Quantum Goethals-Preparata Codes

Markus Grassl
Inst. for Quantum Optics & 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 present a family of non-additive quantum codes based on Goethals and Preparata codes with parameters $((2^m, 2^{2^m-5m+1}, 8))$. The dimension of these codes is eight times higher than the dimension of the best known additive quantum codes of equal length and minimum distance.**

***Index Terms*—Non-additive quantum code, Goethals code, Preparata code**

I. Introduction

Most of the known quantum error-correcting codes (QECCs) are based on the so-called stabilizer formalism which relates quantum codes to certain additive codes over $GF(4)$ (see, e. g., [3], [7]). It is known that non-additive QECCs can have a higher dimension compared to additive QECCs with the same length and minimum distance [5], [14], [17], [18]. All these examples of non-additive QECCs are examples of so-called codeword stabilized quantum codes which are obtained as the complex span of some so-called stabilizer states, which correspond to self-dual additive codes. In [9] we have extended the framework of stabilizer codes to the union of stabilizer codes. This allows to construct non-additive codes from any stabilizer code. In general, these non-additive QECCs correspond to non-additive codes over $GF(4)$ which can be decomposed into cosets of an additive code which contains its dual. Using a construction similar to that of so-called CSS codes (see [4], [15]), families of non-additive quantum codes based on the binary Goethals and Preparata codes were derived in [9]. Here we present a new family of non-additive quantum codes which have a dimension that is eight times higher than the dimension of the best known additive quantum codes.

II. Union Stabilizer Codes

A. Stabilizer codes

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., [3], [7]). 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 [2], [3]. 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.,

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

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^*. In terms of the correspondence to vectors over $GF(4)$, the stabilizer and normalizer correspond to an additive code over

978-1-4244-2571-6/08/$25.00 ©2008 IEEE

$GF(4)$ and its dual with respect to a symplectic inner product, respectively, which we will also denote by C and C^*. The term *additive quantum code* refers to this correspondence. The minimum distance d of the quantum code is given as the minimum weight in the set $C^* \setminus C \subset GF(4)^n$ which is lower bounded by the minimum distance d^* of the additive code 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^*.

Fixing the logical operators $\overline{X}_i$ and $\overline{Z}_j$, there is a canonical basis for the additive quantum code $\mathcal{C}$. The stabilizer group $\mathcal{S}$ of the quantum code together with the logical operators $\overline{Z}_j$ generate an Abelian group of order 2^n which corresponds to a self-dual additive code. The joint $+1$-eigenspace is one-dimensional, hence there is a unique quantum state $|\overline{00\dots0}\rangle \in \mathcal{C}$ stabilized by all elements of $\mathcal{S}$. An orthonormal basis of the code $\mathcal{C}$ is given by the states

$$|\overline{i_1 i_2 \dots i_k}\rangle = \overline{X}_1^{i_1} \cdots \overline{X}_k^{i_k} |\overline{00\dots0}\rangle, \tag{2}$$

where $(i_1 i_2 \dots i_k) \in \mathbb{F}_2^k$.

B. Union stabilizer codes

The stabilizer group $\mathcal{S}$ gives rise to an orthogonal decomposition of the space $(\mathbb{C}^2)^{\otimes n}$ into common eigenspaces of equal dimension. The stabilizer code $\mathcal{C}$ is the joint $+1$-eigenspace of dimension 2^k. In general, the joint eigenspaces of $\mathcal{S}$ can be labeled by the eigenvalues of a set of $n-k$ generators of $\mathcal{S}$. Moreover, the n-qubit Pauli group $\mathcal{P}_n$ operates transitively on the eigenspaces. Hence one can identify a set $\mathcal{T} \subset \mathcal{P}_n$ of 2^{n-k} operators such that

$$(\mathbb{C}^2)^{\otimes n} = \bigoplus_{t \in \mathcal{T}} t\mathcal{C}. \tag{3}$$

Note that each of the spaces $t\mathcal{C}$ is a quantum error-correcting code with the same parameters as the code $\mathcal{C}$ and stabilizer group $t\mathcal{S}t^{-1}$. The decomposition (3) corresponds to the decomposition of the n-qubit Pauli group $\mathcal{P}_n$ into cosets with respect to the normalizer $\mathcal{N}$ of the code $\mathcal{C}$ and likewise to the decomposition of the full vector space $GF(4)^n$ into cosets of the additive code C^*.

The main idea of union stabilizer codes is to find a subset $\mathcal{T}_0$ of the *translations* $\mathcal{T}$ such that the space $\bigoplus_{t \in \mathcal{T}_0} t\mathcal{C}$ is a good quantum code (see [8], [9]).

Definition 1 (union stabilizer code): Let $\mathcal{C}_0 = [[n,k]]$ be a stabilizer code and let $\mathcal{T}_0 = \{t_1, \dots, t_K\}$ 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. The dimension of $\mathcal{C}$ is $K2^k$, and we will use the notation $\mathcal{C} = ((n, K2^k, d))$.

Similar to (2) a canonical basis of the union stabilizer code $\mathcal{C}$ is given by

$$|\overline{j; i_1 i_2 \dots i_k}\rangle = t_j \overline{X}_1^{i_1} \cdots \overline{X}_k^{i_k} |\overline{00\dots0}\rangle, \tag{4}$$

where $j = 1, \dots, K$, $(i_1 i_2 \dots i_k) \in \mathbb{F}_2^k$, and $\overline{X}_i$ are logical operators of the stabilizer code $\mathcal{C}_0$.

In order to compute the minimum distance of this code, we first consider the distance between two spaces $t_1\mathcal{C}_0$ and $t_2\mathcal{C}_0$. As for a fixed stabilizer code $\mathcal{C}_0$ two spaces $t_1\mathcal{C}_0$ and $t_2\mathcal{C}_0$ are either identical or orthogonal, we can define the distance of them as follows:

$$\operatorname{dist}(t_1\mathcal{C}_0, t_2\mathcal{C}_0) := \min\{\operatorname{wgt}(p) \colon p \in \mathcal{P}_n \mid p t_1 \mathcal{C}_0 = t_2 \mathcal{C}_0\}. \tag{5}$$

Here $\operatorname{wgt}(p)$ is the number of tensor factors in the n-qubit Pauli operator p that are different from identity. Clearly, $\operatorname{dist}(t_1\mathcal{C}_0, t_2\mathcal{C}_0) = \operatorname{dist}(t_2^{-1}t_1\mathcal{C}_0, \mathcal{C}_0)$. The two spaces are identical if and only if $t_2^{-1}t_1$ is an element of the normalizer group $\mathcal{N}_0$, or equivalently, if the cosets $C_0^* + t_1$ and $C_0^* + t_2$ of the additive normalizer code C_0^* are identical. (Note that we denote both an n-qubit Pauli operator and the corresponding vector over $GF(4)$ by t_i.) Hence the distance (5) can also be expressed in terms of the associated vectors over $GF(4)$.

Lemma 2: The distance of the spaces $t_1\mathcal{C}_0$ and $t_2\mathcal{C}_0$ equals the minimum weight in the coset $C_0^* + t_1 - t_2$.

Proof: Direct computation shows

$$\begin{aligned}
\operatorname{dist}(t_1\mathcal{C}_0, t_2\mathcal{C}_0) &= \operatorname{dist}(C_0^* + t_1, C_0^* + t_2) \\
&= \operatorname{dist}(C_0^* + (t_1 - t_2), C_0^*) \\
&= \min\{\operatorname{wgt}(c + t_1 - t_2) \colon c \in C_0^*\} \\
&= \min\{\operatorname{wgt}(v) \colon v \in C_0^* + t_1 - t_2\}.
\end{aligned}$$

■

While the distance between the cosets $C_0^* + t_j$ is an upper bound on the minimum distance of the union code $\mathcal{C}$, the true minimum distance can be derived from the following code over $GF(4)$.

Definition 3 (union normalizer code): With the union stabilizer code $\mathcal{C}$ we associate the (in general non-additive) *union normalizer code* given by

$$C^* = \bigcup_{t \in \mathcal{T}_0} C_0^* + t = \{c + t_j \colon c \in C_0^*,\ j = 1, \dots, K\},$$

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

Theorem 4: The minimum distance of a union stabilizer code with union normalizer code C^* is given by

$$\begin{aligned}
d &= \min\{\operatorname{wgt}(v) : v \in (C^* - C^*) \setminus \widetilde{C}_0\} \\
&\geq d_{\min}(C^*) \\
&= \min\{\operatorname{dist}(c + t_i, c' + t_{i'}) \colon t_i, t_{i'} \in \mathcal{T}_0, c, c' \in C_0^* \\
&\qquad\qquad c + t_i \neq c' + t_{i'}\},
\end{aligned}$$

where $C^* - C^* := \{a - b \colon a, b \in C^*\}$ denotes the set of all differences of vectors in C^*, and $\widetilde{C}_0 \leq C_0$ is the additive code that corresponds to all elements of the stabilizer group $\mathcal{S}$ that commute with all $t_j \in \mathcal{T}_0$.

Proof: Let $E \in \mathcal{P}_n$ be an n-qubit Pauli error of weight $0 < \operatorname{wgt}(E) < d$. For two canonical basis states $|\psi_a\rangle$ and $|\psi_b\rangle$

as given in (4) we consider the inner product

$$\begin{aligned}\langle\psi_a|E|\psi_b\rangle =&\langle\overline{j;i_1i_2\dots i_k}|E|\overline{j';i'_1i'_2\dots i'_k}\rangle\\ =&\langle\overline{00\dots0}|\overline{X}_1^{i_1}\cdots\overline{X}_k^{i_k}t_jEt_{j'}\overline{X}_1^{i'_1}\cdots\overline{X}_k^{i'_k}|\overline{00\dots0}\rangle\\ =&\pm\langle\overline{00\dots0}|\overline{X}_1^{i_1+i'_1}\cdots\overline{X}_k^{i_k+i'_k}t_jt_{j'}E|\overline{00\dots0}\rangle.\end{aligned}$$

If $E\in\mathcal{S}$ commutes with all $t_j\in\mathcal{T}_0$, then $\langle\psi_a|E|\psi_b\rangle=\delta_{ab}$. Otherwise, $E\notin C^*-C^*$ since $0<\mathrm{wgt}(E)<d$, and hence the inner product vanishes. ∎

III. The Binary Goethals and Preparata Codes

In this section we recall some properties of the binary Goethals codes [6] and the Preparata codes [13]. It has been shown that variations of these codes have a simple description as $\mathbb{Z}_4$-linear codes [10], but in our context the description in terms of cosets of linear binary codes is used.

In the following m is an even integer ($m\geq 6$) and $n=2^{m-1}-1$. Let α be a primitive element of the finite field $GF(2^{m-1})$. By $\mu_i(z)$ we denote the minimal polynomial of α^i over $GF(2)$, i. e., the polynomial with roots α^j for $j=i2^k$. The idempotent $\theta_i(z)$ is the unique polynomial satisfying

$$\theta_i(\alpha^i)=1\quad\text{and}\quad\theta_i(\alpha^j)=0\text{ for }j\neq i2^k.$$

Codewords of a cyclic code can be represented by polynomials $f(z)$, and we use $(f(z);f(1))$ to denote the codeword of the extended cyclic code obtained by adding an overall parity check. Similar, we use $(f(z);f(1);g(z);g(1))$ to denote the juxtaposition of codewords of two extended cyclic codes.

Definition 5 (Goethals code [6]): The Goethals code $\mathcal{G}(m)$ of length 2^m is the union of 2^{m-1} cosets of the linear binary code $C_{\mathcal{G}}=[2^m,2^m-4m+2,8]$. The code $C_{\mathcal{G}}$ is obtained via the $|u|u+v|$ construction applied to the extended cyclic codes $\overline{C_1}$ and $\overline{C_2}$. The cyclic code C_1 is a single-error correcting code with generator polynomial $\mu_1(z)$, and C_2 is generated by $\mu_1(z)\mu_r(z)\mu_s(z)$ where $r=1+2^{m/2-2}$ and $s=1+2^{m/2-1}$. The non-zero coset representatives are given by $(z^i;1;z^i\theta_1(z);0)$ for $i=1,\dots,n-1$.

An alternative description of Goethals codes has been given in [1]. The codewords are described by pairs (X,Y) of subsets of $GF(2^{m-1})$. The corresponding codeword is given by the juxtaposition of the characteristic functions 1_X and 1_Y of the two sets X and Y, i. e.

$$(X,Y)\mathrel{\hat{=}}(1_X(\alpha^i);1_X(0);1_Y(\alpha^i);1_Y(0)),$$

where $1_X(\alpha^i)$ is a short-hand for the vector

$$1_X(\alpha^i)=(1_X(\alpha^0),1_X(\alpha^1),\dots,1_X(\alpha^{n-1}))$$

and

$$1_S(x)=\begin{cases}1 & \text{if } x\in S,\\ 0 & \text{if } x\notin S.\end{cases}$$

The non-zero elements of X and Y give rise to the polynomials $f_X(z)$ and $f_Y(z)$ given by

$$f_S(z)=\sum_{i=0}^{n-1}1_S(\alpha^i)z^i. \tag{6}$$

Definition 6 (Goethals code [1]): The Goethals code $\mathcal{G}(m)$ of length 2^m consists of the codewords described by all pairs (X,Y) satisfying:

a) $|X|$ is even, $|Y|$ is even,

b) $\displaystyle\sum_{x\in X}x=\sum_{y\in Y}y,$

c) $\displaystyle\sum_{x\in X}x^r+\left(\sum_{x\in X}x\right)^r=\sum_{y\in Y}y^r,$

d) $\displaystyle\sum_{x\in X}x^s+\left(\sum_{x\in X}x\right)^s=\sum_{y\in Y}y^s.$

In order to relate the two definitions, we distinguish three cases.

1) $X=Y$: Conditions c) and d) imply that $\sum_{x\in X}x=0$. This is true for all codewords of the cyclic code generated by $\mu_1(z)$. Adding an overall parity check implies Condition a).
2) $X=\emptyset$: The left hand side of Conditions b), c), and d) vanishes, so the solutions for Y correspond to an extended cyclic code with generator polynomial $\mu_1(z)\mu_r(z)\mu_s(z)$.
3) $X=\{0,x=\alpha^i\}$: From (6) it follows that $f_Y(\alpha)=\sum_{y\in Y}y$. So Condition b) holds for the set Y corresponding to $f_Y(z)=z^i\theta_1(z)$. The left hand side of Conditions c) and d) vanishes, so the solutions for Y are elements of the extended cyclic code with generator polynomial $\mu_r(z)\mu_s(z)$. As neither r nor s is a power of two, the polynomial $\theta_1(z)$ and hence $f_Y(z)=z^i\theta_1(z)$ vanishes for α^r and α^s, i. e., Conditions c) and d) hold.

Finally, all codewords of the Goethals code as given in Definition 5 are the juxtaposition of two binary vectors of even weight, i. e., Condition a) holds. Hence any codeword given by Definition 5 fulfills the conditions of Definition 6. The equivalence of the definitions follows from the fact that the codes have equal size.

Next we consider the definition of Preparata codes similar to Definition 6 given in [1].

Definition 7 (Preparata code [1]): The extended Preparata code $\mathcal{P}(m)$ of length 2^m and parameter σ consists of the codewords described by all pairs (X,Y) satisfying:

a) $|X|$ is even, $|Y|$ is even,

b) $\displaystyle\sum_{x\in X}x=\sum_{y\in Y}y,$

c) $\displaystyle\sum_{x\in X}x^{\sigma+1}+\left(\sum_{x\in X}x\right)^{\sigma+1}=\sum_{y\in Y}y^{\sigma+1},$

Here σ is a power of two and $\gcd(\sigma\pm1,n)=1$. For $\sigma=2^{m/2-1}$ and $n=2^{m-1}-1$ we compute

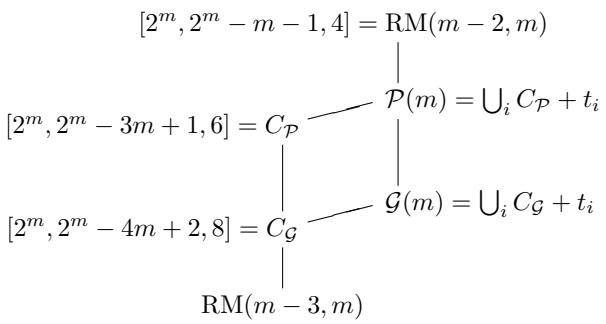
$$\left(2^{m-1}-1\right)-\left(2^{m/2-1}\pm1\right)\left(2^{m/2}\mp2\right)=1,$$

showing that $\gcd(\sigma\pm1,n)=1$. Hence for this particular choice of σ, the Preparata code of Definition 7 contains the Goethals code. What is even more, we can describe the Preparata code similar to Definition 5 as the union of cosets

of the linear binary code $C_{\mathcal{P}}$ which contains the linear binary code $C_{\mathcal{G}}$.

Definition 8: The extended Preparata code $\mathcal{P}(m)$ of length 2^m is the union of 2^{m-1} cosets of the linear binary code $C_{\mathcal{P}} = [2^m, 2^m - 3m + 1, 6]$. The code $C_{\mathcal{P}}$ is obtained via the $|u|u+v|$ construction applied to the extended cyclic codes $\overline{C_1}$ and $\overline{C_3}$. The cyclic code C_1 is a single-error correcting code with generator polynomial $\mu_1(z)$, and C_3 is generated by $\mu_1(z)\mu_s(z)$ where $s = 1 + 2^{m/2-1}$. The non-zero coset representatives are given by $(z^i; 1; z^i\theta_1(z); 0)$.

Comparing Definitions 5 and 8 we see that we can use the very same coset representatives to construct the Goethals and the Preparata code as union of cosets of the linear binary codes $C_{\mathcal{G}}$ and $C_{\mathcal{P}}$, respectively. Moreover, all codes lie between codes that are equivalent to the Reed-Muller codes $RM(m-3, m)$ and $RM(m-2, m) = [2^m, 2^m - m - 1, 4]$ (see [11]). This is illustrated by the following diagram:



The components of the codes are summarized as follows:

- C_1: cyclic code generated by $\mu_1(z)$
- C_3: cyclic code generated by $\mu_1(z)\mu_s(z)$
- C_2: cyclic code generated by $\mu_1(z)\mu_r(z)\mu_s(z)$ $r = 1 + 2^{m/2-2}$, $s = 1 + 2^{m/2-1}$
- $C_{\mathcal{G}}$: $|u|u+v|$ construction applied to the extended cyclic codes $\overline{C_1}$ and $\overline{C_2}$
- $C_{\mathcal{P}}$: $|u|u+v|$ construction applied to the extended cyclic codes $\overline{C_1}$ and $\overline{C_3}$
- t_i: $n+1$ coset representatives with

$$t_i = \begin{cases} (z^i; 1; z^i\theta_1(z); 0) & \text{for } i = 0, \ldots, n-1, \\ (0, \ldots, 0) & \text{for } i = n. \end{cases}$$

IV. The Quantum Goethals-Preparata Codes

Before presenting the new family of non-additive quantum codes, we recall Steane's construction to enlarge the dimension of CSS codes.

Theorem 9 (see [16]): Let $C = [n, k, d]$ and $C' = [n, k' > k + 1, d']$ be linear binary codes with $C^\perp \leq C < C'$. Then there exists an additive quantum code $\mathcal{C} = [[n, k + k' - n, \geq \min(d, 3d'/2)]]$. Given a generator matrix G of the code C and a generator matrix D of the complement of C in C', the normalizer of the code $\mathcal{C}$ is generated by

$$\left(\begin{array}{c|c} G & 0 \\ 0 & G \\ D & AD \end{array}\right),$$

where A is a fixed-point free linear transformation.

As the code $C_{\mathcal{G}}$ contains a code that is isomorphic to the Reed-Muller code $RM(m-3, m)$ it follows that $C_{\mathcal{G}}^\perp \leq C_{\mathcal{G}}$. Hence we can apply Steane's construction [16] to the chain $C_{\mathcal{G}}^\perp \leq C_{\mathcal{G}} < C_{\mathcal{P}}$ of linear binary codes and obtain an additive quantum code with parameters $\mathcal{C}_0 = [[2^m, 2^m - 7m + 3, 8]]$. In a second step we use the $K = 2^{m-1}$ coset representatives t_i of the decomposition of both the Goethals and the Preparata code. This yields a non-additive code with dimension $K^2 2^{2^m - 7m + 3} = 2^\ell$ where $\ell = 2^m - 5m + 1$.

$$\left(\begin{array}{c|c} G & 0 \\ 0 & G \\ D & AD \end{array}\right) \left\{\begin{array}{c|c} t_1 & t_1 \\ \vdots & \vdots \\ t_1 & t_K \\ \vdots & \vdots \\ t_K & t_1 \\ \vdots & \vdots \\ t_K & t_K \end{array}\right\}$$

Fig. 1. Structure of the non-additive union normalizer code of the quantum Goethals-Preparata codes.

Theorem 10: Let $\mathcal{C}_0 = [[2^m, 2^m - 7m + 3, 8]]$ be the additive quantum code obtained from the chain of linear binary codes $C_{\mathcal{G}}^\perp \leq C_{\mathcal{G}} \leq C_{\mathcal{P}}$ using Steane's enlargement construction. Furthermore, let $\mathcal{T}_0 = \{(t_i|t_j) \colon i, j = 0, \ldots, 2^{m-1} - 1\}$ where t_i are the coset representatives used to obtain the Goethals and Preparata code. Then the *quantum Goethals-Preparata code* is a union stabilizer code given by $\mathcal{C}_0$ and $\mathcal{T}_0$. The minimum distance of the quantum Goethals-Preparata code is eight.

Proof: Let G denote a generator matrix of the code $C_{\mathcal{G}}$ and let D be such that $\binom{G}{D}$ generates $C_{\mathcal{P}}$. The structure of the non-additive union-normalizer code of the quantum Goethals-Preparata codes is illustrated in Fig. 1. A generator matrix of the normalizer of the additive quantum code $\mathcal{C}_0$ is given above the horizontal line, while the set of translations is listed below the horizontal line. Every codeword of the non-additive union normalizer code is of the form

$$g = (g^X | g^Z) = (c_1 + v + t_i | c_2 + w + t_j),$$

where $c_1, c_2 \in C_{\mathcal{G}} = [2^m, 2^m - 4m + 2, 8]$ and $v, w \in C_{\mathcal{P}}/C_{\mathcal{G}}$. For $g, g' \in C^*, g \neq g'$ we compute

$$\begin{aligned} \mathrm{dist}(g, g') &= \mathrm{dist}((c_1 + v + t_i | c_2 + w + t_j), \\ &\qquad (c_1' + v' + t_i' | c_2' + w' + t_j')) \\ &= \mathrm{wgt}((c_1'' + v'' + t_i - t_i' | c_2'' + w'' + t_j - t_j')), \end{aligned}$$

where $c_1'' = c_1 - c_1'$ and $c_1'' = c_1 - c_1'$ are codewords of $C_{\mathcal{G}}$, and $v'' = v - v'$, $w'' = w - w'$ are codewords of $C_{\mathcal{P}}/C_{\mathcal{G}}$. In general, the weight of $g = (g^X|g^Z)$ is given by

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

Hence we get

$$\begin{aligned}
&\mathrm{dist}(g, g') = \\
&\quad \frac{1}{2}\,\mathrm{wgt}(c_1'' + v'' + t_i - t_i') && \text{(7a)}\\
&\quad +\frac{1}{2}\,\mathrm{wgt}(c_2'' + w'' + t_j - t_j') && \text{(7b)}\\
&\quad +\frac{1}{2}\,\mathrm{wgt}(c_1'' + c_2'' + v'' + w'' + t_i - t_i' + t_j - t_j'). && \text{(7c)}
\end{aligned}$$

By Steane's construction the vectors v'' and w'' are either both zero, or both are non-zero and they are different. For $v'' = w'' = 0$, we can assume without loss of generality that the vectors in (7a) and (7b) are both non-zero. The weight of these vectors equals the distance between two codewords of the Goethals code, so it is at least 8. For $v'' \neq 0 \neq w''$ the terms (7a) and (7b) equal the distance of two codewords of the Preparata code, so they are lower bounded by 6. We will show that for $v'' \neq w''$, the vector in (7c) is a non-zero codeword of the linear code isomorphic to the Reed-Muller code $RM(m-2, m)$, hence its weight is at least 4. For this, consider the vectors $a = (a_1; a_2) = c_1'' + c_2'' + v'' + w'' \neq 0$ and $b = (b_1; b_2) = t_i - t_i' + t_j - t_j'$. The coset representatives are of the form $t_i = (z^i; 1; z^i\theta_1(z); 0)$, so the second half b_2 of b is a codeword of the extended cyclic code generated by $\theta_1(z)$, while a_2 is a codeword of the extended cyclic code generated by $\mu_1(z)$. The intersection of the two codes is trivial, so $a_2 = b_2$ only if $a_2 = b_2 = 0$. Then $\mathrm{wgt}(b) \leq 4$ while $\mathrm{wgt}(a) \geq 6$ since $0 \neq a \in C_{\mathcal{P}}$. Hence $a \neq b$. ∎

To our best knowledge, the best additive quantum code with the same length and minimum distance has dimension $2^m - 5m - 2$. Codes with these parameters can, e. g., be obtained by applying Steane's construction to extended primitive BCH codes $[2^m, 2^m - 2m - 1, 8]$ and $[2^m, 2^m - 3m - 1, 6]$ (see [16]). In the following table we give the parameters of the first codes in these families. Additionally, we give the parameters of the non-additive quantum codes derived from Goethals codes in [9].

Goethals	enlarged BCH	Goethals-Preparata
$((64, 2^{30}, 8))$	$[[64, 32, 8]]$	$((64, 2^{35}, 8))$
$((256, 2^{210}, 8))$	$[[256, 214, 8]]$	$((256, 2^{217}, 8))$
$((1024, 2^{966}, 8))$	$[[1024, 972, 8]]$	$((1024, 2^{975}, 8))$

V. Conclusions

We have constructed some new non-additive quantum codes from nested non-linear binary codes which can be decomposed into cosets of linear codes which contain their dual. It is interesting to find more good non-linear binary or quaternary codes with this property. Recently, Ling and Solé have constructed some non-additive quantum codes from $\mathbb{Z}_4$-linear codes using a CSS-like construction [12]. So far it is not clear whether the non-additive codes presented here can also be put into the framework of $\mathbb{Z}_4$-linear codes.

Finally, we would like to note that despite the fact that the quantum codes presented in this paper are based on non-additive classical codes, it is open whether the quantum codes are equivalent to stabilizer codes corresponding to additive classical 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, as well as Tero Laihonen, Kalle Ranto, and Sanna Ranto for discussions on variations of Goethals codes. This work was partially supported by the FWF (project P17838).

References

[1] R. D. Baker, J. H. van Lint, and R. M. Wilson, "On the Preparata and Goethals Codes," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 342–345, May 1983.

[2] 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.

[3] ——, "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.

[4] A. R. Calderbank and P. W. Shor, "Good Quantum Error-Correcting Codes Exist," *Physical Review A*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996, preprint quant-ph/9512032.

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

[6] J.-M. Goethals, "Two Families of Nonlinear Binary Codes," *Electronic Letters*, vol. 10, no. 23, pp. 471–472, Nov. 1974.

[7] 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.

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

[9] M. Grassl and M. Rötteler, "Non-Additive Quantum Codes from Goethals and Preparata Codes," in *Proceedings 2008 IEEE Information Theory Workshop*, Porto, Portugal, May 2008, preprint arXiv:0801.2144 [quant-ph].

[10] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 301–319, Mar. 1994.

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

[12] S. Ling and P. Solé, "Nonadditive Quantum Codes from $\mathbb{Z}_4$-Codes," 2007, manuscript.

[13] F. P. Preparata, "A Class of Optimum Nonlinear Double-Error-Correcting Codes," *Information and Control*, vol. 13, no. 4, pp. 378–400, Oct. 1968.

[14] 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.

[15] A. M. Steane, "Simple Quantum Error Correcting Codes," *Physical Review A*, vol. 54, no. 6, pp. 4741–4751, Dec. 1996, preprint quant-ph/9605021.

[16] ——, "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.

[17] S. Yu, Q. Chen, C. H. Lai, and C. H. Oh, "Nonadditive Quantum Error-Correcting Code," Apr. 2007, preprint arXiv.0704.2122v1 [quant-ph].

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