{N-2}{3}. \tag{60}$$

If we come back to integer numbers, then we proved that if $k \in [\![0, \left\lfloor \frac{N-2}{3} \right\rfloor]\!]$ the periodic state defined by $l = k$ and $r = N - 1 - 2k$ has only two basis states in its writing.

So, the number of states equivalent to $|GHZ_n\rangle$ on the anti-diagonal is equal to $\left\lfloor \frac{N-2}{3} \right\rfloor + 1$, without counting the $\{l = \frac{N}{2} - 1, r = 1\}$ case. In other words, from $\{l = 0, r = N - 1\}$ to $\{l = \left\lfloor \frac{N-2}{3} \right\rfloor, r = N - 1 - 2\left\lfloor \frac{N-2}{3} \right\rfloor\}$, all the states on the anti-diagonal are SLOCC equivalent to $|GHZ_n\rangle$. □

In this subsection, we were able to study entanglement of periodic states from a qualitative point of view. These states, which are involved in Shor's algorithm after the measurement step, show some entanglement properties that depend on the shift and the period of the considered periodic state. Indeed, we were able to point out some "rules" permitting to simplify the identification of the entanglement type of a given periodic state defined by his shift l and period r. In the next subsection, we try to continue this work by considering periodic states after the application of the quantum Fourier transform, which is in fact the next step of Shor's algorithm.

4.4 Entanglement of periodic states after QFT

In this subsection, we investigate the entanglement of periodic states after the application of the quantum Fourier transform for four-qubit systems, and we try to generalize some results for n-qubit periodic states.

From the results presented in Table 3, as we did for the case before the QFT, we can extract the following properties for four-qubit periodic states after the quantum Fourier transform:

Table 3 Verstraete et al. families of the resulting states after applying the QFT on periodic states depending on their shift l and period r

r	l															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Gr_1	G_{00cc}	G_{abc0}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	$L_{a_20_{3\oplus\bar{1}}}$	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	$L_{a_20_{3\oplus\bar{1}}}$	L_{00c_2}	Gr_1
2	Gr_1	Gr_1	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_1	Gr_1
3	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1
4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_2	Gr_2	Gr_2	Gr_2	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1
5	G_{abcd}	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
6	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
7	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
8	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
9	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
10	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
11	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
12	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
13	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
14	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
15	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1

- When $r = 8$, the state always belongs to the Gr_1 orbit (separable),
- For all the states that have the shift l and period r satisfying $l + r \geq N$ (i.e., we are on or under the anti-diagonal from $\{l = 1, r = 15\}$ and $\{l = 15, r = 1\}$), they belong to the Gr_1 orbit of the nullcone and thus are separable states,
- If the period takes the values $r = 1$, $r = 2$, $r = 4$ and $r = 8$, and if the shift $0 \leq l \leq r - 1$, then the state is a separable state,
- If the period takes the values $r = 1$, $r = 2$ and $r = 4$, and if the shift $\frac{N}{2} \leq l \leq \frac{N}{2} + r - 1$, then the state is not a separable state,
- If the period is equal to $r = 2$, then if the shift $2 \leq l \leq N - 3$, then the state belongs to the Gr_4 orbit and thus is not a separable state.

We were not able, as it was the case for periodic states before the QFT, to generalize all these observations to the general n-qubit case. Most of these behaviors were observed for both three-qubit (see "Appendix B") and four-qubit case, but such a table cannot be constructed for the case of five qubits as there is no known SLOCC classification.

We were able, however, to propose one result with respect to periodic states after QFT that are separable, and we use for that a basic property of the quantum Fourier transform:

Proposition 4.6 *Let $\left|\Psi^n_{l,r}\right\rangle$ be a n-qubit periodic state with shift l and period r, and let $N = 2^n$. Then, after the application of the QFT, all the states on and under the anti-diagonal, defined from the cell $\{l = 1, r = N - 1\}$ to $\{l = N - 1, r = 1\}$, are separable states.*

Proof We demonstrate in Proposition 4.3 that the number of states in the writing of the periodic states $\left|\Psi^n_{l,r}\right\rangle$ with $l + r \geq N$ (under or on the anti-diagonal) is one, and thus, they are computational basis states. By using Remark 4.1, we can conclude that after the application of QFT, we always will retrieve a factorized and separable state.

4.5 Entanglement of periodic states through QFT

In this subsection, we use the four-qubit hyperdeterminant $|Det_{2222}|$ as a quantitative measure of entanglement to investigate the amount of entanglement after each gate composing the quantum Fourier transform. We focus on the case when only four-qubit periodic states are input of the QFT.

In fact, when we look at the absolute value of Det_{2222} after each unitary gate composing QFT, when applied on a four-qubit periodic state, we can distinguish three different cases:

1. The value of hyperdeterminant is never equal to zero before, after and during QFT,
2. The value of hyperdeterminant is zero before QFT, then becomes non-null after a particular step of QFT and does not vanish through next gates,
3. The value of hyperdeterminant is always equal to zero before, after and during QFT.

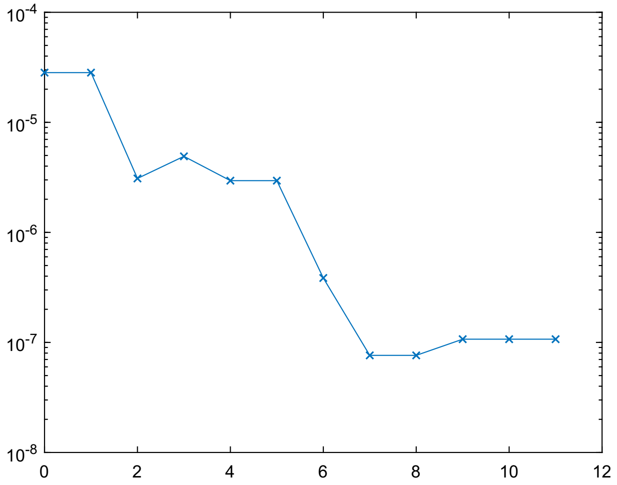

Fig. 7 Evolution of the absolute value of hyperdeterminant in function of the QFT steps, for the periodic state with $(l, r) = (1, 3)$

The first case only happens when we have as input the couples (1,3) and (2, 3), with (l, r) representing a given periodic state with l the shift and r the period. In both cases, the periodic state generated belongs to the family G_{abc0}, which does not annihilate the four-qubit hyperdeterminant. After applying the QFT to these states, we retrieve states belonging to G_{abcd} generic family. We plot in Fig. 7 the evolution of $|\text{Det}_{2222}|$ throughout the gates composing the QFT. For instance, at Step 0 we retrieve the input periodic state; at Step 1, we apply Hadamard gate to the initial state; at Step 3, we retrieve the state resulting of the application of first Hadamard, the first c-R_2 and the first c-R_3 to the initial periodic state; and so on. We observe a global decreasing of the absolute value of the hyperdeterminant while we move to a more generic Verstraete et al. family.

The second case happens for couples $(l, r) \in \mathcal{S}$, with $\mathcal{S}$ the set defined in Eq. (61) :

$$\begin{aligned}\mathcal{S} = \{&(0, 3), (0, 5), (2, 1), (3, 1), (3, 3), (4, 1), (4, 3), (5, 1), (5, 3), (6, 1),\\ &(6, 3), (7, 1), (9, 1), (10, 1), (11, 1), (12, 1)\}\ . \end{aligned} \tag{61}$$

We start with states in the dual variety X^*, where Det_{2222} vanishes. Then depending on the periodic state, the value of the hyperdeterminant will become non-null after one of the c-R_k gate. We can distinguish different types of behavior concerning the evolution of $|\text{Det}_{2222}|$ throughout QFT gates, represented in Fig. 8.

The third case (when the value of hyperdeterminant is always zero during the QFT) happens with all remaining couples $(l, r) \notin \mathcal{S} \cup \{(1, 3), (2, 3)\}$. It does not necessarily mean that QFT does not modify entanglement class and type of these periodic states, but it means that all gates composing the QFT do not bring these states out of the dual variety.

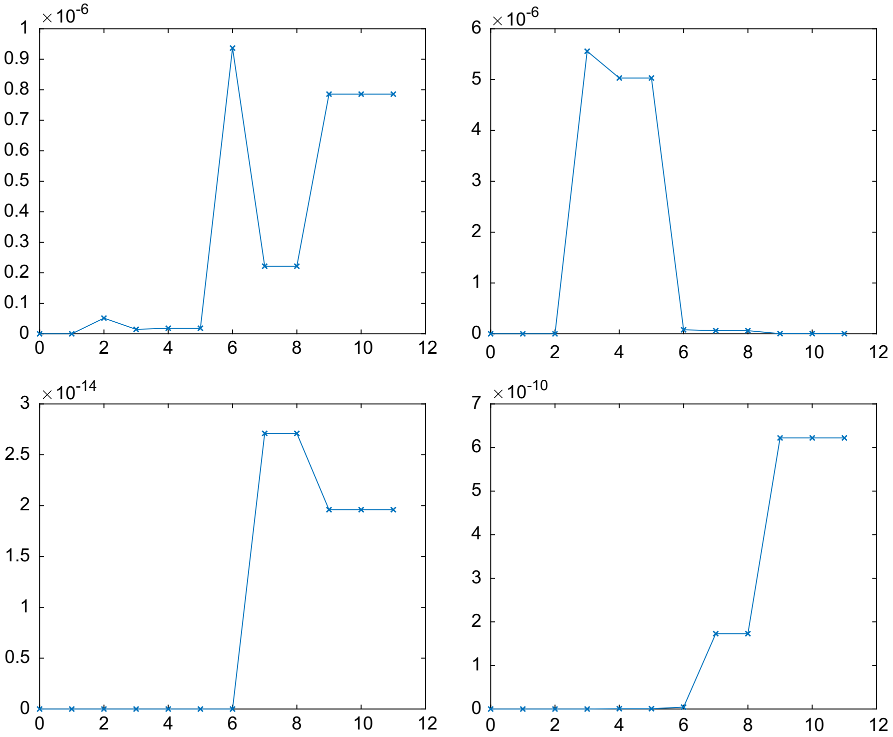

Fig. 8 Evolution of the absolute value of hyperdeterminant in function of the QFT steps, for periodic states with $(l, r) = (0, 3)$ (top left), $(l, r) = (5, 3)$ (top right), $(l, r) = (11, 1)$ (bottom left) and $(l, r) = (9, 1)$ (bottom right)

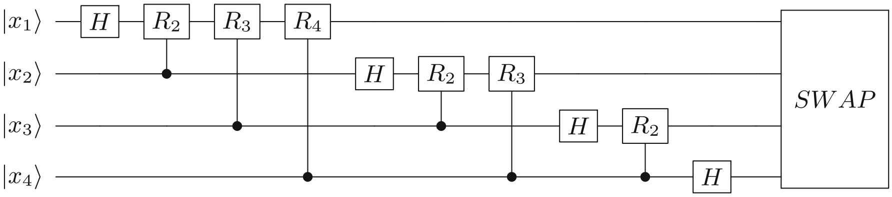

Fig. 9 Eleven gates composing the quantum circuit for four-qubit quantum Fourier transform

Besides, we remark that the value of the hyperdeterminant does not change after the application of Hadamard gates (first, fifth, eighth and tenth gate) and the last Swap gate, as expected (Det_{2222} is invariant under local unitary operation and permutation of qubits). In fact, changes only appear after applying the c-R_k gates, and thus, they are responsible of generation or modification of entanglement by the quantum Fourier transform.

Moreover, for most of the four-qubit periodic states (92.5%), the hyperdeterminant measure does not change after or during the QFT (staying at zero), and this has already been pointed out by Shimoni et al. [44] for the Groverian measure of entanglement. One can also remark that the hyperdeterminant is always null and never changes for a couple (l, r) when r is a power of 2, as it was mentioned by Kendon and Munro [45]. However, we can have a qualitative change in entanglement, as it has been seen in the previous sections. We also observe that the only values of r for which Det_{2222} changes are $r = 1, r = 3$ and $r = 5$.

4.6 Entanglement and quantum Fourier transform

We now no more consider the specific case of Shor's algorithm, to come back to general quantum states. In this subsection, we will briefly discuss the influence of applying the QFT on the entanglement nature of quantum systems. It is well known that quantum Fourier transform can "create" or modify the entanglement when it is applied in the general case, but we yet do not know how this is actually happening. We will thus try to give some elements of answer.

4.6.1 Linear shift invariant property

One of the most important properties of the quantum Fourier transform is what is called the *linear shift invariant* property. It is known that if a n-qubit state shows some periodic behavior with a shift, after the application of QFT, we will retrieve a non-shifted state (a periodic state starting with the basis state $|00\dots0\rangle$) with some periodic behavior directly related to the previous period and the number of basis states $Q = 2^n$.

In their work, Most et al. investigated this property to deduce an approximate description of periodic quantum states after QFT. We wanted to quote precisely the authors [48]:

"In analogy to the discrete Fourier transform (DFT), the QFT is used in order to reveal periodicities in its input. In particular, the amplitudes of the state $\left|\Psi^n_{r,l}\right\rangle$ make out a periodic series, and when the DFT is applied to it, the resulting series can be approximated by a periodic series of the same sort, that is, one in which the indices of the nonzero terms make out an arithmetic progression. In the resulting series, though, the common difference is Q/r, the initial term is zero, and additional phases are added. [...] Since applying the QFT to a quantum state is equivalent to applying the DFT to its amplitudes, the action of the QFT on periodic states can be approximately described as: $\left|\Psi^n_{r,l}\right\rangle \xrightarrow{QFT} \left|\Psi^n_{Q/r,0}\right\rangle$."

While this approximation may be needed to compute more easily some numerical measure of entanglement, we believe that this numerical measure does not preserve the entanglement nature of periodic states after QFT in terms of SLOCC orbit. We would like to illustrate this, with a basic. Let us consider the following periodic state:

$$\left|\Psi^3_{2,2}\right\rangle = \frac{1}{\sqrt{3}}(|010\rangle + |100\rangle + |110\rangle) = \frac{1}{\sqrt{3}}\Big(|01\rangle + |10\rangle + |11\rangle\Big) \otimes |0\rangle. \qquad (62)$$

This state certainly belongs to the $\mathcal{O}_4$ orbit of the three-qubit classification (see Fig. 2). When we apply the quantum Fourier transform to this state, we retrieve the state $|\Psi^*\rangle$:

$$\left|\Psi^*\right\rangle = QFT\left|\Psi^3_{2,2}\right\rangle = \frac{1}{\sqrt{8\times 3}}\Big(3|000\rangle - |001\rangle - |010\rangle - |011\rangle$$
$$+\,3|100\rangle - |101\rangle - |110\rangle - |111\rangle\Big). \tag{63}$$

This last state shows in fact some periodic properties, and it can be written as $|\Psi^*\rangle = \alpha|+\rangle^{\otimes 3} + \beta|000\rangle + \beta|100\rangle = \alpha|+\rangle^{\otimes 3} + \delta|+\rangle|00\rangle = |+\rangle \otimes \big(\alpha|+\rangle^{\otimes 2} + \delta|0\rangle^{\otimes 2}\big)$ and thus belongs to the $\mathcal{O}_3$ orbit.

However, if we focus on the periodic state with the shift $l = 0$ and the period $r = \frac{N}{2} = \frac{8}{2} = 4$, we obtain the following state

$$\left|\Psi^3_{4,0}\right\rangle = \frac{1}{\sqrt{2}}\big(|000\rangle + |100\rangle\big) = \frac{1}{\sqrt{2}}|+\rangle \otimes |00\rangle, \tag{64}$$

which is a separable state, and it is not SLOCC equivalent to the state $|\Psi^*\rangle$. Therefore, from a qualitative point of view, the approximation used in [48] cannot be used. However, if we compute the absolute value of the three-qubit Cayley hyperdeterminant and consider it as a measure of entanglement, we retrieve the same value (which is zero) for both $|\Psi^*\rangle$ and $\left|\Psi^3_{4,0}\right\rangle$ states.

4.6.2 Other remarks on quantum fourier transform

Usually, when the quantum Fourier transform is defined, some of its properties are also mentioned. One basic property of QFT is that it sends the basis state $|0\rangle^{\otimes n}$ to the state $|+\rangle^{\otimes n}$, and so it has the property of building fully parallelized states. This property can be generalized to any basis state:

Remark 4.1 If we apply the quantum Fourier transform to one of the computational basis states, then we always retrieve a separable state. We can in fact directly deduce this from the **product representation** recalled in equation (5.4) of section II.5 of the book [49]. For a basis state $|j_1 j_2 \cdots j_n\rangle$, we retrieve the factorized state $\frac{1}{\sqrt{2^n}}(|0\rangle + e^{2i\pi 0\cdot j_n}|1\rangle)\cdot(|0\rangle + e^{2i\pi 0\cdot j_{n-1}j_n}|1\rangle)\cdots(|0\rangle + e^{2i\pi 0\cdot j_1 j_2\cdots j_n}|1\rangle)$ after the application of the quantum Fourier transform.

But this property is also related to entanglement, since one can deduce that any basis state stays in the set of separable states after the application of quantum Fourier transform. However, it is not true for all separable states, as given in Tables 2 and 3, and at the end of this section.

Tables 2 and 3 show that QFT can transform separable states to entangled one and can change the nature of entanglement. Let us propose another simple but clear example for three-qubit systems. Let us apply the QFT to the well-known state $|W\rangle =$

$\frac{1}{\sqrt{3}}\big(|001\rangle + |010\rangle + |100\rangle\big)$. We know that the $|W\rangle$ state belongs to the $\mathcal{O}_5$ orbit for the 3-qubits. After QFT we obtain the following state:

$$\begin{aligned} TFQ_8|W\rangle = \frac{1}{\sqrt{8}}\frac{1}{\sqrt{3}}\Big(&3|000\rangle + (\omega+\omega^2+\omega^4)|001\rangle + \omega^2|010\rangle + (\omega^3+\omega^6+\omega^4)|011\rangle \\ &+|100\rangle + (\omega^5+\omega^2+\omega^4)|101\rangle + \omega^6|110\rangle + (\omega^7+\omega^6+\omega^4)|111\rangle\Big) \end{aligned}, \tag{65}$$

with $\omega = e^{\frac{2i\pi}{8}}$.

By computing the Cayley hyperdeterminant, one can verify that it is equal to $\frac{-i}{36}$, which means that this state belongs to the $\mathcal{O}_6$ orbit (the $|\text{GHZ}\rangle$ orbit). Therefore, we modified the entanglement class of the state by applying the QFT.

It can thus be interesting to look at the equivalence classes related to the action of the group SLOCC $\cup\,\{QFT, QFT^{-1}\}$ or SLOCC $\cup\,\{H, c\text{-}R_k, \text{SWAP}\}$ (where $c - Rk$ is the controlled R_k gate, see Fig. 9). It could be interesting to study entanglement generated by circuit of H, SWAP, and c-R_k gates (composing QFT), as it was done by Bataille et al. [12] for c-Z and SWAP gates, to understand more deeply the influence of such gates on entanglement.

As a first step in that direction, we choose to focus on the case of two qubits and three qubits to study this last question. In the case of two-qubit systems, we can find that there is only one equivalence class under the action of $G' = \text{SLOCC} \cup \{QFT, QFT^{-1}\}$. In fact, if we take the state $|\Psi_1\rangle$ defined by

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |01\rangle\right). \tag{66}$$

When we apply the quantum Fourier transform to this state, we retrieve the entangled state

$$|\Psi_2\rangle = \frac{1}{2\sqrt{2}}\left(2|00\rangle + (1+i)|01\rangle + (1-i)|11\rangle\right). \tag{67}$$

We know that for two-qubit systems, there is only two SLOCC entanglement classes: separable or entangled (EPR). Since we can move from the separable state $|\Psi_1\rangle$ to the entangled state $|\Psi_2\rangle$, there is only one orbit under the action of G' .

In order to investigate the three-qubit case, let us compute the QFT for several examples of three-qubit states:

$$|\Phi_1\rangle = \frac{1}{\sqrt{3}}\Big(|001\rangle + |010\rangle + |100\rangle\Big) \in \mathcal{O}_5, \tag{68}$$

$$\begin{aligned} |\Phi_2\rangle = \frac{1}{\sqrt{24}}\Big(&3|000\rangle + (\omega+\omega^2+\omega^4)|001\rangle + \omega^2|010\rangle + (\omega^3+\omega^6+\omega^4)|011\rangle \\ &+|100\rangle + (\omega^5+\omega^2+\omega^4)|101\rangle + \omega^6|110\rangle + (\omega^7+\omega^6+\omega^4)|111\rangle\Big) \in \mathcal{O}_6, \end{aligned} \tag{69}$$

$$|\Phi_3\rangle = \frac{1}{\sqrt{3}}\Big(|100\rangle + |110\rangle + |111\rangle\Big) \in \mathcal{O}_3, \tag{70}$$

$$|\Phi_4\rangle = \frac{1}{\sqrt{2}}\Big(|110\rangle + |111\rangle\Big) \in \mathcal{O}_4, \tag{71}$$

$$\begin{aligned}|\Phi_5\rangle = \frac{1}{4}\Big(&2|000\rangle + (\omega^7 - i)|001\rangle - (1+i)|010\rangle + (i+\omega^5)|011\rangle \\ &+(\omega^3 - i)|101\rangle + (i-1)|110\rangle + (\omega + i)|111\rangle\Big) \in \mathcal{O}_6,\end{aligned} \tag{72}$$

$$|\Phi_6\rangle = \frac{1}{\sqrt{2}}\Big(|001\rangle + |010\rangle\Big) \in \mathcal{O}_3, \tag{73}$$

$$|\Phi_7\rangle = \frac{1}{\sqrt{2}}\Big(|101\rangle + |111\rangle\Big) \in \mathcal{O}_1, \tag{74}$$

$$\begin{aligned}|\Phi_8\rangle = \frac{1}{4}\Big(&2|000\rangle + (\omega^5 + \omega^7)|001\rangle + (\omega^5 + \omega^7)|011\rangle - 2|100\rangle + (\omega + \omega^3)|101\rangle \\ &+(\omega + \omega^3)|111\rangle\Big) \in \mathcal{O}_3,\end{aligned} \tag{75}$$

$$|\Phi_9\rangle = \frac{1}{\sqrt{2}}\Big(|001\rangle + |011\rangle\Big) \in \mathcal{O}_1, \tag{76}$$

$$|\Phi_{10}\rangle = \frac{1}{\sqrt{2}}\Big(|000\rangle + |101\rangle\Big) \in \mathcal{O}_2, \tag{77}$$

$$\begin{aligned}|\Phi_{11}\rangle = \frac{1}{4}\Big(&2|000\rangle + (1 + \omega^5)|001\rangle + (1+i)|010\rangle + (1 + \omega^7)|011\rangle \\ &+ (1+\omega)|101\rangle + (1-i)|110\rangle + (1+\omega^3)|111\rangle\Big) \in \mathcal{O}_6,\end{aligned} \tag{78}$$

$$|\Phi_{12}\rangle = \frac{1}{\sqrt{2}}\Big(|000\rangle + |011\rangle\Big) \in \mathcal{O}_3, \tag{79}$$

$$|\Phi_{13}\rangle = \frac{1}{\sqrt{2}}\Big(|000\rangle + |110\rangle\Big) \in \mathcal{O}_4, \tag{80}$$

$$\begin{aligned}|\Phi_{14}\rangle = \frac{1}{4}\Big(&2|000\rangle + (1-i)|001\rangle + (1+i)|011\rangle + 2|100\rangle \\ &+ (1-i)|101\rangle + (1+i)|111\rangle\Big) \in \mathcal{O}_3,\end{aligned} \tag{81}$$

$$|\Phi_{15}\rangle = \frac{1}{\sqrt{2}}\Big(|000\rangle + |010\rangle\Big) \in \mathcal{O}_1\ . \tag{82}$$

These states are related to each other, using the QFT, detailed as follows:

$$\begin{aligned}&|\Phi_1\rangle \xrightarrow{QFT} |\Phi_2\rangle \xrightarrow{QFT} |\Phi_3\rangle, \quad |\Phi_4\rangle \xrightarrow{QFT} |\Phi_5\rangle \xrightarrow{QFT} |\Phi_6\rangle, \\ &|\Phi_7\rangle \xrightarrow{QFT} |\Phi_8\rangle \xrightarrow{QFT} |\Phi_9\rangle, \quad |\Phi_{10}\rangle \xrightarrow{QFT} |\Phi_{11}\rangle \xrightarrow{QFT} |\Phi_{12}\rangle, \\ &|\Phi_{13}\rangle \xrightarrow{QFT} |\Phi_{14}\rangle \xrightarrow{QFT} |\Phi_{15}\rangle.\end{aligned}$$

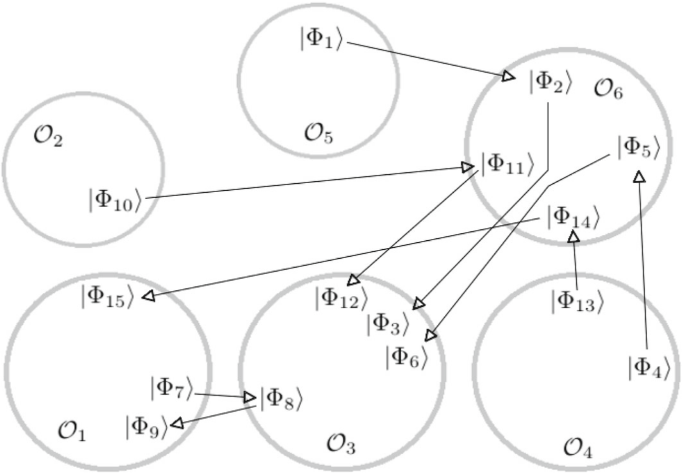

Fig. 10 Quantum states in the same gray circle belong to the same SLOCC orbit. White-headed arrows correspond to the application of the quantum Fourier transform (The state close to the arrow's head is the result of the application of QFT to the state at the arrow's root.)

By using the visual representation proposed in Fig. 10, one can verify that, starting from a specific state $|\Phi_i\rangle$, we can reach any state in any orbit, by applying a succession of operations in SLOCC group and/or the QFT (and its inverse).

We can thus conclude that there is only one orbit under the action of G', both in two-qubit three-qubit cases. It can be more difficult to investigate the four-qubit case, because there are an infinite number of SLOCC orbits. However, we can first tackle the problem by only considering Verstraete et al. families of sub-families, and the nine orbits of the nullcone. One can use for that the results presented in Tables 2 and 3 to extract four-qubit states equivalents by quantum Fourier transform.

5 Conclusion

In this work, we were able to produce a detailed study of the entanglement classes emerging during Grover's and Shor's algorithm, in the case of four-qubit systems. For Grover's algorithm, we determined what type of entanglement is generated depending on the marked elements and their number. For Shor's algorithm, we focused on periodic states generated after the first measure in the period-finding algorithm. We presented entanglement families of periodic states depending on their parameters (shift and period), and how these classes change after the application of the quantum Fourier transform. Some of these results were generalized to any n-qubit version of the algorithm.

Our analysis shows that some four-qubit states never show up in both algorithms. It is the case of the famous $|W\rangle$ state (as it was observed in [39] for Grover's algorithm on some tripartite systems for the standard regime) but also $\left|L_{abc_2}\right\rangle$ or $\left|L_{ab_3}\right\rangle$. So far we do not have any (geometric) explanations of this phenomenon.

Regarding the QFT and its influence on entanglement we have shown that for $n = 2$ and $n = 3$ qubits, we have shown that all quantum states are equivalent up to a sequence of transformation of the set SLOCC $\cup \{QFT\}$.

Acknowledgements This work is supported by the Région Bourgogne Franche-Comté, Project PHYFA (Contract 20174-06235) and the French "Investissements d'Avenir" program, Project ISITE-BFC (Contract ANR-15-IDEX-03).

Appendix A: Examples of orbits related with sets of marked elements

Table 4 provides examples of sets of marked elements which allows to reach the corresponding orbits and Verstraete families by running Grover's algorithm in the four-qubit case.

Table 4 Examples of family of marked elements S and the corresponding family or orbit reached by the algorithm in the $2 \times 2 \times 2 \times 2$ case

Orbit	S
G_{abcd}	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0101\rangle, \|1010\rangle, \|1111\rangle\}$
G_{abc0}	$\{\|0000\rangle, \|1111\rangle\}$
G_{00cc}	$\{\|0000\rangle\}$
G_{a000}	$\{\|0000\rangle, \|0011\rangle, \|1100\rangle, \|1111\rangle\}$
G_{ab00}	$\{\|0000\rangle, \|0011\rangle, \|1101\rangle, \|1110\rangle\}$
L_{abc_2}	$\emptyset$
L_{00c_2}	$\{\|0000\rangle, \|0011\rangle\}$
L_{aa0_2}	$\{\|0000\rangle, \|0101\rangle\}$
L_{a00_2}	$\{\|0000\rangle, \|0110\rangle, \|1001\rangle, \|1111\rangle\}$
L_{ab0_2}	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0101\rangle, \|1010\rangle\}$
$L_{a_2b_2}$	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0100\rangle, \|1001\rangle\}$
$L_{0_2b_2}$	$\{\|0000\rangle, \|0001\rangle, \|0110\rangle\}$
L_{ab_3}	$\emptyset$
L_{0b_3}	$\emptyset$
L_{a0_3}	$\emptyset$
L_{a_4}	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0101\rangle, \|0110\rangle, \|1101\rangle\}$
$L_{a_2 0_{3\oplus\bar{1}}}$	$\{\|0000\rangle, \|0001\rangle, \|1110\rangle\}$
Gr_8	$\{\|0000\rangle, \|0111\rangle\}$
Gr_7	$\{\|0000\rangle, \|0001\rangle, \|0110\rangle, \|1011\rangle\}$
Gr_6	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|1100\rangle\}$
Gr_5	$\{\|0000\rangle, \|0011\rangle, \|0101\rangle, \|1001\rangle\}$
Gr_4	$\{\|0000\rangle, \|0001\rangle\}$
Gr_3	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0100\rangle\}$
Gr_2	$\{\|0000\rangle, \|0001\rangle, \|0110\rangle, \|0111\rangle\}$
Gr_1	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0011\rangle\}$

Appendix B: Three-qubit periodic states

See Tables 5 and 6.

Table 5 Three-qubit SLOCC orbits of periodic states depending on their shift l and period r

r	l							
	0	1	2	3	4	5	6	7
1	$\mathcal{O}_1$	$\mathcal{O}_6$	$\mathcal{O}_4$	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_3$	$\mathcal{O}_1$	$\mathcal{O}_1$
2	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_4$	$\mathcal{O}_4$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
3	$\mathcal{O}_5$	$\mathcal{O}_5$	$\mathcal{O}_6$	$\mathcal{O}_2$	$\mathcal{O}_3$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
4	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
5	$\mathcal{O}_2$	$\mathcal{O}_6$	$\mathcal{O}_2$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
6	$\mathcal{O}_4$	$\mathcal{O}_4$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
7	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$

Table 6 Three-qubit SLOCC orbits of the resulting states after applying the QFT on periodic states depending on their shift l and period r

r	l							
	0	1	2	3	4	5	6	7
1	$\mathcal{O}_1$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_1$
2	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_3$	$\mathcal{O}_3$	$\mathcal{O}_3$	$\mathcal{O}_3$	$\mathcal{O}_1$	$\mathcal{O}_1$
3	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
4	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
5	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
6	$\mathcal{O}_3$	$\mathcal{O}_3$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
7	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$

Appendix C: Algorithm

Algorithm 2 VerstraeteType

```
Require: $Y$ an array of size 16, the four-qubit state
Ensure: The Verstraete et al. type of $Y$

  Hess1 ← $Hess(\mathcal{Q}_1)$
  Hess2 ← $Hess(\mathcal{Q}_2)$
  Hess3 ← $Hess(\mathcal{Q}_3)$
  T1 ← $T(\mathcal{Q}_1)$
  T2 ← $T(\mathcal{Q}_2)$
  T3 ← $T(\mathcal{Q}_3)$

                                        ▷ If the input form belongs to the nullcone
  if isInNullcone($Y$) then
     return NilpotentType($Y$)
  end if

                                        ▷ The three quartics have at least a zero root
  if $L = 0$ and $M = 0$ then
                                        ▷ All the roots are simple
     if $D_{xy} \neq 0$ and $Hyper \neq 0$ then
        return $G_{abc0}$

                                        ▷ All the zero roots are simple and there is a nonzero double root
     else if $D_{xy} \neq 0$ and $Hyper = 0$ then
        vectCov ← $[\mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0] then
           return $G_{aa(-2a)0}$
        else
           return $L_{0b(\frac{b}{2})_2}$
        end if

                                        ▷ All the zero roots are double
     else if $D_{xy} = 0$ and $H \neq 0$ then
        vectCov ← $[\overline{\mathcal{G}}, \mathcal{G}, \mathcal{H}, \mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0, 0, 0, 0] then
           return $G_{00cc}$
        else if eval = [0, 1, 1, 0] then
           return $L_{aa0_2}$
        else if eval = [0, 0, 1, 0] then
           return $L_{00c_2}$
        else if eval = [1, 1, 1, 0] then
           return $L_{0_2b_2}$
        else if eval = [1, 1, 1, 1] then
           return $L_{a_2 0_{3\oplus\bar{1}}}$
        end if
     end if

                                        ▷ Only one of the quartics $\mathcal{Q}_i$ has a zero root then
                                        ▷ The quartic $\mathcal{Q}_1$ has a zero root
  else if $L = 0$ and $M \neq 0$ then
                                        ▷ $\mathcal{Q}_1$ has only simple roots
     if $Hyper \neq 0$ then
        return $G_{abc0}$
```

```
                                        ▷ $\mathcal{Q}_1$ has a double zero root and two simple roots
    else if $D_{xy} = H \cdot M$ and $H^2 + 4M \neq 0$ then
        vectCov ← $[\mathcal{K}_3, \mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0, 0] then
            return $G_{ab00}$
        else if eval = [1, 0] then
            return $L_{ab0_2}$
        else if eval = [1, 1] then
            return $L_{a_2b_2}$
        end if

                                        ▷ $\mathcal{Q}_1$ has a double nonzero root and two simple roots
    else if $D_{xy} \neq H \cdot M$ and T1≠ 0 and T2≠ 0 then
        vectCov ← $[\mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0] then
            return $G_{abb0}$
        else if eval = [1] then
            return $L_{a0c_2}$
        end if

                                        ▷ $\mathcal{Q}_1$ has a triple zero root and a simple root
    else if $D_{xy} = H \cdot M$ and $H^2 + 4M = 0$ and Hess2= 0 then
        vectCov ← $[\mathcal{C}, \mathcal{D}, \mathcal{K}_5, \mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0, 0, 0, 0] then
            return $G_{a000}$
        else if eval = [1, 0, 0, 0] then
            return $L_{a00_2}$
        else if eval = [1, 1, 1, 0] then
            return $L_{0b_3}$
        else if eval = [1, 1, 0, 0] then
            return $L_{a_2a_2}$
        else if eval = [1, 1, 1, 1] then
            return $L_{a_4}$
        end if

                                        ▷ $\mathcal{Q}_1$ has a triple nonzero root
    else if $D_{xy} \neq H \cdot M$ and $I_2 = 0$ and $Hyper = 0$ then
        vectCov ← $[\mathcal{D}, \mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0, 0] then
            return $G_{aaa0}$
        else if eval = [1, 0] then
            return $L_{0bb_2}$
        else if eval = [1, 1] then
            return $L_{a0_3}$
        end if
    end if

                                        ▷ The quartic $\mathcal{Q}_2$ has a zero root
else if $M = 0$ and $L \neq 0$ then
                                        ▷ $\mathcal{Q}_2$ has only simple roots
    if $Hyper \neq 0$ then
        return $G_{abc0}$
```

```
                                ▷ $\mathcal{Q}_2$ has a double zero root and two simple roots
  else if $D_{xy} = 0$ and $H^2 \neq 4L$ then
    vectCov ← $[\mathcal{K}_3, \mathcal{L}]$
    eval ← evaluate(vectCov,$Y$)
    if eval $= [0, 0]$ then
      return $G_{ab00}$
    else if eval $= [1, 0]$ then
      return $L_{ab0_2}$
    else if eval $= [1, 1]$ then
      return $L_{a_2b_2}$
    end if

                                ▷ $\mathcal{Q}_2$ has a double nonzero root and two simple roots
  else if $D_{xy} \neq 0$ and T1$\neq 0$ and T2$\neq 0$ then
    vectCov ← $[\mathcal{L}]$
    eval ← evaluate(vectCov,$Y$)
    if eval $= [0]$ then
      return $G_{abb0}$
    else if eval $= [1]$ then
      return $L_{a0c_2}$
    end if

                                ▷ $\mathcal{Q}_2$ has a triple zero root and a simple root
  else if $D_{xy} = 0$ and $H^2 = 4L$ then
    vectCov ← $[\mathcal{C}, \mathcal{D}, \mathcal{K}_5, \mathcal{L}]$
    eval ← evaluate(vectCov,$Y$)
    if eval $= [0, 0, 0, 0]$ then
      return $G_{a000}$
    else if eval $= [1, 0, 0, 0]$ then
      return $L_{a00_2}$
    else if eval $= [1, 1, 1, 0]$ then
      return $L_{0b_3}$
    else if eval $= [1, 1, 0, 0]$ then
      return $L_{a_2a_2}$
    else if eval $= [1, 1, 1, 1]$ then
      return $L_{a_4}$
    end if

                                ▷ $\mathcal{Q}_2$ has a triple nonzero root
  else if $D_{xy} \neq 0$ and $I_2 = 0$ and $Hyper = 0$ then
    vectCov ← $[\mathcal{D}, \mathcal{L}]$
    eval ← evaluate(vectCov,$Y$)
    if eval $= [0, 0]$ then
      return $G_{aaa0}$
    else if eval $= [1, 0]$ then
      return $L_{0bb_2}$
    else if eval $= [1, 1]$ then
      return $L_{a0_3}$
    end if
  end if

                                ▷ The quartic $\mathcal{Q}_3$ has a zero root
else if $N = 0$ and $L \neq 0$ and $M \neq 0$ then
                                ▷ $\mathcal{Q}_3$ has only simple roots
  if $Hyper \neq 0$ then
    return $G_{abc0}$
```

```
                                    ▷ $\mathcal{Q}_3$ has a double zero root and two simple roots
    else if $D_{xy} = 0$ and $H^2 \neq 4M$ then
        vectCov ← $[\mathcal{K}_3, \mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0, 0] then
            return $G_{ab00}$
        else if eval = [1, 0] then
            return $L_{ab0_2}$
        else if eval = [1, 1] then
            return $L_{a_2b_2}$
        end if

                                    ▷ $\mathcal{Q}_3$ has a double nonzero root and two simple roots
    else if $D_{xy} \neq 0$ and T1≠ 0 and T2≠ 0 then
        vectCov ← $[\mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0] then
            return $G_{abb0}$
        else if eval = [1] then
            return $L_{a0c_2}$
        end if

                                    ▷ $\mathcal{Q}_3$ has a triple zero root and a simple root
    else if $D_{xy} = 0$ and $H^2 = 4M$ then
        vectCov ← $[\mathcal{C}, \mathcal{D}, \mathcal{K}_5, \mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0, 0, 0, 0] then
            return $G_{a000}$
        else if eval = [1, 0, 0, 0] then
            return $L_{a00_2}$
        else if eval = [1, 1, 1, 0] then
            return $L_{0b_3}$
        else if eval = [1, 1, 0, 0] then
            return $L_{a_2a_2}$
        else if eval = [1, 1, 1, 1] then
            return $L_{a_4}$
        end if

                                    ▷ $\mathcal{Q}_3$ has a triple nonzero root
    else if $D_{xy} \neq 0$ and $I_2 = 0$ and $Hyper = 0$ then
        vectCov ← $[\mathcal{D}, \mathcal{L}]$
        eval ← evaluate(vectCov,$Y$)
        if eval = [0, 0] then
            return $G_{aaa0}$
        else if eval = [1, 0] then
            return $L_{0bb_2}$
        else if eval = [1, 1] then
            return $L_{a0_3}$
        end if
    end if

                                    ▷ All the quartics have only nonzero roots
else
                                    ▷ All the roots are simple
    if $Hyper \neq 0$ then
        return $G_{abcd}$
```

```
                                  ▹ Each quartic has a double root and two simple roots
    else if T1 $\neq 0$ and T2 $\neq 0$ and T3 $\neq 0$ and $I_2 \neq 0$ and $I_3 \neq 0$ then
        vectCov ← [$\mathcal{L}$]
        eval ← evaluate(vectCov,$Y$)
        if eval = [0] then
            return $G_{abcc}$
        else if eval = [1] then
            return $L_{abc_2}$
        end if

                                  ▹ Each quartic has a single simple root and a triple root
    else if $I_2 \neq 0$ and $I_3 \neq 0$ and Hess1 $\neq 0$ then
        vectCov ← [$\mathcal{K}_5, \mathcal{L}$]
        eval ← evaluate(vectCov,$Y$)
        if eval = [0, 0] then
            return $G_{abbb}$
        else if eval = [1, 0] then
            return $L_{abb_2}$
        else if eval = [1, 1] then
            return $L_{ab_3}$
        end if

    end if

end if
```

References

1. Ekert, A., Jozsa, R.: Quantum algorithms: entanglement-enhanced information processing. Philos. Trans. R. Soc. Lond. A **1998**(356), 1769–1782 (1998)
2. Jozsa, R., Linden, N.: On the role of entanglement in quantum-computational speed-up. Proc. R. Soc. Lond. A **2003**(459), 2011–2032 (2003)
3. Haddadi, S., Bohloul, M.: A brief overview of bipartite and multipartite entanglement measures. Int. J. Theor. Phys. **57**, 3912 (2018)
4. Latorre, J.I., Martín-Delgado, M.A.: Majorization arrow in quantum-algorithm design. Phys. Rev. A **66**, 022305 (2002)
5. Orús, R., Latorre, J.I., Martín-Delgado, M.A.: Natural majorization of the quantum fourier transformation in phase-estimation algorithms. Quantum Inf. Process. **1**(4), 283–302 (2002)
6. Orús, R., Latorre, J.I., Martin-Delgado, M.A.: Systematic analysis of majorization in quantum algorithms. Eur. Phys. J. D Atom. Mol. Opt. Plasma Phys. **29**(1), 119–132 (2004)
7. Verstraete, F., Dehaene, J., De Moor, B., Verschelde, H.: Four qubits can be entangled in nine different ways. Phys. Rev. A **65**(5), 052112 (2002)
8. Chterental, O., Djokovic, D.: Normal forms and tensor ranks of pure states of four qubits. arXiv preprint arXiv:quant-ph/0612184 (2006)
9. Holweck, F., Luque, J.G., Thibon, J.Y.: Entanglement of four qubit systems: a geometric atlas with polynomial compass I (the finite world). J. Math. Phys. **55**(1), 012202 (2014)
10. Holweck, F., Luque, J.G., Thibon, J.Y.: Entanglement of four qubit systems: a geometric atlas with polynomial compass II (the tame world). J. Math. Phys. **58**, 022201 (2017)
11. Holweck, F., Luque, J.G., Thibon, J.Y.: Geometric descriptions of entangled states by auxiliary varieties. J. Math. Phys. **53**(10), 102203 (2012)
12. Bataille, M., Luque, J.G.: Quantum circuits of c–Z and SWAP gates optimization and entanglement. arXiv preprint arXiv:1810.01769 (2018)
13. Enríquez, M., Delgado, F., Życzkowski, K.: Entanglement of three-qubit random pure states. Entropy **20**(10), 745 (2018)
14. Luque, J.G., Thibon, J.Y.: Polynomial invariants of four qubits. Phys. Rev. A **67**(4), 042303 (2003)

15. Heydari, H.: Geometrical structure of entangled states and the secant variety. Quantum Inf. Process. **7**(1), 43–50 (2008)
16. Brylinski, J.L.: Algebraic measures of entanglement. In: Mathematics of Quantum Computation (pp. 19-40). Chapman and Hall/CRC (2002)
17. Sanz, M., Braak, D., Solano, E., Egusquiza, I.L.: Entanglement classification with algebraic geometry. J. Phys. A Math. Theor. **50**(19), 195303 (2017)
18. Sawicki, A., Tsanov, V.V.: A link between quantum entanglement, secant varieties and sphericity. J. Phys. A Math. Theor. **46**(26), 265301 (2013)
19. Sawicki, A., Maciażek, T., Karnas, K., Kowalczyk-Murynka, K., Kuś, M., Oszmaniec, M.: Multipartite quantum correlations: symplectic and algebraic geometry approach. Rep. Math. Phys. **82**(1), 81–111 (2018)
20. Miyake, A., Wadati, M.: Multipartite entanglement and hyperdeterminants. Quantum Inf. Comput. **2**(7), 540–555 (2002)
21. Miyake, A.: Classification of multipartite entangled states by multidimensional determinants. Phys. Rev. A **67**(1), 012108 (2003)
22. Miyake, A., Verstraete, F.: Multipartite entanglement in $2 \times 2 \times n$ quantum systems. Phys. Rev. A **69**(1), 012101 (2004)
23. Grover, L.K.: Quantum computers can search arbitrarily large databases by a single query. Phys. Rev. Lett. **79**(23), 4709 (1997)
24. Braunstein, S.L., Pati, A.K.: Speed-up and entanglement in quantum searching. Quantum Info. Comput. **2**(5), 399–409 (2002)
25. Biham, O., Nielsen, M.A., Osborne, T.J.: Entanglement monotone derived from Grover's algorithm. Phys. Rev. A **65**(6), 062312 (2002)
26. Forcer, T.M., Hey, A.J.G., Ross, D.A., Smith, P.G.R.: Superposition, entanglement and quantum computation. Quantum Inf. Comput. **2**(2), 97–116 (2002)
27. Biham, O., Shapira, D., Shimoni, Yishai: Analysis of Grover's quantum search algorithm as a dynamical system. Phys. Rev. A **68**, 022326 (2003). Published 29 August 2003
28. Orús, R., Latorre, J.I.: Universality of entanglement and quantum-computation complexity. Phys. Rev. A **69**(5), 052308 (2004)
29. Fang, Y., Kaszlikowski, D., Chin, C., Tay, K., Kwek, L.C., Oh, C.H.: Entanglement in the Grover search algorithm. Phys. Lett. A **345**(4), 265–272 (2005)
30. Iwai, T., Hayashi, N., Mizobe, K.: The geometry of entanglement and Grover's algorithm. J. Phys. A Math. Theor. **41**(10), 105202 (2008)
31. Iwai, T.: The geometry of multi-qubit entanglement. J. Phys. A Math. Theor. **40**(40), 12161 (2007)
32. Wen, J., Cao, W.: Multipartite entanglement in adiabatic quantum searching algorithm. In: 2012 Eighth International Conference on Natural Computation (ICNC), (pp. 893–897). IEEE (2012)
33. Meyer, D.A., Wallach, N.R.: Global entanglement in multiparticle systems. J. Math. Phys **43**, 4273 (2002)
34. Rossi, M., Bruß, D., Macchiavello, C.: Scale invariance of entanglement dynamics in Grover's quantum search algorithm. Phys. Rev. A **87**(2), 022331 (2013)
35. Chakraborty, S., Banerjee, S., Adhikari, S., Kumar, A.: Entanglement in the Grover's Search Algorithm. arXiv preprint arXiv:1305.4454 (2013)
36. Rossi, M., Bruß, D., Macchiavello, C.: Hypergraph states in Grover's quantum search algorithm. Phys. Scr. **2014**(T160), 014036 (2014)
37. Qu, R., Shang, B., Bao, Y., Song, D., Teng, C., Zhou, Z.: Multipartite entanglement in Grover's search algorithm. Nat. Comput. **14**(4), 683–689 (2015)
38. Ye, B., Zhang, T., Qiu, L., et al.: Quantum discord and entanglement in grover search algorithm. Open Phys. **14**(1), 71–176 (2016). https://doi.org/10.1515/phys-2016-0020. Retrieved 24 Aug. 2018, from
39. Holweck, F., Jaffali, H., Nounouh, I.: Grover's algorithm and the secant varieties. Quantum Inf. Process. **15**(11), 4391–4413 (2016)
40. Pan, M., Qiu, D., Zheng, S.: Global multipartite entanglement dynamics in Grover's search algorithm. Quantum Inf. Process. **16**(9), 211 (2017)
41. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997). (October 1997)
42. Parker, S., Plenio, M.B.: Entanglement simulations of Shor's algorithm. J. Mod. Opt. **49**(8), 1325–1353 (2001)

43. Vidal, G.: Efficient classical simulation of slightly entangled quantum computations. Phys. Rev. Lett. **91**, 147902 (2003)
44. Shimoni, Yishai, Shapira, Daniel, Biham, Ofer: Entangled quantum states generated by Shor's factoring algorithm. Phys. Rev. A **72**, 062308 (2005). Published 6 December 2005
45. Kendon, V.M., Munro, W.J.: Entanglement and its role in Shor's algorithm. Quantum Inf. Comput. **6**(7), 630–640 (2006). (November 2006)
46. Lanyon, B.P., Weinhold, T.J., Langford, N.K., Barbieri, M., James, D.F., Gilchrist, A., White, A.G.: Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement. Phys. Rev. Lett. **99**(25), 250505 (2007). 2007 Dec 21
47. Lu, C.Y., Browne, D.E., Yang, T., Pan, J.W.: Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. Phys. Rev. Lett. **99**(25), 250504 (2007). 2007 Dec 21
48. Most, Y., Shimoni, Y., Biham, Ofer: Entanglement of periodic states, the quantum fourier transform, and Shor's factoring algorithm. Phys. Rev. A **81**, 052306 (2010)
49. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition, 10th edn. Cambridge University Press, New York (2011)
50. Laugerotte, E., Luque, J.G., Mignot, L., Nicart, F.: Multilinear representations of Free PROs. arXiv preprint arXiv:1803.00228 (2018)
51. Cao, Z., Cao, Z.: On Shor's factoring algorithm with more registers and the problem to certify quantum computers. IACR Cryptol. ePrint Arch. **2014**, 721 (2014)
52. Gelfand, I.M., Kapranov, M., Zelevinsky, A.: Discriminants, Resultants, and Multidimensional Determinants. Springer Science & Business Media, New York (2008)
53. Harris, J.: Algebraic Geometry: A First Course, vol. 133. Springer Science & Business Media, New York (2013)
54. Galindo, A., Martin-Delgado, M.A.: Information and computation: classical and quantum aspects. Rev. Mod. Phys. **74**(2), 347 (2002)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.