

Quantum Stabilizer Codes based on BCH Error-correcting Codes

Salah A. Aly

Joint work with Dr. Andreas Klappenecker and Pradeep K. Sarvepalli
Department of Computer Science
Texas A& M University

Student Research Week, March 28, 2006

Outline

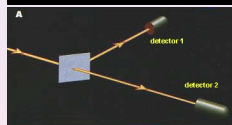
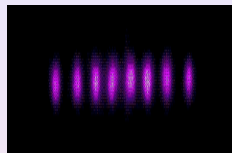
- 1 Background and Motivation
 - Quantum Computers!!!
 - Quantum Codes
- 2 New Results and Contribution
 - New Results in BCH Codes
 - Duals of BCH Codes
 - Families of Quantum BCH Codes
- 3 Summary and Conclusion

Quantum Computers!!! How far to make it real?

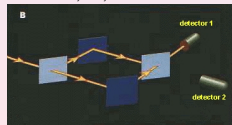
- Quantum computers are much faster than classical computers.
- Quantum computers are useful for many applications [in cryptography, database search, distributed systems, etc].
- Much progress has been done during the last decade to build them...

However,

quantum information is extremely sensitive to noise, it appears unlikely that any large scale quantum computation is practicable without **applying quantum error-correction.**



Shown in a paper by Deutsch and Ekert, 93, Nov 96.

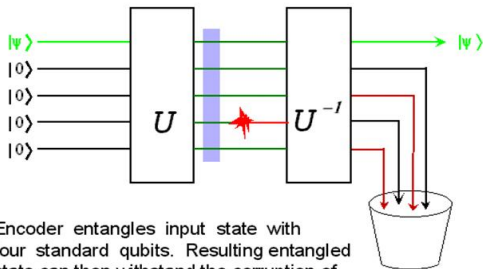


the beam (light) did not reach detector 2.

Quantum Error-correcting Codes Framework...

The Simplest Quantum Error-Correcting Code

(IBM and Los Alamos in 1996)



Encoder entangles input state with four standard qubits. Resulting entangled state can then withstand the corruption of any one of its qubits, and still allow recovery of the exact initial state by a decoder at the receiving end of the channel

U Unitary operation

$$|\Psi\rangle = a|0\rangle + b|1\rangle$$

$[[5, 1, 3]]_2$ code

Are we able to get it?

How it works?

What about the noise?

See Next?



Quantum Codes Construction

- A classical code is denoted by $[n, k, d]_q$ that

- Encodes k bits in n bits
- q levels, k dimension, and n length of the code.
- Distance d_{min} can correct $t = \lfloor (d-1)/2 \rfloor$ errors.



- A classical code $[n, k, d]_q$ implies the existence of an $[[n, 2k - n, d']]_q$ quantum code if the classical code contains its dual.

Definition:

A q -ary quantum code Q , denoted by $[[n, k, d]]_q$, is a q^k dimensional subspace of the Hilbert space \mathbb{C}^{q^n} and can correct all errors upto $\lfloor \frac{d-1}{2} \rfloor$

Let $G = \{E = E_1 \otimes E_2 \cdots \otimes E_n\}$ ($q^n \times q^n$ matrices)

Quantum Codes Construction

- A classical code is denoted by $[n, k, d]_q$ that

- Encodes k bits in n bits
- q levels, k dimension, and n length of the code.
- Distance d_{min} can correct $t = \lfloor (d-1)/2 \rfloor$ errors.



- A classical code $[n, k, d]_q$ implies the existence of an $[[n, 2k - n, d']]_q$ quantum code if the classical code contains its dual.

Definition:

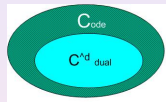
A q -ary quantum code Q , denoted by $[[n, k, d]]_q$, is a q^k dimensional subspace of the Hilbert space \mathbb{C}^{q^n} and can correct all errors upto $\lfloor \frac{d-1}{2} \rfloor$

Let $G = \{E = E_1 \otimes E_2 \cdots \otimes E_n\}$ ($q^n \times q^n$ matrices)

Q is the joint eigenspace of a commutative subgroup, $S \subseteq G$

$$E|v\rangle = |v\rangle, E \in S, \text{ for all } |v\rangle \in Q$$

S can be mapped to a classical code that contains its dual, i.e. $C^\perp \subseteq C$.



Constructing Q reduces to constructing self-orthogonal C

- Euclidean self-orthogonal codes over F_q^n
- Hermitian self-orthogonal codes over $F_{q^2}^n$.

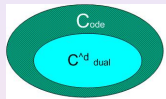
Lemma

CSS Construction : Let $C_1 = [n, k_1, d_1]_q$, $C_2 = [n, k_2, d_2]_q$ be linear codes over F_q with $C_1 \subseteq C_2$ and $d = \min wt\{(C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\}$. Then there exists an $[[n, k_2 - k_1, d]]_q$ quantum code

Q is the joint eigenspace of a commutative subgroup, $S \subseteq G$

$$E|v\rangle = |v\rangle, E \in S, \text{ for all } |v\rangle \in Q$$

S can be mapped to a classical code that contains its dual, i.e. $C^\perp \subseteq C$.



Constructing Q reduces to constructing self-orthogonal C

- Euclidean self-orthogonal codes over F_q^n
- Hermitian self-orthogonal codes over $F_{q^2}^n$.

Lemma

CSS Construction : Let $C_1 = [n, k_1, d_1]_q$, $C_2 = [n, k_2, d_2]_q$ be linear codes over F_q with $C_1 \subseteq C_2$ and $d = \min wt\{(C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\}$. Then there exists an $[[n, k_2 - k_1, d]]_q$ quantum code

BCH Codes

- A cyclic code of length $n = q^m - 1$ and designed distance δ over F_q is called a **primitive, narrow sense BCH code**, if its generator polynomial is of the form

$$g(x) = \prod_{s \in S} (x - \alpha^s), \quad \text{with } S = C_1 \cup C_2 \dots \cup C_{\delta-1}$$

- In this case the code has parameters $[n, k, \delta]_q$.
- Once we know the generator polynomial we can construct the code
- Can we find a formula for the dimension k given n and δ ?
A formula for the dimension was not known.

Dimension of BCH Codes

By looking at the cyclotomic cosets of the generator polynomial of BCH codes, we were able to drive a new formula for the dimension of the codes when their design distance is $O(n^{1/2})$.

Theorem

A primitive, narrow-sense BCH code of length $q^m - 1$ over \mathbf{F}_q with designed distance δ in the range $2 \leq \delta \leq q^{\lceil m/2 \rceil} + 1$ has dimension

$$k = q^m - 1 - m \lceil (\delta - 1)(1 - 1/q) \rceil.$$

Idea of the proof:

Number of cyclotomic cosets are $(d - 1)$

Every cyclotomic coset has length m

Exclude the repeated cyclotomic cosets $C_q = C_x/q$

The generator polynomial has $\deg(g(x)) = m(d - 1) - m \lceil (d - 1)/q \rceil$

Euclidean Duals

We were able to derive conditions when BCH codes contain their Euclidean and Hermitian duals.



Euclidean Duals

Recall that the Euclidean dual code C^\perp of a code $C \subseteq \mathbb{F}_q^n$ is given by $C^\perp = \{y \in \mathbb{F}_q^n \mid x \cdot y = 0 \text{ for all } x \in C\}$.

Theorem

A primitive, narrow-sense BCH code of length $q^m - 1$, with $m \geq 2$, over the finite field \mathbb{F}_q contains its dual code if and only if its designed distance δ satisfies

$$\delta \leq \delta_{\max} = q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}].$$

Hermitian Duals

We were able to derive conditions when BCH codes contain their Euclidean and Hermitian duals.



Hermitian Duals

Recall that if the code C is a subspace of the vector space $\mathbf{F}_{q^2}^n$, then its Hermitian dual code C^{\perp_h} is given by

$$C^{\perp_h} = \{y \in \mathbf{F}_{q^2}^n \mid y^q \cdot x = 0 \text{ for all } x \in C\}$$

Theorem

A primitive, narrow-sense BCH code of length $q^{2m} - 1$ over \mathbf{F}_{q^2} , where $m \neq 2$, contains its Hermitian dual code if and only if its designed distance δ satisfies

$$\delta \leq \delta_{\max} = q^{m+[m \text{ even}]} - 1 - (q^2 - 2)[m \text{ even}].$$

Constructing Families of Quantum BCH Codes

We were able to construct two families of quantum BCH codes.

If C is a classical linear $[n, k, d]_q$ code containing its dual, $C^\perp \leq C$, then there exists a $[[n, 2k - n, d]]_q$ stabilizer code.

Theorem

If q is a power of a prime, and m and δ are integers such that $m \geq 2$ and $2 \leq \delta \leq \delta_{\max} = q^{\lceil m/2 \rceil} - 1 - (q - 2)[m \text{ odd}]$, then there exists a quantum stabilizer code Q with parameters

$$[[q^m - 1, q^m - 1 - 2m[(\delta - 1)(1 - 1/q)], d_Q \geq \delta]]_q$$

that is pure up to δ .

Proof.

Sketch of the proof.

Proof.

- From our results in the dimension and dual of BCH codes, imply that there exists a classical BCH code with parameters $[q^m - 1, q^m - 1 - m\lceil(\delta - 1)(1 - 1/q)\rceil, \geq \delta]_q$ which contains its dual code.
- An $[n, k, d]_q$ code that contains its dual code implies the existence of the quantum code with parameters $[[n, 2k - n, \geq d]]_q$ by the CSS construction.
- The dual distance exceeds δ_{\max} ; the statement about the purity and minimum distance is an immediate consequence.



Constructing Families of Quantum BCH Codes

Similarly, we constructed a family of quantum BCH codes using hermitian duals of the classical codes.

Theorem

If q is a power of a prime, m is a positive integer, and δ is an integer in the range

$2 \leq \delta \leq \delta_{\max} = q^{m+[m \text{ even}]} - 1 - (q^2 - 2)[m \text{ even}]$, then there exists a quantum code Q with parameters

$$[[q^{2m} - 1, q^{2m} - 1 - 2m[(\delta - 1)(1 - 1/q^2)], d_Q \geq \delta]]_q$$

that is pure up to δ .

Summary

- **Quantum Error-correcting Codes** are needed to build quantum computers
- We have shown new results in quantum and Classical BCH codes.
- We established conditions when primitive, narrow-sense BCH codes contain their Euclidean and Hermitian dual codes.
- And this allowed us to derive two families of **quantum stabilizer codes**.



References I

<http://faculty.cs.tamu.edu/klappi/pub.html>



S. A. Aly, A. Klappenecker, and P. K. Sarvepalli
Primitive Quantum BCH Codes,
submitted to ISIT06.



S. A. Aly, A. Klappenecker, and P. K. Sarvepalli
Quantum and Classical BCH Codes,
(under preparation).



Ketkar, A. and Klappenecker, A. and Kumar, S. and
Sarvepalli, P. K.
Nonbinary stabilizer codes over finite fields,
IEEE Tran. Info. Theory (submitted 2005).