Physical Review A, vol 68, 2003

The Clifford group, stabilizer states, and linear and quadratic operations over GF(2).

Jeroen Dehaene* and Bart De Moor
Katholieke Universiteit Leuven, ESAT-SCD, Belgium

(Dated: April 18, 2003)

We describe stabilizer states and Clifford group operations using linear operations and quadratic forms over binary vector spaces. We show how the n-qubit Clifford group is isomorphic to a group with an operation that is defined in terms of a $(2n+1)\times(2n+1)$ binary matrix product and binary quadratic forms. As an application we give two schemes to efficiently decompose Clifford group operations into one and two-qubit operations. We also show how the coefficients of stabilizer states and Clifford group operations in a standard basis expansion can be described by binary quadratic forms. Our results are useful for quantum error correction, entanglement distillation and possibly quantum computing.

PACS numbers: 03.67.-a

I. INTRODUCTION

Stabilizer states and Clifford group operations play a central role in quantum error correction, quantum computing, and entanglement distillation. A stabilizer state is a state of an n-qubit system that is a simultaneous eigenvector of a commutative subgroup of the Pauli group. The latter consists of all tensor products of n single-qubit Pauli operations. The Clifford group is the group of unitary operations that map the Pauli group to itself under conjugation. In quantum error correction these concepts play a central role in the theory of stabilizer codes [1]. Although a quantum computer working with only stabilizer states and Clifford group operations is not powerful enough to disallow efficient simulation on a classical computer [2, 3], it is not unlikely that possible new quantum algorithms will exploit the rich structure of this group. In [4], we also showed the relevance of a quotient group of the Clifford group in mixed state entanglement distillation.

In this paper, we link stabilizer states and Clifford operations with binary linear algebra and binary quadratic forms (over GF(2)). The connection between multiplication of Pauli group elements and binary addition is well known as is the connection between commutability of Pauli group operations and a binary symplectic inner product [1]. In [4] we extended this connection to a link between a quotient group of the Clifford group and binary symplectic matrices (there termed P orthogonal). In this paper we give a binary characterization of the full Clifford group, by adding quadratic forms to the symplectic operations. In addition we show how the coefficients, with respect to a standard basis, of both stabilizer states and Clifford operations can also be described using binary quadratic forms. Our results also lead to efficient ways for decomposing Clifford group operations in a product of 2-qubit operations.

II. CLIFFORD GROUP OPERATIONS AND BINARY LINEAR AND QUADRATIC OPERATIONS

In this section, we show how the Clifford group is isomorphic to a group that can be entirely described in terms of binary linear algebra, by means of symplectic linear operations and quadratic forms.

We use the following notation for Pauli matrices.

$$\begin{aligned}
\sigma_{00} &= \tau_{00} &= \sigma_0 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \\
\sigma_{01} &= \tau_{01} &= \sigma_x &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\
\sigma_{10} &= \tau_{10} &= \sigma_z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \\
\sigma_{11} & &= \sigma_y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \\
& \tau_{11} &= i\sigma_y &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.
\end{aligned}$$

We also use vector indices to indicate tensor products of Pauli matrices. If $v, w \in \mathbb{Z}_2^n$ and $a = \begin{bmatrix} v \\ w \end{bmatrix} \in \mathbb{Z}_2^{2n}$, then we denote

$$\begin{aligned}
\sigma_a &= \sigma_{v_1 w_1} \otimes \ldots \otimes \sigma_{v_n w_n}, \\
\tau_a &= \tau_{v_1 w_1} \otimes \ldots \otimes \tau_{v_n w_n}
\end{aligned} \qquad (1)$$

If we define the Pauli group to contain all tensor products of Pauli matrices with an additional complex phase in $\{1, i, -1, -i\}$, an arbitrary Pauli group element can be represented as $i^\delta(-1)^\epsilon \tau_u$, where $\delta, \epsilon \in \mathbb{Z}_2$ and $u \in \mathbb{Z}_2^{2n}$. The separation of δ and ϵ, rather than having i^γ with $\gamma \in \mathbb{Z}_4$, is deliberate and will simplify formulas below. Throughout this paper exponents of i will always be binary. As a result $i^{\delta_1} i^{\delta_2} = i^{\delta_1+\delta_2}(-1)^{\delta_1\delta_2}$. Multiplication of two Pauli group elements can now be translated into binary terms in the following way:

Lemma 1 *If $a_1, a_2 \in \mathbb{Z}_2^{2n}$, $\delta_1, \delta_2, \epsilon_1, \epsilon_2 \in \mathbb{Z}_2$ and τ is*

*Electronic address: Jeroen.Dehaene@esat.kuleuven.ac.be

That symplecticity is also sufficient was first implied by Theorem 1 of [4] (almost, as this result was set in the context of entanglement distillation where the signs ϵ play no significant role). The idea is to give a constructive way of realizing the Clifford operation Q given by $\bar{C}$ and $\bar{h}$. This can be done using only one and two-qubit operations, which makes the result also of practical use. In Sec. IV we give two such decompositions that are more transparent than the results of [4].

First, to conclude this section, we complete the binary group picture by a formula for the inverse of a Clifford group element, given in binary terms.

Theorem 3 *Given $\bar{C}_1$ and $\bar{h}_1$, defining a Clifford operation Q_1 as above, the inverse $Q_2 = Q_1^{-1}$ is represented by*

$$\begin{aligned}\bar{C}_2 &= \bar{C}_1^{-1} = \begin{bmatrix} C_1^{-1} & 0 \\ d^T C^{-1} & 1 \end{bmatrix} = \begin{bmatrix} PC_1^T P & 0 \\ d_1^T PC_1^T P & 1 \end{bmatrix} \\ \bar{h}_2 &= \bar{C}^{-T}\bar{h} + diag(\bar{C}^{-T} lows(\bar{C}^T \bar{U} \bar{C})\bar{C}^{-1})\end{aligned}$$

These formulas can be verified using Theorem 2. Finally note that since the Clifford operations form a group and the matrices $\bar{C}$ are simply multiplied when composing Clifford group operations, the matrices $\bar{C}$ with C symplectic and $d = \text{diag}(C^T UC)$ must form a group of $(2n+1) \times (2n+1)$ matrices that is isomorphic to the symplectic group of $2n \times 2n$ matrices. This can be easily verified by showing that

$$\text{diag}(C_1^T C_2^T U C_2 C_1) = C_1^T \text{diag}(C_2^T U C_2) + \text{diag}(C_1^T U C_1)$$

This follows from the fact that $C^T UC + U$ is symmetric when $C^T PC = P$ and $x^T Sx = x^T \text{diag}(S)$ when S is symmetric. In a similar way it can be proven that $\text{diag}(C^{-T} UC^{-1}) = C^{-T}\text{diag}(C^T UC)$.

III. SPECIAL CLIFFORD OPERATIONS IN THE BINARY PICTURE

In this section we consider a selected set of Clifford group operations and their representation in the binary picture of Sec. II.

First, we consider the Pauli group operations $Q = \tau_a$ as Clifford operations. Note that a global phase cannot be represented as it does not affect the action $X \to QXQ^\dagger$. To construct C and h we have to consider the images of the operators τ_{e_k} representing one-qubit operations σ_x and σ_z. One can easily verify that τ_a is represented by

$$\begin{aligned} C &= I_{2n} \\ h &= Pa \end{aligned} \tag{2}$$

Second, note that Clifford operations acting on a subset $\alpha \subset \{1, \ldots, n\}$ consist of a symplectic matrix on the rows and columns with indices in $\alpha \cup (\alpha + n)$, embedded in an identity matrix (that is, with ones on positions $C_{k,k} = 1$, $k \notin \alpha \cup (\alpha + n)$ and $C_{k,l} = 0$ if $k \neq l$ and k or $l \notin \alpha \cup (\alpha + n)$.) Also $h_k = 0$ if $k \notin \alpha \cup (\alpha + n)$.

Third, qubit permutations, are represented by

$$\begin{aligned} C &= \begin{bmatrix} \Pi & 0 \\ 0 & \Pi \end{bmatrix} \\ h &= 0 \end{aligned}$$

where Π is a permutation matrix.

Fourth, the conditional not or CNOT operation on two qubits is represented by

$$\begin{aligned} C &= \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \\ h &= 0 \end{aligned}$$

Fifth, by composing qubit permutations and CNOT operations on selected qubits any linear transformation of the index space $|x\rangle \to |Rx\rangle$ can be realized, where $x \in \mathbb{Z}_2^n$ labels the standard basis states $|x\rangle = |x_1\rangle \otimes \ldots \otimes |x_n\rangle$ and $R \in \mathbb{Z}_2^{n \times n}$ is an invertible matrix (modulo 2). This operation is represented in the symplectic picture by

$$\begin{aligned} C &= \begin{bmatrix} R^{-T} & 0 \\ 0 & R \end{bmatrix} \\ h &= 0 \end{aligned} \tag{3}$$

The qubit permutations and CNOT operation discussed above are special cases of such operations as qubit permutations can be represented as $|x\rangle \to |\Pi x\rangle$ and the CNOT operation as $|x\rangle \to |\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} x\rangle$.

Decomposing a general linear transformation R into CNOTS and qubit permutations can be done by Gauss elimination (a well known technique for the solution of systems of linear equations). In this process R is operated on on the left by CNOTS and qubit permutations to be gradually transformed in an identity matrix. The process operates on R, column by column, first moving a nonzero element into the diagonal position by a qubit permutation, then zeroing the rest of the column by CNOTS. The inverses of the applied operations yield a decomposition of R.

Sixth, we consider Hadamard operations. The Hadamard operation on a single qubit $Q = H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is represented by $C = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $h = 0$. A Hadamard operation on a selected set of qubits is represented by the embedding of such matrices in an identity matrix as explained above. As a special case we mention the Hadamard operation on all qubits, which is represented by $C = P$ and $h = 0$.

Seventh, we consider operations $e^{i(\pi/4)\tau_{\bar{a}}} = \frac{1}{\sqrt{2}}(I + i\tau_{\bar{a}})$ where $a \in \mathbb{Z}_2^{2n}$, $\bar{a} = \begin{bmatrix} a \\ a^T Ua \end{bmatrix}$, and $\tau_{\bar{a}} = i^{a^T Ua}\tau_a$. These operations are represented by

$$\begin{aligned} C &= I + aa^T P \\ h &= C^T Ua \end{aligned} \tag{4}$$

R_2 equal to a basis of the kernel of G', (2) choosing the other columns of R_2 as to make it invertible, (3) setting the last r columns of R_1 equal to the last r columns of R_2 multiplied on the left by G' (This yields a basis of the range of G'), and (4) choosing the other columns of R_1 as to make it invertible. By construction, this implies $G'R_2 = R_1 \begin{bmatrix} 0 & 0 \\ 0 & I_r \end{bmatrix}$.

Now we set

$$\begin{bmatrix} R_1^T & 0 \\ 0 & R_1^{-1} \end{bmatrix} C \begin{bmatrix} R_2 & 0 \\ 0 & R_2^{-T} \end{bmatrix} = \begin{bmatrix} E_{11} & E_{12} & F_{11} & F_{12} \\ E_{21} & E_{22} & F_{21} & F_{22} \\ 0 & 0 & H_{11} & H_{12} \\ 0 & I_r & H_{21} & H_{12} \end{bmatrix} \tag{7}$$

Because the three matrices in the left-hand side of Eq. (7) are symplectic, so is the right-hand side. This leads to the following relations between its submatrices:

$$E_{21}^T = 0 \tag{8}$$
$$E_{11}^T H_{11} + E_{21}^T H_{21} = I \tag{9}$$
$$E_{11}^T H_{12} + E_{21}^T H_{22} = 0 \tag{10}$$
$$E_{22}^T + E_{22} = 0 \tag{11}$$
$$E_{12}^T H_{11} + E_{22}^T H_{21} + F_{21} = 0 \tag{12}$$
$$E_{12}^T H_{12} + E_{22}^T H_{22} + F_{22} = I \tag{13}$$
$$F_{11}^T H_{11} + F_{21}^T H_{21} + H_{11}^T F_{11} + H_{21}^T F_{21} = 0 \tag{14}$$
$$F_{11}^T H_{12} + F_{21}^T H_{22} + H_{11}^T F_{12} + H_{21}^T F_{21} = 0 \tag{15}$$
$$F_{12}^T H_{12} + F_{22}^T H_{22} + H_{12}^T F_{12} + H_{22}^T F_{22} = 0 \tag{16}$$

With Eq. (8) and Eq. (9) we find $H_{11}{=}E_{11}^{-T}$. Now, if we replace R_2 by $R_2 \begin{bmatrix} E_{11}^{-1} & 0 \\ 0 & I_r \end{bmatrix}$, both H_{11} and E_{11} are replaced by I_{n-r}. We will assume that this choice of R_2 was taken from the start. Then, from Eq. (8) and Eq. (10) we find $H_{12} = 0$. From Eq. (11) we learn that E_{22} is symmetric. From Eq. (12) and Eq. (13) we find $F_{21} = E_{12}^T + E_{22}^T H_{21}$ and $F_{22} = I + E_{22}H_{22}$. Substituting these equations in Eqs. (14),(15) and (16), we find that $F_{11} + H_{21}^T E_{12}^T$ is symmetric, $F_{12} = H_{21}^T + E_{12}H_{22}$, and H_{22} is symmetric. Setting $T_1 = R_1$, $T_2 = R_2^T$ (with R_2 chosen as to make $E_{11} = H_{11} = I$), $V_1 = E_{12}$, $V_2 = H_{21}^T$, $Z_1 = E_{22}$, $Z_2 = H_{22}$ and $Z_3 = F_{11} + V_1 V_2^T$, we obtain Eq. (5). Note that Z_3 is symmetric because $F_{11} + V_2 V_1^T$ and $V_2 V_1^T + V_1 V_2^T$ are symmetric. Finally Eq. 6 can be easily verified. This completes the proof. □

To find a decomposition of C in one and two-qubit operations we concentrate on the five matrices in the right-hand side of Eq. (6), all of which are symplectic. Clearly the first and last matrix are linear index space transformations as discussed in Sec. III. These can be decomposed into CNOTs and qubit permutations. The middle matrix corresponds to Hadamard operations on the last r qubits. We will now show that the second and fourth matrix can be realized by one and two-qubit operations of the type $e^{i(\pi/4)\tau_a}$. First note that both matrices are of the form $\begin{bmatrix} I & Z \\ 0 & I \end{bmatrix}$ with Z symmetric. These matrices form a commutative subgroup of the symplectic matrices with

$$\begin{bmatrix} I & Z_a \\ 0 & I \end{bmatrix} \begin{bmatrix} I & Z_b \\ 0 & I \end{bmatrix} = \begin{bmatrix} I & Z_a + Z_b \\ 0 & I \end{bmatrix}.$$

Now, we realize $\begin{bmatrix} I & Z \\ 0 & I \end{bmatrix}$ with one and two-qubit operations by first realizing the ones on off-diagonal positions in Z and then realizing the diagonal. Entries $Z_{k,l} = Z_{l,k} = 1$ are realized by operations $e^{i(\pi/4)\tau_a}$ with $a_k = a_l = 1$ and $a_m = 0$ if $m \neq k$ and $m \neq l$. These are two-qubit operations which realize the off-diagonal part of Z and as a by-product produce some diagonal. Now this diagonal can be replaced by the diagonal of Z by one-qubit operations $e^{i(\pi/4)\tau_a}$ with $a_k = 1$ and $a_m = 0$ if $m \neq k$, which affect only the diagonal entries $Z_{k,k}$. This completes the construction of C by means of one and two-qubit operations.

V. DESCRIPTION OF STABILIZER STATES AND CLIFFORD OPERATIONS USING BINARY QUADRATIC FORMS

In this section we use our binary language to get further results on stabilizer states and Clifford operations. First, we take the binary picture of stabilizer states and their stabilizers and show how Clifford operations act on stabilizer states in the binary picture. We also discuss the binary equivalent of replacing one set of generators of a stabilizer by another. Then we move to two seemingly unrelated results. One is the expansion of a stabilizer state in the standard basis, describing the coefficients with binary quadratic forms. The other is a similar description of the entries of the unitary matrix of a Clifford operation with respect to the same standard basis.

A stabilizer state $|\psi\rangle$ is the simultaneous eigenvector, with eigenvalues 1, of n commutable Hermitian Pauli group elements $i^{f_k}(-1)^{b_k}\tau_{s_k}$, $k = 1, \ldots, n$, where $s_k \in \mathbb{Z}_2^{2n}, k = 1, \ldots, n$ are linearly independent, $f_k, b_k \in \mathbb{Z}_2$ and $f_k = s_k^T U s_k$. The n Hermitian Pauli group elements generate a commutable subgroup of the Pauli group, called the stabilizer $\mathcal{S}$ of the state. We will assemble the vectors s_k as the columns of a matrix $S \in \mathbb{Z}_2^{2n\times n}$ and the scalars f_k and b_k in vectors f and $b \in \mathbb{Z}_2^n$. This binary representation of stabilizer states is common in the literature of stabilizer codes [1]. The fact that the Pauli group elements are commutable is reflected by $S^T P S = 0$. One can think of S, f^T and b^T as the "left half" of C, d^T and h^T of Sec. II. In the style of that section we also define $\bar{S} = \begin{bmatrix} S \\ f^T \end{bmatrix}$.

If $|\psi\rangle$ is operated on by a Clifford operation Q, $Q|\psi\rangle$ is a new stabilizer state whose stabilizer is given by $Q\mathcal{S}Q^\dagger$. As a result, the new set of generators, represented by $\bar{S}'$

$V' = V^{(3)}R_3 = \begin{bmatrix} Z & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & I_{r_c} \end{bmatrix}$ and leaves $W^{(3)} = W'$ unchanged. Through all the transformations we also have to keep track of f and b. We find $f' = \text{diag}(S'^T U S') = \begin{bmatrix} \text{diag}(Z) \\ 0 \end{bmatrix}$. Setting $R = R_1 R_2 R_3$ we find $\begin{bmatrix} b_{ab} \\ b_c \end{bmatrix} = R^T b + \text{diag}(R^T \text{lows}(V^T W + dd^T)R)$.

We still have to prove that Z is full rank. First note that $Z = W_a^{(2)^T} V_a^{(2)}$. From $S^{(2)^T} P S^{(2)} = 0$ and the fact that $[V_a^{(2)}\ V_c^{(2)}]$ and $[W_a^{(2)}\ W_b^{(2)}]$ are full rank, it follows that the columns of $W_b^{(2)}$ span the orthogonal complement of $[V_a^{(2)}\ V_c^{(2)}]$ and the columns of $V_c^{(2)}$ span the orthogonal complement of $[W_a^{(2)}\ W_b^{(2)}]$. Assume now that there exists some $x \in \mathbb{Z}_2^{r_a}$ with $x \neq 0$ and $Zx = 0$, then $V_a^{(2)}x$ is orthogonal to the columns of $W_a^{(2)}$. And $V_a^{(2)}x$ is also orthogonal to the columns of $W_b^{(2)}$. Therefore $V_a^{(2)}x$ is a linear combination of the columns of $V_c^{(2)}$. This is in contradiction with the fact that $[V_a^{(2)}\ V_c^{(2)}]$ is full rank. Therefore, Z is full rank. This completes the proof of part (i).

To prove part (ii), first observe that applying $|x\rangle \rightarrow |T^{-1}x\rangle$ to $|\psi\rangle$ simply replaces $|T\begin{bmatrix} y \\ b_c \end{bmatrix}\rangle$ by $|\begin{bmatrix} y \\ b_c \end{bmatrix}\rangle$, and stabilizer basis transformations only change the description of a stabilizer state but not the state itself. Therefore, we have to prove that

$$|\phi\rangle = \sum_{y \in \mathbb{Z}_2^{(r_a+r_b)}} (-i)^{f_a^T y_a} (-1)^{(y_a^T \text{lows}(Z + f_a f_a^T) y_a + b_{ab}^T y)} |\begin{bmatrix} y \\ b_c \end{bmatrix}\rangle \tag{19}$$

is an eigenvector with eigenvalue one of the operators $i^{f'_k}(-1)^{b'_k}\tau_{s'_k}$ described by $\bar{S}'$ and b'. For $k = 1, \ldots, r_a$, we have

$$\begin{aligned} s'_k &= \begin{bmatrix} Ze_k \\ 0 \\ e_k \\ 0 \end{bmatrix} \\ f'_k &= f_{ak} = z_{k,k} \\ b'_k &= b_{abk} \end{aligned}$$

where e_k is the k-th column of I_{r_a}. With Eq. (17) we find

$$\begin{aligned} & i^{f'_k}(-1)^{b'_k}\tau_{s'_k}|\phi\rangle \\ &= \textstyle\sum_y [i^{f_{ak}} (-1)^{b_{abk}} (-1)^{(Ze_k)^T y_a} (-i)^{f_a^T (y_a + e_k)} \times \\ & (-1)^{((y_a+e_k)^T \text{lows}(Z + f_a f_a^T)(y_a+e_k) + b_a^T (y_a + e_k) + b_b^T y_b)} \times \\ & |\begin{bmatrix} y \\ b_c \end{bmatrix}\rangle] \\ &= \textstyle\sum_y [i^{f_{ak}} (-i)^{f_a^T y_a} (-i)^{f_{ak}} (-1)^{f_a^T y_a f_{ak}} \times \\ & (-1)^{e_k^T Z y_a + b_{abk}} (-1)^{(y_a^T \text{lows}(Z + f_a f_a^T) y_a)} \times \\ & (-1)^{(e_k^T (Z + f_a f_a^T) y_a + b_a^T y_a + b_{abk} + b_b^T y_b)} |\begin{bmatrix} y \\ b_c \end{bmatrix}\rangle] \\ &= |\phi\rangle \end{aligned}$$

For $k = r_a + 1, \ldots, r_b$ we have

$$\begin{aligned} s'_k &= \begin{bmatrix} 0 \\ e_k \\ 0 \end{bmatrix} \\ f'_k &= 0 \\ b'_k &= b_{abk} \end{aligned}$$

where now e_k is the k-th column of $I_{(r_a+r_b)}$. With Eq. (17) we find

$$\begin{aligned} & i^{f'_k}(-1)^{b'_k}\tau_{s'_k}|\phi\rangle \\ &= \textstyle\sum_y [(-1)^{b_{abk}} (-i)^{f_a^T y_a} \times \\ & (-1)^{(y_a \text{lows}(Z + f_a f_a^T) y_a + b_{ab}^T (y + e_k))} |\begin{bmatrix} y \\ b_c \end{bmatrix}\rangle] \\ &= |\phi\rangle \end{aligned}$$

For $k = r_b + 1, \ldots, n$, we find with Eq. (17) that $i^{f'_k}(-1)^{b'_k}\tau_{s'_k}|x\rangle = (-1)^{x_k + b'_k}|x\rangle$. The state $|\phi\rangle$ is clearly an eigenstate of this operator as $x_k + b'_k = 0$ for all states $|x\rangle = |\begin{bmatrix} y \\ b_c \end{bmatrix}\rangle$ and $k = r_b + 1, \ldots, n$. This completes the proof. □

Finally, we show how also the entries of a Clifford matrix can be described with binary quadratic forms, by using Theorem 4. This leads to the following theorem for which we give a constructive proof.

Theorem 6 *Given a Clifford operation Q, represented by $\bar{C}$ and h (or C,d and h) as in Sec. II, Q can be written as*

$$\begin{aligned} Q = \ & (1/\sqrt{2^r}) \textstyle\sum_{x_b \in \mathbb{Z}_2^{n-r}} \sum_{x_r \in \mathbb{Z}_2^r} \sum_{x_c \in \mathbb{Z}_2^r} \\ & [(-i)^{d_{br}^T x_{br}} (-i)^{d_{bc}^T x_{bc}} (-1)^{(h_{bc}^T x_{bc} + x_r^T x_c)} \times \\ & (-1)^{x_{br}^T lows(Z_{br} + d_{br} d_{br}^T) x_{br}} \times \\ & (-1)^{x_{bc}^T lows(Z_{bc} + d_{bc} d_{bc}^T) x_{bc}} |T_1 x_{br}\rangle\langle T_2^{-1} x_{bc} + t|] \end{aligned}$$

where $x_{br} = \begin{bmatrix} x_b \\ x_r \end{bmatrix}$ and $x_{bc} = \begin{bmatrix} x_b \\ x_c \end{bmatrix}$, $T_1, T_2 \in \mathbb{Z}_2^{n \times n}$ are invertible matrices, $Z_{br}, Z_{bc} \in \mathbb{Z}_2^{n \times n}$ are symmetric, $d_{br} = diag(Z_{br})$, $d_{bc} = diag(Z_{bc})$ and $h_{bc}, t \in \mathbb{Z}_2^n$.

Proof: The proof is based on the decomposition of C as a product of five matrices as in Theorem 4. Due to the isomorphism between the group of symplectic matrices C and the extended matrices $\bar{C}$ as defined in Sec. II, this decomposition can be converted into a decomposition of $\bar{C}$ as follows.

$$\begin{aligned} \bar{C} &= \bar{C}^{(1)} \bar{C}^{(2)} \bar{C}^{(3)} \bar{C}^{(4)} \bar{C}^{(5)} \\ &= \begin{bmatrix} T_1^{-T} & 0 & 0 \\ 0 & T_1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} I_n & Z_{br} & 0 \\ 0 & I_n & 0 \\ 0 & d_{br}^T & 1 \end{bmatrix} \times \\ & \begin{bmatrix} I_{n-r} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I_r & 0 \\ 0 & 0 & I_{n-r} & 0 & 0 \\ 0 & I_r & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} I_n & Z_{bc} & 0 \\ 0 & I_n & 0 \\ 0 & d_{bc}^T & 1 \end{bmatrix} \begin{bmatrix} T_2^{-T} & 0 & 0 \\ 0 & T_2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \end{aligned}$$

$C = (I + aa^T P)$. For h we find $h_k = (e_k^T Pa)(a^T Ua + e_k^T Ua)$. With $(e_k^T Pa)(e_k^T Ua) = e_k^T Ua$ this reduces to $h_k = e_k^T(Paa^T Ua + Ua)$ and $h = (I + aa^T P)^T Ua$. This completes the proof. □

ACKNOWLEDGMENTS

We thank Frank Verstraete for useful discussions. Our research is supported by grants from several funding agencies and sources: Research Council KULeuven: Concerted Research Action GOA-Mefisto 666 (Mathematical Engineering); Flemish Government: Fund for Scientific Research Flanders: several PhD/postdoc grants, projects G.0240.99 (multilinear algebra), G.0120.03 (QIT), research communities ICCoS, ANMMM; Belgian Federal Government: DWTC (IUAP IV-02 (1996-2001) and IUAP V-22 (2002-2006): Dynamical Systems and Control: Computation, Identification & Modelling

[1] D. Gottesman, Ph.D. thesis, Caltech (1997), quant-ph/9705052.

[2] I. Chuang and M. Nielsen, *Quantum computation and quantum information* (Cambridge University Press, 2000).

[3] D. Gottesman, *The Heisenberg representation of quantum computers*, quant-ph/9807006.

[4] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, Phys. Rev. A **67**, 022310 (2003).