

# Primitive Quantum BCH Codes

Salah A. Aly

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

ISIT 2006  
Seattle, WA

# Overview

- For small designed distance, we determine the dimension of primitive narrow-sense BCH codes.
- We study when primitive, narrow-sense BCH codes contain their Euclidean or Hermitian dual codes.
- We construct two families of quantum stabilizer BCH codes.

# BCH Codes

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

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

where  $C_x = \{xq^k \pmod n \mid k \in \mathbf{Z}\}$  denotes the q-ary cyclotomic cosets of x modulo n.

- Once we know the generator polynomial, we can construct the code, with parameters  $[n, k, \geq \delta]_q$ .

## Questions

- Is there an analytical result for the dimension k given n and  $\delta$ ?
- What is the minimum distance d of the code?

# 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  $\delta$  in the range  $2 \leq \delta \leq q^{\lceil m/2 \rceil} + 1$  has dimension*

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

## Sketch of the proof.

- The total number of cyclotomic cosets are  $(\delta - 1)$
- Exclude the repeated cyclotomic cosets  $C_q = C_x/q$
- Every cyclotomic coset  $C_x$  has length  $m$  if  $1 \leq x < q^{\lceil m/2 \rceil} + 1$
- The generator polynomial has  

$$\deg(g(x)) = m(\delta - 1) - m\lceil(\delta - 1)/q\rceil$$
- Finally, the dimension  $k = n - \deg(g(x))$ .

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



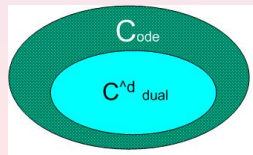
# Euclidean Duals

## Definition (Euclidean Duals)

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

It has been shown by A. Steane that a primitive binary narrow-sense BCH code of length  $n = 2^m - 1$  contains its Euclidean dual if and only if its designed distance  $\delta$  is in the range  $2 \leq \delta \leq 2^{m/2} - 1$ .

We were able to derive conditions when primitive **nonbinary** narrow-sense BCH codes contain their Euclidean duals.



# Euclidean Duals

## 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  $\delta$  satisfies*

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

The proof uses the following lemma [Grassl99]

## Lemma

*A cyclic code of length  $n$  and defining set  $Z$  contains its Euclidean dual if and only if  $Z \cap Z^{-1} = \emptyset$  where  $Z^{-1} = \{-z \pmod n \mid z \in Z\}$ .*

## Sketch of the proof for even $m$ .

- Idea of the proof lies on  $Z \cap Z^{-1} = \emptyset$ , where  $Z$  is the defining set.
- Seeking a contradiction, assume  $\delta > \delta_{max}$  and  $C^\perp \subseteq C$ .
- $Z$  contains the set  $\{1, 2, \dots, s\}$  with  $s = \delta_{max} = q^{m/2} - 1$ .
- Then  $s = q^{m/2} - 1$ , and  $Z^{-1}$  contains the element

$$-sq^{m/2} \equiv -q^m + q^{m/2} \equiv q^{m/2} - 1 \equiv s \pmod{n},$$

which means that  $Z \cap Z^{-1} \neq \emptyset$ .

Hence  $C^\perp \not\subseteq C$ , contradiction.



# Quantum Codes Constructions

## Definition:

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

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

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

The stabilizer group,  $S$ , is the largest subgroup of the error group  $G$  that fixes every element in  $Q$ .  $S$  can be mapped to a classical code that is self-orthogonal, i.e.  $C$  is isomorphic to  $S$ .

Constructing  $Q$  reduces to constructing self-orthogonal  $C$

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

# Quantum Codes Constructions

## Definition:

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

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

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

The stabilizer group,  $S$ , is the largest subgroup of the error group  $G$  that fixes every element in  $Q$ .  $S$  can be mapped to a classical code that is self-orthogonal, i.e.  $C$  is isomorphic to  $S$ .

Constructing  $Q$  reduces to constructing self-orthogonal  $C$

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

# Constructing Families of Quantum BCH Codes

## CSS construction

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.

This can be applied to BCH codes that contain their duals.

## Theorem

*If  $q$  is a power of a prime, and  $m$  and  $\delta$  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  $\delta$ .*

## Sketch of the proof.

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



## Sketch of the proof.

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



# Hermitian Dual Codes

- We were able to derive conditions when BCH codes contain their 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  $\delta$  satisfies*

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

# Constructing Families of Quantum BCH Codes

Similarly, quantum codes can be constructed from BCH codes that contain their hermitian duals.

## Theorem

*If  $q$  is a power of a prime,  $m$  is a positive integer, and  $\delta$  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  $\delta$ .*

# Summary

- We precisely determined the dimension of primitive nonbinary narrow-sense BCH codes over finite fields.
- We established conditions when primitive, narrow-sense BCH codes contain their Euclidean and Hermitian dual codes,  $\delta = O(\sqrt{n})$ .
- We derived two families of quantum stabilizer codes.

Our results has been generalized to non-primitive BCH codes over finite fields.



## Lemma

If  $C$  is primitive, narrow-sense BCH code of length  $q^m - 1$  over  $\mathbb{F}_q$  with designed distance  $\delta$  in the range  $2 \leq \delta \leq q^{\lceil m/2 \rceil} + 1$  such that

$$\sum_{i=0}^{\lfloor (\delta+1)/2 \rfloor} \binom{q^m - 1}{i} (q - 1)^i > q^{m \lceil (\delta-1)(1-1/q) \rceil}, \quad (1)$$

then  $C$  has minimum distance  $d = \delta$  or  $\delta + 1$ ; if, furthermore,  $\delta \equiv 0 \pmod{q}$ , then  $d = \delta + 1$ .