ISIT'2013 1569719583

Asymmetric Quantum Codes Detecting a Single Amplitude Error

Martianus Frederic Ezerman and Markus Grassl
Centre for Quantum Technologies, National University of Singapore
3 Science Drive 2, Singapore, 117543
Email: frederic.ezerman@gmail.com, Markus.Grassl@nus.edu.sg

***Abstract*—We consider asymmetric quantum error-correcting codes that detect a single amplitude error. Both optimal additive and non-additive codes are presented.**

***Index Terms*—Asymmetric quantum codes, self-complementary codes, Grey-Rankin bound**

I. Introduction

Quantum error-correction is a vital component of devices for information processing based on quantum mechanics. There is by now a well-established connection between the class of so-called stabilizer quantum error-correcting codes (stabilizer QECC) and classical codes which are self-orthogonal with respect to a symplectic inner product, see, e. g., [7]. An important subclass of QECC which are related to pairs of classical codes and the Euclidean inner product are the so-called CSS codes, named after the initial work by Calderbank and Shor [8] as well as Steane [20]. While quite often only the quantum analogues of the Hamming distance and the uniform symmetric channel are considered in the design of quantum codes, already Steane had realized that the CSS construction allows to adjust the error-correction capabilities to more realistic physical channels where an asymmetry between phase and amplitude errors is likely. This situation of asymmetric QECC (AQECC) has been further studied about 10 years later [13], followed by code constructions based on classical codes, see, e. g., [18], [21], [9]. Schemes for fault-tolerant quantum computation based on AQECC have been investigated as well, see, e. g., [1].

In this work, we investigate quantum codes that can detect a single amplitude error, and which are at the same time able to correct a larger number of phase errors. Our construction is based on self-complementary binary codes and their non-binary generalization. We present a new class of classical linear codes that has the largest possible dimension, extending the results of [3]. Furthermore, we give optimal families of AQECC derived from $\mathbb{Z}_4$-linear codes, and we list the parameters of good AQECC with small length based on linear or non-linear codes.

II. Background and Notation

A quantum error-error correcting code $\mathcal{C}$ is a K-dimensional subspace of the n-fold tensor product of complex vector spaces $\mathbb{C}^q$, i. e., $\mathcal{C} \leq (\mathbb{C}^q)^{\otimes n}$. We will denote such a code by $\mathcal{C} = (\!(n, K, d)\!)_q$, where d denotes the minimum distance of the code. If the dimension q of the subsystems is a prime power, we can chose a basis $\{|x\rangle : x \in \mathbb{F}_q\}$ of $\mathbb{C}^q$ labeled by elements of the finite field $\mathbb{F}_q$. For $\alpha, \beta \in \mathbb{F}_q$, we define the operators

$$X^\alpha = \sum_{x\in\mathbb{F}_q} |x+\alpha\rangle\langle x| \quad \text{and} \quad Z^\beta = \sum_{y\in\mathbb{F}_q} \omega_p^{\mathrm{tr}(\beta y)} |y\rangle\langle y|, \quad (1)$$

where $\omega_p = \exp(2\pi i/p)$ is a complex primitive pth root of unity and $q = p^r$, p prime. The operators X^α and Z^β correspond to amplitude and phase errors, respectively. General errors can be modeled as products and linear combinations of tensor products of the operators in (1). A QECC is said to have x-distance d_x if any error that is a tensor product of n operators X^{α_i}, where less than d_x of the operators X^{α_i} are different from identity, can be detected or has no effect on the code. The z-distance d_z is defined analogously. We use the notation $\mathcal{C} = (\!(n, K, \{d_z, d_x\})\!)_q$ to denote such an asymmetric QECC. If the code $\mathcal{C}$ is a stabilizer code, we use the notation $\mathcal{C} = [\![n, k, \{d_z, d_x\}]\!]_q$, where $k = \log_q K$. Usually we assume that $d_z \geq d_x$ as applying a Fourier transformation with respect to the additive group $\mathbb{F}_q^n$ interchanges the role of X^α and Z^β.

Our code construction is based on the following result:

Proposition 1: Let $C = (n, Kq, d)_q \subset \mathbb{F}_q^n$ be a classical code of size Kq and minimum distance d that can be decomposed into cosets of the repetition code $C_0 = (n, q, n)_q$. Then there exists an AQECC $\mathcal{C} = (\!(n, K, \{d_z = d, d_x = 2\})\!)_q$.

Proof: Starting with the decomposition of C into cosets given by

$$C = \bigcup_{\boldsymbol{t}\in T} (C_0 + \boldsymbol{t}), \quad (2)$$

we define the quantum states

$$|\psi_{\boldsymbol{t}}\rangle = \frac{1}{\sqrt{q}} \sum_{\boldsymbol{x}\in C_0} |\boldsymbol{x} + \boldsymbol{t}\rangle. \quad (3)$$

As the cosets $C_0 + \boldsymbol{t}$ are invariant with respect to translation by a vector $\alpha\mathbf{1}$, where $\mathbf{1} \in \mathbb{F}_q^n$ denotes the all-one vector and $\alpha \in \mathbb{F}_q$, every state $|\psi_{\boldsymbol{t}}\rangle$ is an eigenvector of the operators of the form $(X^\alpha)^{\otimes n}$. This implies that a single Z-error can be detected. Furthermore, an X-error $X^{e_1} \otimes \cdots \otimes X^{e_n}$ changes $|\psi_{\boldsymbol{t}}\rangle$ into $|\psi_{\boldsymbol{t}+\boldsymbol{e}}\rangle$. If the weight of $\boldsymbol{e}$ is strictly smaller than the minimum distance d of the classical code C, the erroneous state is orthogonal to the states in (3), and the error can be detected. In summary, the space $\mathcal{C}'$ spanned by the states (3) is an AQECC with parameters $\mathcal{C}' = (\!(n, K, \{d_z = 2, d_x = d\})\!)_q$. Applying a Fourier transformation, interchanging X and Z, to the code $\mathcal{C}'$, we obtain the code $\mathcal{C}$ with the desired parameters. ∎

Note that the states in (3) are similar to the basis states of CSS codes, where a classical code C_1 is decomposed into cosets of a subcode $C_2 \leq C_1$. Therefore, we call the codes of Proposition 1 CSS-like.

In the binary case, a code with a decomposition (2) contains the all-one vector $\mathbf{1}$ and is called self-complementary. In the non-binary situation, we call a code fulfilling (2) *n-shift invariant*, as it is invariant with respect to addition of multiples of $\mathbf{1}$. Clearly, the vector $\mathbf{1}$ can be replaced by any fixed vector of weight n. For linear codes, this yields in particular the following (see also [9, Theorem 6]):

Corollary 2: Assume that $C = [n, k+1, d]_q$ is an $\mathbb{F}_q$-linear code that contains a word of maximal weight n. Then there exists an AQECC $\mathcal{C} = [\![n, k, \{d_z = d, d_x = 2\}]\!]_q$.

For a self-complementary binary code, the following upper bound on its size has been derived [11]

Proposition 3 (Grey-Rankin bound): Let $C = (n, M, d)_2$ be a self-complementary binary code. Then for $n - \sqrt{n} < 2d \leq n$,

$$|C| = M \leq \frac{8d(n-d)}{n-(n-2d)^2}. \tag{4}$$

The following generalization to the non-binary case from [2] applies to our situation as well:

Proposition 4 (q-ary Grey-Rankin bound): Assume the code $C = (n, M, d)_q$ can be partitioned into M/q codes C_i with parameters $C_i = (n, q, n)_q$. Then

$$|C| = M \leq \frac{q^2(n-d)(qd-(q-2)n)}{n-((q-1)n-qd)^2}, \tag{5}$$

provided that $\frac{(q-1)n-\sqrt{n}}{q} < d \leq \frac{q-1}{q}n$.

In the following, we will refer to this bound as the q-ary Grey-Rankin bound, abbreviated as q-ary GR-bound or just GR-bound. For $q = 2$, the bound reduces to the binary GR-bound. Note that in both cases the bound can only be applied to codes with relatively large minimum distance.

So, for small minimum distance, other bounds have to be derived. For the linear programming (LP) bound, the condition that a binary code is self-complementary is rather strong because it enforces the distance enumerator to be symmetric. In general, however, we can only add the minor restriction that there are codewords at distance n.

Several families of codes achieving the GR-bound are known, in particular for the binary case (see Section IV below and, e. g., [15]). In [2], q-ary codes with the largest possible distance $n(q-1)/q$ meeting the GR-bound are given.

Next, we present families of q-ary linear n-shift invariant codes that are optimal with respect to the GR-bound, i. e., their dimension k is the largest such that $M = q^k$ obeys (5). The construction includes the codes from [3] as a special case.

III. Families of Optimal n-shift Invariant Codes

In this section, we derive new families of linear codes that contain a vector of maximal weight. Those codes reach the q-ary Grey-Rankin bound within a factor strictly less then q, and hence they are dimension-optimal.

A. Construction

Let $C_{\text{outer}} = [\nu, 2, \nu-1]_{q^t}$ be an MDS code over $\mathbb{F}_{q^t}$ of length ν, $2 \leq \nu \leq q^t$, where $q^t > 2$. The concatenation of the code C_{outer} with the code $C_{\text{inner}} = [q^t-1, t, (q-1)q^{t-1}]_q$ generated by a matrix formed by all the non-zero vectors in $\mathbb{F}_q^t$ as columns yields a code with parameters

$$C_{\text{concat}} = [n, k, d]_q = [\nu(q^t-1), 2t, (\nu-1)(q-1)q^{t-1}]_q. \tag{6}$$

The code C_{concat} has non-zero weights $w_1 = (\nu-1)(q-1)q^{t-1}$ and $w_2 = \nu(q-1)q^{t-1}$. Note that any non-zero vector in the code C_{inner} contains every non-zero element of $\mathbb{F}_q$ exactly q^{t-1} times. Hence every non-zero vector of the concatenated code C_{concat} contains every non-zero element of $\mathbb{F}_q$ exactly the same number of times. The frequency is either $(\nu-1)q^{t-1}$ or νq^{t-1}. Let $\mathbf{1} = (1, \ldots, 1) \in \mathbb{F}_q^n$ denote the all-one vector. Then for a non-zero codeword $\boldsymbol{c} \in C_{\text{concat}}$ and $\beta \in \mathbb{F}_q \setminus \{0\}$, we have

$$\operatorname{wgt}(\boldsymbol{c} - \beta\mathbf{1}) = \begin{cases} w_3 = n-(\nu-1)q^{t-1}, & \text{if } \operatorname{wgt}\boldsymbol{c} = w_1; \\ w_4 = n-\nu q^{t-1}, & \text{if } \operatorname{wgt}\boldsymbol{c} = w_2. \end{cases}$$

Hence the non-zero-weights of the augmented code $C = [n, k, d]_q$ with $n = \nu(q^t-1)$ and $k = 2t+1$ generated by C_{concat} and $\mathbf{1}$ are

$$\begin{aligned} w_1 &= (\nu-1)(q-1)q^{t-1} &&= (\nu-1)(q^t-q^{t-1}) \\ w_2 &= \nu(q-1)q^{t-1} &&= \nu(q^t-q^{t-1}) \\ w_3 &= n-(\nu-1)q^{t-1} &&= \nu(q^t-q^{t-1}-1)+q^{t-1} \\ w_4 &= n-\nu q^{t-1} &&= \nu(q^t-q^{t-1}-1) \\ w_5 &= n &&= \nu(q^t-1). \end{aligned}$$

For $\nu \leq (q-1)q^{t-1}$, we have $w_1 \leq w_4$, and hence the code has minimum distance $d = w_1$; for $\nu \geq (q-1)q^{t-1}$, the minimum distance is $d = w_4$.

We can also extend the code by adding a generalized parity check symbol such that the sum of all entries in the codeword vanishes. First recall that in the codewords of C_{concat} every non-zero element of $\mathbb{F}_q$ occurs q^{t-1} times, implying that the sum of all entries vanishes. Hence, for the codewords of weight w_1 and w_2 in C, the additional coordinate is zero. The other codewords in C are linear combinations involving the all-one vector of weight $n = \nu(q^t-1)$. So if $n \not\equiv 0 \bmod p$, where p is the characteristic of $\mathbb{F}_q$, a non-zero element will be added to the codewords of weight w_3, w_4, and w_5. Hence, the extended code $C' = [n+1, q^{2t+1}, d']_q$ will have non-zero weights

$$\begin{aligned} w_1' &= (\nu-1)(q-1)q^{t-1} &&= (\nu-1)(q^t-q^{t-1}) \\ w_2' &= \nu(q-1)q^{t-1} &&= \nu(q^t-q^{t-1}) \\ w_3' &= n-(\nu-1)q^{t-1}+1 &&= \nu(q^t-q^{t-1}-1)+q^{t-1}+1 \\ w_4' &= n-\nu q^{t-1}+1 &&= \nu(q^t-q^{t-1}-1)+1 \\ w_5' &= n+1 &&= \nu(q^t-1)+1, \end{aligned}$$

provided $\nu \not\equiv 0 \bmod p$. For $\nu \leq q^t - q^{t-1} + 1$, we have $w_4' \leq w_1'$. In summary, we get the following codes.

Theorem 5: For $2 \leq \nu \leq q^t$, there exist linear codes over $\mathbb{F}_q$ with $q = p^r$ containing the all-one vector with the following parameters:

1) for $q^t - q^{t-1} \leq \nu \leq q^t$:
   $C_{\mathrm{I}} = [\nu(q^t-1), 2t+1, \nu(q^t-q^{t-1}-1)]_q$
2) for $q^t - q^{t-1} + 1 \leq \nu \leq q^t$, $\gcd(\nu, q) = 1$:
   $C_{\mathrm{II}} = [\nu(q^t-1)+1, 2t+1, \nu(q^t-q^{t-1}-1)+1]_q$
3) for $\nu \leq q^t - q^{t-1}$:
   $C_{\mathrm{III}} = [\nu(q^t-1), 2t+1, (\nu-1)(q^t-q^{t-1})]_q$

B. Optimal codes

In order to apply the bound (5), we need $(q-1)n - \sqrt{n} < qd \leq (q-1)n$, or equivalently, $n > ((q-1)n - qd)^2$ and $qd \leq (q-1)n$. The second condition is trivially fulfilled by the parameters of an existing code (see Lemma 7 below). So we have to check whether

$$n - ((q-1)n - qd)^2 > 0. \tag{7}$$

For the code C_{I}, this condition reduces to $0 < \nu < q^t - 1$ when substituting the values for n and d as functions of ν. For the code C_{II}, the parameter ν is constrained by $0 < \nu < q^t + 1$. We get a more complicated quadratic condition for the range of ν for the code C_{III}, i. e., ν has to fall into an interval given by the roots of a quadratic equation depending on q and t.

In order to test whether an n-shift invariant linear code $C = [n, k, d]_q$ has the maximal possible dimension among such codes, we check whether the size of the code $M = q^k$ is the largest power of q for which the GR-bound (5) holds. This is equivalent to the condition that the right hand side of (5) is strictly smaller than q^{k+1} or

$$q^{k+1}(n-((q-1)n-qd)^2) - q^2(n-d)(qd-(q-2)n) > 0. \tag{8}$$

For the code C_{I}, this condition reduces to

$$\nu < \frac{q^{2t+1} - q^{t+1}}{q^{t+1} + q^t - 2} = q^t - q^{t-1} + \frac{q^{t+1} - q^3 + 2q^2 - 2q}{q^{t+1} + q^t - 2} q^{t-1}. \tag{9}$$

For the code C_{II}, we get

$$\nu < \frac{q^{2t+1} + q^{t+1} - 2}{q^{t+1} + q^t - 2} = q^t - q^{t-1} + 1 + \frac{q^t + q - 2}{q^{t+1} + q^t - 2} q^{t-1}. \tag{10}$$

Again, there is a more complicated quadratic condition on the range of ν for the code C_{III}, i.e., ν has to lie in the interval between the two roots of a quadratic polynomial in ν.

In summary, the code C_{I} has the largest possible dimension of a linear code containing a vector of weight n when the parameter ν is in the range

$$q^t - q^{t-1} \leq \nu < q^t - q^{t-1} + \frac{q^{t+1} - q^3 + 2q^2 - 2q}{q^{t+1} + q^t - 2} q^{t-2}, \tag{11}$$

and $t \geq 2$. The code C_{II} is optimal when $t \geq 2$, and ν with $\gcd(\nu, q) = 1$ is in the range

$$q^t - q^{t-1} + 1 \leq \nu < q^t - q^{t-1} + 1 + \frac{q^{t+1} + q^2 - 2q}{q^{t+1} + q^t - 2} q^{t-2}. \tag{12}$$

Note that for large q^t, the length of the interval is approximately q^{t-2}.

The code C_{III} is optimal for ν in the range $\nu_0 < \nu \leq q^t - q^{t-1}$, where ν_0 is the smaller of the roots of the left hand side of condition (8) when substituting $n = \nu(q^t - 1)$ and $d = w_1$.

Remark 6: For $\nu = (q-1)q^{t-1}$, the codes C_{I} have the same parameters as those in [3].

IV. Other Known Families of Optimal n-shift Invariant Codes

First we consider the situation of a stabilizer AQECC encoding a single qudit, i. e, $k = 1$. For this, we need the following:

Lemma 7: Let $C = [n, k, d]_q$ with $k > 1$ be an n-shift invariant linear code. Then

$$d \leq \frac{q-1}{q} n. \tag{13}$$

Proof: Without loss of generality, assume that C contains the all-one vector $\mathbf{1}$. For any codeword $\boldsymbol{w} \in C$ and any $\beta \in \mathbb{F}_q$, the weight of the linear combination $\beta\mathbf{1} - \boldsymbol{w}$ is given by

$$\mathrm{wgt}(\beta\mathbf{1} - \boldsymbol{w}) = |\{i \colon i \in \{1, \ldots, n\} \mid \boldsymbol{w}_i \neq \beta\}|. \tag{14}$$

The minimum of (14) over $\beta \in \mathbb{F}_q$ is largest when all elements occur with the same frequency, yielding the bound (13). ∎

Theorem 8: There exist stabilizer AQECC with parameters $[\![n, 1, \{\lfloor \frac{q-1}{q} n \rfloor, 2\}]\!]_q$. Those codes are optimal among linear CSS-type codes.

Note that $d = n(q-1)/q$ is also the maximal distance for which the GR-bound can be applied. Fixing n, q, and d, there exist non-additive AQECC with larger dimension from classical codes that achieve the GR-bound:

Theorem 9: For $n = \nu q$, $\nu \in \mathbb{N}$, there exist non-additive AQECC with parameters $(\!(\nu q, \nu q, \{\nu(q-1), 2\})\!)_q$.

Proof: From [2], we know that for any q, there exist n-shift invariant classical codes $C = (n, nq, n(q-1)/q)_q$ achieving the GR-bound when the length n is a multiple of q. The result follows using these codes in the construction from Proposition 1. ∎

Puncturing yields AQECC $(\!(\nu q - 1, \nu q, \{\nu(q-1) - 1, 2\})\!)_q$ which are optimal CSS-like codes by the GR-bound as well.

We note that while these CSS-like codes are based on optimal n-shift invariant classical codes, it is open whether the codes are optimal among all AQECC.

In the literature, mainly binary self-complementary codes meeting the GR-bound can be found:

- From [15, Theorem B], a self-complementary linear binary code meeting the Grey-Rankin bound has parameters
  - $C = [2^s - 1, s+1, 2^{s-1} - 1]_2$,
  - $C = [2^{2t-1} - 2^{t-1}, 2t+1, 2^{2t-2} - 2^{t-1}]_2$, or
  - $C = [2^{2t-1} + 2^{t-1}, 2t+1, 2^{2t-2}]_2$,

  where $s \geq 2$, and $t \geq 3$.
  The first code is obtained by shortening a first-order Reed-Muller code $\mathrm{RM}(1, s)$. The codes of even length correspond to the codes C_{I} and C_{II} from Theorem 5 with $\nu = 2^t - 2^{t-1}$ and $\nu = 2^t - 2^{t-1} + 1$, respectively.
- Provided that there exists a Hadamard matrix of order $2u$ and $u-2$ or $u-1$ mutually orthogonal Latin squares, self-complementary binary codes with parameters $(2u^2 -$

$u, 8u^2, u^2-u)_2$ and $(2u^2+u, 8u^2, u^2)_2$, respectively, can be constructed [4].

V. Non-additive AQECC

As demonstrated by Theorems 8 and 9, CSS-like AQECC based on non-linear codes can have a higher dimension than those based on linear codes. Many of the known families of non-linear binary codes give rise to AQECC.

Example 10: The following families of optimal binary codes are self-complementary and hence give rise to families of good asymmetric quantum codes detecting a single bit-flip error.

- The Kerdock code $K = (2^{m+1}, 4^{m+1}, 2^m - 2^{(m-1)/2})_2$ for odd $m \geq 3$ yields an AQECC with parameters $(\!(2^{m+1}, 2^{2m+1}, \{2^m - 2^{(m-1)/2}, 2\})\!)_2$.
- The Preparata code $P = (2^{m+1}, 2^{2^{m+1}-2m-2}, 6)_2$ for odd $m \geq 3$ yields a qubit AQECC with parameters $(\!(2^{m+1}, 2^{2^{m+1}-2m-3}, \{6, 2\})\!)_2$. They have the largest possible dimension among CSS-like codes as the punctured Preparata codes meet the Johnson bound [17, Section 4].
- The Goethals code $G = (2^{m+1}, 2^{2^{m+1}-3m-2}, 8)_2$ for odd $m \geq 3$ yields a qubit AQECC with parameters $(\!(2^{m+1}, 2^{2^{m+1}-3m-3}, \{8, 2\})\!)_2$.
- The Delsarte-Goethals codes: $DG(m+1, \delta) = (2^{m+1}, 2^{(r+2)m+2}, 2^m - 2^{m-\delta})_2$, m odd, $\delta = (m+1)/2 - r$, yields an AQECC with parameters $(\!(2^{m+1}, 2^{(r+2)m+1}, \{2^m - 2^{m-\delta}, 2\})\!)_2$

These codes have been shown to be $\mathbb{Z}_4$-linear [12], motivating the following:

Theorem 11: Let $C = (2n, k, d)_2$ be the image of a $\mathbb{Z}_4$-linear code $C' = (n, k, d_{\text{Lee}})_{\mathbb{Z}_4}$ under the Gray map. Furthermore, assume that C contains the all-one vector. Then C is self-complementary.

Proof: The code C contains the all-one vector $\mathbf{1} \in \mathbb{F}_2^{2n}$ if and only if the code C' contains the vector $\mathbf{2} = (2, 2, \ldots, 2) \in \mathbb{Z}_4^n$. Let ϕ denote the Gray map. Then for any codeword $\boldsymbol{c} \in C$, $\phi^{-1}(\boldsymbol{c}) + \mathbf{2} \in C'$ by $\mathbb{Z}_4$-linearity. Moreover, $\phi(\phi^{-1}(\boldsymbol{c}) + \mathbf{2}) = \boldsymbol{c} + \mathbf{1} \in C$, although the Gray map is not linear. ∎

Corollary 12: Let $C' = (n, 4^{k_1} 2^{k_2}, d_{\text{Lee}})_{\mathbb{Z}_4}$ be a $\mathbb{Z}_4$-linear code of length n and minimum Lee-weight d_{Lee} that contains the vector $\mathbf{2} = (2, 2, \ldots, 2)$. Then there exists a, in general non-additive, AQECC with parameters $(\!(2n, 2^{2k_1+k_2-1}, \{d_{\text{Lee}}, 2\})\!)_2$.

Example 13: The $\mathbb{Z}_4$-linear code $(32, 4^{16}2^5, 12)$ of [5] contains the vector $\mathbf{2}$. Hence it yields an AQECC with parameters $(\!(64, 2^{36}, \{12, 2\})\!)_2$. Similarly, the extended $\mathbb{Z}_4$-linear QR code $(32, 2^{32}, 14)$ of [6] contains the vector $\mathbf{2}$, yielding an AQECC with parameters $(\!(64, 2^{31}, \{14, 2\})\!)_2$. More recent results on $\mathbb{Z}_4$-linear extended QR codes containing the vector $\mathbf{2}$ can be found in [14]. The Gray map images of most of these $\mathbb{Z}_4$-linear codes have more codewords than the best-known comparable binary linear codes.

In the special case $d_x = d_z = 2$, we obtain optimal AQECC $[\![n, n-d, \{2, 2\}]\!]_q$ by applying the CSS-construction to a classical MDS code $C_1 = [n, n-1, 2]_q$ and a subcode $C_2 = [n, 1, n]_q$ (see [9]). These codes exist for all parameters with the exception when $q = 2$ and n is odd. In this case, the MDS code C_1 contains only words of even weight, and hence the code is not self-complementary. In [19], non-additive qubit quantum codes with parameters $(\!(n, 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2}, 2)\!)_2$ for n odd have been constructed from self-complementary binary codes. It turns out that these codes are CSS-like asymmetric AQECC with parameters $d_x = d_z = 2$. With the exception of small lengths, these codes are the best known qubit QECC of odd length detecting a single error; however, they have not been shown to be optimal.

TABLE I
Dimension K of CSS-like qubit AQECC $(\!(n, K, \{d_z, 2\})\!)_2$ based on classical codes. The codes up to length 10 are based on optimal self-complementary binary codes. For linear codes, we use the notation 2^k.

n/d_z	2	3	4	5	6	7	8
5	5						
6	2^4	2^1					
7	22	2^3					
8	2^6	2^3	2^3				
9	93	2^4	8				
10	2^8	2^5	2^4	2^1			
11	386–460	72	17–26	12			
12	2^{10}	2^7	72	13	12		
13	1586–1877	192–213	80–120	2^4–19	13		
14	2^{12}	352–384	192–213	2^5–38	2^4–19	2^1	
15	6476–7606	2^{10}	352–384	128	17–32	2^4	
16	2^{14}	1152–1638	2^{10}	128–170	128	2^4–18	2^4

VI. Codes of Small Length

Finally, we have used various techniques to find n-shift invariant classical codes for small length and $q = 2, 3, 4$. First, we checked whether the best known linear codes of [10] are n-shift invariant. We observed that the fraction of such codes increases with the alphabet size. For small parameters, we performed an exhaustive search based on finding a maximum clique in the distance graph of the cosets of the repetition code using the program `cliquer` [16]. Furthermore, we have used various randomized search techniques to find good n-shift invariant linear codes, or additive codes in the case $q = 4$. The results are summarized in Tables I–III. Upper bounds are obtained using linear programming, via the GR-bound, or from available tables of optimal unrestricted binary codes.

Acknowledgment

The Centre for Quantum Technologies is a Research Centre of Excellence funded by the Ministry of Education and the National Research Foundation of Singapore.

This work was supported in part by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center Contract number DllPC20l66. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of IARPA, DoI/NBC or the U.S. Government.

TABLE II

DIMENSION K OF CSS-LIKE QUTRIT AQECC $(\!(n, K, \{d_z, 2\})\!)_3$ BASED ON CLASSICAL CODES. FOR LINEAR CODES, WE USE THE NOTATION 3^k. ONE REMARKABLE EXAMPLE IS THE EXTENDED TERNARY GOLAY CODE $[12, 6, 6]_3$ THAT CONTAINS A WORD OF WEIGHT 12.

n/d_z	3	4	5	6	7	8	9	10
5	6							
6	11	6						
7	29–48	3^2						
8	84–113	29–41	3^2					
9	3^5–312	3^4–113	3^3–28	3^2				
10	3^6–937	3^5–312	30–76	12–16				
11	3^7–2343	3^5–937	3^5	19–69	12			
12	3^8	3^6–2343	3^5–520	3^5	18–45	12		
13	3^9	3^7–6561	3^6–1366	3^5–520	3^3–117	15–18		
14	3^9–51175	3^8–19683	3^7–3578	3^6–1280	3^4–278	3^3–73	15	
15	3^{10}–144938	3^9–51175	3^7–9841	3^6–3578	3^4–756	3^4–237	3^3–36	15
16	3^{11}–434815	3^{10}–144938	3^8–25739	3^7–9841	3^5–2209	3^4–691	3^3–132	15–21

TABLE III

DIMENSION K OF CSS-LIKE AQECC $(\!(n, K, \{d_z, 2\})\!)_4$ BASED ON CLASSICAL CODES. FOR LINEAR AND ADDITIVE CODES, THE PARAMETER K IS GIVEN AS $K = 4^\ell$ AND $K = 2^m$, RESPECTIVELY.

n/d_z	3	4	5	6	7	8	9	10	11	12
5	4^2									
6	2^5–44	4^2								
7	2^7–153	2^5–44	2^3							
8	2^9–585	2^7–153	4^2–40	2^3						
9	4^5–2340	2^9–585	2^7–153	4^2–32						
10	4^6–7606	4^5–2340	4^4–536	4^3–128	12–16					
11	4^7–27306	4^6–7606	4^5–1560	4^4–512	4^2–76	12				
12	4^8–104857	4^7–27306	4^5–5213	4^5–1560	4^3–320	4^2–59	12			
13	4^9–419430	4^8–104857	4^6–19693	4^5–5213	4^4–1243	2^7–242	4^2–40			
14	4^{10}–1448941	4^9–419430	4^7–72257	4^6–19693	4^5–4710	4^4–971	4^3–152	4^2–19		
15	4^{11}–5338205	4^{10}–1448941	4^8–241979	4^7–72257	4^6–17988	4^4–3884	4^3–624	4^3–98	4^2	
16	4^{12}–20648881	4^{11}–5338205	4^9–838022	4^8–241979	4^7–51193	4^6–13449	4^4–2336	4^3–401	4^3–76	4^2

REFERENCES

[1] P. Aliferis and J. Preskill, "Fault-tolerant quantum computation against biased noise," *Physical Review A*, vol. 78, no. 5, p. 052331, Nov. 2008.

[2] L. Bassalygo, S. Dodunekov, T. Helleseth, and V. Zinoviev, "On a new q-ary combinatorial analog of the binary Grey-Rankin bound and codes meeting this bound," in *Proceedings 2006 IEEE Information Theory Workshop (ITW 2006)*, Punta del Este, Uruguay, 13–17 March 2006, pp. 278–282.

[3] C. Bracken, Y. M. Chee, and P. Purkayastha, "Optimal family of q-ary codes obtained from a substructure of generalised Hadamard matrices," in *Proceedings 2012 IEEE International Symposium on Information Theory (ISIT 2012)*, Cambridge, MA, July 2012, pp. 116–119.

[4] C. Bracken, G. McGuire, and H. Ward, "New quasi-symmetric designs constructed using mutually orthogonal Latin squares and Hadamard matrices," *Designs, Codes and Cryptography*, vol. 41, no. 2, pp. 195–198, Nov. 2006.

[5] A. R. Calderbank and G. McGuire, "Construction of a $(64, 2^{37}, 12)$ code via Galois rings," *Designs, Codes and Cryptography*, vol. 10, no. 2, pp. 157–165, Feb. 1997.

[6] A. R. Calderbank, G. McGuire, P. V. Kumar, and T. Helleseth, "Cyclic codes over $\mathbb{Z}_4$, locator polynomials, and Newton's identities," *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 217–226, Jan. 1996.

[7] 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*, vol. 44, no. 4, pp. 1369–1387, July 1998.

[8] 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.

[9] M. F. Ezerman, S. Jitman, H. M. Kiah, and S. Ling, "Pure asymmetric quantum MDS codes from CSS construction: A complete characterization," May 2013, preprint arXiv:1006.1694v4 [cs.IT], accepted for publication by International Journal of Quantum Information.

[10] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," online available at http://www.codetables.de, 2007, accessed on 2013-01-11.

[11] L. D. Grey, "Some bounds for error-correcting codes," *IRE Transactions on Information Theory*, vol. 8, no. 3, pp. 200–202, Apr. 1962.

[12] 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.

[13] L. Ioffe and M. Mézard, "Asymmetric quantum error-correcting codes," *Physical Review A*, vol. 75, no. 3, p. 032345, Mar. 2007.

[14] M. Kiermaier and A. Wassermann, "Minimum weights and weight enumerators of $\mathbb{Z}_4$-linear quadratic residue codes," , *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4870–4883, July 2012.

[15] G. McGuire, "Quasi-symmetric designs and codes meeting the Grey-Rankin bound," *Journal of Combinatorial Theory*, vol. 78, no. 2, pp. 280–291, 1997.

[16] S. Niskanen and P. R. J. Östergård, "Cliquer User's Guide, Version 1.0," Communications Laboratory, Helsinki University of Technology, Espoo, Finland, Tech. Rep. Tech. Rep. T48, 2003, available at http://users.tkk.fi/~pat/cliquer.html.

[17] F. P. Preparata, "A class of optimum nonlinear double-error-correcting codes," *Information and Control*, vol. 13, no. 4, pp. 378–400, Oct. 1968.

[18] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, "Asymmetric quantum codes: constructions, bounds, and performance," *Proceedings of the Royal Society London, Series A*, vol. 465, no. 2105, pp. 1645–1672, May 2009.

[19] J. A. Smolin, G. Smith, and S. Wehner, "Simple family of nonadditive quantum codes," *Physical Review Letters*, vol. 99, no. 13, p. 130505, Sept. 2007.

[20] A. M. Steane, "Simple quantum error correcting codes," *Physical Review A*, vol. 54, no. 6, pp. 4741–4751, Dec. 1996.

[21] L. Wang, K. Feng, S. Ling, and C. Xing, "Asymmetric quantum codes: Characterization and constructions," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2938–2945, June 2010.