Non-Additive Quantum Codes from Goethals and Preparata Codes

Markus Grassl
Institute for Quantum Optics and Quantum Information
Austrian Academy of Sciences
Technikerstraße 21a, 6020 Innsbruck, Austria
Email: markus.grassl@oeaw.ac.at

Martin Rötteler
NEC Laboratories America, Inc.
4 Independence Way, Suite 200
Princeton, NJ 08540, USA
Email: mroetteler@nec-labs.com

***Abstract*— We extend the stabilizer formalism to a class of non-additive quantum codes which are constructed from non-linear classical codes. As an example, we present infinite families of non-additive codes which are derived from Goethals and Preparata codes.**

I. Introduction

Recently, several new non-additive quantum error-correcting codes (QECCs) have been constructed that have higher dimension than additive QECCs with the same length and minimum distance [5], [16], [17]. The first example of such a code is the code $((5, 6, 2))$ of [11] which has been found via numerical optimization. Afterwards, the code has been identified as the span of a particular state and its image under five unitary transformations (see also [7]). The recently discovered codes $((9, 12, 3))$ and $((10, 24, 3))$ (see [16], [17]) start with a so-called graph state which corresponds to a stabilizer state, i. e., a stabilizer code with parameters $[[n, 0, d]]$ (see [8], [13]). A basis of the quantum code is obtained by this initial state together with its image under some tensor products of Pauli matrices and identity (Pauli operators). The distance between any pair of these states can be defined as the minimal weight of a Pauli operator transforming one state into the other (see below). The problem of finding a code of high dimension can be stated as finding a maximal clique in a *search graph* whose vertices are all images of the initial state. There is an edge between two states if their distance is at least the prescribed minimum distance. Using the formalism of graph states, Cross et al. show in [5] that it is sufficient to consider Z-only operators in order to define the search graph, but this has the disadvantage that the distance between two of these states is not necessarily equal to the number of Z operators in the tensor product. Moreover, constructing a code $((n, K, d))$ requires to find a clique of size K in a search graph with 2^n vertices. Fixing one basis state, the graph can be slightly simplified. However, for the code $((10, 24, 3))$ the simplified graph still has 678 vertices and 149.178 edges.

A different approach for constructing non-additive QECCs based on Boolean functions and projection operators has been presented in [1]. Evaluating the Boolean function at the projection operators, the code is given as the sum of the image of products of the projections. Finally, we mention the non-additive QECCs obtained by the method given in [12]. Those codes have the same parameters as the additive CSS codes that can be obtained using the same underlying binary codes.

In this paper, we extend the approach of combining unitary images of stabilizer *states* to arbitrary stabilizer *codes* as starting point. For a stabilizer code $[[n, k, d]]$, the search graph has only 2^{n-k} vertices, and a clique of size K yields a quantum code of dimension $K \times 2^k$. What is more, we present some infinite families of non-additive quantum codes which are constructed using non-linear binary codes, avoiding the NP-hard problem of finding a maximal clique in the search graph. Finally, we show how to obtain encoding circuits for the resulting non-additive codes using encoding circuits for the underlying stabilizer codes.

II. A brief review of the stabilizer formalism

We start with a brief review of the stabilizer formalism for quantum error-correcting codes and the connection to additive codes over $GF(4)$ (see, e. g., [4], [6]). A stabilizer code encoding k qubits into n qubits having minimum distance d, denoted by $\mathcal{C} = [[n, k, d]]$, is a subspace of dimension 2^k of the complex Hilbert space $(\mathbb{C}^2)^{\otimes n}$ of dimension 2^n. The code is the joint eigenspace of a set of $n-k$ commuting operators $S_1, \ldots, S_{n-k}$ which are tensor products of the Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

or identity. The operators S_i generate an Abelian group $\mathcal{S}$ with 2^{n-k} elements, called the *stabilizer* of the code. It is a subgroup of the n-qubit Pauli group $\mathcal{P}_n$ which itself is generated by the tensor product of n Pauli matrices and identity. We further require that $\mathcal{S}$ does not contain any non-trivial multiple of identity. The *normalizer* of $\mathcal{S}$ in $\mathcal{P}_n$, denoted by $\mathcal{N}$, acts on the code $\mathcal{C} = [[n, k, d]]$. It is possible to identify $2k$ logical operators $\overline{X}_1, \ldots, \overline{X}_k$ and $\overline{Z}_1, \ldots, \overline{Z}_k$ such that these operators commute with any element in the stabilizer $\mathcal{S}$, and such that together with $\mathcal{S}$ they generate the normalizer $\mathcal{N}$ of the code. The operators $\overline{X}_i$ mutually commute, and so do the operators $\overline{Z}_j$. The operator $\overline{X}_i$ anti-commutes with the operator $\overline{Z}_j$ if $i = j$ and otherwise commutes with it.

It has been shown that the n-qubit Pauli group corresponds to a symplectic geometry and that one can reduce the problem of constructing stabilizer codes to finding additive codes over

$GF(4)$ that are self-orthogonal with respect to a symplectic inner product [3], [4]. Up to a scalar multiple, the elements of $\mathcal{P}_1$ can be expressed as $\sigma_x^a \sigma_z^b$ where $(a,b) \in \mathbb{F}_2^2$ is a binary vector. Choosing the basis $\{1, \omega\}$ of $GF(4)$, where ω is a primitive element of $GF(4)$ with $\omega^2 + \omega + 1 = 0$, we get the following correspondence between the Pauli matrices, elements of $GF(4)$, and binary vectors of length two:

operator	$GF(4)$	$\mathbb{F}_2^2$
I	0	(00)
σ_x	1	(10)
σ_y	ω^2	(11)
σ_z	ω	(01)

This mapping extends naturally to tensor products of n Pauli matrices being mapped to vectors of length n over $GF(4)$ or binary vectors of length $2n$. We rearrange the latter in such a way that the first n coordinates correspond to the exponents of the operators σ_x and write the vector as $(a|b)$, i. e.,

$$g = \sigma_x^{a_1}\sigma_z^{b_1} \otimes \ldots \otimes \sigma_x^{a_n}\sigma_z^{b_n} \mathrel{\hat{=}} (a|b) = (g^X|g^Z). \quad (1)$$

Two operators corresponding to the binary vectors $(a|b)$ and $(c|d)$ commute if and only if the symplectic inner product $a \cdot d - b \cdot c = 0$. In terms of the binary representation, the stabilizer corresponds to a binary code C which is self-orthogonal with respect to this symplectic inner product, and the normalizer corresponds to the symplectic dual code C^*. The stabilizer together with the logical operators $\overline{Z}_i$ generate a self-dual code. In terms of the correspondence to vectors over $GF(4)$, the stabilizer and normalizer correspond to an additive code over $GF(4)$ and its dual with respect to an symplectic inner product, respectively, which we will also denote by C and C^*. The minimum distance d of the quantum code is given as the minimum weight in the set $C^* \setminus C$ which is lower bounded by the minimum distance d^* of C^*. If $d = d^*$, the code is said to be *pure*, and for $d \geq d^*$, the code is said to be *pure up to* d^*.

III. The union of stabilizer codes

Note that we have defined a stabilizer code $\mathcal{C}$ as the joint eigenspace of the commuting operators S_i generating the stabilizer $\mathcal{S}$. The term *stabilizer* suggests that the code is the joint $+1$ eigenspace of the operators. However, for each of the generators S_i we may choose either the eigenspace with eigenvalue $+1$ or the eigenspace with eigenvalue -1. This gives rise to a decomposition of the space $(\mathbb{C}^2)^{\otimes n}$ into 2^{n-k} mutually orthogonal spaces which can be labeled by the eigenvalues of the $n-k$ generators S_i, or equivalently, by the characters χ of the stabilizer group $\mathcal{S}$. Moreover, the n-qubit Pauli group $\mathcal{P}_n$ acts transitively on these spaces.

From now on we fix the code $\mathcal{C}$ as the the joint $+1$ eigenspace corresponding to the trivial character. Let $t \in \mathcal{P}_n$ be an arbitrary n-qubit Pauli operator. Then we can define a character of $\mathcal{S}$ on the generators S_i as follows

$$\chi_t(S_i) := \begin{cases} +1 & \text{if } t \text{ and } S_i \text{ commute,} \\ -1 & \text{if } t \text{ and } S_i \text{ anti-commute.} \end{cases}$$

As the elements of the normalizer $\mathcal{N}$ commute with all elements of the stabilizer $\mathcal{S}$, two elements t_1 and t_2 define the same character if $t_2^{-1}t_1 \in \mathcal{N}$. Hence the set of characters corresponds to the cosets of $\mathcal{N}$ in $\mathcal{P}_n$. If $\mathcal{T}$ is a set of coset representatives, we can write the decomposition of the full space as

$$(\mathbb{C}^2)^{\otimes n} = \bigoplus_{t \in \mathcal{T}} t\mathcal{C}. \quad (2)$$

Note that measuring the eigenvalues of the generators S_i projects onto one of these space $t\mathcal{C}$, corresponding to the character χ_t given by the sequence of eigenvalues. In terms of the classical codes, the eigenvalues correspond to an error-syndrome which is obtained by computing the symplectic inner product of the received vector with the $n-k$ vectors corresponding to the generators of the stabilizer, i. e., a basis of the code C. For all vectors of the dual code C^* corresponding to the normalizer $\mathcal{N}$, the inner product is zero. So the different spaces $t\mathcal{C}$ correspond to cosets $C^* + t$ of the code C^*.

As for a fixed code $\mathcal{C}$ two spaces $t_1\mathcal{C}$ and $t_2\mathcal{C}$ are either identical or orthogonal, we can define the distance of them as follows:

$$\operatorname{dist}(t_1\mathcal{C}, t_2\mathcal{C}) := \min\{\operatorname{wgt}(p) : p \in \mathcal{P}_n \mid pt_1\mathcal{C} = t_2\mathcal{C}\}. \quad (3)$$

Here $\operatorname{wgt}(p)$ is the number of tensor factors in the n-qubit Pauli operator p that are different from identity. Clearly, $\operatorname{dist}(t_1\mathcal{C}, t_2\mathcal{C}) = \operatorname{dist}(t_2^{-1}t_1\mathcal{C}, \mathcal{C})$. The distance (3) can also be expressed in terms of the associated vectors over $GF(4)$.

Lemma 1: The distance of the spaces $t_1\mathcal{C}$ and $t_2\mathcal{C}$ equals the minimum weight in the coset $C^* + t_1 - t_2$, where we use t_i to denote both an n-qubit Pauli operator and the corresponding vector over $GF(4)$.

Proof: Direct computation shows

$$\begin{aligned} \operatorname{dist}(t_1\mathcal{C}, t_2\mathcal{C}) &= \operatorname{dist}(C^* + t_1, C^* + t_2) \\ &= \operatorname{dist}(C^* + (t_1 - t_2), C^*) \\ &= \min\{\operatorname{wgt}(c + t_1 - t_2) : c \in C^*\} \\ &= \min\{\operatorname{wgt}(v) : v \in C^* + t_1 - t_2\}. \end{aligned}$$

■

With this preparation, we are ready to present the general construction of the union of stabilizer codes (see also [7]). The quantum code will be defined as the span of some of the summands in (2).

Definition 2 (union stabilizer code): Let $\mathcal{C}_0 = [[n, k, d_0]]$ be a stabilizer code and let $\mathcal{T}_0 = \{t_1, \ldots, t_K\}$ be a subset of the coset representatives of the normalizer $\mathcal{N}_0$ of the code $\mathcal{C}_0$ in $\mathcal{P}_n$. Then the *union stabilizer code* is defined as

$$\mathcal{C} = \bigoplus_{t \in \mathcal{T}_0} t\mathcal{C}_0.$$

Without loss of generality we assume that $\mathcal{T}_0$ contains identity. With the union stabilizer code $\mathcal{C}$ we associate the (in general non-additive) *union normalizer code* given by

$$C^* = \bigcup_{t \in \mathcal{T}_0} C_0^* + t = \{c + t_i : c \in C_0^*, i = 1, \ldots, K\},$$

where C_0^* denotes the additive code associated with the normalizer $\mathcal{N}_0$ of the stabilizer code $\mathcal{C}_0$. We will refer to

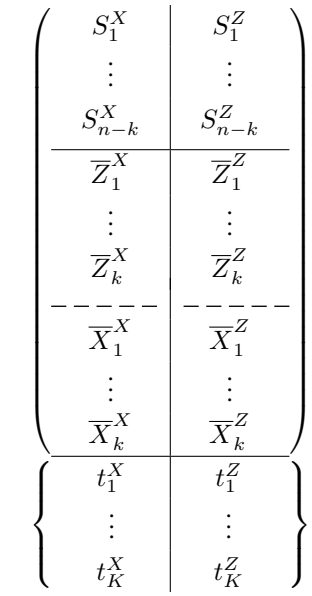

Fig. 1. Arrangements of the vectors associated with a union stabilizer code.

both, the vectors t_i and the corresponding unitary operators, as *translations*.

A union stabilizer code can be defined in terms of binary vectors as shown in Fig. 1. The first $n-k$ rows correspond to the binary vectors (cf. (1)) associated with the generators S_i of the stabilizer $\mathcal{S}$ of the code $\mathcal{C}_0$. They generate the classical code C_0. The next k rows correspond to the logical operators $\overline{Z}_j$, followed by the k logical operators $\overline{X}_i$. The last K rows correspond to the K translations t_i defining the cosets of the classical code C_0^* and the unitary images of the stabilizer code $\mathcal{C}_0$, respectively. We use curly brackets to stress the fact that the set of operators $\mathcal{T}_0$ need not be closed under group operation. In general, the quantum code is not invariant under these *generalized logical X-operators*. On the other hand, if $\mathcal{T}_0$ is closed under group operation, the resulting code will be a stabilizer code where a basis of $\mathcal{T}_0$ defines an additional set of logical X-operators.

Theorem 3: Let $\mathcal{C}$ be a union stabilizer code as in Definition 2. The dimension of $\mathcal{C}$ is $|\mathcal{T}_0|2^k = K2^k$, and the minimum distance is lower bounded by the minimum distance d of the union normalizer code C^*.

Proof: As $\mathcal{T}_0$ is a subset of the coset representatives of the normalizer $\mathcal{N}_0$, the spaces $t_i\mathcal{C}_0$, each of which has dimension 2^k, are mutually orthogonal. Hence the dimension of the union code is $K2^k$. Fixing an orthonormal basis $\{|c_j\rangle : j = 1, \ldots, 2^k\}$ of the stabilizer code $\mathcal{C}_0$, the set $\{t_i|c_j\rangle : i = 1, \ldots, K,\ j = 1, \ldots, 2^k\}$ is an orthonormal basis of the union stabilizer code. Let $E \in \mathcal{P}_n$ be an n-qubit Pauli error of weight $0 < \mathrm{wgt}(E) < d$. For basis states $|c_{i,j}\rangle = t_i|c_j\rangle \in t_i\mathcal{C}_0$ and $|c_{i',j'}\rangle = t_{i'}|c_{j'}\rangle \in t_{i'}\mathcal{C}_0$ we consider the inner product

$$\langle c_{i,j}|E|c_{i',j'}\rangle = \langle c_j|t_i^\dagger E t_{i'}|c_{j'}\rangle. \tag{4}$$

For $i \neq i'$, we have $\mathrm{dist}(t_i\mathcal{C}_0, t_{i'}\mathcal{C}_0) = \min\{\mathrm{wgt}(c + t_i - t_{i'}) : c \in C_0^*\} \geq d$, and hence (4) vanishes for $\mathrm{wgt}(E) < d$. For $i = i'$, we get

$$\langle c_j|t_i^\dagger E t_i|c_{j'}\rangle = \pm\langle c_j|E|c_{j'}\rangle. \tag{5}$$

As the code $\mathcal{C}_0$ is pure up to the minimum distance of $C_0^* \subset C^*$, equation (5) vanishes as well. ∎

Remark 4: We note that similar to stabilizer codes, the true minimum distance of a union stabilizer code might be higher. The true minimum distance is given by

$$\begin{aligned}\min\{\mathrm{dist}(c + t_i, c' + t_{i'}) : t_i, t_{i'} \in \mathcal{T}_0,& \\ c, c' \in C_0^* | c + t_i - (c' + t_{i'}) \notin \widetilde{C}_0\}& \\ = \min\{\mathrm{wgt}(v) : v \in (C^* - C^*) \setminus \widetilde{C}_0\},&\end{aligned}$$

where $(C^* - C^*) = \{a - b : a, b \in C^*\}$ denotes the set of all differences of vectors in C_0^*, and $\widetilde{C}_0$ is the symplectic dual of the additive closure of C^*.

In order to construct union quantum codes, we may start with a stabilizer code $\mathcal{C}_0$ and use a *search graph* whose vertices are the mutually orthogonal translates $\{t\mathcal{C}_0 : t \in \mathcal{T}_0\}$ of the stabilizer code. Two vertices are connected by an edge if and only if the distance between them is at least d, where d is the desired minimum distance. For simplicity, we also require that the code $\mathcal{C}_0$ is pure up to $d_0 \geq d$. The distance between two translates can be computed using Lemma 1. This allows to use stabilizer codes $\mathcal{C}_0$ of arbitrary dimension, and hence allows to go beyond the case of stabilizer states (or graph states) as, e. g., in [5], [17]. We note that the construction of non-additive quantum codes of [2] is also based on taking the union of orthogonal images of a stabilizer code.

IV. Union Stabilizer Codes from Binary Codes

A. CSS-like codes

Given two linear binary codes $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$ with $C_2^\perp \subset C_1$, the so-called CSS construction (see, e. g., [14]) yields a quantum error-correcting code $\mathcal{C} = [[n, k_1 + k_2 - n, d]]$ with $d \geq \min(d_1, d_2)$. Starting with this CSS code, we consider unions of cosets of the binary codes C_i, i. e.,

$$\widetilde{C}_i = \bigcup_{t^{(i)} \in \mathcal{T}_i} C_i + t^{(i)}$$

such that the minimum distance of the codes $\widetilde{C}_i$ is at least $\widetilde{d} \leq d$. Using the translations $\{(t^{(1)}|t^{(2)}) : t^{(1)} \in \mathcal{T}_1, t^{(2)} \in \mathcal{T}_2\}$ we obtain a CSS-like union stabilizer code of dimension $|\mathcal{T}_1| \cdot |\mathcal{T}_2| \cdot 2^{k_1+k_2-n}$ whose minimum distance is at least $\widetilde{d}$. If $G_1 = \left(\frac{H_2}{G_{12}}\right)$ and $G_2 = \left(\frac{H_1}{G_{21}}\right)$ are generator matrices of the codes C_i, where H_i is a generator matrix of the dual code $C_i^\perp$, the corresponding vectors are as shown in Fig. 2.

B. Enlargement construction

Steane has presented a construction that allows to increase the dimension of a CSS code [14]. For this, he starts with the CSS construction applied to a binary code $C = [n, k, d]$ which contains its dual, yielding a CSS code $\mathcal{C}_0 = [[n, 2k - n, d]]$. Using a code $C' = [n, k' > k + 1, d']$ which contains C, he obtains a quantum code $[[n, k + k' - n, \min(d, \lceil 3d'/2 \rceil)]]$. The

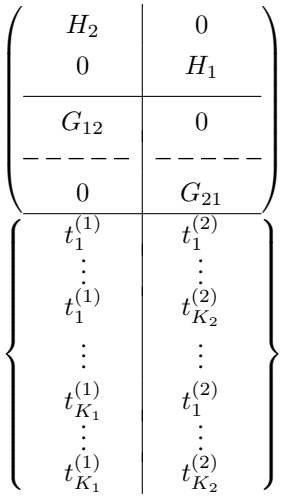

Fig. 2. Arrangements of the vectors associated with a CSS-like union stabilizer code.

resulting code can also be considered as a union stabilizer code. If D is a generator matrix of the complement of C in C' and A is a fixed point free, invertible linear map, the translations can be defined as

$$\mathcal{T}_0 = \{(vD|vAD) : v \in \mathbb{F}_2^{k'-k}\}.$$

The key observation [14] for proving the lower bound on the minimum distance is that the weight of an operator $g = (g^X|g^Z)$ can be expressed in terms of the Hamming weight of the binary vectors and their sum:

$$\mathrm{wgt}((g^X|g^Z)) = \frac{1}{2}(\mathrm{wgt}(g^X) + \mathrm{wgt}(g^Z) + \mathrm{wgt}(g^X + g^Z)).$$

As $\mathcal{T}_0$ is closed under addition and the properties of A ensure that $0 \neq t^X \neq t^Z \neq 0$ for any non-zero element $(t^X|t^Z) \in \mathcal{T}_0$, the weight of all three binary vectors is lower bounded by d'.

V. Quantum Codes from Reed-Muller, Goethals, and Preparata Codes

Using the CSS-like construction of the previous section, we now construct some families of non-additive quantum codes. For this, we use the Goethals codes $\mathcal{G}(m)$ and the Preparata codes which are nonlinear binary codes of length $n = 2^m$ for $m \geq 4$, m even. Some of the properties of these codes are summarized as follows (see, e. g., [10]):

- Both the Goethals code $\mathcal{G}(m)$ and the Preparata code $\mathcal{P}(m)$ are unions of cosets of the Reed-Muller code $\mathcal{R}(m) := \mathrm{RM}(m-3, m)$. Furthermore, they are nested subcodes of $\mathrm{RM}(m-2, m)$, i. e.,

$$\mathrm{RM}(m-3, m) \subset \mathcal{G}(m) \subset \mathcal{P}(m) \subset \mathrm{RM}(m-2, m).$$

- The parameters of the codes are

$$\begin{aligned} \mathrm{RM}(m-3, m) = \mathcal{R}(m) &= [2^m, 2^m - \tbinom{m}{2} - m - 1, 8] \\ \mathcal{G}(m) &= (2^m, 2^{2^m - 3m + 1}, 8) \\ \mathcal{P}(m) &= (2^m, 2^{2^m - 2m}, 6) \\ \mathrm{RM}(m-2, m) &= [2^m, 2^m - m - 1, 4]. \end{aligned}$$

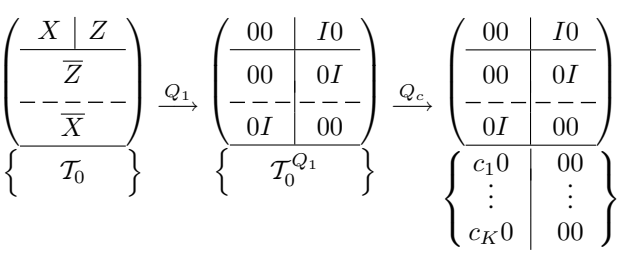

Fig. 3. Transformation of the union stabilizer code given by the inverse encoding circuits Q_1 and Q_c.

Steane has constructed a family of additive quantum codes from Reed-Muller codes [15]. The codes are obtained applying the enlargement construction of [14] to the chain of codes

$$\begin{aligned} \mathrm{RM}(r, m) \subset \mathrm{RM}(r, m)^\perp &= \mathrm{RM}(m-r-1, m) \\ &\subset \mathrm{RM}(m-r, m). \end{aligned}$$

In particular, for $r = 2$ and $m \geq 5$ this yields additive QECCs $\mathcal{C}_1 = [[2^m, 2^m - \binom{m}{2} - 2m - 2, 6]]$, while using only the CSS construction, one obtains $\mathcal{C}_0 = [[2^m, 2^m - 2\binom{m}{2} - 2m - 2, 8]]$. As the Goethals code $\mathcal{G}(m)$ is the union of $K_G = 2^{\binom{m}{2}-2m+2}$ cosets of $\mathcal{R}(m)$, we can construct a CSS-like union stabilizer code based on $\mathcal{C}_0$. The minimum distance of the resulting non-additive code is 8 and its dimension is $K_G^2 \dim(\mathcal{C}_0) = 2^{2^m - 6m + 2}$.

Replacing the Goethals code by the Preparata code $\mathcal{P}(m)$, we have $K_P = 2^{\binom{m}{2}-m+1}$ cosets of $\mathcal{R}(m)$. This results in a CSS-like union stabilizer code with minimum distance 6 and dimension $K_P^2 \dim(\mathcal{C}_0) = 2^{2^m - 4m}$.

Both the union stabilizer codes based on Goethals codes and those based on Preparata codes are superior to the additive codes derived from Reed-Muller codes. The parameters of the first codes in these families are as follows:

enlarged RM	Goethals	Preparata
$[[64, 35, 6]]$	$((64, 2^{30}, 8))$	$((64, 2^{40}, 6))$
$[[256, 210, 6]]$	$((256, 2^{210}, 8))$	$((256, 2^{224}, 6))$
$[[1024, 957, 6]]$	$((1024, 2^{966}, 8))$	$((1024, 2^{984}, 6))$

However, applying the enlargement construction to extended primitive BCH codes results in stabilizer codes with parameters $[[2^m, 2^m - 5m - 2, 8]]$ and $[[2^m, 2^m - 3m - 2, 6]]$ (see [14]).

VI. Encoding Circuits

In [9] we have shown how to compute a quantum circuit consisting of Clifford gates only that transforms any stabilizer $\mathcal{S}$ given by the binary $(n-k) \times 2n$ matrix $(X|Z)$ into the stabilizer of a trivial code given by $(0|I0)$, where I is an identity matrix of size $n-k$. The corresponding trivial code corresponds to the mapping $|\phi\rangle \mapsto |0 \ldots 0\rangle|\phi\rangle$. We denote the resulting quantum circuit that corresponds to the inverse encoding circuit of $(X|Z)$ by Q_1. Note that we can apply Q_1 to all the operators defining the code as illustrated in Fig. 3. Further note, that for the trivial stabilizer code, the "encoded"

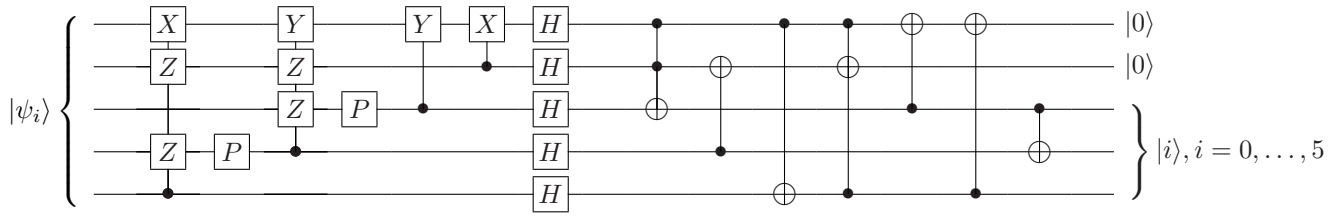

Fig. 4. Inverse encoding circuit for the non-additive code $((5, 6, 2))$. The first set of gates including the Hadamard transformations implements the inverse encoding circuit Q_1 for the stabilizer code $[[5, 0, 3]]$, followed by 5 CNOT and 2 Toffoli gates implementing the classical circuit Q_c.

X- and Z-operators are weight-one Pauli operators σ_x and σ_z, respectively, acting on the last k qubits. As the transformed translations $\mathcal{T}_0^{Q_1}$ define cosets of the normalizer, we may choose them such that they are tensor products of operators σ_x and identity acting on the first $n-k$ qubits only. Then we have the trivial union code spanned by a set of $K2^k$ basis states of the form $|c_i\rangle|j\rangle$, where $\{|j\rangle : j = 0, \ldots, 2^k - 1\}$ is the computational basis of k qubits and $\{c_i : i = 0, \ldots, K - 1\}$ is a set of bit strings of length $n - k$. In order to obtain a standard basis for our input space of dimension $K2^k$, we need a quantum circuit Q_c mapping $|c_i\rangle \mapsto |i\rangle$ for $i = 0, \ldots, K-1$. Note that this is a purely classical circuit which can be realized, e. g., using σ_x, CNOT gates, and Toffoli gates.

We illustrate this for the non-additive code $((5, 6, 2))$ which is a union stabilizer code derived from the stabilizer state $\mathcal{C}_0 = [[5, 0, 3]]$. For a stabilizer code with $k = 0$, there are no encoded X- and Z-operators. So the code $((5, 6, 2))$ is specified by five generators of the stabilizer and six translations. Using an inverse encoding circuit Q_1, these operators are transformed as follows:

$$\left(\begin{array}{ccccc} X & X & X & X & X \\ X & X & Z & I & Z \\ X & Z & I & Z & X \\ Y & I & Y & Z & Z \\ Y & Z & Z & Y & I \end{array}\right) \left\{\begin{array}{ccccc} I & I & I & I & I \\ I & I & Z & Z & X \\ I & I & I & X & X \\ I & I & I & Z & Y \\ I & I & Z & Y & Y \\ I & I & Z & X & Z \end{array}\right\} \xrightarrow{Q_1} \left(\begin{array}{c|c} 00000 & 10000 \\ 00000 & 01000 \\ 00000 & 00100 \\ 00000 & 00010 \\ 00000 & 00001 \end{array}\right) \left\{\begin{array}{c|c} 00000 & 00000 \\ 01010 & 00000 \\ 11011 & 00000 \\ 01111 & 00000 \\ 11100 & 00000 \\ 10010 & 00000 \end{array}\right\} \quad (6)$$

It remains to find a (classical) quantum circuit Q_c that maps the six binary strings on the right hand side of (6) to say the binary representations of $i = 0, \ldots, 5$. Using a breath-first search among all circuits composed of σ_x, CNOT, and Toffoli gates, we found the minimal realization shown together with the circuit Q_1 in Fig. 4.

VII. Conclusions

The approach presented in this paper generalizes naturally to the construction of non-additive quantum codes for higher dimensional systems. In order to obtain other families of non-additive quantum codes, it is interesting to study classical non-linear codes which can be decomposed into cosets of linear codes, similar to the Preparata and Goethals codes.

Acknowledgments

We acknowledge fruitful discussions with Vaneet Aggarwal and Robert Calderbank. Markus Grassl would like to thank NEC Labs., Princeton for the hospitality during his visit. This work was partially supported by the FWF (project P17838).

References

[1] V. Aggarwal and A. R. Calderbank, "Boolean Functions, Projection Operators and Quantum Error Correcting Codes," in *Proceedings of the 2007 IEEE International Symposium on Information Theory*, Nice, France, June 24 – June 29 2007, pp. 2091–2095, preprint cs/0610159.

[2] V. Arvind, P. P. Kurur, and K. R. Parthasarathy, "Non-stabilizer quantum codes from Abelian subgroups of the error group," *Quantum Information and Computation*, vol. 4, no. 6 & 7, pp. 411–436, 2004.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum Error Correction and Orthogonal Geometry," *Physical Review Letters*, vol. 78, no. 3, pp. 405–408, Jan. 1997, preprint quant-ph/9605005.

[4] ——, "Quantum Error Correction Via Codes Over GF(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998, preprint quant-ph/9608006.

[5] A. Cross, G. Smith, J. A. Smolin, and B. Zeng, "Codewords Stabilized Quantum Codes," 2007, preprint arXiv:0708.1021v4 [quant-ph].

[6] D. Gottesman, "A Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound," *Physical Review A*, vol. 54, no. 3, pp. 1862–1868, Sep. 1996, preprint quant-ph/9604038.

[7] M. Grassl and T. Beth, "A Note on Non-Additive Quantum Codes," 1997, preprint quant-ph/9703016.

[8] M. Grassl, A. Klappenecker, and M. Rötteler, "Graphs, Quadratic Forms, and Quantum Codes," in *Proceedings of the 2002 IEEE International Symposium on Information Theory*, Lausanne, Switzerland, June 30 – July 5 2002, p. 45, preprint quant-ph/0703112.

[9] M. Grassl, M. Rötteler, and T. Beth, "Efficient Quantum Circuits for Non-Qubit Quantum Error-correcting Codes," *International Journal of Foundations of Computer Science*, vol. 14, no. 5, pp. 757–775, Oct. 2003, preprint quant-ph/0211014.

[10] F. B. Hergert, "On the Delsarte-Goethals Codes and Their Formal Duals," *Discrete Mathematics*, vol. 83, pp. 249–263, 1990.

[11] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, "Nonadditive Quantum Code," *Physical Review Letters*, vol. 79, no. 5, pp. 953–954, Aug. 1997, preprint quant-ph/9703002.

[12] V. P. Roychowdhury and F. Vatan, "On the Existence of Nonadditive Quantum Codes," in *QCQC'98*, C. P. Williams, Ed., vol. 1509. Heidelberg: Springer, 1999, pp. 325–336.

[13] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs," *Physical Review A*, vol. 65, no. 012308, 2002, quant-ph/0012111.

[14] A. M. Steane, "Enlargement of Calderbank-Shor-Steane Quantum Codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999, preprint quant-ph/9802061.

[15] ——, "Quantum Reed-Muller Codes," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1701–1703, Jul. 1999, preprint quant-ph/9608026.

[16] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, "Nonadditive quantum error-correcting code," Apr. 2007, preprint arXiv.0704.2122v1 [quant-ph].

[17] S. Yu, Q. Chen, and C. H. Oh, "Graphical Quantum Error-Correcting Codes," Sep. 2007, preprint arXiv.0709.1780v1 [quant-ph].