# Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic

Erik Hostens,* Jeroen Dehaene, and Bart De Moor
*Katholieke Universiteit Leuven, ESAT-SCD, B-3001, Belgium*
(Received 31 August 2004; published 11 April 2005)

We describe generalizations of the Pauli group, the Clifford group, and stabilizer states for qudits in a Hilbert space of arbitrary dimension $d$. We examine a link with modular arithmetic, which yields an efficient way of representing the Pauli group and the Clifford group with matrices over $\mathbb{Z}_d$. We further show how a Clifford operation can be efficiently decomposed into one and two-qudit operations. We also focus in detail on standard basis expansions of stabilizer states.

DOI: 10.1103/PhysRevA.71.042315 PACS number(s): 03.67.−a

## I. INTRODUCTION

We study stabilizer states and Clifford operations for systems built from qudits (systems with a $d$-dimensional Hilbert space). We work in a matrix framework using modular arithmetic, generalizing results for qubits from Ref. [1]. We put special emphasis on the less studied case where $d$ is not prime.

The stabilizer formalism has already proved to be useful in many applications such as quantum error correction, entanglement distillation, and quantum computation [2–5]. The $n$-qudit generalized Pauli group and Clifford group and the related concepts of stabilizer codes and states have been studied in various levels of detail in a number of papers [6–15].

Our motivation is not so much the study of stabilizer codes and their error correcting capacities, but the study of mathematically interesting states and operations that could play a role in quantum algorithms. Although it is well known that building quantum algorithms with stabilizer states and Clifford operations only is not sufficient to disallow efficient simulation on a classical computer, we think it is likely that the rich structure of this formalism will play a role in future quantum algorithms. Due to this focus, we pay attention to describing and realizing Clifford operations in more detail than is usually needed for coding applications. [To specify a Clifford operation "completely" (that is, up to only a global phase), one has to specify the image under conjugation of $2n$ independent Pauli operations including the resulting phase, whereas to realize an encoding operator for a $k$-dimenional code, only $k$ images are needed and the phases are of minor importance.]

In addition to presenting known results in an often different, and in our opinion practical language, we also present results not contained in the references above. We give a description of an $n$-qudit Clifford operation by a $2n \times 2n$ matrix $C$ with entries in $\mathbb{Z}_d$ and a $2n$-dimensional vector $h$ with entries in $\mathbb{Z}_{2d}$ and derive necessary and sufficient conditions for $C$ and $h$ to define a Clifford operation. We give formulas for multiplying and inverting Clifford operations represented in this way.

We present a decomposition of a general Clifford operation, specified in full detail by a matrix $C$ and $h$, into a selected set of one and two-qudit operations, by thinking in terms of matrix manipulations on $C$ and $h$. We also focus in detail on the standard basis expansion of stabilizer states. From Refs. [13–15] formulas can be derived describing the standard basis expansion of graph states by means of a quadratical form. In Refs. [14,15] this is done for the case when the one-qudit configuration space $\{1, \ldots, d\}$ is given the structure of a finite field. In Ref. [13] this space can be any finite Abelian group. In this paper we consider cyclic groups. References [14,15] state the equivalence of graph states and general stabilizer states. In Ref. [15] this equivalence is to be understood as local Clifford equivalence. That is, any $n$-qudit stabilizer state (with a field as one-qudit configuration space) can be transformed into a graph state through the action of $n$ one-qudit Clifford operations. In our setting, however, as we are not focusing on codes, we want a description of the original stabilizer state (without the local Clifford operations) as well. In Ref. [14] another notion of equivalence between graph states and stabilizer states is used (introducing the concept of auxiliary nodes in the graph). As a result the standard basis expansion of a general stabilizer state is not described directly but as a sum of a large number of states. Moreover, for the case where the configuration space is not a field (in our case that is when $d$ is not prime) not all stabilizer states are equivalent to graph states but an extra condition has to be imposed. In the present paper we work with a more general description of stabilizer states without this extra condition (described below by matrices $S$ with possibly more than $n$ columns) and we give a direct description (without sum) of the standard basis expansion of general stabilizer states. We believe that standard basis expansions of stabilizer states can be an essential ingredient in understanding the action of non-Clifford operations on stabilizer states.

This paper is structured as follows. Definitions of generalizations of the Pauli group and the Clifford group for qudits are given in Sec. II, together with their matrix representation. Special Clifford operations, that are of particular interest in the decomposition of a Clifford operation, are discussed in Sec. III. An efficient decomposition of a Clifford operation on $n$ qudits into a selected set of one and two-qubit Clifford operations, is explained in Sec. IV. In Sec. V, we define sta-

*Electronic address: erik.hostens@esat.kuleuven.ac.be

 

bilizer states of $n$ qudits and show the expansion in the standard basis can be described with linear and quadratic operations.

In the following, by $A=B \bmod d$ we mean that all corresponding entries of matrices $A$ and $B$ are equal modulo $d$, where $d$ is an integer different from 0. We will also write $a=b \bmod c$ with $a$, $b$, and $c$ vectors, as a shorthand notation for $a_i=b_i \bmod c_i$, for every $i=1,\ldots,n$.

## II. THE GENERALIZED PAULI GROUP AND CLIFFORD GROUP

In this section, we discuss the description of the generalized Pauli group on $n$ qudits and the generalized Clifford group in modular arithmetic. Generalizations of the Pauli group to systems of arbitrary dimensions are discussed in Refs. [6–8]. The Clifford group is defined as the group containing all unitary operations that map the Pauli group to itself under conjugation.

### A. The generalized Pauli group

Let $d$ be the Hilbert space dimension of one qudit. We define unitary operations $X^{(d)}$ and $Z^{(d)}$ as follows:

$$X^{(d)}|j\rangle = |j+1\rangle,$$

$$Z^{(d)}|j\rangle = \omega^j|j\rangle, \tag{1}$$

where $j \in \mathbb{Z}_d$ and $\omega$ is a primitive $d$th root of unity. Addition in the ket is carried out modulo $d$. Tensor products of these operations will be denoted as follows: for $v,w \in \mathbb{Z}_d^n$, and $a := \left[\begin{smallmatrix} v \\ w \end{smallmatrix}\right] \in \mathbb{Z}_d^{2n}$, we denote

$$XZ(a) := X^{v_1}Z^{w_1} \otimes \cdots \otimes X^{v_n}Z^{w_n}. \tag{2}$$

From Eqs. (1) and (2), it follows that, for $x \in \mathbb{Z}_d^n$,

$$XZ(a)|x\rangle = \omega^{w^T x}|x+v\rangle. \tag{3}$$

We define the Pauli group $\mathcal{P}_n$ on $n$ qudits to contain all $d^{2n}$ tensor products (2) with an additional complex phase factor $\zeta^\delta$, where $\zeta$ is a square root of $\omega$ and $\delta \in \mathbb{Z}_{2d}$. In the following, we will omit the superscript $(d)$ and refer to the generalized Pauli group simply as Pauli group.

Multiplication of two Pauli group elements can be translated into operations on vectors in $\mathbb{Z}_d^{2n}$ as follows:

$$\zeta^\delta XZ(a)\zeta^\epsilon XZ(b) = \zeta^{\delta+\epsilon+2a^T U b} XZ(a+b), \tag{4}$$

where $U := \left[\begin{smallmatrix} 0_n & 0_n \\ I_n & 0_n \end{smallmatrix}\right]$. Addition in the argument of $XZ$ is done modulo $d$, and addition in the exponent of $\zeta$ is done modulo $2d$. Equation (4) yields the commutation relation

$$XZ(a)XZ(b) = \omega^{a^T P b} XZ(b)XZ(a), \tag{5}$$

$$\text{where } P = U - U^T \bmod d. \tag{6}$$

Note that the order of $XZ(a)$ divides $d$ unless $d$ is an even number and $a^T U a$ is odd. In the latter case the order is $2d$. Indeed, with Eq. (4) one can easily verify that $XZ(a)^d = \zeta^{d(d-1)a^T U a} I$. The introduction of a phase $\zeta^\delta$ rather than $\omega^\delta$ is only necessary when $d$ is even. Simplifications for odd $d$ are considered in Appendix C.

### B. The generalized Clifford group

We now define a generalization of the Clifford group on $n$ qudits in an analogous way as for qubits. A Clifford operation $Q$ is a unitary operation that maps the Pauli group on $n$ qudits to itself under conjugation or

$$Q\mathcal{P}_n Q^\dagger = \mathcal{P}_n.$$

Because $QXZ(a)XZ(b)Q^\dagger = [QXZ(a)Q^\dagger][QXZ(b)Q^\dagger]$, it is sufficient to know the image of a generating set of the Pauli group in order to know the image of all Pauli group elements. $Q$ is then defined up to a global phase factor. This can be seen as follows. Suppose that two Clifford operations $Q_1$ and $Q_2$ give rise to the same image for every Pauli group element or for every $A \in \mathcal{P}_n: Q_1 A Q_1^\dagger = Q_2 A Q_2^\dagger$. It follows for every $A$ that $Q_2^\dagger Q_1 A = A Q_2^\dagger Q_1$. The only unitary operations that commute with every single Pauli group element are multiples of the identity [18], which completes the proof. We take the generating set of the Pauli group to be $XZ(E_k)$, $k=1,\ldots,2n$, where $E_k$ are the standard basis vectors of $\mathbb{Z}_d^{2n}$. We denote their images under conjugation by $Q$ as $\zeta^{h_k}XZ(C_k)$. We will assemble the vectors $C_k$ as the columns of a matrix $C \in \mathbb{Z}_d^{2n\times 2n}$ and the scalars $h_k$ in a vector $h \in \mathbb{Z}_{2d}^{2n}$. The image $\zeta^\epsilon XZ(b)$ of $\zeta^\delta XZ(a)$ under conjugation by $Q$, where $a$ is an arbitrary vector in $\mathbb{Z}_d^{2n}$, can be found by repeated application of Eq. (4). This yields

$$b = Ca \bmod d,$$

$$\epsilon = \delta + [h - \mathcal{V}_{\text{diag}}(C^T U C)]^T a + a^T[2\mathcal{P}_{\text{upps}}(C^T U C) + \mathcal{P}_{\text{diag}}(C^T U C)]a \bmod 2d, \tag{7}$$

where $\mathcal{V}_{\text{diag}}(M)$ is defined as the vector containing the diagonal of $M$, $\mathcal{P}_{\text{diag}}(M)$ the diagonal matrix with the diagonal of $M$, and $\mathcal{P}_{\text{upps}}(M)$ the strictly upper triangular part of $M$. The Clifford operation $Q$ is (up to a global phase factor) completely defined by $C$ and $h$. Note that the right-hand side (RHS) of Eq. (7) is calculated modulo $2d$, although it contains matrices over $\mathbb{Z}_d$. It can be verified that every entry modulo $d$ in the expression is multiplied by an even factor.

We can compose two Clifford operations $Q$ and $Q'$, which again yields a Clifford operation $Q''=Q'Q$. To find its corresponding $C''$ and $h''$ we have to find the images under the second operation of the images under the first operation of the standard basis vectors. By using Eq. (7), we get

$$C'' = C'C \bmod d,$$

$$h'' = h + C^T h' + \mathcal{V}_{\text{diag}}(C^T[2\mathcal{P}_{\text{upps}}(C'^T U C') + \mathcal{P}_{\text{diag}}(C'^T U C')]C) - C^T \mathcal{V}_{\text{diag}}(C'^T U C') \bmod 2d. \tag{8}$$

The inverse $Q^\dagger$ of a Clifford operation $Q$ defined by $C$ and $h$ is defined by $C'$ and $h'$, where

$$C' = C^{-1} \bmod d,$$

$$h' = -C^{-T}\{h + \mathcal{V}_{\mathrm{diag}}(C^T[2\mathcal{P}_{\mathrm{upps}}(C^{-T}UC^{-1}) + \mathcal{P}_{\mathrm{diag}}(C^{-T}UC^{-1})]C) - C^T\mathcal{V}_{\mathrm{diag}}(C^{-T}UC^{-1})\} \bmod 2d, \tag{9}$$

which can be verified with Eq. (8). $M^{-T}$ is short for $(M^{-1})^T$. We will show below that $C^{-1}=-PC^TP \bmod d$.

### C. Conditions on $C$ and $h$

Not all $C \in \mathbb{Z}_d^{2n\times 2n}$ and $h \in \mathbb{Z}_{2d}^{2n}$ define a Clifford operation. To see this, consider a Clifford operation $Q$ with corresponding $C$ and $h$. From the commutation relation (5) it follows that $C$ is a symplectic matrix, i.e., $C$ satisfies $C^TPC=P \bmod d$. Indeed, we have

$$XZ(a)XZ(b) = \omega^{a^TPb}XZ(b)XZ(a),$$

$$QXZ(a)Q^\dagger QXZ(b)Q^\dagger = \omega^{a^TPb}QXZ(b)Q^\dagger QXZ(a)Q^\dagger,$$

$$XZ(Ca)XZ(Cb) = \omega^{a^TPb}XZ(Cb)XZ(Ca),$$

where we omitted global phase factors on the LHS and RHS, as they cancel each other. Also,

$$XZ(Ca)XZ(Cb) = \omega^{a^TC^TPCb}XZ(Cb)XZ(Ca).$$

Since this holds for every value of $a$ and $b$, it follows that $C$ is symplectic. Note that the inverse of a symplectic matrix $C$ is simply $C^{-1}=-PC^TP \bmod d$. Secondly, $h$ satisfies

$$(d-1)\mathcal{V}_{\mathrm{diag}}(C^TUC) + h = 0 \bmod 2, \tag{10}$$

for $\zeta^{h_k}XZ(C_k)=QXZ(E_k)Q^\dagger$ has, similar to $XZ(E_k)$, order $d$. With Eq. (4) we have $[\zeta^{h_k}XZ(C_k)]^d=\zeta^{d[(d-1)C_k^TUC_k+h_k]}I$, and it follows that Eq. (10) is satisfied. We will prove below that every symplectic $C$ and $h$ satisfying Eq. (10) define a Clifford operation $Q$.

## III. SPECIAL CLIFFORD OPERATIONS

In this section we present a number of special Clifford operations and their defining $C$ and $h$. These will be of particular interest for the decomposition of an arbitrary Clifford operation into one and two-qubit Clifford operations.

The Pauli group elements $XZ(a)$ are a special class of the Clifford operations. Note that, as for any Clifford operation, the global phase factor of a Pauli group element cannot be represented. Considering the images of $XZ(E_k)$, it can be easily verified that $XZ(a)$ is defined by

$$C = I \mod d,$$

$$h = -2Pa \mod 2d.$$

A Clifford operation acting on a subset $\alpha\subset\{1,\ldots,n\}$ of $n$ qudits gives rise to a symplectic matrix on the rows and columns with indices in $\alpha\cup(\alpha+n)$, embedded in an identity matrix [that is, $C_{kk}=1 \bmod d$, for every $k\notin\alpha\cup(\alpha+n)$ and $C_{kl}=0 \bmod d$ if $k\neq l$ and $k$ or $l\notin\alpha\cup(\alpha+n)$]. Also $h_k=0 \bmod 2d$ if $k\notin\alpha\cup(\alpha+n)$.

Any invertible linear transformation of the configuration space $|x\rangle\rightarrow|Tx\rangle$ can be realized by a Clifford operation, with $x\in\mathbb{Z}_d^n$ and $T\in\mathbb{Z}_d^{n\times n}$ an invertible matrix modulo $d$. This operation is defined by

$$C = \begin{bmatrix} T & 0 \\ 0 & T^{-T} \end{bmatrix} \mod d,$$

$$h = 0 \mod 2d.$$

This can be verified by looking at the image of $XZ(a)$, with an arbitrary $a=\left[\begin{smallmatrix} v \\ w \end{smallmatrix}\right] \in \mathbb{Z}_d^{2n}$:

$$QXZ(a)Q^\dagger = \left(\sum_{x\in\mathbb{Z}_d^n}|Tx\rangle\langle x|\right)\left(\sum_{y\in\mathbb{Z}_d^n}\omega^{w^Ty}|y+v\rangle\langle y|\right) \times\left(\sum_{z\in\mathbb{Z}_d^n}|z\rangle\langle Tz|\right)$$

$$= \sum_{y\in\mathbb{Z}_d^n}\omega^{w^Ty}|Ty+Tv\rangle\langle Ty|$$

$$= \sum_{y\in\mathbb{Z}_d^n}\omega^{w^TT^{-1}y}|y+Tv\rangle\langle y|$$

$$= XZ\left(\begin{bmatrix} Tv \\ T^{-T}w \end{bmatrix}\right).$$

As $C^TUC=U \bmod d$, we see with Eq. (7) that $h=0 \bmod 2d$. Special cases of this class of Clifford operations are qudit permutations, with $C=\left[\begin{smallmatrix} \Pi & 0 \\ 0 & \Pi \end{smallmatrix}\right]$, where $\Pi$ is a permutation matrix, and the two-qudit SUM gate $|x\rangle|y\rangle\rightarrow|x\rangle|x+y\rangle$ with $x,y\in\mathbb{Z}_d$, with

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mod d.$$

Note that this operation is a natural generalization of the two-qubit controlled-NOT (CNOT) gate.

The $d$-dimensional discrete Fourier transform $|x\rangle\rightarrow(1/\sqrt{d})\Sigma_{k=0}^{d-1}\omega^{kx}|k\rangle$ on one qudit, with $x\in\mathbb{Z}_d$, is defined by $C=\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \bmod d$ and $h=0 \bmod 2d$. We verify this in the same way as for the invertible configuration space transformation, now with $a=\left[\begin{smallmatrix} v \\ w \end{smallmatrix}\right] \in \mathbb{Z}_d^2$:

$$QXZ(a)Q^\dagger = \left(\frac{1}{\sqrt{d}}\sum_{t,u\in\mathbb{Z}_d}\omega^{tu}|t\rangle\langle u|\right)\left(\sum_{y\in\mathbb{Z}_d}\omega^{wy}|y+v\rangle\langle y|\right) \times\left(\frac{1}{\sqrt{d}}\sum_{x,z\in\mathbb{Z}_d}\omega^{-xz}|z\rangle\langle x|\right)$$

$$= \frac{1}{d}\sum_{t,y,x\in\mathbb{Z}_d}\omega^{t(y+v)+wy-xy}|t\rangle\langle x|$$

$$= \frac{1}{d}\sum_{y\in\mathbb{Z}_d}\omega^{(t+w-x)y}\sum_{t,x\in\mathbb{Z}_d}\omega^{tv}|t\rangle\langle x|$$

$$= \sum_{x \in \mathbb{Z}_d} \omega^{(x-w)v} |x-w\rangle\langle x|$$

$$= \omega^{-vw} XZ\left(\begin{bmatrix} -w \\ v \end{bmatrix}\right).$$

As $C^T U C = -U^T \bmod d$, we see with Eq. (7) that $h = 0 \bmod 2d$. This operation is the qudit equivalent of the Hadamard gate on one qubit.

Analogous to the qubit phase gate, a phase gate on one qudit can be defined as $|x\rangle \to \zeta^{x(x+d)}|x\rangle$, with $x \in \mathbb{Z}_d$. This operation corresponds to $C = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right] \bmod d$ and $h = \left[\begin{smallmatrix} d+1 \\ 0 \end{smallmatrix}\right] \bmod 2d$. Indeed, for all $a = \left[\begin{smallmatrix} v \\ w \end{smallmatrix}\right] \in \mathbb{Z}_d^2$:

$$QXZ(a)Q^\dagger = \sum_{y \in \mathbb{Z}_d} \zeta^{2wy+(y+v)(y+v+d)-y(y+d)} |y+v\rangle\langle y|$$

$$= \zeta^{v(v+d)} \sum_{y \in \mathbb{Z}_d} \omega^{(v+w)y} |y+v\rangle\langle y|.$$

As $C^T U C = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right] \bmod d$, $v(v+d)$ must be equal to $(h - \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right])^T a + v^2 \bmod 2d$ according to Eq. (7), which is the case for the given $h$.

## IV. DECOMPOSITION OF A CLIFFORD OPERATION IN ONE AND TWO-QUDIT OPERATIONS

In order to prove that any symplectic matrix $C$ and $h$ satisfying Eq. (10) define a Clifford operation, we will expand an arbitrary symplectic $C$ into symplectic elementary row operations that can be realized as Clifford operations on maximally two qudits at the same time. What is more, this decomposition is a worthy candidate as a practical realization of a Clifford operation. The possibility of this kind of decomposition into a selected set of one and two-qudit operations is briefly discussed in Ref. [8]. Our scheme is related to the method of Ref. [6] in which Euclid's algorithm is incorporated in order to generate any one-qudit Clifford operation.

First, we mention that the main problem is realizing $C$, not $h$, for once a Clifford operation $Q$ defined by $C$ and $h$ is realized, we can realize $Q'$ defined by $C$ and an arbitrary $h'$ satisfying Eq. (10) by doing an extra operation $XZ\{CP[(h'-h)/2]\}$ on the left or $XZ\{P[(h'-h)/2]\}$ on the right of $Q$. Note that as both $h$ and $h'$ satisfy (10), $h'-h$ is even.

We first give an overview of the elementary row operations that we will use to transform an arbitrary symplectic matrix $C$ into the $2n \times 2n$ identity matrix $I$. As $I$ is formed by left multiplication of such elementary row operations on $C$, a decomposition of $C$ then consists of the inverses of these operations in reverse order. Since these operations act on maximally two qudits at the same time, they are defined by a symplectic $4 \times 4$ or $2 \times 2$ matrix embedded in the identity matrix as explained in the preceding section. In the following, we will only show this part of the operations.

First, we consider some configuration space transformations (of the form $C = \left[\begin{smallmatrix} T & 0 \\ 0 & T^{-T} \end{smallmatrix}\right]$). These operations combine only rows from the same block (we call rows $1, \ldots, n$ the upper block and rows $n+1, \ldots, 2n$ the lower block) and have a similar action in both blocks at the same time. For instance, we can switch two rows $i$ and $j$ in the upper block: at the same time, rows $n+i$ and $n+j$ in the lower block are also switched. This operation is defined by

$$C = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \bmod d.$$

Multiplying a row $i$ with an invertible number $r \in \mathbb{Z}_d$ results in multiplying the corresponding row $n+i$ in the other block by $r^{-1}$. A number $r \in \mathbb{Z}_d$ has an inverse if $r$ and $d$ are coprime, i.e., $\gcd(r,d) = 1$. This operation is defined by $C = \left[\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right]$. The last configuration space transformation we consider, is adding one row $i$ multiplied by an arbitrary factor $g \in \mathbb{Z}_d$ to another row $j$. At the same time, row $n+j$, multiplied by $-g$, is added to row $n+i$. This operation is defined by

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ g & 1 & 0 & 0 \\ 0 & 0 & 1 & -g \\ 0 & 0 & 0 & 1 \end{bmatrix} \bmod d.$$

Secondly, we will also need operations that combine rows of different blocks. Switching two rows $i$ and $n+i$ can be carried out by the discrete Fourier transform. Recall that this operation is defined by $C = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. After switching of the rows, row $i$ is multiplied by $-1$. By applying the inverse of the discrete Fourier transform, row $n+i$ instead of row $i$ is multiplied by $-1$. Applying $\Sigma_{x \in \mathbb{Z}_d} \zeta^{gx(x+d)} |x\rangle\langle x|$ (which is the same as applying the phase gate $g$ times) on the $i$th qudit, with $g \in \mathbb{Z}_d$, results in the addition of row $i$ multiplied by $g$ to its corresponding row $n+i$, according to

$$C = \begin{bmatrix} 1 & 0 \\ g & 1 \end{bmatrix} \bmod d.$$

We could introduce more row operations that define one or two-qudit Clifford operations, but the ones described so far suffice. Next we give a constructive way of transforming $C$ into the identity matrix $I$. If we are able to transform $C$ into $C'$ by transforming columns $C_1$ and $C_{n+1}$ into the corresponding columns $E_1$ and $E_{n+1}$ of $I$, it follows from the symplecticity of $C'$ that the first and $(n+1)$-th row of $C'$ are equal to the corresponding rows of $I$. We then have

$$C' = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & & & & 0 & & & \\ \vdots & & C'_{(11)} & & \vdots & & C'_{(12)} & \\ 0 & & & & 0 & & & \\ 0 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 0 & & & & 0 & & & \\ \vdots & & C'_{(21)} & & \vdots & & C'_{(22)} & \\ 0 & & & & 0 & & & \end{bmatrix}.$$

Leaving the first qudit out, we can continue by transforming the second and $(n+2)$-th column of $C'$ into the corresponding columns of $I$, and so on. This recursive procedure eventually leads to $I$. Now we only have to show how columns $C_1$ and $C_{n+1}$ are transformed into $E_1$ and $E_{n+1}$. Let us first consider the case where the upper left entry $C_{11}$ has an inverse in $\mathbb{Z}_d$. Multiplying the first row by $C_{11}^{-1}$ changes this entry to 1. Next we add the first row, multiplied by $-C_{k1}$, to row $k$, and this for $k=2,\ldots,n$, setting the $k$th entry of $C_1$ to 0. The first column now has the form $[1\ 0,\ldots,0|C'_{n+1,1}C_{n+2,1},\ldots,C_{2n,1}]^T$. Now we add the first row multiplied by $-C'_{n+1,1}$ to row $n+1$, setting the $(n+1)$-th entry of $C_1$ to 0. The discrete Fourier transform on the first qudit changes $C_1$ into $[0\ 0,\ldots,0|1\ C_{n+2,1},\ldots,C_{2n,1}]^T$. In the same way as for the upper half of $C_1$, we make zeros below the $(n+1)$-th position. Note that nothing happens to the upper half, for all entries there are 0. Switching the first (now we use the inverse of the discrete Fourier transform) with the $(n+1)$-th row again yields $E_1$. We call the matrix made so far $C''$. From the symplecticity of $C''$ it follows that $C''_{n+1,n+1}=1 \bmod d$, and we can repeat for the $(n+1)$-th column the same procedure we did for the first column. Note that none of the operations yielding $E_{n+1}$ out of $C''_{n+1}$ will affect $C''_1=E_1$, except the discrete Fourier transform and its inverse on the first qudit, but they cancel each other. Since the number of elementary operations for one column is $O(n)$, the total number of operations transforming $C$ into $I$ is $O(n^2)$.

If the entry $C_{11}$ has no inverse modulo $d$, but there is a $C_{k1}$ in the first row that does have an inverse, this entry can be switched into the first position by a permutation of two qudits and possibly the discrete Fourier transform on the first qudit. Note that it is possible that none of the entries of $C_1$ has an inverse. Indeed, since $C$ is invertible, the only restriction on one single column of $C$ is that the greatest common divisor of all its entries has an inverse. For every two entries $C_{i1}$ and $C_{n+i,1}$ or $C_{i1}$ and $C_{j1}$ from the same block, the gcd of these two can be formed in one of the two entries by recursively substracting a multiple of one row from the other following Euclid's algorithm [16]. The other entry can then be made 0 since it is a multiple of the gcd. A worst case scenario would be that all $2n$ combinations of $2n-1$ entries have a gcd that is not invertible. The procedure goes as follows:

$$\begin{bmatrix} C_{11} \\ C_{21} \\ \vdots \\ C_{n1} \\ C_{n+1,1} \\ C_{n+2,1} \\ \vdots \\ C_{2n,1} \end{bmatrix} \rightarrow \begin{bmatrix} \gcd(C_{11},C_{n+1,1}) \\ \gcd(C_{21},C_{n+2,1}) \\ \vdots \\ \gcd(C_{n1},C_{2n,1}) \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} \gcd(C_{11},\ldots,C_{2n,1}) \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

In this way, $C$ is decomposed into $O[n^2\ln(d)]$ elementary operations, as the computational complexity for finding the gcd of two positive integers less than $d$ with Euclid's algorithm is $O[\ln(d)]$ [16].

## V. STABILIZER STATES

In this section we define stabilizer states for qudits of arbitrary dimensions. A stabilizer state is a state of an $n$-qudit system that is a simultaneous eigenvector, with eigenvalues 1, of a subgroup of $d^n$ commuting elements of the Pauli group, which is called the stabilizer $\mathcal{S}$ of the stabilizer state. The stabilizer state is completely determined by a generating set for $\mathcal{S}$. The description of such a generating set in modular arithmetic provides an efficient tool of describing the stabilizer state and its behavior under the action of a Clifford operation. Finally, we give an expansion of an arbitrary stabilizer state in the standard basis.

### A. Definition and description in modular arithmetic

A stabilizer state $|\psi\rangle$ is the simultaneous eigenvector, with eigenvalues 1, of a subgroup of $d^n$ commuting elements of the Pauli group which does not contain multiples of the identity other than the identity itself. We call this subgroup the stabilizer $\mathcal{S}$ of $|\psi\rangle$. A generating set for $\mathcal{S}$ consists of elements $\zeta^{f_k}XZ(S_k)$, $k=1,\ldots,m$, where $S_k\in\mathbb{Z}_d^{2n}$ and $f_k\in\mathbb{Z}_{2d}$. We will assemble the vectors $S_k$ as the columns of a matrix $S\in\mathbb{Z}_d^{2n\times m}$ and the scalars $f_k$ in a vector $f\in\mathbb{Z}_{2d}^m$. We call $S$ a generator matrix and $f$ the corresponding phase vector that together define $\mathcal{S}$. The fact that the elements of $\mathcal{S}$ commute is reflected by $S^TPS=0 \bmod d$. We choose $m$ to be the minimal cardinality of a generating set of $\mathcal{S}$. Note that, as opposed to the situation for qubits, $m$ can be larger than $n$. It can be verified that if $m>n$, the imposed condition in Ref. [14] for a stabilizer state to be equivalent to a graph state, is not fulfilled. If $d$ has only single prime factors, then $m=n$. If $d$ has multiple prime factors, then $n\leqslant m\leqslant 2n$. A simple example for $d=4$ and $n=1$ is the state $1/\sqrt{2}(|0\rangle+|2\rangle)$ with stabilizer $\{I,X^2,Z^2,X^2Z^2\}$: in this case $m=2$. We will describe below how to construct such a minimal generating set. The fact that $\mathcal{S}$ does not contain multiples of the identity other than the identity itself implies that the phase vector $f$ satisfies

$$[f-\mathcal{V}_{\mathrm{diag}}(S^TUS)]^Tr+r^T[\mathcal{P}_{\mathrm{diag}}(S^TUS)+2\mathcal{P}_{\mathrm{upps}}(S^TUS)]r = 0 \bmod 2d, \quad \forall\, r\in\mathbb{Z}_d^m | Sr=0 \bmod d \tag{11}$$

The description of $\mathcal{S}$ by $S$ and $f$ is not unique, as they represent a generating set for $\mathcal{S}$. By applying an invertible

linear transformation $R \in \mathbb{Z}_d^{m\times m}$ to the right on $S$ and transforming $f$ appropriately, another generating set $\zeta^{f'_k} XZ(S'_k)$ is formed. By repeated application of Eq. (4), one finds

$$S' = SR \bmod d,$$

$$f' = R^T[f - \mathcal{V}_{\text{diag}}(S^T U S)] + \mathcal{V}_{\text{diag}}(R^T[2\mathcal{P}_{\text{upps}}(S^T U S) + \mathcal{P}_{\text{diag}}(S^T U S)]R) \bmod 2d. \quad (12)$$

We will refer to this as a stabilizer generator matrix change.

If $|\psi\rangle$ is operated on by a Clifford operation $Q$, defined by $C$ and $h$, then $Q|\psi\rangle$ is a new stabilizer state whose stabilizer is given by $Q\mathcal{S}Q^\dagger$. By application of Eq. (7), we can calculate an $S'$ and $f'$ for this stabilizer, resulting in

$$S' = CS \mod d,$$

$$f' = f + S^T[h - \mathcal{V}_{\text{diag}}(C^T U C)] + \mathcal{V}_{\text{diag}}(S^T[2\mathcal{P}_{\text{upps}}(C^T U C) + \mathcal{P}_{\text{diag}}(C^T U C)]S) \mod 2d. \quad (13)$$

We can construct a minimal generating set $\zeta^{f_k} XZ(S_k)$, $k=1,\ldots,m$, for an arbitrary stabilizer $\mathcal{S}$, given a generating set $\zeta^{f'_l} XZ(S'_l)$, $l=1,\ldots,m'$, for $\mathcal{S}$ using the Smith normal form (see Appendix A). This can be done as follows. The $S'_l$ are assembled in the matrix $S'$. Now we compute the Smith normal form $F=KS'L$ of $S'$, with $K \in \mathbb{Z}_d^{2n\times 2n}$ and $L \in \mathbb{Z}_d^{m'\times m'}$ invertible matrices. $S'L$ is just another generator matrix of the stabilizer. From the definition of the Smith normal form it follows that $S'L$ is a generator matrix having a minimal number of nonzero columns. The rightmost $m-m'$ columns of $S'L$ that are zero (as $S'L=K^{-1}F$) can be omitted. We call this new generator matrix $S$ and $f$ is formed out of $f'$ with Eq. (12). Note that no linear combination of the columns $S_k$ of $S$ is zero unless the coefficients in this linear combination are a multiple of the order of the columns or, for $k=1,\ldots,m$,

$$\text{if } \sum_k r_k S_k = 0 \mod d, \quad \text{then } r_k S_k = 0 \mod d. \quad (14)$$

With this, the stabilizer phase condition (11) can be simplified to, for $k=1,\ldots,m$:

$$(r_k - 1) r_k S_k^T U S_k + r_k f_k = 0 \mod 2d,$$

$$\forall r_k \in \mathbb{Z}_d | r_k S_k = 0 \mod d. \quad (15)$$

### B. Description of a stabilizer state with linear and quadratic forms

We provide an expansion of an arbitrary stabilizer state in the standard basis for an $n$-qudit state. This is stated in the following theorem.

*Theorem 1*. (i) If $S \in \mathbb{Z}_d^{2n\times m}$ and $f \in \mathbb{Z}_{2d}^m$ define a stabilizer state $|\psi\rangle$ as described above, then $S$ and $f$ can be transformed by a configuration space transformation $|x\rangle \to |T^{-1}x\rangle$, with $T \in \mathbb{Z}_d^{n\times n}$, and a stabilizer generator matrix change $R \in \mathbb{Z}_d^{m\times m}$ into the form $S'$ and $f'$, with

$$S' = \begin{bmatrix} T^{-1} & 0 \\ 0 & T^T \end{bmatrix} SR = \begin{bmatrix} \overline{Q} & 0 \\ \overline{B} & \bar{\bar{B}} \end{bmatrix} = \begin{bmatrix} Q \\ B \end{bmatrix} \mod d,$$

$$f'^T = [\overline{f'}^T \quad \bar{\bar{f}}'^T] \mod 2d, \quad (16)$$

where $Q$ is a pseudodiagonal matrix in Smith normal form and $Q^T B \bmod d$ is symmetric. $\overline{Q}$ and $\overline{B}$ are the left square $n\times n$ parts of $Q$ and $B$.

(ii) The state $|\psi\rangle$ can be expanded in the standard basis (up to a normalization factor) as

$$|\psi\rangle = \sum_{t\in\mathbb{Z}_d^n} \zeta^{t^T M t + p^T t} |T(\overline{Q}t + x^*)\rangle, \quad (17)$$

where $M := \overline{QB} \bmod d$, $p := \overline{f'} - \mathcal{V}_{\text{diag}}(M) + 2\overline{B}^T x^* \bmod 2d$.

If we define the vector $\overline{q}$ of flength $n$ with entries

$$q_k := \begin{cases} d & \text{if } Q_{kk} = 0 \mod d, \\ Q_{kk} & \text{if } Q_{kk} \neq 0 \mod d, \end{cases} \quad k = 1,\ldots,n$$

and the vector $q$ of length $m$ as

$$q = [\overline{q}^T \underbrace{d \ldots d}_{m-n}]^T.$$

Then $x^* \in G_{\overline{q}} := \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_n}$ is defined as the unique solution of

$$B^T x = y \mod q, \quad (18)$$

where $y \in G_q$ has entries

$$y_k := \begin{cases} -\dfrac{(d-q_k)B_{kk} + f'_k}{2} \mod q_k, & \text{for } k = 1,\ldots,n, \\ -\dfrac{f'_k}{2} \mod q_k, & \text{for } k = n+1,\ldots,m. \end{cases}$$

Note that from the stabilizer phase condition (15) (choose $r_k := d$), it follows that the numerators in the expressions for $y_k$ are even. An efficient way of solving Eq. (18) can be found in Appendix B. A definition of the Smith normal form of a matrix $\in \mathbb{Z}_d^{n\times m}$ is given in Appendix A.

*Proof*. (i) We assume that $S$ already has a minimal number of columns $m$ as described above and we write $S$ as $\begin{bmatrix} S_{(1)} \\ S_{(2)} \end{bmatrix}$ with $S_{(1)}, S_{(2)} \in \mathbb{Z}_d^{n\times m}$. Then we define $Q$ as the Smith normal form of $S_{(1)}$ with invertible transformation matrices $T^{-1}$ and $R$, i.e., $Q = T^{-1} S_{(1)} R$. With $B = T^T S_{(2)} R$, this yields the expression for $S'$ in Eq. (16). According to Eqs. (12) and (13), $f$ is transformed to $f'$, yielding

$$f' = R^T[f - \mathcal{V}_{\text{diag}}(S^T U S)] + \mathcal{V}_{\text{diag}}(R^T[2\mathcal{P}_{\text{upps}}(S^T U S) + \mathcal{P}_{\text{diag}}(S^T U S)]R) \mod 2d.$$

Note that $\begin{bmatrix} T^{-1} & 0 \\ 0 & T^T \end{bmatrix}^T U \begin{bmatrix} T^{-1} & 0 \\ 0 & T^T \end{bmatrix} = U \bmod d$. It follows directly from $S^T P S = 0 \bmod d$ that $Q^T B$ is symmetric modulo $d$.

(ii) We show that Eq. (17) is a simultaneous eigenvector with eigenvalue 1 of $\zeta^{f_k} XZ(S_k)$, $k=1,\ldots,m$. Equivalently, the state

$$|\psi'\rangle := \sum_{t\in\mathbb{Z}_d^n} \zeta^{t^T M t + p^T t} |\overline{Qt + x^*}\rangle \tag{19}$$

is a simultaneous eigenvector with eigenvalue 1 of $\zeta^{f'_k} XZ(S'_k)$, $k=1,\ldots,m$. First, note that in Eq. (19), different values of $t$ may yield the same basis state $|\overline{Qt+x^*}\rangle$, since $\overline{Qt+x^*}$ mod $d$ is periodic. The coefficient of $|\overline{Qt+x^*}\rangle$ in Eq. (19) displays the same periodic behavior: if $\overline{Qt}=\overline{Qt'}$ mod $d$ then $t^T M t + p^T t = t'^T M t' + p^T t'$ mod $2d$. It is sufficient to check this for $t'=t+(d/q_k)E_k$, $k=1,\ldots,n$, where $E_k$ are the standard basis vectors of $\mathbb{Z}_d^n$. We have

$$\left(t+\frac{d}{q_k}E_k\right)^T M\left(t+\frac{d}{q_k}E_k\right) + p^T\left(t+\frac{d}{q_k}E_k\right) - t^T M t - p^T t$$
$$= \frac{d}{q_k}[(d-q_k)B_{kk} + f'_k + 2B_k^T x^*] = 0 \mod 2d$$

for $k=1\ldots n$. Indeed, from the definition of $x^*$: $B_k^T x^* = -[(d-q_k)B_{kk}+f'_k]/2$ mod $q_k$, $k=1,\ldots,n$, it follows that $2(d/q_k)B_k^T x^* = -(d/q_k)[(d-q_k)B_{kk}+f'_k]$ mod $2d$, $k=1,\ldots,n$. We made use of the fact that $M=\overline{QB}$ mod $d \Rightarrow M=\overline{QB}+D$ mod $2d$, where every entry of $D$ mod $2d$ can be either $d$ or 0, i.e., $2D=0$ mod $2d$.

Next, we check for $k=1,\ldots,n$ that Eq. (19) is an eigenvector of $\zeta^{f'_k} XZ(S'_k)$ with eigenvalue 1. We have

$$\zeta^{f'_k} XZ\left(\begin{bmatrix} Q_k \\ B_k \end{bmatrix}\right)|\psi'\rangle$$
$$= \sum_{t\in\mathbb{Z}_d^n} \zeta^{t^T M t + p^T t + f'_k + 2B_k^T(\overline{Qt+x^*})} |\overline{Qt} + x^* + Q_k\rangle$$
$$= \sum_{t\in\mathbb{Z}_d^n} \zeta^{(t-E_k)^T M(t-E_k) + p^T(t-E_k) + f'_k + 2B_k^T(\overline{Q(t-E_k)+x^*})} |\overline{Qt} + x^*\rangle$$
$$= \sum_{t\in\mathbb{Z}_d^n} \zeta^{t^T M t + p^T t} |\overline{Qt} + x^*\rangle = |\psi'\rangle.$$

Finally, $\zeta^{f'_k} XZ(S'_k)$ acting on the left of Eq. (19) yields, for $k=n+1,\ldots,m$,

$$\zeta^{f'_k} XZ\left(\begin{bmatrix} 0 \\ B_k \end{bmatrix}\right)|\psi'\rangle = \sum_{t\in\mathbb{Z}_d^n} \zeta^{t^T M t + p^T t + f'_k + 2B_k^T(\overline{Qt+x^*})} |\overline{Qt} + x^*\rangle$$
$$= \sum_{t\in\mathbb{Z}_d^n} \zeta^{t^T M t + p^T t} |\overline{Qt} + x^*\rangle = |\psi'\rangle.$$

In Appendix B we prove that Eq. (18) has a unique solution $x^* \in G_{\overline{q}}$. ■

It is possible to remove all identical terms in the summation of expression (17) as follows. We define $r$ as the number of nonzero diagonal elements of $Q$. We denote the upper left $r\times r$ part of a matrix $A$ as $A_{(r)}$, the upper $r$ part of a vector $a$ as $a_{(r)}$ and the part of $a$ below $a_{(r)}$ as $\overline{a}_{(r)}$. Then Eq. (17) is equivalent to

$$|\psi\rangle = \sqrt{\frac{\prod_{i=1}^r q_i}{d^r}} \sum_{t\in G_*} \zeta^{t^T M_{(r)} t + p_{(r)}^T t} \left| T\begin{bmatrix} Q_{(r)}t + x^*_{(r)} \\ \overline{x}^*_{(r)} \end{bmatrix}\right\rangle,$$

where $G_* := \mathbb{Z}_{d/q_1} \times \cdots \times \mathbb{Z}_{d/q_r}$. Note that the normalizing factor is just the inverse of the square root of the number of terms in the summation, as each basis state is orthogonal to the others and occurs only once. Finally, it is interesting to mention that, for an arbitray $S$ and $f$ defining a stabilizer state $|\psi\rangle$, we have (up to a normalization factor)

$$|\psi\rangle = \sum_{t\in\mathbb{Z}_d^m} \zeta^{t^T M t + p^T t} |S_{(1)}t + x'\rangle,$$

where $S=\begin{bmatrix} S_{(1)} \\ S_{(2)} \end{bmatrix}$, $M = S_{(1)}^T S_{(2)}$ mod $d$, $p = f - \mathcal{V}_{\mathrm{diag}}(M) + 2S_{(2)}^T x'$ mod $2d$, and $x' = Tx^*$ mod $d$, where $T$ and $x^*$ are the same as in Eq. (17). Yet, this formula has two disadvantages: first, to find $x'$, we still have to calculate the Smith normal form of $S_{(1)}$ and second, in Eq. (17) it is clearer which basis states have nonzero coefficients.

## VI. CONCLUSION

We have shown that for the Pauli group, the Clifford group and stabilizer states, straightforward extensions in Hilbert spaces of arbitrary dimensions can be compactly described with matrices over $\mathbb{Z}_d$. We have given a way of efficiently decomposing an $n$-qudit Clifford operation in $O(n^2)$ one and two-qudit operations. With these tools in modular arithmetic, we provide an expansion of an arbitrary stabilizer state of $n$ qudits in the standard basis.

## ACKNOWLEDGMENTS

We thank Maarten Van den Nest for useful comments. B. D. M. acknowledges the Katholieke Universiteit Leuven, Belgium for financial support. Research supported by the Research Council KUL: Grant No. GOA-Mefisto 666; GOA AMBioRICS; the Flemish Government: FWO project Nos. G.0240.99 (multilinear algebra), G.0407.02 (support vector machines), G.0197.02 (power islands), G.0141.03 (identification and cryptography), G.0491.03 (control for intensive care glycemia), G.0120.03 (QIT), G.0452.04 (new quantum algorithms), G.0499.04 (Robust SVM); research communities (ICCoS, ANMMM, MLDM); AWI: Bil. Int. Collaboration Hungary/Poland; IWT grants, GBOU (McKnow); Belgian Federal Science Policy Office Grant No. IUAP P5/22 ("Dynamical Systems and Control: Computation, Identification and Modelling," 2002-2006); PODO-II (CP/40: TMS and Sustainability); EU: FP5-Quprodis; ERNSI; Eureka 2063-IMPACT; Eureka 2419-FliTE. Contract Research agreements were provided by ISMC/IPCOS, Data4s, TML, Elia, LMS, and Mastercard.

## APPENDIX A: THE SMITH NORMAL FORM

The Smith normal form is a canonical diagonal form for equivalence of matrices over a principal ideal ring $R$. In this paper we consider matrices over $\mathbb{Z}_d$. For any $A \in \mathbb{Z}_d^{n\times m}$ there

exist invertible matrices $K \in \mathbb{Z}_d^{n\times n}$ and $L \in \mathbb{Z}_d^{m\times m}$ such that

$$F = KAL = \begin{bmatrix} f_1 & & & & & \\ & \ddots & & & & \\ & & f_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix} \mod d$$

with each $f_i$ a nonzero and with $f_i | f_{i+1}$ for $1 \leqslant i \leqslant r-1$. The $f_i$ are unique up to units. Uniqueness of $F$ can be ensured by specifying that each $f_i$ should be a positive divisor of $d$ in $\mathbb{Z}$. There exist fast algorithms for computing the Smith normal form [17].

## APPENDIX B: A UNIQUE SOLUTION OF EQ. (18)

Here we prove that Eq. (18) $B^T x = y \mod q$ has a unique solution $x^* \in G_{\overline{q}} := \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_n}$. We rewrite Eq. (18) as the following system of equations:

$$\sum_{i=1}^{n} B_{ij} x_i = y_j \mod q_j, \quad j = 1, \ldots, m. \tag{B1}$$

If, for fixed $j$, the $B_{ij}$ and $q_j$ have a common factor, then also $y_j$ must be a multiple of this factor, otherwise there is no solution. Define $g_j := \gcd(B_{1j}, \ldots, B_{nj}, q_j)$ and $r_j := d/g_j$. Note that $r_j$ is the order of $S_j$. A necessary condition for solvability of Eq. (B1) is or $r_j y_j = 0 \mod d$, for every $k = 1, \ldots, m$. We show that this condition holds. We have $r_j S_j = 0 \mod d$. From the stabilizer phase condition (15) it follows that

$$(r_j - 1) r_j q_j B_{jj} + r_j f_j' = 0 \mod 2d, \quad 1 \leqslant j \leqslant n,$$

$$r_j f_j' = 0 \mod 2d, \quad j > n,$$

and by definition of $y$, consequently $r_j y_j = 0 \mod d$, $j = 1, \ldots, m$.

An equivalent system to Eq. (B1) is now

$$\sum_{i=1}^{n} \frac{B_{ij}}{g_j} x_i = \frac{y_j}{g_j} \mod \frac{q_j}{g_j}, \quad j = 1, \ldots, m.$$

We define the map $b$: $x = [x_1, \ldots, x_n]^T \to b(x) = [\Sigma_{i=1}^n (B_{i1}/g_1) x_i | \cdots | \Sigma_{i=1}^n (B_{im}/g_m) x_i]^T \mod [q_1/g_1, \ldots, q_m/g_m]^T$, which is a homomorphism from the group of vectors of length $n$ with entries $x_i$ modulo $q_i$, $i = 1, \ldots, n$ to the group of vectors of length $m$ with entries $y_j'$ modulo $q_j/g_j$, $j = 1, \ldots, m$. Equation (B1) has a unique solution if $b$ is an isomorphism. We prove this by showing that the number of elements in both groups are the same and that only 0 is in the kernel. It follows from Eq. (14) and the fact that, by definition, the columns of $S$ generate a set of $d^n$ elements, that the product of the orders of the columns of $S$ is equal to $d^n$, or $\Pi_{j=1}^m r_j = d^n$. Therefore,

$$\prod_{j=1}^{m} \frac{q_j}{g_j} = \frac{d^{m-n}}{\prod_{j=1}^{m} g_j} \prod_{i=1}^{m} q_i = \prod_{i=1}^{m} q_i$$

thus the number of elements of both groups are the same. Next we show that $B^T x = 0 \mod q$ if and only if $x = 0 \mod \overline{q}$. We rewrite this as

$$(\exists v \in \mathbb{Z}_d^n : B^T x = Q^T v \mod d) \Leftrightarrow (\exists x' \in \mathbb{Z}_d^m : x = Q x' \mod d), \quad \forall x \in \mathbb{Z}_d^n. \tag{B2}$$

*Proof.* $\Leftarrow$) $Q^T B$ is symmetric modulo $d$. We therefore have $B^T x = B^T Q x' = Q^T B x' \mod d$, so $v = B x' \mod d$.

$\Rightarrow$) We show that the number of $x \in \mathbb{Z}_d^n$ satisfying the LHS of Eq. (B2) is equal to the number of $x$ satisfying the RHS. The number of elements generated by the columns of a matrix is equal to the product of the orders of the diagonal elements of its Smith normal form. Therefore the columns of $S^T$, similar to the columns of $S$, also generate $d^n$ elements. Consequently, the mapping $s$: $a \in \mathbb{Z}_d^{2n} \to S^T a \in \mathbb{Z}_d^m$ is a homomorphism from $\mathbb{Z}_d^{2n}$ to a group $Y \subset \mathbb{Z}_d^m$, with $|Y| = d^n$. The kernel in $\mathbb{Z}_d^{2n}$ of $s$ contains $|\mathbb{Z}_d^{2n}|/|Y| = d^n$ elements. Equivalently, with $a^T = [v^T \; w^T]$, $s$ is a homomorphism from $\mathbb{Z}_d^n \times \mathbb{Z}_d^n$ to $Y$:

$$s\left(\begin{bmatrix} v \\ w \end{bmatrix}\right) = S^T \begin{bmatrix} v \\ w \end{bmatrix} = [Q^T \quad B^T] \begin{bmatrix} v \\ w \end{bmatrix} = Q^T v + B^T w.$$

There are exactly $d^n$ different pairs $(v, w)$ that satisfy $Q^T v + B^T w = 0 \mod d$. Replacing $w$ by $-x$, we have exactly $d^n$ pairs $(x, v)$ satisfying $B^T x = Q^T v \mod d$. Fixing such an $x$, we have a total of $\Pi_{i=1}^n q_i$ different $v$ for which, together with $x$, the equality still holds (this is because we can add an arbitrary multiple of $d/q_i$ to $v_i$). Therefore, the total number of $x$ for which a $v$ exists such that $B^T x = Q^T v \mod d$, is equal to $d^n / \Pi_{i=1}^n q_i$. This is equal to the number of $x$ that can be written as $x = Q x'$. ■

Next, we describe a method for easily finding the solution $x^*$ of Eq. (18). We define a diagonal matrix $Z \in \mathbb{Z}_d^{m\times m}$ with diagonal entries equal to $d/q_k$, $k = 1, \ldots, m$. Equation (18) is equivalent to the equation $Z B^T x = Z y \mod d$. We calculate the Smith normal form $F = KZB^T L \mod d$. Defining $x' := L^{-1} x \mod d$ and $y' := KZy \mod d$, we have the following equation $Fx' = y' \mod d$, for which a solution $x^{*\prime} \in \mathbb{Z}_d^n$ can be easily found (note that this solution is most likely not unique). We then find $x^* = L x^{*\prime} \mod \overline{q}$.

## APPENDIX C: SIMPLIFICATIONS FOR ODD *d*

In this section we consider the special case of odd $d$. Most of the formulas in this paper can be simplified for odd $d$. We will only give an overview and omit the derivations, as they are completely analogous to the general case. If $d$ is odd, then 2 has an inverse in $\mathbb{Z}_d$, equal to $(d+1)/2$, which we will denote by $2^{-1}$.

For odd $d$, we can use a restricted definition for the Pauli group: it contains all $d^{2n}$ tensor products (2) with an additional complex phase factor $\omega^\delta$ (instead of a power of $\zeta$). Equation (4) becomes

$$\omega^{\delta}XZ(a)\omega^{\epsilon}XZ(b) = \omega^{\delta+\epsilon+a^TUb}XZ(a+b). \quad \text{(C1)}$$

The order of an arbitrary element of this newly defined Pauli group is never equal to $2d$. In the same way as for the general case, we find the image $\omega^{\epsilon}XZ(b)$ of $\omega^{\delta}XZ(a)$ under conjugation by a Clifford operation, which is now defined by $C$ and $g=h/2$:

$$b = Ca \mod d,$$

$$\epsilon = \delta + [g - 2^{-1}\mathcal{V}_{\text{diag}}(C^TUC)]^Ta + 2^{-1}a^T(C^TUC - U)a \mod d. \quad \text{(C2)}$$

Note that, contrary to the general case, $g$ is a vector in $\mathbb{Z}_d^{2n}$. There is no longer a restriction on $g$. Indeed, from Eq. (10), it follows that $h$ in the general setting is always even for odd $d$. Symplecticity of $C$ is of course still required. The product of two Clifford operations $Q''=Q'Q$ corresponds to $C''$ and $g''$, where

$$C'' = C'C \mod d,$$

$$g'' = g + C^Tg' + 2^{-1}[\mathcal{V}_{\text{diag}}(C^T(C'^TUC' - U)C) - C^T\mathcal{V}_{\text{diag}}(C'^TUC')] \mod d. \quad \text{(C3)}$$

The inverse $Q^{\dagger}$ of a Clifford operation $Q$ defined by $C$ and $g$ is defined by $C'$ and $g'$, where

$$C' = C^{-1} = -PC^TP \mod d,$$

$$g' = -C^{-T}g + 2^{-1}[C^{-T}\mathcal{V}_{\text{diag}}(C^TUC) + \mathcal{V}_{\text{diag}}(C^{-T}UC^{-1})] \mod d. \quad \text{(C4)}$$

The definition of a stabilizer state remains the same except for the fact that now the stabilizer is a subgroup of the restricted Pauli group. Note that for odd $d$, no subgroup of the general Pauli group can be found that fulfills all stabilizer conditions but is not a subgroup of the restricted Pauli group. Thus, nothing is lost by restricting the definition of the Pauli group for odd $d$. A generating set for the stabilizer $\mathcal{S}$ consists of elements $\omega^{b_k}XZ(S_k)$, $k=1,\ldots,m$, where $S_k \in \mathbb{Z}_d^{2n}$ and $b_k \in \mathbb{Z}_d^m$. Analogously to the definition of $g$, $b$ is equal to half the value of $f$ in the general setting (as it is the exponent of $\omega$ instead of $\zeta$). The stabilizer phase condition (11) on $b$ simplifies to

$$[2b - \mathcal{V}_{\text{diag}}(S^TUS)]^Tr + r^T(S^TUS)r = 0 \mod d, \quad \text{(C5)}$$

$$\forall r \in \mathbb{Z}_d^m | Sr = 0 \mod d.$$

A stabilizer generator matrix change, by applying an invertible linear transformation $R \in \mathbb{Z}_d^{m\times m}$ to the right on $S$, results in

$$S' = SR \mod d,$$

$$b' = R^T[b - 2^{-1}\mathcal{V}_{\text{diag}}(S^TUS)] + 2^{-1}\mathcal{V}_{\text{diag}}(R^TS^TUSR) \mod d. \quad \text{(C6)}$$

A stabilizer state defined by $S$ and $b$, operated on by a Clifford operation defined by $C$ and $g$, is a new stabilizer state defined by

$$S' = CS \mod d,$$

$$b' = b + S^T[g - 2^{-1}\mathcal{V}_{\text{diag}}(C^TUC)] + 2^{-1}\mathcal{V}_{\text{diag}}[S^T(C^TUC - U)S] \mod d. \quad \text{(C7)}$$

It is not hard to verify that part (ii) of theorem 1 simplifies to

$$|\psi\rangle = \sum_{t\in\mathbb{Z}_d^n} \omega^{t^TMt+p^Tt}|T(\overline{Q}t + x^*)\rangle, \quad \text{(C8)}$$

where $M := 2^{-1}\overline{QB} \mod d$, $p := \overline{b'} - \mathcal{V}_{\text{diag}}(M) + \overline{B}^Tx^* \mod d$. In this setting, $x^* \in G_{\overline{q}} := \mathbb{Z}_{q_1}\times\cdots\times\mathbb{Z}_{q_n}$ is defined as the unique solution of $B^Tx = -b' \mod q$. For calculating $x^*$ we refer to Appendix B.


[1] J. Dehaene and B. De Moor, Phys. Rev. A **68**, 042318 (2003).
[2] D. Gottesman, Ph.D. thesis, Caltech, Pasadena, 1997.
[3] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, Phys. Rev. A **67**, 022310 (2003).
[4] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[5] D. Gottesman, Phys. Rev. A **57**, 127 (1998).
[6] M. A. Nielsen, M. J. Bremner, J. L. Dodd, A. M. Childs, and C. M. Dawson, Phys. Rev. A **66**, 022317 (2002).
[7] A. Y. Vlasov, e-print quant-ph/0210049.
[8] D. Gottesman, e-print quant-ph/9802007.
[9] E. Knill, e-print quant-ph/9608048.
[10] A. Ashikhmin and E. Knill, IEEE Trans. Inf. Theory **47**, 3065 (2001).
[11] M. Grassl, M. Roetteler, and T. Beth, Int. J. Found. Comput. Sci. **14**, 757 (2003).
[12] M. Grassl, T. Beth, and M. Roetteler, Chin. Ann. Math., Ser. A **2**, 55 (2004).
[13] D. Schlingemann and R. F. Werner, Phys. Rev. A **65**, 012308 (2002).
[14] D. Schlingemann, e-print quant-ph/0111080.
[15] M. Grassl, A. Klappenecker, and M. Roetteler (unpublished).
[16] E. Bach and J. Shallit, *Algorithmic Number Theory, Vol. 1: Efficient Algorithms* (MIT Press, Cambridge, MA, 1996).
[17] A. Storjohann (unpublished).

[18] Indeed, let $U=\Sigma_{x,y\in\mathbb{Z}_d^n}q_{xy}|x\rangle\langle y|$ be a unitary operation that commutes with every Pauli group element. From $Z(w)U=UZ(w)$, for all $w\in\mathbb{Z}_d^n$, where $Z(w)$ stands for $Z^{w_1}\otimes\cdots\otimes Z^{w_n}$, it follows that $q_{xy}=0$ for all $x\neq y$. Thus $U=\Sigma_{x\in\mathbb{Z}_d^n}q_x|x\rangle\langle x|$. From $U=X(v)UX(v)^{\dagger}$, for all $v\in\mathbb{Z}_d^n$, where $X(v)$ stands for $X^{v_1}\otimes\cdots\otimes X^{v_n}$, it follows that all $q_x$ are equal.