Quantum codes from generalized quadrangles

Petr Lisoněk
Simon Fraser University
Burnaby, BC, Canada

CanaDAM 2013
Memorial University of Newfoundland, St. John's

12 June 2013

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.

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.

Entanglement-assisted stabilizer formalism

The entanglement-assisted (EA) stabilizer formalism was introduced in (Brun, Devetak, Hsieh, *Science* 2006). It relies on already shared (noiseless) entanglement bits, which we'll call ebits, between the sender and the receiver. The number of ebits should be kept small. The formulas are worked out in case of Calderbank-Shor-Steane (CSS) entanglement-assisted code in (Hsieh, Devetak, Brun,*Physical Review A* 2007) and for the general case in (Wilde, Brun, *Physical Review A* 2008).

Entanglement-assisted stabilizer formalism

Entanglement-assisted quantum error correcting code (EAQECC) utilizes e copies of maximally entangled states (the code requires e ebits). The EAQECC model removes the self-orthogonality requirement imposed on stabilizer quantum codes.

As was mentioned on the previous slide, the number of ebits should be small. For an LDPC EAQECC that uses one ebit, Fujiwara and Tonchev showed recently that the girth of its Tanner graph is at most six. We study the LDPC EAQECC that arises from the symplectic generalized quadrangle $W(q)$ where q is even. The girth of the Tanner graph is eight and we prove that the proportion of ebits tends to zero as q grows.

EA codes from classical linear codes

Proposition (L., Singh)

1. *Suppose C is an $[n,k]$ linear code over $\mathbb{F}_2$ and denote*

$$e := \dim(C^\perp) - \dim(C \cap C^\perp) = \dim(C + C^\perp) - \dim(C).$$

Then we can construct an $[[n, 2k-n+e; e]]$ EAQECC.

2. *Suppose C is an $[n,k]$ linear code over $\mathbb{F}_4$ and denote*

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

Then we can construct an $[[n, n-2k+e; e]]$ EAQECC.

Here e is the number of ebits that the code requires.

LDPC EA QECC

Let H be a parity check matrix of a binary code. The homogeneous EAQECC derived from H requires e ebits where $e = \mathrm{rank}(HH^T)$.

If $e = 0$, then $HH^T = 0$ and the Tanner graph associated with H has girth 4, due to an even overlap of any two rows of H.

For $e = 1$ Fujiwara and Tonchev (arXiv:1108.0679, to appear in *IEEE Transactions on Information Theory*) gave a combinatorial description of these codes in terms of block designs. They showed that the Tanner graph has girth at most 6, and they asked about the case when two or more ebits are allowed.

LDPC EA QECC (cont'd)

For girth 8 and higher, one natural source of parity check matrices are the incidence matrices of generalized quadrangles. These matrices are highly structured, have a compact presentation and allow easier encoding and decoding due to their quasi-cyclic structure.

Generalized quadrangles

A *generalized quadrangle* (GQ) of order (s, t) is an incidence structure of points and lines in which each line contains $s + 1$ points and each point is on $t + 1$ lines. Two distinct points are incident with at most one line. Two distinct lines intersect in at most one point. For a point p and line ℓ such that $p \notin \ell$ there is a *unique* line ℓ' such that $p \in \ell'$ and ℓ' intersects ℓ.

Example: A quadrangle is a GQ of order $(1, 1)$.

The *dual* of a generalized quadrangle of order (s, t) is a generalized quadrangle of order (t, s) obtained by interchanging the roles of points and lines. We say that a generalized quadrangle is *self-dual* if it is isomorphic to its dual.

Example: GQ of order $(1, 1)$ is self-dual.

Codes from GQs

The parity check matrix associated with a generalized quadrangle Q is the incidence matrix of Q. This is the binary matrix H such that the rows of H correspond to the lines of Q and the columns of H correspond to the points of Q. We set $H_{i,j} = 1$ if line i contains point j, and $H_{i,j} = 0$ otherwise.

H can be made symmetric iff Q is self-dual.

Note that the last axiom of GQ assures that the girth of the Tanner graph of H is at least 8. (There are no triangles in a GQ.)

A GQ of order (s, t) has $(s + 1)(st + 1)$ points which then is the block length of the associated LDPC code.

Two ebits are enough for girth 8

Consider the $m \times m$ square grid G_m which is a GQ of order $(m-1, 1)$, and suppose that m is even. Let H be the $2m \times m^2$ incidence matrix of G_m in which the top m rows correspond to one set of parallel lines of G_m and the bottom m rows correspond to the other set of parallel lines of G_m.

We have $HH^T = \begin{pmatrix} 0 & J \\ J & 0 \end{pmatrix}$ where 0 and J are all-zero and all-one square matrices, respectively. Thus $\mathrm{rank}(HH^T) = 2$ and H is an example of a LDPC matrix whose Tanner graph has girth 8 and the EAQECC constructed from H requires only two ebits.

Codes from the symplectic classical GQ $W(q)$

Theorem (L.)

Let $q = 2^e$ and let H be the incidence matrix of GQ $W(q)$. Then $\mathrm{rank}(HH^T) = q^2 + 1$. Thus we get an EAQECC of block length $(q+1)(q^2+1)$ requiring q^2+1 ebits whose Tanner graph has girth 8.

Proof. $W(q)$ has order (q, q). The points of $W(q)$ are the points of $\mathrm{PG}(3, q)$ and the $q+1$ lines incident with any point of $W(q)$ lie in the same plane of $\mathrm{PG}(3, q)$. If q is even, then $W(q)$ is self-dual. After dualizing and a geometric argument, HH^T is shown to be the point-hyperplane incidence matrix of $\mathrm{PG}(3, 2^e)$, whose $\mathbb{F}_2$-rank is known to be $4^e + 1 = q^2 + 1$.

SAC 2013

Selected Areas in Cryptography 2013

14–16 August 2013, Burnaby, BC, Canada

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