Physics Letters A 378 (2014) 505–509

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Standard form of qudit stabilizer groups

Vlad Gheorghiu

Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

ARTICLE INFO

Article history:
Received 30 August 2013
Accepted 6 December 2013
Available online 12 December 2013
Communicated by P.R. Holland

ABSTRACT

We investigate stabilizer codes with carrier qudits of equal dimension D, an arbitrary integer greater than 1. We prove that there is a direct relation between the dimension of a qudit stabilizer code and the size of its corresponding stabilizer, and this implies that the code and its stabilizer are dual to each other. We also show that any qudit stabilizer can be put in a canonical, or standard, form using a series of Clifford gates, and we provide an explicit efficient algorithm for doing this. Our work generalizes known results that were valid only for prime dimensional systems and may be useful in constructing efficient encoding/decoding quantum circuits for qudit stabilizer codes and better qudit quantum error correcting codes.

1. Introduction

Quantum error correction is an important part of various schemes for quantum computation and quantum communication, and hence quantum error correcting codes, first introduced about a decade ago [1–3] have received a great deal of attention. For a detailed discussion see Chapter 10 of [4]. Most of the early work dealt with codes for qubits, with a Hilbert space of dimension $D = 2$, but qudit codes with $D > 2$ have also been studied [5–15]. They are of intrinsic interest and could turn out to be of some practical value.

The stabilizer formalism introduced by Gottesman in [16] for $D = 2$ (qubits) provides a compact and powerful way of generating quantum error correcting codes and extends the notion of linear classical error correcting codes [17] to the quantum domain. The stabilizer formalism has been generalized to cases where D is prime or a prime power, see e.g. [6,18,12,19]. For composite D things are more complicated and there is no immediate and natural way of generalizing the notions. Our approach is to use generalized Pauli operators and stabilizers defined in the same way as in the prime case, see e.g. [13,15]. This has the virtue that many (although not all) results that are valid in the prime dimensional case can be extended without too much difficulty to the more general composite case.

An important problem in the theory of stabilizer codes is what is their structure. Is there any "canonical" way of representing an arbitrary stabilizer code? If yes, can one use this fact for implementing various quantum error-correcting tasks? For qubits it turns out that there is such a canonical form, see e.g. Chapter 10.5.7 of [4] or [20], and this allows for a better understanding of the error-correcting capabilities of the stabilizer code and also provides an efficient way of constructing encoding/decoding circuits for such stabilizer codes. Both of these canonical forms are immediately generalizable to prime D. For composite D we are not aware of any such canonical form (except for the case of stabilizer codes over prime-power finite fields [12]), and the proof that such a form exists is one of the main results of the current article.

The reminder of the paper is organized as follows. Section 2 contains definitions of the generalized Pauli group and some quantum gates used later in the paper. It also defines rigorously qudit stabilizers and their corresponding stabilized subspaces (or codes), together with an alternative algebraic notation that we employ later. Section 3 contains our main results: a "size" theorem that relates the size of the stabilizer group to the dimension of its stabilized subspace, followed by a "structure" theorem that shows that any qudit stabilizer can be brought to a canonical form through a series of elementary quantum gates. Finally, Section 4 contains a summary, conclusions, and some open questions.

2. Preliminary remarks and definitions

2.1. The generalized Pauli group on n qudits

We generalize Pauli operators to higher dimensional systems of arbitrary dimension D in the following way. The X and Z operators acting on a single qudit are defined as

$$Z = \sum_{j=0}^{D-1} \omega^j |j\rangle\langle j|, \qquad X = \sum_{j=0}^{D-1} |j\rangle\langle j+1|, \tag{1}$$

and satisfy

$$X^D = Z^D = I, \qquad XZ = \omega ZX, \quad \omega = \mathrm{e}^{2\pi \mathrm{i}/D}, \tag{2}$$

E-mail address: vgheorgh@gmail.com.

0375-9601/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.physleta.2013.12.009

where *the addition of integers is modulo D*, as will be assumed from now on. For a collection of n qudits we use subscripts to identify the corresponding Pauli operators: thus Z_i and X_i operate on the space of qudit i. The Hilbert space of a single qudit is denoted by $\mathcal{H}$, and the Hilbert space of n qudits by $\mathcal{H}_n$, respectively. Operators of the form

$$\omega^\lambda X^{\mathbf{x}} Z^{\mathbf{z}} := \omega^\lambda X_1^{x_1} Z_1^{z_1} \otimes X_2^{x_2} Z_2^{z_2} \otimes \cdots \otimes X_n^{x_n} Z_n^{z_n} \tag{3}$$

will be referred to as *Pauli products*, where λ is an integer in $\mathbb{Z}_D$ and $\mathbf{x}$ and $\mathbf{z}$ are n-tuples in $\mathbb{Z}_D^n$, the additive group of n-tuple integers mod D. For a fixed n the collection of all possible Pauli products (3) form a group under operator multiplication, the *Pauli group* $\mathcal{P}_n$. If p is a Pauli product, then $p^D = I$ is the identity operator on $\mathcal{H}_n$, and hence the order of any element of $\mathcal{P}_n$ is either D or else an integer that divides D. While $\mathcal{P}_n$ is not Abelian, it has the property that two elements *commute up to a phase*:

$$p_1 p_2 = \omega^{\lambda_{12}} p_2 p_1, \tag{4}$$

with λ_{12} an integer in $\mathbb{Z}_D$ that depends on p_1 and p_2.

2.2. Generalization of qubit quantum gates to higher dimensions

In this subsection we define some one and two qudit gates generalizing various qubit gates. The qudit generalization of the Hadamard gate is the *Fourier gate*

$$\mathrm{F} := \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} \omega^{jk} |j\rangle\langle k|. \tag{5}$$

For an invertible integer $q \in \mathbb{Z}_D$ (i.e. integer for which there exists $\bar{q} \in \mathbb{Z}_D$ such that $q\bar{q} \equiv 1 \bmod D$), we define a *multiplicative gate*

$$\mathrm{S}_q := \sum_{j=0}^{D-1} |j\rangle\langle jq|, \tag{6}$$

where qj means multiplication mod D. The requirement that q be invertible ensures that S_q is unitary; for a qubit S_q is just the identity.

For two distinct qudits a and b we define the CNOT gate as

$$\mathrm{CNOT}_{ab} := \sum_{j=0}^{D-1} |j\rangle\langle j|_a \otimes X_b^j = \sum_{j,k=0}^{D-1} |j\rangle\langle j|_a \otimes |k\rangle\langle k+j|_b, \tag{7}$$

the obvious generalization of the qubit Controlled-NOT, where a labels the control qudit and b labels the target qudit. Next the SWAP gate is defined as

$$\mathrm{SWAP}_{ab} := \sum_{j,k=0}^{D-1} |k\rangle\langle j|_a \otimes |j\rangle\langle k|_b. \tag{8}$$

It is easy to check that SWAP gate is hermitian and does indeed swap qudits a and b. Unlike the qubit case, the qudit SWAP gate is not a product of three CNOT gates, but can be expressed in terms of CNOT gates and Fourier gates as

$$\mathrm{SWAP}_{ab} = \mathrm{CNOT}_{ab}(\mathrm{CNOT}_{ba})^\dagger \mathrm{CNOT}_{ab}\big(\mathrm{F}_a^2 \otimes I_b\big), \tag{9}$$

with

$$(\mathrm{CNOT}_{ba})^\dagger = (\mathrm{CNOT}_{ba})^{D-1} = \big(I_a \otimes \mathrm{F}_b^2\big)\mathrm{CNOT}_{ba}\big(I_a \otimes \mathrm{F}_b^2\big). \tag{10}$$

Finally we define the generalized Controlled-phase or CP gate as

$$\mathrm{CP}_{ab} = \sum_{j=0}^{D-1} |j\rangle\langle j|_a \otimes Z_b^j = \sum_{j,k=0}^{D-1} \omega^{jk} |j\rangle\langle j|_a \otimes |k\rangle\langle k|_b. \tag{11}$$

Table 1
The conjugation of Pauli operators by one-qudit gates F and S_q ($\bar{q}$ is the multiplicative inverse of q mod D).

Pauli operator	S_q	F
Z	Z^q	X
X	$X^{\bar{q}}$	Z^{D-1}

Table 2
The conjugation of Pauli products on qudits a and b by two-qudit gates CNOT, SWAP and CP. For the CNOT gate, the first qudit a is the control and the second qudit b the target.

Pauli product	CNOT_{ab}	SWAP_{ab}	CP_{ab}
$I_a \otimes Z_b$	$Z_a \otimes Z_b$	$Z_a \otimes I_b$	$I_a \otimes Z_b$
$Z_a \otimes I_b$	$Z_a \otimes I_b$	$I_a \otimes Z_b$	$Z_a \otimes I_b$
$I_a \otimes X_b$	$I_a \otimes X_b$	$X_a \otimes I_b$	$Z_a^{D-1} \otimes X_b$
$X_a \otimes I_b$	$X_a \otimes X_b^{D-1}$	$I_a \otimes X_b$	$X_a \otimes Z_b^{D-1}$

The CP and CNOT gates are related by a local Fourier gate, similar to the qubit case

$$\mathrm{CNOT}_{ab} = (I_a \otimes \mathrm{F}_b)\mathrm{CP}_{ab}(I_a \otimes \mathrm{F}_b)^\dagger, \tag{12}$$

since F maps Z into X under conjugation (see Table 1).

The gates F, S_q, SWAP, CNOT and CP are unitary operators that map Pauli operators to Pauli operators under conjugation, as can be seen from Tables 1 and 2. They are elements of the so called *Clifford group* on n qudits [21,22], the group of n-qudit unitary operators that leaves $\mathcal{P}_n$ invariant under conjugation, i.e. if O is a Clifford operator, then $\forall p \in \mathcal{P}_n$, $OpO^\dagger \in \mathcal{P}_n$. From Tables 1 and 2 one can easily deduce the result of conjugation by F, S_q, SWAP, CNOT and CP on *any* Pauli product.

2.3. Qudit stabilizer codes

Relative to this group we define a *stabilizer* code $\mathcal{C}$ to be a $K \geqslant 1$-dimensional subspace of the Hilbert space satisfying three conditions:

C1 There is a subgroup $\mathcal{S}$ of $\mathcal{P}_n$ such that for *every* s in $\mathcal{S}$ and *every* $|\psi\rangle$ in $\mathcal{C}$

$$s|\psi\rangle = |\psi\rangle. \tag{13}$$

C2 The subgroup $\mathcal{S}$ is maximal in the sense that every s in $\mathcal{P}_n$ for which (13) is satisfied for all $|\psi\rangle \in \mathcal{C}$ belongs to $\mathcal{S}$.

C3 The coding space $\mathcal{C}$ is maximal in the sense that any ket $|\psi\rangle$ that satisfies (13) for every $s \in \mathcal{S}$ lies in $\mathcal{C}$.

If these conditions are fulfilled we call $\mathcal{S}$ the *stabilizer* of the code $\mathcal{C}$. That it is Abelian follows from the commutation relation (4), since for $K > 0$ there is some nonzero $|\psi\rangle$ satisfying (13).

Note that one can always find a subgroup $\mathcal{S}$ of $\mathcal{P}_n$ satisfying C1 and C2 for any subspace $\mathcal{C}$ of the Hilbert space, but it might consist of nothing but the identity. Thus it is condition C3 that distinguishes stabilizer codes from nonadditive codes. A stabilizer code is uniquely determined by $\mathcal{S}$ as well as by $\mathcal{C}$, since $\mathcal{S}$ determines $\mathcal{C}$ through C3, so in a sense the code and its stabilizer are dual to each other.

2.4. Stabilizer generators and equivalent algebraic descriptions of qudit stabilizer codes

Any stabilizer group can be compactly described using a set of *group generators*. A generator corresponds to a specific Pauli product and can be completely specified, see (3), by a phase λ and two