Construction X for quantum error-correcting codes

Petr Lisoněk
Simon Fraser University
Burnaby, BC, Canada

joint work with Vijaykumar Singh

International Workshop on Coding and Cryptography
WCC 2013
Bergen, Norway
15 April 2013

Overview

Construction X is known from the theory of classical error control codes. We present a variant of this construction that produces stabilizer quantum error control codes from arbitrary linear codes.

Our construction does not require the classical linear code that is used as an ingredient to satisfy the dual containment (equivalently, self-orthogonality) condition.

We prove lower bounds on the minimum distance of quantum codes obtained from our construction.

We give examples of record breaking quantum codes produced from our construction.

Notation

For $x, y \in \mathbb{F}_4^n$ let $\langle x, y \rangle = \sum_{i=1}^n x_i \overline{y_i} = \sum_{i=1}^n x_i {y_i}^2$ be their Hermitian inner product.

$C^{\perp_h} := \{u \in \mathbb{F}_4^n : (\forall x \in C) \langle u, x \rangle = 0\}$ ... the *Hermitian dual of* C

$\mathrm{Tr}(a) := a + a^2$ ... the trace from $\mathbb{F}_4$ to $\mathbb{F}_2$

$\mathrm{wt}(x)$ ... the Hamming weight of $x \in \mathbb{F}_4^n$

$\mathrm{wt}(C) := \min\{\mathrm{wt}(x) : x \in C, x \neq 0\}$
... the minimum distance of linear code C

Quantum codes

A quantum error-correcting code (QECC) is a code that protects quantum information from corruption by noise (decoherence) on the quantum channel in a way that is similar to how classical error-correcting codes protect information on the classical channel.

We denote by $[[n, k, d]]$ the parameters of a binary quantum code that encodes k logical qubits into n physical qubits and has minimum distance d. We only deal with *binary* quantum codes in this talk, but our method can be generalized to odd characteristic as well.

For fixed n and k, the higher d is, the more error control the code achieves.

Stabilizer quantum codes

A binary stabilizer quantum code of length n is equivalent to a quaternary additive code (an additive subgroup) $C \subset \mathbb{F}_4^n$ such that $\mathrm{Tr}(\langle x, y \rangle) = 0$ for all $x, y \in C$.

A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory* 1998, and some earlier papers.

Stabilizer quantum codes from linear quaternary codes

If we further restrict our attention to linear subspaces of $\mathbb{F}_4^n$, then the following theorem expresses the parameters of the quantum code that can be constructed from a classical linear, Hermitian dual containing quaternary code.

Theorem

Given a linear $[n, k, d]_4$ code C such that $C^{\perp_h} \subseteq C$, we can construct an $[[n, 2k - n, d]]$ quantum code.

Quaternary additive codes are less developed but this is an active current topic.

Preliminaries

For $x \in \mathbb{F}_4^n$ let $\|x\| = \langle x, x \rangle$ be the *norm* of x. Note that $\|x\|$ is always 0 or 1 and it equals the parity of $\mathrm{wt}(x)$.

A subset $S \subset \mathbb{F}_4^n$ is called *orthonormal* if $\langle x, y \rangle = 0$ for any two distinct $x, y \in S$ and $\langle x, x \rangle = 1$ for any $x \in S$.

Proposition

Let D be a subspace of $\mathbb{F}_4^n$ and assume that M is a basis for $D \cap D^{\perp_h}$. Then there exists an orthonormal set B such that $M \cup B$ is a basis for D.

We prove the Proposition from scratch in our paper, in order to give an algorithm for constructing such a set B for any given D. (The algorithm can be randomized to construct many different instances of admissible sets B.)

Construction X for QECC

Theorem (L., Singh)

For an $[n, k]_4$ *linear code* C *denote* $e := n - k - \dim(C \cap C^{\perp_h})$. *Then there exists an* $[[n + e, 2k - n + e, d]]$ *quantum code with* $d \geq \min\{\mathrm{wt}(C), \mathrm{wt}(C + C^{\perp_h}) + 1\}$.

Note that for $e = 0$ we get the standard construction mentioned earlier.

Proof

Note

$$e = \dim(C^{\perp_h}) - \dim(C \cap C^{\perp_h}) = \dim(C + C^{\perp_h}) - \dim(C).$$

To simplify notation on slides we identify a matrix with its set of rows.

Denote $s := \dim(C \cap C^{\perp_h})$ and let

$$G = \begin{pmatrix} M_{s\times n} & 0_{s\times e} \\ A_{(n-e-2s)\times n} & 0_{(n-e-2s)\times e} \\ B_{e\times n} & I_{e\times e} \end{pmatrix}$$

be such that M is a basis for $C \cap C^{\perp_h}$, $M \cup A$ is a basis for C, $M \cup B$ is a basis for $C^{\perp_h}$, and B is an orthonormal set. Note that $M \cup A \cup B$ is a basis for $C + C^{\perp_h}$.

Proof (cont'd)

Let E be the row span of G.

Let S be the submatrix of G given by

$$S = \begin{pmatrix} M_{s\times n} & 0_{s\times e} \\ B_{e\times n} & I_{e\times e} \end{pmatrix}.$$

By construction, each vector in S is orthogonal to each row of G, thus each vector in S belongs to $E^{\perp_h}$. Since

$$\dim(E^{\perp_h}) = n + e - (n - s) = e + s = |S|$$

it follows that S is a basis for $E^{\perp_h}$. Since S is a subset of E by construction, it follows that $E^{\perp_h} \subseteq E$.

Proof (cont'd)

Recall that E is generated by

$$G = \begin{pmatrix} M_{s\times n} & 0_{s\times e} \\ A_{(n-e-2s)\times n} & 0_{(n-e-2s)\times e} \\ B_{e\times n} & I_{e\times e} \end{pmatrix}$$

where $M \cup A$ generates C and $M \cup A \cup B$ generates $C + C^{\perp_h}$.

Let $x \in E$, $x \neq 0$. By considering two cases, we have

$$\mathrm{wt}(x) \geq \mathrm{wt}(C) \qquad \text{or} \qquad \mathrm{wt}(x) \geq \mathrm{wt}(C + C^{\perp_h}) + 1.$$

Thus E is an $[n+e, k+e, d]_4$ code with $d \geq \min\{\mathrm{wt}(C), \mathrm{wt}(C + C^{\perp_h}) + 1\}$ and $E^{\perp_h} \subseteq E$. An application of the general theorem on construction of quantum codes from linear codes to the code E finishes the proof of our theorem.

Applying our construction

If e is large then $\mathrm{wt}(C + C^{\perp_h}) + 1$ may be a weak lower bound on the minimum weight of E. Thus it seems reasonable to focus on codes for which e is positive but small. Thus characterizing such codes is an interesting problem as it leads to applications of our construction. Next we give such a characterization for cyclic codes.

In general this problem appears to be similar to one of central problems in quantum coding theory: characterizing dual containing (or, equivalently, self-orthogonal) linear codes.

Using linear cyclic codes for C in our construction

Let a linear cyclic code $C \subset \mathbb{F}_4^n$ with n odd be given as $C = \langle g(x) \rangle \subset \mathbb{F}_4[x]/(x^n - 1)$. Let $\beta \in \mathbb{F}_{4^m}$ be a fixed primitive nth root of unity. The *defining set* of C is $\{k : g(\beta^k) = 0,\ 0 \leq k < n\}$.

Denote $C_a := \{a4^j \bmod n : 0 \leq j < m\} \subset \mathbb{Z}_n$ the *cyclotomic coset modulo n containing a*. The defining set of a cyclic code is the union of some cyclotomic cosets.

Proposition (L., Singh)

If C is a quaternary linear cyclic code with defining set Z, then $\dim(C^{\perp_h}) - \dim(C \cap C^{\perp_h}) = |Z \cap -2Z|$.

Using cyclic codes for C in our construction

Note $e = \dim(C^{\perp_h}) - \dim(C \cap C^{\perp_h}) = |Z \cap -2Z|$ in our construction.

Backtracking algorithm to enumerate all cyclic codes of length n with an *upper bound on* e:
Start with $Z = \emptyset$ and add one cyclotomic coset to Z at a time.
Backtracking rule follows from:

$$Z' \supseteq Z \Longrightarrow |Z' \cap -2Z'| \geq |Z \cap -2Z|.$$

If C is cyclic, then both $C^{\perp_h}$ and $C + C^{\perp_h}$ are cyclic too. This makes computing their minimum distance, and thus bounding the minimum distance of our QECC, much easier. We used the built-in function in Magma.

A special lower bound for certain cyclic codes

If n is divisible by 3, then $\{0\}$, $\{\frac{n}{3}\}$ and $\{\frac{2n}{3}\}$ are singleton cyclotomic cosets and each of them is fixed under the map $S \mapsto -2S$.

Theorem (L., Singh)

Assume that n is divisible by 3 and let C be an $[n,k]_4$ cyclic code with defining set Z such that $Z \cap -2Z \subseteq \{0, \frac{n}{3}, \frac{2n}{3}\}$. Denote $e := |Z \cap -2Z|$. Then there exists an $[[n+e, 2k-n+e, d]]$ quantum code with $d \geq \min\{\mathrm{wt}(C), \mathrm{wt}(C_u)+1, \mathrm{wt}(C+C^{\perp_h})+2\}$ where the minimum is taken over the cyclic codes C_u with defining set $Z \setminus \{u\}$ for each $u \in Z \cap -2Z$.

Proof

Denote $n = 3\ell$ and let ω denote a primitive cube root of unity in $\mathbb{F}_4$. For $t \in \{0, 1, 2\}$ define the polynomials

$$b_t(x) := \frac{x^{3\ell} - 1}{x - \beta^{\frac{tn}{3}}} = \frac{x^{3\ell} - 1}{x - \omega^t} = \sum_{i=0}^{\ell-1} \left(x^{3i+2} + \omega^t x^{3i+1} + \omega^{2t} x^{3i} \right).$$

The set $\{b_0, b_1, b_2\}$ is orthonormal since n is odd.

We now follow the proof of our main theorem, where for the rows of B we now take the set $U = \{b_t : \frac{tn}{3} \in Z \cap -2Z\}$. Note that $b_t \in C^{\perp_h} \setminus C$ for each $b_t \in U$ and also each $b_t \in U$ is linearly independent of $C \cup U \setminus \{b_t\}$.

Proof (cont'd)

Let $a \in E$, $a \neq 0$. The proof of

$$\mathrm{wt}(a) \geq \min\{\mathrm{wt}(C),\ \mathrm{wt}(C_u) + 1,\ \mathrm{wt}(C + C^{\perp_h}) + 2\}$$

is similar as in the main theorem (1st and 3rd case). In the 2nd case we have $a \in \mathrm{span}(C \cup \{b_t\})$, which is the cyclic code with the defining set $Z \setminus \{\frac{tn}{3}\}$: consider that b_t is divisible by $\prod_{k \in Z \setminus \{\frac{tn}{3}\}} (x - \beta^k)$.

Our record breaking quantum codes

Quantum codes listed on the next slide have a *higher* minimum distance than those found at `http://codetables.de/` (M. Grassl, Tables of linear codes and quantum codes).

Secondary constructions applied to our codes produce many more record breaking codes; for example our $[[53, 17, 10]]$ code alone leads to at least 28 new record breaking codes.

Notation: $Cy(n; a_1, \ldots, a_t)$ is the cyclic code with block length n and the defining set $\bigcup_{i=1}^{t} C_{a_i}$.

Our record breaking quantum codes

quantum code	C
$[[52, 26, 7]]$	$Cy(51; 0, 1, 6, 35)$
$[[53, 17, 10]]$	$Cy(51; 0, 1, 2, 6, 17, 22)$
$[[54, 8, 12]]$	$Cy(51; 0, 1, 3, 9, 17, 22, 34, 35)$
$[[54, 24, 8]]$	$Cy(51; 0, 1, 3, 17, 34, 35)$
$[[65, 31, 9]]$	$Cy(63; 0, 2, 3, 11, 15, 31, 42)$
$[[86, 8, 19]]$	$Cy(85; 0, 10, 13, 15, 18, 21, 29, 34, 37, 41, 57)$
$[[86, 12, 17]]$	$Cy(85; 0, 2, 6, 7, 9, 10, 14, 18, 30, 41)$
$[[86, 24, 15]]$	$Cy(85; 0, 7, 9, 15, 17, 18, 21, 37, 57)$
$[[86, 56, 8]]$	$Cy(85; 0, 7, 30, 34, 57)$
$[[92, 30, 14]]$	$Cy(91; 0, 2, 3, 9, 14, 34)$
$[[92, 48, 10]]$	$Cy(91; 0, 1, 14, 19, 39)$

quantum code	C
$[[85, 9, 19]]$	$Cy(85; 3, 7, 9, 10, 17, 19, 21, 30, 37, 57)$
$[[85, 13, 17]]$	$Cy(85; 3, 10, 13, 19, 21, 29, 30, 37, 57)$
$[[93, 3, 21]]$	$Cy(93; 1, 5, 9, 13, 17, 23, 33, 34, 45)$

SAC 2013

Selected Areas in Cryptography 2013

14–16 August 2013, Burnaby, BC, Canada

http://sac2013.irmacs.sfu.ca/

submission deadline **10 May 2013**

flyers available