International Journal of Foundations of Computer Science

EFFICIENT QUANTUM CIRCUITS FOR NON-QUBIT QUANTUM ERROR-CORRECTING CODES

MARKUS GRASSL,* MARTIN RÖTTELER,† and THOMAS BETH‡

Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, 76 128 Karlsruhe, Germany.

Received (November 4, 2002)
Revised
Communicated by Jozef Gruska

ABSTRACT

We present two methods for the construction of quantum circuits for quantum error-correcting codes (QECC). The underlying quantum systems are tensor products of subsystems (qudits) of equal dimension which is a prime power. For a QECC encoding k qudits into n qudits, the resulting quantum circuit has $O(n(n-k))$ gates. The running time of the classical algorithm to compute the quantum circuit is $O(n(n-k)^2)$.

Keywords: Quantum circuits, quantum error correction.

1. Introduction

Most quantum error-correction codes (QECC) have been constructed for quantum systems that are composed of two-dimensional subsystems—quantum bits or short qubits. At first glance, the size of the alphabet used to encode the information to be processed seems to be irrelevant. But already in the context of classical information processing and communication this is not true. For example, the entropy of a message depends on the alphabet used for the encoding, and increasing the size of the alphabet allows the construction of better error-correcting codes [22, 27].

In the context of quantum information, a quantum system consisting of two three-dimensional subsystems—qutrits—shows new features when compared to a two-qubit system. For example, bound entanglement exists only for the former [15], and for two qutrits there is even "nonlocality without entanglement" [3].

In this paper, we consider quantum systems which have subsystems of dimension $d = p^m$, where p is prime. As a shorthand, we will use the term "qudit". Quantum codes for qudit systems have been studied, e. g., in [1, 2, 10, 24]. The question of encoding and decoding these codes, however, was not explicitly addressed. Here

*Current address: The Mathematical Sciences Research Institute, 1000 Centennial Drive, #5070, Berkeley, CA 94720-5070, USA. E-mail: grassl@ira.uka.de

†E-mail: roettele@ira.uka.de

‡E-mail: EISS_Office@ira.uka.de

we present efficient (classical) algorithms to compute efficient quantum networks for the encoding process. The method applies to qubit codes as well, for which encoding algorithms have been discussed, e. g., in [6, 11, 12, 13, 14].

In the following section, we present the mathematical framework of quantum information processing using composed quantum systems. In Section 3 we recall the basic concepts and constructions of quantum error-correcting codes. A first encoding algorithm for the class of CSS codes is presented in Section 4. The main result, an encoding algorithm for stabilizer codes over higher dimensional quantum-systems, is derived in Section 5 and illustrated in Section 6.

2. Non-binary Quantum Systems

2.1. Quantum States and Registers

In the context of classical information processing, information is encoded using words over some finite alphabet $\mathcal{A}$, most often $\mathcal{A} = \{0, 1\}$. The elementary "symbols" of quantum information processing are states of a finite dimensional quantum system. Those can be modeled by normalized vectors in a complex Hilbert space $\mathcal{H} = \mathbb{C}^d$. Again, the simplest case of $\mathcal{H} = \mathbb{C}^2$ is considered most often. Then the orthonormal basis states of such a quantum bit, or short qubit, are written as $|0\rangle$ and $|1\rangle$. (The notation of quantum states as "ket vectors" $|\cdot\rangle$ is attributed to Dirac [7]). A general state of a qubit is given by

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad \text{where } \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1.$$

If both α and β are non-zero, the state $|\phi\rangle$ is a so-called superposition of $|0\rangle$ and $|1\rangle$ with amplitudes α and β. For a d-dimensional system, we label the orthonormal basis states by the elements of some alphabet of size d, e. g., the numbers $\{0, 1, \ldots, d-1\}$ or the elements of a finite field, if d is a prime power. The general state of a qudit is given by

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle, \qquad \text{where } \alpha_i \in \mathbb{C} \text{ and } \sum_{i=0}^{d-1} |\alpha_i|^2 = 1.$$

Combining several qudits, we obtain a quantum register. The canonical basis states of a quantum register of length n are tensor products of the basis states of the single qudits. Hence we can label them by words $x \in \mathcal{A}^n$ of length n. For the basis states of a quantum register we use the following notations:

$$|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle = |x_1\rangle|x_2\rangle \ldots |x_n\rangle = |x_1, x_2, \ldots, x_n\rangle = |x\rangle.$$

A general state of a quantum register of length n is a normalized vector in the exponentially large Hilbert space $\mathcal{H} = (\mathbb{C}^d)^{\otimes n} \cong \mathbb{C}^{d^n}$, given by

$$|\Psi\rangle = \sum_{x \in \mathcal{A}^n} \alpha_x |x\rangle, \qquad \text{where } \alpha_x \in \mathbb{C} \text{ and } \sum_{x \in \mathcal{A}^n} |\alpha_x|^2 = 1.$$

When writing states of quantum registers, normalization factors may be omitted.

The elements of the dual space $\mathcal{H}^*$ will be denoted by "bra vectors" $\langle y|$. Then the inner product of two vectors $|x\rangle$ and $|y\rangle$ reads $\langle x|y\rangle$, and linear operators M can be written in the form

$$M = (M_{i,j}) = \sum_{i,j} M_{ij}|i\rangle\langle j|.$$

As the operations have to preserve the normalization of the vectors, the admissible operations are unitary operators, which we will discuss next.

2.2. Elementary Gates

In the following we will consider qudit systems where each qudit corresponds to a q-dimensional Hilbert space where $q = p^m$ is a prime power.

Definition 1 (Elementary Gates) *Let q be a prime power, i. e., $q = p^m$ where p is prime. By ω we denote a primitive complex p-th root of unity, i. e., $\omega = \exp(2\pi i/p)$. Furthermore, let $\mathrm{tr}(\alpha)$ denote the trace of an element $\alpha \in \mathbb{F}_q = \mathbb{F}_{p^m}$ which is defined as $\mathrm{tr}(\alpha) := \sum_{i=0}^{m-1} \alpha^{p^i} \in \mathbb{F}_p$. Then we define the following operations:*

(i) $X_\alpha := \sum_{x\in\mathbb{F}_q} |x+\alpha\rangle\langle x|$ *for* $\alpha \in \mathbb{F}_q$

(ii) $Z_\beta := \sum_{z\in\mathbb{F}_q} \omega^{\mathrm{tr}(\beta z)}|z\rangle\langle z|$ *for* $\beta \in \mathbb{F}_q$

(iii) $M_\gamma := \sum_{y\in\mathbb{F}_q} |\gamma y\rangle\langle y|$ *for* $\gamma \in \mathbb{F}_q \setminus \{0\}$

(iv) $\mathrm{DFT} := \frac{1}{\sqrt{q}} \sum_{x,z\in\mathbb{F}_q} \omega^{\mathrm{tr}(xz)}|z\rangle\langle x|$

(v) $\mathrm{ADD}^{(1,2)} := \sum_{x,y\in\mathbb{F}_q} |x\rangle_1|x+y\rangle_2\langle y|_2\langle x|_1$

(vi) $\mathrm{HORNER}^{(1,2,3)} := \sum_{a,x,b\in\mathbb{F}_q} |a\rangle_1|x\rangle_2|ax+b\rangle_3\langle b|_3\langle x|_2\langle a|_1$

Here, when writing $\omega^{\mathrm{tr}(\beta z)}$, we identify $\mathbb{F}_p$ and $\mathbb{Z}/p\mathbb{Z}$, the integers modulo p. Then the function $\chi_\beta\colon z \mapsto \omega^{\mathrm{tr}(\beta z)}$ is an additive character of $\mathbb{F}_q$. Different values of β yield the q different additive characters of $\mathbb{F}_q$ (see, e. g., [17, 21]).

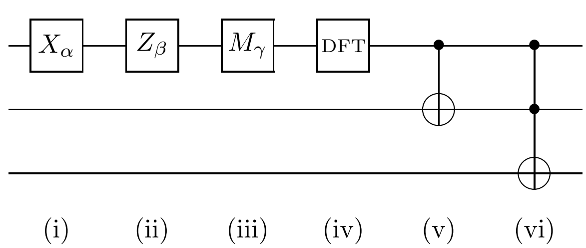

Fig. 1. Graphical representation of the elementary gates of Definition 1.

A graphical representation of these elementary operations—so-called quantum gates—is given in Figure 1. Each horizontal line corresponds to one qudit. The first three operations operate on single qudits. A superscript in brackets indicates on which subsystem the transformation acts, e. g., $X_\alpha^{(2)} = id \otimes X_\alpha \otimes id \otimes \ldots \otimes id$. The operations X_α and M_γ correspond to the addition of a fixed element $\alpha \in \mathbb{F}_q$ and the multiplication with a fixed element $\gamma \neq 0$, respectively. The operation Z_β has no direct classical analogue, it changes the phases of the basis states. The Fourier transformation DFT can be used to transform the state $|0\rangle$ to a superposition of all basis states with equal amplitudes, i.e.,

$$\mathrm{DFT}|0\rangle = \frac{1}{\sqrt{q}} \sum_{\alpha \in \mathbb{F}_q} |\alpha\rangle.$$

Starting from this superposition, a quantum computation can, e. g., evaluate a function in parallel for all possible inputs. Arbitrary classical functions over $\mathbb{F}_q$ can be implemented using the gates $\mathrm{ADD}^{(1,2)}$ and $\mathrm{HORNER}^{(1,2,3)}$. The former corresponds to the reversible implementation of the addition of two elements. The first qudit is called "control", the second "target". The latter is a universal reversible gate over $\mathbb{F}_q$, as any function over $\mathbb{F}_q$ corresponds to a polynomial which can be evaluated using the Horner scheme. It is the generalization of the so-called Toffoli gate [26] for qubits, which is universal gate for reversible boolean functions, as well as the Fredkin gate [8].

3. Quantum Error-Correcting Codes

3.1. Unitary Error Bases

In the following, we will recall the basic properties and constructions of quantum error-correcting codes. In order to construct an error-correcting code, one has to specify an error model. The error model can be specified by a (finite) set $\mathcal{E}$ of error operators. In [20], the following characterization of error-correcting codes is given.

Theorem 1 *Let $\mathcal{C}$ be a subspace of the Hilbert space $\mathcal{H}$ with orthonormal basis $\{|c_1\rangle, \ldots, |c_K\rangle\}$. Then $\mathcal{C}$ is a quantum error-correcting code for the error-operators $\mathcal{E} = \{E_1, \ldots, E_\mu\}$ if and only if there exists $\alpha_{k,l} \in \mathbb{C}$ such that for all $|c_i\rangle$, $|c_j\rangle$ and $E_k, E_l \in \mathcal{E}$*

$$\langle c_i | E_k^\dagger E_l | c_j \rangle = \delta_{i,j} \alpha_{k,l}. \tag{1}$$

Most quantum error-correcting codes are designed to correct local errors, i. e., errors that effect only some subsystems. The error acting on a single subsystem can be any linear transformation. It is sufficient that condition (1) holds for a basis of the linear space of error operators. For qudit systems of prime power dimension q, we consider the following set of unitary operators:

$$\mathcal{E} = \{X_\alpha Z_\beta \colon \alpha, \beta \in \mathbb{F}_q\}. \tag{2}$$

It is not hard to show that those q^2 operators are an orthogonal basis with respect to the inner product $\langle A, B\rangle = \mathrm{tr}(A^\dagger B)$. Furthermore, they generate an error group $\mathcal{G}_1$

of size pq^2 with center $\zeta(\mathcal{G}_1) = \langle \omega I \rangle$ (see [18, 19]). Any element of $\mathcal{G}_1$ can uniquely be written as $\omega^\gamma X_\alpha Z_\beta$ where $\gamma \in \{0, \ldots, p-1\}$ and $\alpha, \beta \in \mathbb{F}_q$. The commutation relations of two elements are derived from

$$\begin{aligned}
X_\alpha Z_\beta X_\alpha^{-1} &= \sum_{x \in \mathbb{F}_q} |x+\alpha\rangle\langle x| \sum_{z \in \mathbb{F}_q} \omega^{\operatorname{tr}(\beta z)} |z\rangle\langle z| \sum_{y \in \mathbb{F}_q} |y\rangle\langle y+\alpha| \\
&= \sum_{z \in \mathbb{F}_q} \omega^{\operatorname{tr}(\beta z)} |z+\alpha\rangle\langle z+\alpha| \\
&= \sum_{z \in \mathbb{F}_q} \omega^{\operatorname{tr}(\beta(z-\alpha))} |z\rangle\langle z| \\
&= \omega^{-\operatorname{tr}(\alpha\beta)} Z_\beta.
\end{aligned}$$

Hence commuting two elements results in a phase factor, i. e.,

$$(X_\alpha Z_\beta)(X_{\alpha'} Z_{\beta'}) = \omega^{\operatorname{tr}(\alpha'\beta - \alpha\beta')} (X_{\alpha'} Z_{\beta'})(X_\alpha Z_\beta). \tag{3}$$

For an n-qudit system, the error basis and the error group are the n-fold tensor products $\mathcal{E}^{\otimes n}$ and $\mathcal{G}_n := \mathcal{G}_1^{\otimes n}$, respectively. The weight of an error-operator $E \in \mathcal{E}^{\otimes n}$ is the number of tensor factors that are different from identity. If a K-dimensional subspace $\mathcal{C}$ of $(\mathbb{C}^q)^{\otimes n}$ can correct all errors of weight no greater than t, $\mathcal{C}$ is a t-error-correcting code with minimum distance $2t+1$, denoted by $((n, K, 2t+1))$.

3.2. Stabilizer Codes

A particular class of quantum error-correcting codes are so-called stabilizer codes (see [2, 4, 9]). The basic idea is to consider an Abelian subgroup $\mathcal{S}$ of the error group $\mathcal{G}_n$ such that its intersection with the center of $\mathcal{G}_n$ is trivial. The stabilizer code $\mathcal{C}$ is defined as the common eigenspace of the operators in $\mathcal{S}$. Stabilizer codes can be described in terms of certain classical codes over finite fields.

Any element E of the error group $\mathcal{G}_n$ can uniquely be written as

$$E = \omega^\gamma (X_{\alpha_1} Z_{\beta_1}) \otimes (X_{\alpha_2} Z_{\beta_2}) \otimes \ldots \otimes (X_{\alpha_n} Z_{\beta_n}) =: \omega^\gamma X_\alpha Z_\beta,$$

where $\gamma \in \{0, \ldots, p-1\}$ and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n), \beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{F}_q^n$. The weight of an element $X_\alpha Z_\beta$ is the number of indices i for which not both α_i and β_i are zero. From the commutation relation (3), it follows that for $(\alpha, \beta), (\alpha', \beta') \in \mathbb{F}_q^n \times \mathbb{F}_q^n$

$$(X_\alpha Z_\beta)(X_{\alpha'} Z_{\beta'}) = \omega^{(\alpha,\beta)*(\alpha',\beta')} (X_{\alpha'} Z_{\beta'})(X_\alpha Z_\beta),$$

where the inner product $*$ is defined by

$$(\alpha, \beta) * (\alpha', \beta') := \sum_{i=1}^n \operatorname{tr}(\alpha_i' \beta_i - \alpha_i \beta_i'). \tag{4}$$

This shows that the group $\overline{\mathcal{G}}_n := \mathcal{G}_n / \langle \omega I \rangle$ is isomorphic to $\mathbb{F}_q^n \times \mathbb{F}_q^n$. Furthermore, two elements $X_\alpha Z_\beta$ and $X_{\alpha'} Z_{\beta'}$ commute if and only if $(\alpha, \beta) * (\alpha', \beta') = 0$. Hence an Abelian subgroup $\mathcal{S}$ of $\mathcal{G}_n$ corresponds to a subspace C of $\mathbb{F}_q^n \times \mathbb{F}_q^n$ that is contained in its dual C^* with respect to the inner product (4).

Definition 2 (Stabilizer Matrix) *Let $\mathcal{S}$ be an Abelian subgroup of $\mathcal{G}_n$ which has trivial intersection with the center of $\mathcal{G}_n$. Furthermore, let $\{g_1, g_2, \ldots, g_{n-k}\}$ where $g_i = \omega^{\gamma_i} X_{\alpha_i} Z_{\beta_i}$ with $\gamma_i \in \{0, \ldots, p-1\}$ and $(\alpha_i, \beta_i) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ be a minimal set of generators for $\mathcal{S}$. Then a stabilizer matrix of the corresponding stabilizer code $\mathcal{C}$ is a generator matrix of the (classical) linear code $C \subseteq F_q^n \times F_q^n$. We will write this matrix in the form*

$$\left(\begin{array}{c|c} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \\ \vdots & \vdots \\ \alpha_{n-k} & \beta_{n-k} \end{array}\right) \in \mathbb{F}_q^{(n-k)\times 2n}.$$

Any error operator E that does not commute with all elements $S \in \mathcal{S}$ will change the eigenvalue of an eigenstate $|\psi\rangle$ of S which can be detected by a measurement. Recall that $E = X_\alpha Z_\beta$ does not commute with all $S \in \mathcal{S}$ if and only if $(\alpha, \beta) \notin C^*$. Finally, the minimum distance of a stabilizer code is the minimum weight of the vectors $(\alpha, \beta) \in C^* \setminus C$, since the errors corresponding to C^* are those that cannot be detected, and the operators corresponding to C have no effect on the code.

4. Encoding CSS Codes

A special class of stabilizer codes are so-called CSS codes named after Calderbank, Shor [5] and Steane [25]. Originally, they have been designed for qubit systems, but they can easily generalized to any dimension (see, e. g., [1]). Given two linear codes $C_1 = [n, k_1, d_1]_q$ and $C_2 = [n, k_2, d_2]_q$ over $\mathbb{F}_q$ with $C_2^\perp \subseteq C_1$, the basis states of the corresponding CSS code are

$$|\psi_w\rangle := \frac{1}{\sqrt{|C_2^\perp|}} \sum_{c \in C_2^\perp} |c + w\rangle, \qquad \text{where } w \in C_1. \tag{5}$$

Two states $|\psi_w\rangle$ and $|\psi_{w'}\rangle$ are identical if and only if $w - w' \in C_2^\perp$, otherwise they are orthogonal. As the dimension of $C_2^\perp$ is $n - k_2$, there are q^k different cosets where $k = k_1 + k_2 - n$. Hence the dimension of the CSS code is q^k. Its minimum distance is $d \geq \min(d_1, d_2)$.

We illustrate the encoding of a CSS code for the code $[\![7, 3, 3]\!]_8$ over seven 8-dimensional quantum systems. Let $\alpha \in \mathbb{F}_8$ be a primitive element of $\mathbb{F}_8$ with minimal polynomial $\mu_\alpha(X) = X^3 + X + 1$. The code $C = [7, 2, 6]_8$ with generator matrix

$$G = \begin{pmatrix} 1 & 0 & \alpha^3 & 1 & \alpha^3 & \alpha & \alpha \\ 0 & 1 & \alpha^4 & 1 & \alpha^5 & \alpha^5 & \alpha^4 \end{pmatrix}$$

is contained in its dual $C^\perp = [7, 5, 3]$ with generator matrix

$$H = \left(\begin{array}{ccccccc} 1 & 0 & \alpha^3 & 1 & \alpha^3 & \alpha & \alpha \\ 0 & 1 & \alpha^4 & 1 & \alpha^5 & \alpha^5 & \alpha^4 \\ \hline 0 & 0 & 1 & 0 & 0 & \alpha^3 & \alpha^5 \\ 0 & 0 & 0 & 1 & 0 & \alpha & \alpha^5 \\ 0 & 0 & 0 & 0 & 1 & \alpha & \alpha^4 \end{array}\right).$$

The first two rows of H are equal to G. The cosets of $C^{\perp}/C$ are given by linear combinations of the last three rows. Denoting the rows of H by $h_1, h_2, \ldots, h_5$, we can rewrite equation (5) as

$$|\psi_{a,b,c}\rangle = \frac{1}{\sqrt{|C|}} \sum_{i,j\in\mathbb{F}_8} |ih_1 + jh_2 + ah_3 + bh_4 + ch_5\rangle,$$

where $a, b, c \in \mathbb{F}_8$. Applying a Fourier transformation to the first and second qudit of the initial state $|00\rangle|a\rangle|b\rangle|c\rangle|00\rangle$, we obtain

$$\frac{1}{8} \sum_{i,j\in\mathbb{F}_8} |i\rangle|j\rangle|a\rangle|b\rangle|c\rangle|00\rangle. \tag{6}$$

Now we sequentially add the corresponding multiple of the rows of H in reverse order, i. e., starting with h_5. As H is in row echelon form, this corresponds to a sequence of modified ADD gates—instead of adding the first qudit to the second, we have to add a multiple of it. The resulting encoding circuit is shown in Figure 2.

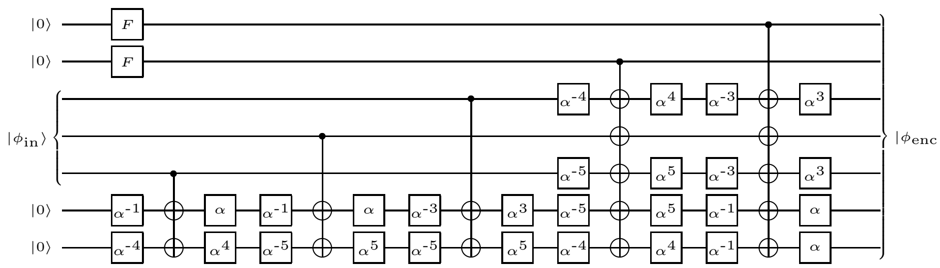

Fig. 2. Encoding circuit for the CSS code $[\![7,3,3]\!]_8$. The Fourier transformation DFT is abbreviated by F, and for the gate M_α we give only the value of α.

For each row h_k of H, we have a sequence of gates $\mathrm{ADD}^{(k,l)}$ corresponding to the non-zero entries H_{kl} for $k \neq l$. The gate $\mathrm{ADD}^{(k,l)}$ is conjugated by a multiplication gate M_γ where $\gamma = H_{kl}$. Note that we have not combined adjacent multiplication gates. In general, G is a generator matrix of $C_2^{\perp} \subseteq C_1$, and H is its completion to a generator matrix of C_1. Using the construction illustrated above, we get

Proposition 1 *Let $C_1 = [n, k_1, d_1]_q$ and $C_2 = [n, k_2, d_2]_q$ be linear codes over $\mathbb{F}_q$ with $C_2^{\perp} \subseteq C_1$. Then there exists a quantum circuit to encode the resulting CSS code $\mathcal{C} = [\![n, k, d]\!]_q$ over qudits of dimension q, where $k = k_1 + k_2 - n$, using $n - k_2$* DFT *gates, at most $A := k_1 n - \binom{k_1+1}{2}$* ADD *gates, and at most $A + (n-1)$ multiplication gates.*

Proof. To create a state similar to (6), we need $\dim C_2^{\perp} = n - k_2$ DFT gates. A generator matrix H for C_1 has k_1 rows. Hence the number A of ADD gates is at most $k_1 n$. As H can be chosen to be in row echelon form, we have k_1 entries that are one. Those correspond to the control qudits. Furthermore, at least $\binom{k_1}{2}$ entries of H are zero, reducing the number of ADD gates further. Finally, each ADD gate is conjugated by a multiplication gate. Adjacent multiplication gates between the

ADD gates can be combined, so we count only the multiplication gates before the ADD gates, plus at most $n-1$ multiplication gates at the end. $\square$

As the rôle of C_1 and C_2 in the construction of CSS codes is completely symmetric, one has the freedom to choose the matrices G and H to be generator matrices of either $C_2^\perp$ and C_1, respectively $C_1^\perp$ and C_2. This may reduce the number of gates by a constant factor, as well as optimizing the particular generator matrices.

5. Encoding Qudit Stabilizer Codes

In this section we derive an encoding algorithm for general stabilizer codes over qudit systems of prime power dimension $q = p^m$. The main idea is to transform the Abelian stabilizer group $\mathcal{S} \subseteq \mathcal{G}_n$ of the stabilizer code $\mathcal{C} = [\![n,k,d]\!]_q$ into a stabilizer group $\mathcal{S}_0$ for which encoding is particularly easy. Up to a permutation $\pi \in S_n$ of the qudits—which we may ignore in the sequel—, that group is $\mathcal{S}_0 := \langle Z_1^{(1)}, Z_1^{(2)}, \ldots, Z_1^{(n-k)}\rangle$. The corresponding stabilizer code $\mathcal{C}_0$ cannot correct single qudit errors at arbitrary positions as the common eigenstates of $\mathcal{S}_0$ are tensor products of the fixed $(n-k)$-qudit state $|00\ldots 0\rangle$ and the unencoded state $|\phi_{\text{in}}\rangle \in (\mathbb{C}^d)^{\otimes k}$, i. e., they are of the form

$$|00\ldots 0\rangle|\phi_{\text{in}}\rangle \in (\mathbb{C}^d)^{\otimes n}. \tag{7}$$

As the stabilizer groups $\mathcal{S}$ and $\mathcal{S}_0$ are conjugated to each other there exists a transformation D such that

$$D^{-1}\mathcal{S}D =_\pi \langle Z^{(1)}, Z^{(2)}, \ldots, Z^{(n-k)}\rangle = \mathcal{S}_0, \tag{8}$$

where $=_\pi$ denotes equality up to the permutation π of the qudits. Combining (7) and (8), it follows that the states $D^{-1}(|00\ldots 0\rangle|\phi_{\text{in}}\rangle)$ are common eigenstates of $\mathcal{S}$. Hence the transformation D^{-1} can be used to encode that states of $\mathcal{C}$. In the following, we show that the transformation D can be efficiently decomposed into single qudit transformations and ADD-gates.

5.1. Conjugating the Error Basis

First we consider the operation of the Fourier transformation over the additive group of the field $\mathbb{F}_q$ (see Definition 1 (iv)) on the error group modulo the center. The action on Z_β is given by

$$\begin{aligned}
\mathrm{DFT}^{-1} Z_\beta \mathrm{DFT} &= \frac{1}{\sqrt{q}} \sum_{i,j\in\mathbb{F}_q} \omega^{-\operatorname{tr}(ij)} |i\rangle\langle j| \sum_{z\in\mathbb{F}_q} \omega^{\operatorname{tr}(\beta z)} |z\rangle\langle z| \frac{1}{\sqrt{q}} \sum_{k,l\in\mathbb{F}_q} \omega^{\operatorname{tr}(kl)} |k\rangle\langle l| \\
&= \frac{1}{q} \sum_{i,l\in\mathbb{F}_q} \sum_{j\in\mathbb{F}_q}^{d-1} \omega^{-\operatorname{tr}(ij)} \omega^{\operatorname{tr}(\beta j)} \omega^{\operatorname{tr}(jl)} |i\rangle\langle l| \\
&= \frac{1}{q} \sum_{i,l\in\mathbb{F}_q} \sum_{j\in\mathbb{F}_q} \omega^{\operatorname{tr}((l-i+\beta)j)} |i\rangle\langle l| \\
&= \sum_{l\in\mathbb{F}_q} |l+\beta\rangle\langle l| = X_\beta.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\mathrm{DFT}^{-1}X_\alpha\mathrm{DFT} &= \frac{1}{\sqrt{q}}\sum_{i,j\in\mathbb{F}_q}\omega^{-\operatorname{tr}(ij)}|i\rangle\langle j|\sum_{x\in\mathbb{F}_q}|x+\alpha\rangle\langle x|\frac{1}{\sqrt{q}}\sum_{k,l\in\mathbb{F}_q}\omega^{\operatorname{tr}(kl)}|k\rangle\langle l| \\
&= \frac{1}{q}\sum_{i,l\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q}\omega^{-\operatorname{tr}(i(x+\alpha))}\omega^{\operatorname{tr}(xl)}|i\rangle\langle l| \\
&= \frac{1}{q}\sum_{i,l\in\mathbb{F}_q}\omega^{\operatorname{tr}(-i\alpha)}\sum_{x\in\mathbb{F}_q}\omega^{\operatorname{tr}(x(l-i))}|i\rangle\langle l| \\
&= \sum_{i\in\mathbb{F}_q}\omega^{\operatorname{tr}(-i\alpha)}|i\rangle\langle i| = Z_{-\alpha}
\end{aligned}$$

As any element of $\overline{\mathcal{G}}_1$ corresponds to a row vector (α,β), we can describe the action of DFT on $\overline{\mathcal{G}}_1$ as the linear transformation $\overline{\mathrm{DFT}} := \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$.

Next we investigate the action of the matrix M_γ corresponding to the multiplication with $\gamma\in\mathbb{F}_q$, $\gamma\neq 0$ (see Definition 1 (iv)). We compute

$$\begin{aligned}
M_\gamma^{-1}X_\alpha Z_\beta M_\gamma &= \sum_{y\in\mathbb{F}_q}|y\rangle\langle\gamma y|\sum_{x\in\mathbb{F}_q}|x+\alpha\rangle\langle x|\sum_{z\in\mathbb{F}_q}\omega^{\operatorname{tr}(\beta z)}|z\rangle\langle z|\sum_{v\in\mathbb{F}_q}|\gamma v\rangle\langle v| \\
&= \sum_{y\in\mathbb{F}_q}|y\rangle\langle\gamma y|\sum_{x\in\mathbb{F}_q}|x+\alpha\rangle\langle x|\sum_{v\in\mathbb{F}_q}\omega^{\operatorname{tr}(\beta\gamma v)}|\gamma v\rangle\langle v| \\
&= \sum_{y\in\mathbb{F}_q}|\gamma^{-1}y\rangle\langle y|\sum_{v\in\mathbb{F}_q}\omega^{\operatorname{tr}(\beta\gamma v)}|\gamma v+\alpha\rangle\langle v| \\
&= \sum_{v\in\mathbb{F}_q}\omega^{\operatorname{tr}(\beta\gamma v)}|v+\gamma^{-1}\alpha\rangle\langle v| \\
&= \sum_{x\in\mathbb{F}_q}|x+\gamma^{-1}\alpha\rangle\langle x|\sum_{z\in\mathbb{F}_q}\omega^{\operatorname{tr}(\beta\gamma z)}|z\rangle\langle z| \\
&= X_{\gamma^{-1}\alpha}Z_{\gamma\beta}.
\end{aligned}$$

Hence, M_γ acts on (α,β) as $\overline{M}_\gamma := \begin{pmatrix}\gamma^{-1} & 0\\ 0 & \gamma\end{pmatrix}$.

For the next operation, we have to distinguish the cases whether q is odd or q is even. If q is odd, we define the operator

$$P_\gamma := \sum_{y\in\mathbb{F}_q}\omega^{-\operatorname{tr}(\frac{1}{2}\gamma y^2)}|y\rangle\langle y| \tag{9}$$

which commutes with Z_β. Furthermore, X_α acts on P_γ^{-1} as follows:

$$\begin{aligned}
X_\alpha^{-1}P_\gamma^{-1}X_\alpha &= \sum_{x\in\mathbb{F}_q}|x\rangle\langle x+\alpha|\sum_{y\in\mathbb{F}_q}\omega^{\operatorname{tr}(\frac{1}{2}\gamma y^2)}|y\rangle\langle y|\sum_{z\in\mathbb{F}_q}|z+\alpha\rangle\langle z| \\
&= \sum_{y\in\mathbb{F}_q}\omega^{\operatorname{tr}(\frac{1}{2}\gamma(y+\alpha)^2)}|y\rangle\langle y| \\
&= \omega^{\operatorname{tr}(\frac{1}{2}\gamma\alpha^2)}\sum_{z\in\mathbb{F}_q}\omega^{\operatorname{tr}(\gamma\alpha z)}|z\rangle\langle z|\sum_{y\in\mathbb{F}_q}\omega^{\operatorname{tr}(\frac{1}{2}\gamma y^2)}|y\rangle\langle y| \\
&= \omega^{\operatorname{tr}(\frac{1}{2}\gamma\alpha^2)}Z_{\gamma\alpha}P_\gamma^{-1}.
\end{aligned}$$

Equivalently, we get

$$P_\gamma^{-1} X_\alpha P_\gamma = \omega^{\operatorname{tr}(\frac{1}{2}\gamma\alpha^2)} X_\alpha Z_{\gamma\alpha}.$$

Hence P_γ acts on (α, β) as $\overline{P}_\gamma := \left(\begin{smallmatrix} 1 & \gamma \\ 0 & 1 \end{smallmatrix}\right)$.

If q is even, we have to use another definition for the operator P_γ as we cannot divide by two. For this, we fix an arbitrary self-dual basis $B = \{b_1, \ldots, b_m\}$ of $\mathbb{F}_q = \mathbb{F}_{2^m}$ over $\mathbb{F}_2$ (see e. g., [17]). Hence, by definition, $\operatorname{tr}(b_i b_j) = \delta_{i,j}$. Any element $\alpha \in \mathbb{F}_q$ can uniquely be written as $\sum_{i=1}^m \alpha_i b_i$ where $\alpha_i \in \mathbb{F}_2$. The coefficients α_i are given by $\alpha_i = \operatorname{tr}(b_i \alpha)$ since

$$\operatorname{tr}(b_i\alpha) = \operatorname{tr}(b_i \sum_{j=1}^m \alpha_j b_j) = \sum_{j=1}^m \alpha_j \operatorname{tr}(b_i b_j) = \sum_{j=1}^m \alpha_j \delta_{i,j} = \alpha_i.$$

Lemma 1 *Let $q = 2^m$ and let $B = \{b_1, \ldots, b_m\}$ be an arbitrary self-dual basis of $\mathbb{F}_q$ over $\mathbb{F}_2$. Furthermore, we define an integer-valued function on $\mathbb{F}_q$ as*

$$\operatorname{wgt}\colon \mathbb{F}_q \to \mathbb{Z}, \alpha \mapsto |\{j : j \in \{1, 2, \ldots, m\} | \operatorname{tr}(\alpha b_j) \neq 0\}|.$$

Then the following holds for all $\alpha, y \in \mathbb{F}_q$:

$$i^{\operatorname{wgt}(y+\alpha)} = i^{\operatorname{wgt}(\alpha)} i^{\operatorname{wgt}(y)} (-1)^{\operatorname{tr}(\alpha y)},$$

where $i \in \mathbb{C}$ with $i^2 = -1$.

Proof. First we observe that $\operatorname{wgt}(y + \alpha) = \operatorname{wgt}(y) + \operatorname{wgt}(\alpha) - 2|\{j : y_j = \alpha_j = 1\}|$. Second, the size of this set modulo two is given by

$$\operatorname{tr}(\alpha y) = \operatorname{tr}\left(\left(\sum_{j=1}^m \alpha_j b_j\right)\left(\sum_{k=1}^m y_k b_k\right)\right) = \sum_{j,k=1}^m \alpha_j y_k \operatorname{tr}(b_j b_k) = \sum_{j=1}^m \alpha_j y_j,$$

which completes the proof. □

Now we are ready to define an operator P_1 as

$$P_1 := \sum_{y \in \mathbb{F}_q} (-i)^{\operatorname{wgt}(y)} |y\rangle\langle y| = \sum_{y \in \mathbb{F}_q} \prod_{j=1}^m (-i)^{\operatorname{tr}(y b_i)} |y\rangle\langle y|.$$

Again, P_1 commutes with all matrices Z_β. The action on X_α is derived from

$$\begin{aligned} X_\alpha^{-1} P_1^{-1} X_\alpha &= \sum_{x \in \mathbb{F}_q} |x\rangle\langle x + \alpha| \sum_{y \in \mathbb{F}_q} i^{\operatorname{wgt}(y)} |y\rangle\langle y| \sum_{z \in \mathbb{F}_q} |z + \alpha\rangle\langle z| \\ &= \sum_{y \in \mathbb{F}_q} i^{\operatorname{wgt}(y+\alpha)} |y\rangle\langle y| \\ &= i^{\operatorname{wgt}(\alpha)} \sum_{z \in \mathbb{F}_q} (-1)^{\operatorname{tr}(\alpha z)} |z\rangle\langle z| \sum_{y \in \mathbb{F}_q} i^{\operatorname{wgt}(y)} |y\rangle\langle y| \\ &= i^{\operatorname{wgt}(\alpha)} Z_\alpha P_1^{-1}. \end{aligned}$$

Hence

$$P_1^{-1} X_\alpha P_1 = i^{\operatorname{wgt}(\alpha)} X_\alpha Z_\alpha.$$

Finally, for any $\gamma \in \mathbb{F}_q$, $\gamma \neq 0$, we define P_γ as

$$P_\gamma := M_{\gamma_0}^{-1} P_1 M_{\gamma_0} \qquad \text{where } \gamma_0^2 = \gamma. \tag{10}$$

(Note that γ_0 is uniquely defined as $x \mapsto x^2$ is an automorphism of $\mathbb{F}_q = \mathbb{F}_{2^m}$.) The matrix M_γ is a permutation matrix, hence P_γ is diagonal and commutes with Z_β. The action of P_γ on X_α is given by

$$\begin{aligned}
P_\gamma^{-1} X_\alpha P_\gamma &= M_{\gamma_0}^{-1} P_1^{-1} M_{\gamma_0} X_\alpha M_{\gamma_0}^{-1} P_1 M_{\gamma_0} \\
&= M_{\gamma_0}^{-1} P_1^{-1} X_{\alpha\gamma_0} P_1 M_{\gamma_0} \\
&= M_{\gamma_0}^{-1} i^{\mathrm{wgt}(\alpha\gamma_0)} X_{\alpha\gamma_0} Z_{\alpha\gamma_0} M_{\gamma_0} \\
&= i^{\mathrm{wgt}(\alpha\gamma_0)} X_\alpha Z_{\alpha\gamma_0^2} \\
&= i^{\mathrm{wgt}(\alpha\gamma_0)} X_\alpha Z_{\alpha\gamma}.
\end{aligned}$$

Summarizing, the operators P_γ (defined by (9) for q odd and (10) for q even) acts on (α, β) always as $\overline{P}_\gamma := \left(\begin{smallmatrix} 1 & \gamma \\ 0 & 1 \end{smallmatrix}\right)$.

Altogether, we have shown

Theorem 2 *The group $J_{\mathbb{F}_q} := \langle \mathrm{DFT}, P_\gamma, M_\gamma \colon \gamma \in \mathbb{F}_q^* \rangle$ acts on $\overline{\mathcal{G}}_1$, the error group $\mathcal{G}_1$ modulo the center, as $SL(2, \mathbb{F}_q)$.*

Proof. The action of the matrices DFT, P_γ, M_γ on the error group $\overline{\mathcal{G}}_1$ is given by

$$\overline{\mathrm{DFT}} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \overline{P}_\gamma := \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}, \quad \text{and} \quad \overline{M}_\gamma := \begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix},$$

respectively. These matrices generate $SL(2, \mathbb{F}_q)$ (see, e. g., [23]). □

As $SL(2, \mathbb{F}_q)$ acts transitively on the non-zero vectors (see, e. g., [16]), we obtain

Corollary 1 *The group $J_{\mathbb{F}_q}$ acts transitively on the non-trivial elements of $\overline{\mathcal{G}}_1$.*

So far, we have only considered the action of single qudit operations on the error group $\mathcal{G}_n$. Our goal is to transform an arbitrary Abelian stabilizer group $\mathcal{S} \subseteq \mathcal{G}_n$ into $\mathcal{S}_0$ which corresponds to the code $\mathcal{C}_0 = [\![n, k, 1]\!]$. As $\mathcal{C}_0$ cannot correct errors and single qudit operations do not change the error-correcting properties of a stabilizer code, we need additional transformations which are ADD-gates acting on pairs of qudits. Combining the definitions of X_α and $\mathrm{ADD}^{(1,2)}$ (see Definition 1 (i) and (v)), we can rewrite the ADD-gate as

$$\begin{aligned}
\mathrm{ADD}^{(1,2)} &:= \sum_{x,y \in \mathbb{F}_q} |x\rangle_1 |x+y\rangle_2 \langle y|_2 \langle x|_1 \\
&= \sum_{\alpha \in \mathbb{F}_q} |\alpha\rangle\langle\alpha| \otimes X_\alpha.
\end{aligned} \tag{11}$$

Using (11), it is easy to show that $\mathrm{ADD}^{(1,2)}$ commutes with all matrices of the form $Z_{\beta_1} \otimes X_{\alpha_2}$.

For elements of the form $X_{\alpha_1} \otimes Z_{\beta_2}$ we get

$$
\begin{aligned}
&(\mathrm{ADD}^{(1,2)})^{-1}(X_{\alpha_1} \otimes Z_{\beta_2})\mathrm{ADD}^{(1,2)} \\
&= (\mathrm{ADD}^{(1,2)})^{-1} \sum_{v,w\in\mathbb{F}_q} \omega^{\mathrm{tr}(\beta_2 w)} |v+\alpha_1\rangle_1 |w\rangle_2 \langle w|_2 \langle v|_1 \sum_{x,y\in\mathbb{F}_q} |x\rangle_1 |x+y\rangle_2 \langle y|_2 \langle x|_1 \\
&= (\mathrm{ADD}^{(1,2)})^{-1} \sum_{x,y\in\mathbb{F}_q} \omega^{\mathrm{tr}(\beta_2(x+y))} |x+\alpha_1\rangle_1 |x+y\rangle_2 \langle y|_2 \langle x|_1 \\
&= \sum_{v,w\in\mathbb{F}_q} |v\rangle_1 |w\rangle_2 \langle v+w|_2 \langle v|_1 \sum_{x,y\in\mathbb{F}_q} \omega^{\mathrm{tr}(\beta_2(x+y))} |x+\alpha_1\rangle_1 |x+y\rangle_2 \langle y|_2 \langle x|_1 \\
&= \sum_{x,y\in\mathbb{F}_q} \omega^{\mathrm{tr}(\beta_2 x)} \omega^{\mathrm{tr}(\beta_2 y)} |x+\alpha_1\rangle_1 |y-\alpha_1\rangle_2 \langle y|_2 \langle x|_1 \\
&= (X_{\alpha_1} Z_{\beta_2}) \otimes (X_{-\alpha_1} Z_{\beta_2}).
\end{aligned}
$$

This proofs

Lemma 2 *The transformation* $\mathrm{ADD}^{(1,2)}$ *acts on* $((\alpha_1, \beta_1), (\alpha_2, \beta_2))$ *as*

$$\overline{\mathrm{ADD}}^{(1,2)} := \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

i. e., β_2 *is added to* β_1 *and* α_1 *is subtracted from* α_2.

5.2. Encoding Algorithms

With this preparation, we can formulate our algorithm to efficiently compute efficient quantum circuits for the encoding of stabilizer codes.

Theorem 3 *Let* $\mathcal{C} = [\![n, k, d]\!]_q$ *be a stabilizer code for a qudit system of prime power dimension* $q = p^m$ *with Abelian stabilizer group* $\mathcal{S} \subseteq \mathcal{G}_n$ *and stabilizer matrix* $(X|Z) \in \mathbb{F}_q^{(n-k)\times 2n}$.

Then the algorithm shown in Figure 3 (on page 13) computes a decoding circuit D *for* $\mathcal{C}$ *with at most* $n(n-k) - \binom{n-k+1}{2}$ ADD *gates and* $O(n(n-k))$ *single qudit gates of type* DFT, P_γ, *or* M_γ.

The running time of the algorithm itself is $O(n(n-k)^2)$.

Proof. We show that the algorithm computes a transformation D such that $D^{-1}\mathcal{S}D =_\pi \mathcal{S}_0$ (see eq. (8)). Instead of operating on the stabilizer group $\mathcal{S}$ itself, we use the stabilizer matrix representation. So our goal is to find a transformation $\overline{D}$ such that

$$(X|Z)\overline{D} =_\pi (0|A0), \qquad \text{where } A \in \mathbb{F}_q^{(n-k)\times(n-k)} \text{ has full rank.} \tag{12}$$

In order to obtain a more compact graphical representation of the final quantum circuit, we will first transform the stabilizer matrix first into the form

$$(X|Z)\overline{D}' =_\pi (A0|0), \qquad \text{where } A \in \mathbb{F}_q^{(n-k)\times(n-k)} \text{ has full rank,} \tag{13}$$

and use $(n-k)$ local Fourier transformations to exchange the X- and the Z-part of the stabilizer matrix.

INPUT:	a stabilizer matrix $(X\|Z) \in \mathbb{F}_q^{(n-k)\times 2n}$
OUTPUT:	a decoding transformation $D := F \cdot A_{n-k}T_{n-k} \cdot \ldots \cdot A_2T_2 \cdot A_1T_1$

1 $L \leftarrow \emptyset$
2 foreach row $i = 1$ to $n-k$ do
3   foreach column $j = 1$ to n do
4   if $(X_{ij}, Z_{ij}) \neq (0,0)$ then
5   find a transformation $T_{ij} \in J_{\mathbb{F}_q}$ such that $(X_{ij}, Z_{ij}) \cdot \overline{T}_{ij} = (1,0)$
6   foreach row $l = i$ to $n-k$ do
7         $(X_{lj}, Z_{lj}) \leftarrow (X_{lj}, Z_{lj}) \cdot \overline{T}_{ij}$
8   end for
9   else
10       $T_{ij} \leftarrow id$
11   end if
12   end for
13   $T_i \leftarrow T_{i,1}^{(1)} \otimes T_{i,2}^{(2)} \otimes \ldots \otimes T_{i,n}^{(n)}$
14   find the first column $l \notin L$ where $X_{il} \neq 0$
15   include l into L
16   $A_i \leftarrow id$
17   foreach column $j = 1$ to n do
18   if $l \notin L$ and $X_{ij} = 1$ then
19       $A_i \leftarrow A_i \cdot \mathrm{ADD}^{(l,j)}$
20   foreach row $\mu = i$ to $n-k$ do
21         $(X_{\mu j}, Z_{\mu j}) \leftarrow (X_{\mu j} - X_{lj}, Z_{\mu j} + Z_{lj})$
22   end for
23   end if
24   end for
25 end for
26 $F \leftarrow \prod_{l \in L} \mathrm{DFT}^{(l)}$
27 return $(F, A_{n-k}, T_{n-k}, \ldots, A_2, T_2, A_1, T_1)$

Fig. 3. Algorithm to compute a decoding circuit for a qudit stabilizer code.

We prove the correctness of our algorithm by induction over i, corresponding to the loop steps 2–25. The induction hypothesis is that the first $i-1$ rows of the stabilizer matrix are, again up to a permutation of the columns, in the form $(A_{i-1}0|0)$, where A is an $(i-1)\times(i-1)$ matrix of full rank.

After the loop steps 3–12, the Z-part of the i-th row of the stabilizer matrix will be zero. From Theorem 2 and Corollary 1 it follows that in step 5 we can always find a transformation $T_{ij} \in J_{\mathbb{F}_q}$ with the desired property. The loop steps 6–8 updates the stabilizer matrix. In step 13, we combine the transformations applied to each qudit to a transformation on all qudits. The definition of the stabilizer matrix (see Definition 2) implies that it has full rank. Hence in step 14, we will always find a column l with a non-zero entry X_{il}. That column will be recorded in step 15. Then the loop steps 17–24 searches for columns $j \notin L$ where X_{ij} is non-zero. Applying an ADD-gate with control l and target j will change those positions X_{ij} to zero. The loop steps 20–22 updates the stabilizer matrix accordingly. So after step 24, only the entries X_{il} for $l \in L$ may be non-zero, all other entries in the i-th row of the stabilizer matrix are zero. This completes the induction step from row $i-1$ to row i.

After step 25, the Z-part of the stabilizer matrix is zero, and only the $n-k$ columns $l \in L$ of the X-part are non-zero. Applying the transformation F, i. e., local Fourier transformations at those positions, yields the stabilizer group $\mathcal{S}_0$, completing the proof of the correctness of our algorithm.

The running time of the algorithm follows directly from that fact that at most three for-loops are nested, two of them iterating over the $n-k$ rows, one over the n columns.

Each of the $n-k$ transformations A_j is a product of at most $n-j$ ADD-gates. Hence the total number of ADD gates is at most $\sum_{j=1}^{n-k}(n-j) = n(n-k) - \binom{n-k+1}{2}$. Each of the $n-k$ transformations T_j is the product of $O(n)$ single qudit operations. Together with the $n-k$ local Fourier transformations DFT in the transformation F, the number of single qudit gates is $O(n(n-k))$. $\square$

Note that, in contrast to the situation of qubits, for $q = p^m$, $p > 2$, the ADD-gate over $\mathbb{F}_q$ for $q = p^m$, $p > 2$, is not its own inverse. So a different graphical representation for ADD^{-1} is required. For simplicity, we have not introduced such a representation. This is also the main reason why we do not directly compute the transformation D of (12), but decompose it as $D = F \cdot D'$ (see eq. (13)).

It is not difficult to modify our algorithm such we may save the final $n-k$ local Fourier transformations. In step 5, we have to find a transformation $T_{ij} \in J_{\mathbb{F}_q}$ such that $(X_{ij}, Z_{ij}) \cdot \overline{T}_{ij} = (0,1)$. Furthermore, we have to replace the ADD-gates by inverse ADD-gates. The modified steps of the algorithm are:

5' find a transformation $T_{ij} \in J_{\mathbb{F}_q}$ such that $(X_{ij}, Z_{ij}) \cdot \overline{T}_{ij} = (0,1)$

19' $A_i \leftarrow A_i \cdot (\text{ADD}^{-1})^{(l,j)}$
20' foreach row $\mu = i$ to $n-k$ do
21' $\quad (X_{\mu j}, Z_{\mu j}) \leftarrow (X_{\mu j} + X_{lj}, Z_{\mu j} - Z_{lj})$
22' end for

6. Example

We illustrate the algorithm of Figure 3 using a quantum code over qutrits. A stabilizer matrix of the code $\mathcal{C} = [\![9,5,3]\!]_3$ is given by

$$(X|Z) = \left(\begin{array}{ccccccccc|ccccccccc} 1 & 0 & 0 & 2 & 1 & 2 & 2 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 2 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 0 & 2 & 2 \\ 0 & 0 & 2 & 1 & 2 & 2 & 0 & 1 & 1 & 1 & 0 & 2 & 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 & 1 & 0 & 2 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 2 & 0 & 2 \end{array}\right).$$

In the first step, we transform each pair (α_i, β_i) of the first row that is non-zero to $(1,0)$. This is achieved by the transformation

$$T_1 = id \otimes id \otimes M_2\text{DFT} \otimes P_1 M_2 \otimes P_1 \otimes P_2 M_2 \otimes M_2 \otimes \text{DFT} \otimes P_2.$$

The resulting stabilizer matrix is

$$(X|Z) = \left(\begin{array}{ccccccccc|ccccccccc} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 & 1 & 2 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 2 & 2 & 1 & 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 & 0 & 0 & 2 & 0 & 1 & 1 & 0 & 2 & 1 & 1 & 1 & 0 \end{array}\right).$$

The first non-zero column is the first one. So using the transformation

$$A_1 := \mathrm{ADD}^{(1,3)}\mathrm{ADD}^{(1,4)}\mathrm{ADD}^{(1,5)}\mathrm{ADD}^{(1,6)}\mathrm{ADD}^{(1,7)}\mathrm{ADD}^{(1,8)}\mathrm{ADD}^{(1,9)}$$

we obtain

$$(X|Z) = \left(\begin{array}{ccccccccc|ccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 & 1 & 2 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 2 & 2 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 & 0 & 0 & 2 & 0 & 1 & 1 & 0 & 2 & 1 & 1 & 1 & 0 \end{array}\right).$$

Note that the first column of the Z-matrix is zero. This follows from the fact that the corresponding stabilizer elements commute with the $X^{(1)}$ which corresponds to the first row.

In the next step, we use the transformations

$$T_2 := id \otimes id \otimes P_1M_2 \otimes P_1 \otimes \mathrm{DFT} \otimes P_2 \otimes id \otimes P_2M_2 \otimes M_2\mathrm{DFT}$$

and

$$A_2 := \mathrm{ADD}^{(2,3)}\mathrm{ADD}^{(2,4)}\mathrm{ADD}^{(2,5)}\mathrm{ADD}^{(2,6)}\mathrm{ADD}^{(2,7)}\mathrm{ADD}^{(2,8)}\mathrm{ADD}^{(2,9)}$$

to obtain

$$(X|Z) = \left(\begin{array}{ccccccccc|ccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 2 & 1 & 0 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 2 & 2 \end{array}\right).$$

Using the transformations

$$T_3 := id \otimes id \otimes M_2 \otimes P_1M_2 \otimes P_1M_2 \otimes id \otimes \mathrm{DFT} \otimes P_2M_2 \otimes P_1M_2$$

and

$$A_3 := \mathrm{ADD}^{(3,4)}\mathrm{ADD}^{(3,5)}\mathrm{ADD}^{(3,6)}\mathrm{ADD}^{(3,7)}\mathrm{ADD}^{(3,8)}\mathrm{ADD}^{(3,9)}$$

yields

$$(X|Z) = \left(\begin{array}{ccccccccc|ccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 2 & 2 & 0 & 0 & 0 & 1 & 2 & 2 & 0 & 1 & 1 \end{array}\right).$$

For the last row, we use the transformations

$$T_4 := id \otimes id \otimes id \otimes P_2 \otimes M_2\mathrm{DFT} \otimes P_1 \otimes id \otimes P_1M_2 \otimes P_1M_2$$

and

$$A_4 := \text{ADD}^{(4,5)}\text{ADD}^{(4,6)}\text{ADD}^{(4,8)}\text{ADD}^{(4,9)}$$

and get

$$(X|Z) = \left(\begin{array}{ccccccccc|ccccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Note that after the first three steps, we have $L = \{1, 2, 3\}$. Hence not the third, but the fourth qudit is the control qudit for the ADD gates of the last row. Equivalently, we could have subtracted the third row from the fourth to obtain $X_{4,3} = 0$. The stabilizer group would not have changed as the addition of one row to another corresponds to multiplying one generator by another.

Finally, a Fourier transformation on the first four positions transforms the stabilizer group into the form $S_0 = \langle Z_1^{(1)}, Z_1^{(2)}, Z_1^{(3)}, Z_1^{(4)}\rangle$.

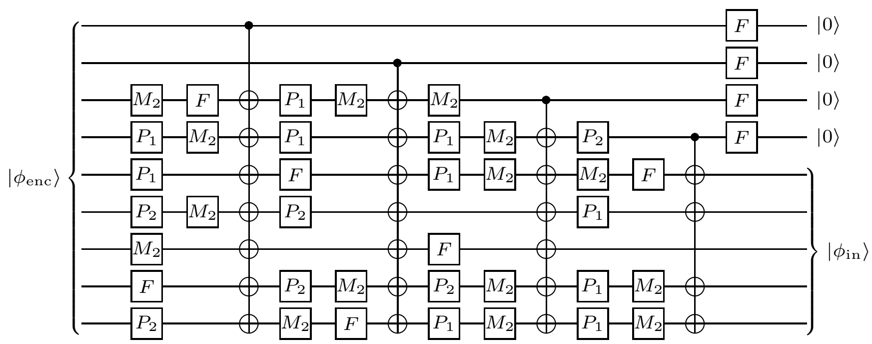

Fig. 4. Decoding circuit for the ternary quantum code $\mathcal{C} = [\![9, 5, 3]\!]_3$. The Fourier transformation DFT is abbreviated as F.

The complete decoding circuit is shown in Figure 4. Reversing the order of the gates and replacing each gate by its inverse yields a quantum circuit for encoding.

7. Conclusions

The quantum circuits for both CSS codes and general stabilizer codes over qudit systems of prime power dimension resulting from our algorithms have a similar structure. They consist of an alternating sequence of single qudit gates and ADD-gates with the same control qudit. The total number of gates is always at most quadratic in the number of qudits. For CSS codes, the single qudit gates are either Fourier transformations or multiplication gates, which are trivial for the case of qubits. Furthermore, some optimizations are possible by interchanging the rôle of the two classical codes involved.

The algorithm of [6], respectively the modified version of [11, 12], to compute quantum circuits for the encoding of qubit stabilizer codes can also be generalized to non-qubit stabilizer codes. It turns out that the resulting quantum circuits have again the same structure and complexity as those presented in this paper. The approach presented here, however, has the advantage that the transformation D used to conjugate the stabilizer group $\mathcal{S}$ to $\mathcal{S}_0$ can also be used to compute "encoded gates" which preserve the code $\mathcal{C}$. Conjugating gates from the error-group which preserve the code $\mathcal{C}_0$ by D results in transformations that are also in the error-group and preserve the code $\mathcal{C}$. As those transformations consist only of single qudit operations, they can be used for fault-tolerant quantum computation.

Acknowledgements

Markus Grassl and Martin Rötteler acknowledge the hospitality of the Mathematical Sciences Research Institute, Berkeley, USA. Part of this work was supported by *Deutsche Forschungsgemeinschaft (DFG), Schwerpunktprogramm Quanten-Informationsverarbeitung (SPP 1078), Projekt AQUA (Be 887/13)* and the IST/FET project Q-ACTA (IST-1999-10596) funded by the European Commission.

References

1. D. Aharonov and M. Ben-Or, *Fault-Tolerant Quantum Computation with Constant Error*, in Proceedings of the 29th Annual ACM Symposium on Theory of Computing, Association for Computing Machinery, 1997, pp. 176–188. See also LANL preprint quant-ph/9611025.
2. A. Ashikhmin and E. Knill, *Nonbinary quantum stabilizer codes*, IEEE Transactions on Information Theory, 47 (2001), pp. 3065–3072. See also LANL preprint quant-ph/0005008.
3. C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, *Quantum nonlocality without entanglement*, Physical Review A, 59 (1999), pp. 1070–1091. See also LANL preprint quant-ph/9804053.
4. A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum Error Correction Via Codes over GF(4)*, IEEE Transactions on Information Theory, 44 (1998), pp. 1369–1387. See also LANL preprint quant-ph/9608006.
5. A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist*, Physical Review A, 54 (1996), pp. 1098–1105. See also LANL preprint quant-ph/9512032.
6. R. Cleve and D. Gottesman, *Efficient computations of encodings for quantum error correction*, Physical Review A, 56 (1997), pp. 76–82. See also LANL preprint quant-ph/9607030.
7. P. M. A. Dirac, *The Principles of Quantum Mechanics*, Clarendon Press, Oxford, 4 ed., 1958.
8. E. Fredkin and T. Toffoli, *Conservative Logic*, International Journal of Theoretical Physics, 21 (1982), pp. 219–253.
9. D. Gottesman, *A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound*, Physical Review A, 54 (1996), pp. 1862–1868. See also LANL preprint quant-ph/9604038.
10. ———, *Fault-Tolerant Quantum Computation with Higher-Dimensional Systems*, in Quantum Computing & Quantum Communications; First NASA International Conference; selected papers, QCQC'98, C. P. Williams, ed., vol. 1509 of Lecture Notes in Computer Science, Palm Springs, February 17–20 1998, Springer, pp. 302–313.

11. M. Grassl, *Algorithmic aspects of quantum error-correcting codes*, in Mathematics of Quantum Computation, R. K. Brylinski and G. Chen, eds., CRC-Press, 2002, pp. 223–252.

12. ———, *Fehlerkorrigierende Codes für Quantensysteme: Konstruktionen und Algorithmen*, Shaker, Aachen, 2002. Zugl.: Universität Karlsruhe, Dissertation, 2001.

13. M. Grassl and T. Beth, *Cyclic quantum error-correcting codes and quantum shift registers*, Proceedings of the Royal Society London A, 456 (2000), pp. 2689–2706. See also LANL preprint quant-ph/9910061.

14. M. Grassl, W. Geiselmann, and T. Beth, *Quantum Reed-Solomon Codes*, in Proceedings Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-13), M. Fossorier, H. Imai, S. Lin, and A. Poli, eds., vol. 1719 of Lecture Notes in Computer Science, Honolulu, Hawaii, November 15–19 1999, Springer, pp. 231–244. See also LANL preprint quant-ph/9910059.

15. P. Horodecki, *Separability criterion and inseparable mixed states with positive partial transposition*, Physics Letter A, 232 (1997), pp. 333–339. See also LANL preprint quant-ph/9703004.

16. B. Huppert, *Endliche Gruppen*, Springer, Berlin, 1967.

17. D. Jungnickel, *Finite Fields*, BI-Wissenschaftsverlag, Mannheim, 1993.

18. A. Klappenecker and M. Rötteler, *Beyond Stabilizer Codes I: Nice Error Bases*, IEEE Transactions on Information Theory, 48 (2002), pp. 2392–2395. See also LANL preprint quant-ph/0010082.

19. E. Knill, *Non-binary Unitary Error Bases and Quantum Codes*, Tech. Rep. LAUR-96-2717, LANL, 1996. See also LANL preprint quant-ph/9608048.

20. E. Knill and R. Laflamme, *Theory of quantum error-correcting codes*, Physical Review A, 55 (1997), pp. 900–911. See also LANL preprint quant-ph/9604034.

21. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Addision-Wesley, Reading, 1983.

22. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes*, North–Holland, Amsterdam, 1977.

23. O. T. O'Meara, *Symplectic Groups*, American Mathematical Society, Providence, 1978.

24. E. M. Rains, *Nonbinary Quantum Codes*, IEEE Transactions on Information Theory, 45 (1999), pp. 1827–1832. See also LANL preprint quant-ph/9703048.

25. A. M. Steane, *Error Correcting Codes in Quantum Theory*, Physical Review Letters, 77 (1996), pp. 793–797.

26. T. Toffoli, *Reversible Computing*, in Automata, Languages and Programming, J. W. de Bakker and J. van Leeuwen, eds., vol. 85 of Lecture Notes in Computer Science, Noordweijkerhout, The Netherlands, 14–18 July 1980, Springer, pp. 632–644.

27. M. A. Tsfasman, S. G. Vladut, and T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Mathematische Nachrichten, 109 (1982), pp. 21–28.