Asymmetric Quantum Codes
Detecting a Single Amplitude Error

Fred Ezerman and Markus Grassl

Centre for Quantum Technologies,
National University of Singapore

IEEE International Symposium on Information Theory,
Istanbul 2013
Outline

1. Introduction

2. Background and Notation

3. $n$-Shift Invariant Codes Meeting GR Bound

4. Other Optimal $n$-Shift Invariant Codes

5. Non-Additive AQECC

6. Optimal Codes of Small Lengths
Motivations

- Quantum error-correction (QECC) is a vital component of devices for information processing based on quantum mechanics.
- An important subclass of QECC which are related to pairs of classical codes and the Euclidean inner product are the so-called CSS codes.
- CSS construction allows to adjust the error-correction capabilities to more realistic physical channels where an asymmetry between phase and amplitude errors is likely.
- Asymmetric QECC (AQECC) has been a subject of more intensive studies since mid 2000. Various code constructions based on classical codes are now known.
- Schemes for fault-tolerant quantum computation based on AQECC have been investigated as well.
This Paper

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.

1. Construction based on self-complementary binary codes and their non-binary generalization.
2. Present a new class of classical linear codes that has the largest possible dimension. It includes previously known results as special cases.
3. Optimal families of AQECC derived from $\mathbb{Z}_4$-linear codes
4. Parameters of good AQECC with small lengths based on linear or non-linear codes.
Basic Model and Notations

1. A QECC code $\mathcal{C} = ((n, K, d))_q :=$ a $K$-dim subspace of the $n$-fold tensor product of complex vector spaces $\mathbb{C}^q$ with distance $d$.

2. A basis $\{|x\rangle : x \in \mathbb{F}_q\}$ of $\mathbb{C}^q$ labeled by elements of $\mathbb{F}_q$.

3. For $\alpha, \beta \in \mathbb{F}_q$, define the operators

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

(1)

where $\omega_p = \exp(2\pi i/p)$ and $q = p^r$, $p$ prime.

4. $\mathcal{C}$ has $x$-distance $d_x$ if any error that is a tensor product of $n$ operators $X^{\alpha_i}$, where less than $d_x$ of the operators $X^{\alpha_i}$ are different from identity, can be detected or has no effect on the code. The $z$-distance $d_z$ is defined analogously.

5. Notation: $\mathcal{C} = ((n, K, \{d_z, d_x\}))_q$. If $\mathcal{C}$ is a stabilizer code, use $\mathcal{C} = [[n, k, \{d_z, d_x\}]]_q$, where $k = \log_q K$.

6. Assume that $d_z \geq d_x$ as applying a Fourier transformation w.r.t the additive group $\mathbb{F}_q^n$ interchanges the role of $X^\alpha$ and $Z^\beta$. 
CSS-like AQECC with $d_x = 2$

**Proposition**

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.**

Decompose $C$ into cosets given by

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

Define the quantum states

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

Note the following:

1. The cosets $C_0 + t$ are invariant w.r.t translation by a vector $\alpha 1$. Every state $|\psi_t\rangle$ is an eigenvector of the operators of the form $(X^\alpha)^\otimes n$. A single $Z$-error can be detected.

2. An $X$-error $X^{e_1} \otimes \cdots \otimes X^{e_n}$ changes $|\psi_t\rangle$ into $|\psi_{t+e}\rangle$. If the weight of $e$ 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.

3. The space $C'$ spanned by the states (3) is an AQECC with parameters $C' = ((n, K, \{d_Z = 2, d_X = d\}))_q$.

4. Applying a Fourier transformation, interchanging $X$ and $Z$, to the code $C'$ completes the proof.
Some Remarks

- The codes in the Proposition above is CSS-like.
- A binary code fulfilling (2) is called self-complementary. More formally, $C$ is self-complementary if $v + 1 \in C$ for every $v \in C$.
- For $q > 2$, a code fulfilling (2) is $n$-shift invariant, as it is invariant with respect to addition of multiples of $1$. The vector $1$ can be replaced by any fixed vector of weight $n$. 
**Grey-Rankin Bound**

**Proposition (Grey-Rankin bound)**

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

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

Bassalygo et al. in ITW 2006 presented a generalization

**Proposition (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

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

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

Agenda

Construct 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).
Construction

1. Start with an MDS code $C_{\text{outer}} = [\nu, 2, \nu - 1]_{q^t}$ over $\mathbb{F}_{q^t}$ of length $\nu$, $2 \leq \nu \leq q^t$, where $q^t > 2$.

2. Concatenate $C_{\text{outer}}$ 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 to get

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

3. Form the augmented code $C = [n, k, d]_q$ with $n = \nu(q^t - 1)$ and $k = 2t + 1$ generated by $C_{\text{concat}}$ and $\mathbf{1}$.

4. Extend the code $C$ by adding a generalized parity check symbol such that the sum of all entries in the codeword vanishes to get the extended code $C' = [n + 1, q^{2t+1}, d']_q$.

5. Analyze the non-zero weights of the codes $C$ and $C'$. See the paper for details.
Summary

We get the following codes.

Theorem

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 $q^t - q^{t-1} \leq \nu \leq q^t$:
   \[ C_I = [\nu(q^t - 1), 2t + 1, \nu(q^t - q^{t-1} - 1)]_q \]

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

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

Remark

For $\nu = q^t - q^{t-1}$, $C_I$ have the same parameters as those in Bracken et al., ISIT 2012.
Checking for Optimality under GR Bound

1. $C_1$ is optimal when the parameter $\nu$ is in the range

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

and $t \geq 2$.

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

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

For large $q^t$, the length of the interval is approximately $q^{t-2}$.

3. The code $C_{III}$ is optimal for $\nu$ in the range $\nu_0 < \nu \leq q^t - q^{t-1}$, where $\nu_0$ is the smaller of the roots of

$$q^{k+1}(n - ((q - 1)n - qd)^2) - q^2(n - d)(qd - (q - 2)n)$$

when substituting $n = \nu(q^t - 1)$ and $d = w_1$. 
Theorem

There exist stabilizer AQECC with parameters $[[n, 1, \left\lfloor q^{-1} n \right\rfloor, 2]]_q$. Those codes are optimal among linear CSS-type codes.

This result is derived based on

Lemma

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

$$d \leq \frac{q - 1}{q} n.$$
AQECC with Larger Dimension

From Bassalygo et al. ITW 2006: 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 $q$. Hence,

**Theorem**

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

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.
Binary Codes reaching GR-Bound

- (McGuire, 97) A self-complementary linear binary code meeting the Grey-Rankin bound has parameters
  - $C = [2^s - 1, s + 1, 2^{s-1} - 1]_2$,
  - $C = [2^{2^{t-1}} - 2^{t-1}, 2t + 1, 2^{2t-2} - 2^{t-1}]_2$, or
  - $C = [2^{2^{t-1}} + 2^{t-1}, 2t + 1, 2^{2t-2}]_2$,

where $s \geq 2$, and $t \geq 3$.

The first code is obtained by shortening a first-order Reed-Muller code $\text{RM}(1, s)$. The codes of even length correspond to our $C_I$ and $C_{II}$ codes with $\nu = 2^t - 2^{t-1}$ and $\nu = 2^t - 2^{t-1} + 1$, respectively.

- (Bracken-McGuire-Ward, 06) Provided that there exists a Hadamard matrix of order $2u$ and $u - 2$ or $u - 1$ MOLS, 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.
Example

The following families of optimal binary codes are self-complementary.

- 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 $(2^{m+1}, 2^{2m+1}, \{2^m - 2^{(m-1)/2}, 2\})_2$.

- The Preparata code $P = (2^{m+1}, 2^{2m+1-2m-2}, 6)_2$ for odd $m \geq 3$ yields an AQECC $(2^{m+1}, 2^{2m+1-2m-3}, \{6, 2\})_2$. They have the largest possible dimension among CSS-like codes.

- The Goethals code $G = (2^{m+1}, 2^{2m+1-3m-2}, 8)_2$ for odd $m \geq 3$ yields an AQECC $(2^{m+1}, 2^{2m+1-3m-3}, \{8, 2\})_2$.

- 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
  
  $(2^{m+1}, 2^{(r+2)m+1}, \{2^m - 2^{m-\delta}, 2\})_2$.
More on AQECC from $\mathbb{Z}_4$ Codes

Corollary

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 $d_{\text{Lee}}$ that contains the vector $2 = (2, 2, \ldots, 2)$. Then there exists a, in general non-additive, AQECC with parameters $((2n, 2^{2k_1+k_2-1}, \{d_{\text{Lee}}, 2\})_2$.

Example

- The $\mathbb{Z}_4$-linear code $(32, 4^{16}2^5, 12)$ of Calderbank & McGuire, 97 contains the vector $2$. Hence it yields an AQECC $((64, 2^{36}, \{12, 2\})_2$.
- The extended $\mathbb{Z}_4$-linear QR code $(32, 2^{32}, 14)$ of Calderbank et al., 96 contains the vector $2$, yielding an AQECC $((64, 2^{31}, \{14, 2\})_2$.
- More recent results on $\mathbb{Z}_4$-linear extended QR codes containing the vector $2$ can be found in Kiermaier & Wassermann, 12.
Various Search Techniques

GR-Bound is limited in the range of $d$. For those values not covered by the bound, we have used various techniques to find $n$-shift invariant classical codes for small length and $q = 2, 3, 4$.

1. Check whether the best known linear codes in Grassl online tables are $n$-shift invariant.

2. For small parameters, perform exhaustive search based on finding a maximum clique in the distance graph of the cosets of the repetition code using the program *cliquer*.

3. Use various randomized search techniques to find good $n$-shift invariant linear codes, or additive codes in the case $q = 4$.

4. Upper bounds are obtained using linear programming, via the GR-bound, or from available tables of optimal unrestricted binary codes.

5. The results for $5 \leq n \leq 16$ are summarized in Tables I to III.
Supporting Agencies

- The Centre for Quantum Technologies is a Research Centre of Excellence funded by the Ministry of Education and the National Research Foundation of Singapore.
- Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center Contract number D1IPC20l66.