Some Recent Results on Asymmetric Quantum Codes

Fred Ezerman

from CQT @ NUS to CCRG @ NTU

The Hong Kong Polytechnic University. Jan 3, 2014
Outline

1 Introduction

2 Background and Notation

3 Good CSS AQCs from XL Codes

4 Extending CSS to CSS-like

5 CSS-like AQCs with $d_x = 2$

6 Still To Do
Motivations

- Quantum error-correction (QEC) 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.
- The asymmetric version of the CSS construction adjust the error-correction capabilities to more realistic physical channels where an asymmetry between phase and amplitude errors is likely.
- Asymmetric QECC (AQC) has been a subject of more intensive studies since mid 2000. Various code constructions based on classical codes are now known.
This Session

We look at the followings

1. To extend the standard CSS construction for AQCs to include nonlinear classical codes.
2. To provide some optimality measures, given the wealth of knowledge from classical codes.
3. To exhibit new optimal AQCs.
Basic Model and Notations

1. A quantum 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
   
   \[ X^\alpha = \sum_{x \in \mathbb{F}_q} |x + \alpha\rangle\langle x| \quad \text{and} \quad Z^\beta = \sum_{y \in \mathbb{F}_q} \omega_p^{tr(\beta y)} |y\rangle\langle y|, \]
   
   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 $\mathcal{C} = \lbrack n, k, \{d_z, d_x\}\rbrack_q$, 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 $Z^\beta$. 

---

Ezerman (CQT@NUS)  
Recent Results on AQCs  
January 3, 2014, 5th WQIS  
5 / 22
Standard CSS Construction for AQC

1. First hinted by Steane circa ’97.
2. Gained traction since Ioffe and Mézard in ’07 [PRA 75, 032345]
   
   [In] the physical devices conceived so far, the noise is typically asymmetric (a phase error is much more probable than a bit flip), and one can exploit this symmetry to develop more efficient QEC codes.

3. CSS for AQC is a natural extension from the symmetric case.

Theorem

Let $C_i$ be linear codes with parameters $[n, k_i, d_i]_q$ for $i \in \{1, 2\}$ with $C_1^\perp \subseteq C_2$. Let

\[ d_z := \text{wt}(C_2 \setminus C_1^\perp) \quad \text{and} \quad d_x := \text{wt}(C_1 \setminus C_2^\perp). \] (2)

Then there exists an AQC $[[n, k_1 + k_2 - n, \{d_z, d_x\}]]_q$. It is said to be pure whenever $d_z = d_2$ and $d_x = d_1$. 
Designing Good CSS AQCs

To design a standard CSS AQC with good parameters:

1. $C_1 \subset C_2$, Euclidean inner product.
2. For fixed values of $(q, n, d_2)$, the dimension $k_2$ must be as large as possible.
3. $k_1$ must also be as large as possible for specified values of $(q, n, d_1)$.
4. Implication: codimension of $C_1$ in $C_2$ should be as large as possible.

Theorem

If there exist a pure standard CSS $[[n, k, \{d_z, d_x\}]]_q$ code $Q$, then

$$k \leq \log_q(B_q(n, d_x)) + \log_q(B_q(n, d_z)) - n.$$  (3)
Previously Considered

Natural choice: families of nested algebraic codes. Main problem: determining exact or good bound for $d(C_i)$.

1. Cyclic codes and their subfamilies (BCH, QR) as well as variants (negacyclic, constacyclic, etc.).
2. Low-density parity-check (LDPC) codes.
3. Reed-Muller codes.
4. Reed-Solomon codes and their generalization (E., Jitman, Kiah, Ling) in [Int. J. Q. Inf. 11(3), Jun ’13].
5. Character codes, the affine-invariant and the product codes.
6. Classical propagation methods (e. g. concatenation) applied to construct AQCs of higher lengths.

Partial summary available in LaGuardia’s list [Q. Inf. Process. 12 (8), 2771 (2013)].
Good AQCs from nested XL Codes

The need to determine the (quantum) distances spurs deeper investigation on the structures of the chosen classical codes.

1. Based on the work of Xing and Ling in [IEEE Trans IT 46, 2184, 2000].

2. XL Codes have great parameters for their range of lengths.

3. Nestedness is self-evident from construction.

4. Must study the structure of the dual code of an appropriately chosen subcode of an XL code.
The Polynomial Space

1. List elements of $\mathbb{F}_{q^2}$ as

$$\{\alpha_1, \alpha_2, \ldots, \alpha_q, \beta_1, \beta_1^q, \beta_2, \beta_2^q, \ldots, \beta_r, \beta_r^q\},$$
where $r = (q^2 - q)/2$.  \hspace{1cm} (4)

2. Define $V_{1,0} := \langle 1 \rangle$. For $2 \leq m \leq q - 1$ and $0 \leq \ell \leq m - 1$, let

$$V_{m,\ell} := \langle \{e_{i,j}(x)\} | 0 \leq i \leq j \leq m - 2 \rangle \cup \{e_{i,m-1}(x) | 0 \leq i \leq \ell\},$$
where

$$e_{i,j}(x) = \begin{cases} x^{iq+j} + x^{jq+i} & \text{if } i \neq j, \\ x^{iq+j} & \text{if } i = j, \end{cases} \hspace{1cm} (5)$$

for all $i, j \geq 0$. 

for all $i, j \geq 0$. 

Ezerman (CQT@NUS) Recent Results on AQCs January 3, 2014, 5th WQIS 10 / 22
XL Codes as Evaluation Codes

Given that $0 \leq t \leq q$, $2 \leq m \leq q - 1$ and $0 \leq \ell \leq m - 1$,

$$C_q(t, m, \ell) := \{(f(\alpha_1), \ldots, f(\alpha_t), f(\beta_1), \ldots, f(\beta_r)) \mid f(x) \in V_{m, \ell}\}. \quad (6)$$

**Theorem**

Let $0 \leq t \leq q$, $2 \leq m \leq q - 1$ and $0 \leq \ell \leq m - 1$. Let $h = \binom{m}{2}$, $r = (q^2 - q)/2$, and

$$g = \begin{cases} 
\min\{\max\{2(m - 2), m + \ell - 1\}, t\} & \text{if } q \text{ is odd}, \\
\max\{\min\{m - 2, t\}, 2t - q\} & \text{if } q \text{ is even and } \ell \leq m - 2, \\
\max\{\min\{m - 1, t\}, 2t - q\} & \text{if } q \text{ is even and } \ell = m - 1.
\end{cases}$$

Then $C_q(t, m, \ell)$ is an $[n, k, d]_q$-code with $n = t + r$, $k = h + \ell + 1$, and

$$d \geq \delta := n - \frac{1}{2}(q(m - 1) + \ell + g). \quad (7)$$
Nestedness

Note that \( V_{m,i} \subset V_{s,j} \) for all \( m < s \) or for \( i < j \) when \( m = s \). Hence, \( C_q(t, m, i) \subset C_q(t, s, j) \) and

\[
\dim(C_q(t, s, j)) - \dim(C_q(t, m, i)) = \binom{s}{2} - \binom{m}{2} + j - i. \tag{8}
\]

The computations to carry out:

1. The inner code \( C_1^\perp \) must be smallest with guaranteed lower bound for \( d(C_1) \).
2. The supercode \( C_2 \) must be optimal or near optimal.
3. Exact values of \( d(C_i) \) using tools from Linear Algebra and Finite Fields.
4. Optimality and goodness certification.
The Main Results
E., Jitman and Solé.  
A more complete picture in the studies of AQCs based on XL codes:

1. For $d_x \in \{2, 3, 4\}$ the exact parameters of the resulting AQCs are explicitly determined.

2. For $d_x = 5$ we have enough information to set a good lower bound on the distances.

3. For prime power $q \leq 9$, the Grassl’s online tables can be efficiently used to provide a performance benchmark as a measure of optimality.

4. Given the current state of the art knowledge on the best classical linear block codes, many of the resulting AQCs are certified best-possible CSS.
A Background Story

1. Theory of QECC has been largely based on the so-called Knill-Laflamme Conditions. The stabilizer approach that includes the CSS method designs quantum codes that satisfy the K-L conditions given some desired set of parameters.

2. Wang, Feng, Ling, and Xing in [IEEE Trans IT 56, 6, 2938, Jun 2010] derived an equivalent set of conditions in the language of combinatorics for AQC. Then they showed that the CSS approach is a special case.

3. A crucial tool in [WFLX10] is the deep connection between orthogonal arrays and classical codes.

4. The connection was built upon major results of Delsarte in the 1970s.

5. Some questions that follow then are: Do we need linearity? Does it have to be Euclidean inner product? Do we gain more by going nonlinear?
Subfield Subcodes, Different Inner Products

E., Sutt Jitman, San Ling and Dima Pasechnik.

The main results are:

1. We can use pairs of nested $\mathbb{F}_r$-linear codes over $\mathbb{F}_q$.
   $\mathbb{F}_r$ is any subfield of $\mathbb{F}_q$.
   Given the appropriate context, the Hermitian, trace Hermitian, and trace Euclidean inner products can be used as well.

2. An improved Linear Programming (LP) Bound.
   Follow Delsarte’s approach on both $C_1^\perp \subset C_2$ and $C_2^\perp \subset C_1$.
   $C_i$ are $\mathbb{F}_r$-linear codes over $\mathbb{F}_q$ and $\ast$ represents a suitable inner product.

3. The extensions lead to pure AQCs with strictly better parameters than relying solely on the best ones obtainable from the standard CSS construction. This justifies going CSS-like.

A SAGE implementation of the improved LP bound is available.
Focusing on AQCs with $d_x = 2$

**Proposition**

Let $C = (n, Kq, d)_q \subset \mathbb{F}_q^n$ be of size $Kq$ and distance $d$, decomposable into cosets of the repetition code $C_0 = (n, q, n)_q$. Then there exists an AQC $C = ((n, K, \{d_z = d, d_x = 2\}))_q$.

**Proof.**

Decompose $C$ into cosets given by

$$C = \bigcup_{t \in T} (C_0 + t), \quad (9)$$

Define the quantum states

$$|\psi_t\rangle = \frac{1}{\sqrt{q}} \sum_{x \in C_0} |x + t\rangle. \quad (10)$$

The rest are just checking the conditions are satisfied.
Some Remarks

- The codes in the Proposition above is CSS-like.
- Sublinearity is NOT needed here.
- How good can we go then, in terms of dimension and dephasing error correction?
- A binary code fulfilling (9) is called self-complementary. More formally, \( C \) is self-complementary if \( \mathbf{v} + \mathbf{1} \in C \) for every \( \mathbf{v} \in C \).
- For \( q > 2 \), a code fulfilling (9) is \( n \)-shift invariant, as it is invariant with respect to addition of multiples of \( \mathbf{1} \). The vector \( \mathbf{1} \) can be replaced by any fixed vector of weight \( n \).
Proposition (Grey-Rankin bound)

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

$$|C| = M \leq \frac{8d(n - d)}{n - (n - 2d)^2}. \quad (11)$$

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

$$|C| = M \leq \frac{q^2(n - d)(qd - (q - 2)n)}{n - ((q - 1)n - qd)^2}, \quad (12)$$

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

Main Results

E. and Markus Grassl, ISIT 2013 Istanbul.

1. Construction of 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 (12). The main tool is by parity-check extension of a certain augmented concatenated MDS code. See the paper for details.

2. Established connection to Hadamard Matrix, MOLS, and quasi-symmetric designs are reconsidered and updated.

3. The application of GR-bound is limited by the range of the minimum distance that it can handle. Other optimal $n$-shift invariant codes are identified. They cover both optimal stabilizer (i.e., additive) codes and non-additive ones.

4. Optimal AQCs derived from the Gray image of $\mathbb{Z}_4$-Linear Codes.

5. Results based on various other search techniques.

6. State-of-the-art values for $q \in \{2, 3, 4\}$ with $5 \leq n \leq 16$ are summarized in tables.
Some Open Problems

1. Construction of better AQCs.
2. Reconsider the whole error model. Does the existing model conform to the physical reality for non qubit cases?
4. From classical to quantum and back to classical.
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.
- Merlion Travel Grant 1.02.10 provided by the Embassy of France in Singapore.
- IARPA via Department of Interior National Business Center Contract number DlIPC20I66.
Collaborators

- Markus Grassl @ CQT, NUS.
- San Ling and Han Mao Kiah @ CCRG, NTU.
- Somphong Jitman, formerly @ CCRG, NTU, now @ Silpakorn Univ., Thailand.
- Dmitrii Pasechnik, NTU and Oxford.
- Patrick Solé, ENST Paristech and King Abdulaziz Univ., Saudi Arabia.