

# Subsystem Code Constructions

Salah A. Aly

Department of Computer Science  
Texas A& M University

Presented in  
First International Conference on Quantum Error Correction  
USC Campus, CA

December 20, 2007

1. Subsys. Codes
2. Bounds
3. Subsys. construction
4. RS & MDS
5. Conclusion

# Subsystem Codes

- Subsystem codes are a relatively new construction of quantum codes based on isolating the active errors into two subsystems.
- Subsystem codes combine the features of decoherence free subspaces, noiseless subsystems, and quantum error-correcting codes.
- Such codes can offer attractive features, such as simple syndrome calculation and a wide variety of easily implementable fault-tolerant operations.
- In this talk, I present bounds, subsystem code constructions, and many families of subsystem codes.

QEC07,  
USC,  
12/20/2007

1. Subsys.  
Codes

2. Bounds

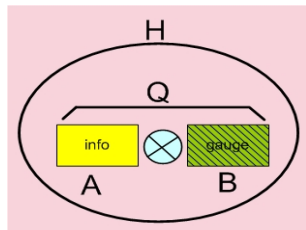
3. Subsys.  
construction

4. RS & MDS

5. Conclusion

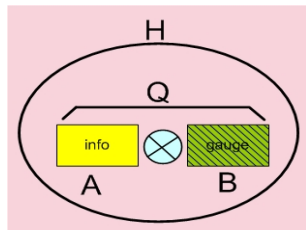
# Subsystem Codes

- A subsystem code  $Q$  can be defined as a subspace of the complex space  $C^{q^n} = C^q \otimes C^q \otimes \dots \otimes C^q$  such that  $Q = A \otimes B$ .
- We can encode the information in the subsystem  $A$  and ignore the error affecting the subsystem  $B$ .



# Subsystem Codes

- A subsystem code  $Q$  can be defined as a subspace of the complex space  $C^{q^n} = C^q \otimes C^q \otimes \dots \otimes C^q$  such that  $Q = A \otimes B$ .
- We can encode the information in the subsystem  $A$  and ignore the error affecting the subsystem  $B$ .

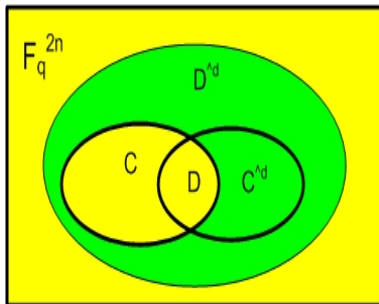


- An  $[[n, k, r, d]]_q$  subsystem code  $Q$  has  $\dim A = q^k$ ,  $\dim B = q^r$ , and can detect all errors of weight less than  $d$ .

# Subsystem Code Constructions (CSS)

Given an arbitrary classical additive code  $C$  of length  $2n$  over  $\mathbb{F}_q$ , let  $D = C \cap C^{\perp_s}$ . Then a subsystem code  $Q$  exists such that:

- $Q = A \otimes B$
- $\dim A = q^k = \sqrt{\frac{|D^{\perp_s}|}{|C|}}$   
 $k = \dim D^{\perp_s} - \dim C$
- $\dim B = q^r = \sqrt{\frac{|C|}{|D|}}$   
 $r = \dim C - \dim D$
- $d = wt(D^{\perp_s} - C)$

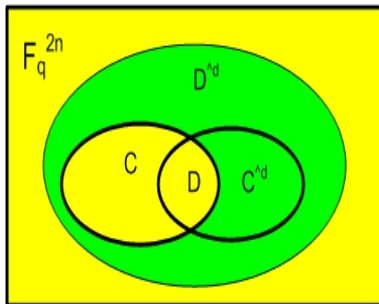


# Subsystem Code Constructions (CSS)

QEC07,  
USC,  
12/20/2007

Given an arbitrary classical additive code  $C$  of length  $2n$  over  $\mathbb{F}_q$ , let  $D = C \cap C^{\perp_s}$ . Then a subsystem code  $Q$  exists such that:

- $Q = A \otimes B$
- $\dim A = q^k = \sqrt{\frac{|D^{\perp_s}|}{|C|}}$   
 $k = \dim D^{\perp_s} - \dim C$
- $\dim B = q^r = \sqrt{\frac{|C|}{|D|}}$   
 $r = \dim C - \dim D$
- $d = wt(D^{\perp_s} - C)$



- Undetectable errors in green,  $D^{\perp_s} - C$
- Detectable Errors in yellow,  $C$  and  $\mathbb{F}_q^{2n} - D^{\perp_s}$

Then a subsystem code exists with parameters  $[[n, k, r, d]]_q = ((n, q^k, q^r, d))_q$ .

1. Subsys. Codes
2. Bounds
3. Subsys. construction
4. RS & MDS
5. Conclusion

- Can subsystem codes be better than stabilizer codes?
- What advantages do they have?
- How to construct families of subsystem codes?
- Can they beat optimal stabilizer codes?

My goal is the code construction, bounds and families of subsystem codes. Then studying properties of these codes and fault-tolerance aspects.

A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction via codes over  $GF(4)$ . IEEE Trans. Inform. Theory, 44:1369(1387), 1998.

Linear pure subsystem codes satisfy Singleton and Hamming bounds.

## Lemma (Singleton Bound)

*Linear pure subsystem codes with the parameters  $[[n, k, r, d]]_q$  satisfy*

$$k + r \leq n - 2d + 2.$$

Subsystem codes with  $k + r + 2d = n + 2$  are called MDS codes.

We answer D. Poulin question, NO  $[[5, 1, r, 3]]_2$  subsystem codes exist with  $r > 1$ .

$$1 + 2 * 3 + r \leq 5 + 2$$

Linear pure subsystem codes satisfy Singleton and Hamming bounds. In terms of packing codes, a Hamming like bound for pure subsystem codes can be stated as

## Lemma (Hamming Bound)

*A pure  $((n, K, K', d))_q$  code satisfies*

$$\sum_{j=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{j} (q^2 - 1)^j \leq q^n / KK'.$$

if  $t = \lfloor \frac{d-1}{2} \rfloor$ , then

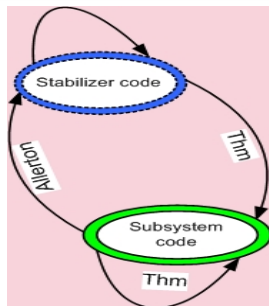
$$KK' \leq \frac{q^n}{\sum_{j=0}^t \binom{n}{j} (q^2 - 1)^j}.$$

# Subsystem Codes & Stabilizer Codes

One can trade the dimensions of subsystem (A) and co-subsystem (B) to obtain new codes from a given subsystem or stabilizer code.

## Theorem

Let  $q$  be a power of a prime  $p$ . If there exists an  $((n, K, R, d))_q$  subsystem code with  $K > p$  that is pure to  $d'$ , then there exists an  $((n, K/p, pR, \geq d))_q$  subsystem code that is pure to  $\min\{d, d'\}$ .



Constructing many subsystem codes from existing stabilizer codes.

### Theorem

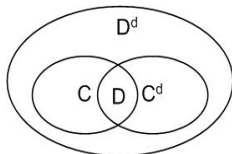
*Let  $q$  be a power of a prime  $p$ . If there exists a pure  $[[n, k, r, d]]_q$  subsystem code with  $r > 0$ , then there exists a pure  $[[n, k + 1, r - 1, d]]_q$  subsystem code.*

### Corollary

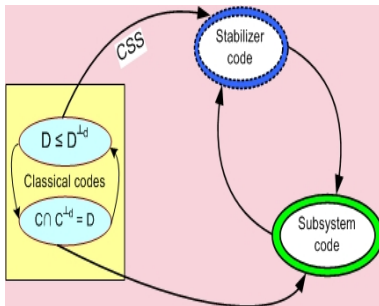
*An  $[[n, k, d]]_q$  stabilizer code can give rise to a subsystem code with the parameters  $[[n, k - r, r, d]]_q$  for  $0 \leq r \leq k$ .*

# Cyclic Subsystem Codes

If a cyclic classical code contains its dual, then there exists a subsystem code.

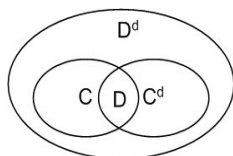


Example: BCH codes.

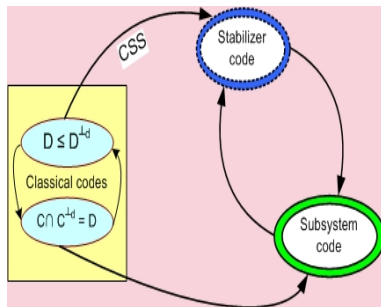


# Cyclic Subsystem Codes

If a cyclic classical code contains its dual, then there exists a subsystem code.



Example: BCH codes.



## Theorem

Let  $D^\perp$  be a cyclic code of length  $n$ , distance  $d^\perp$ , and defining set  $T_{D^\perp}$  that contains its dual code  $D$  with defining set  $T_D$  over  $\mathbb{F}_q$ . Let  $T \subseteq (T_D \setminus T_{D^\perp})$ , and  $C \subseteq \mathbb{F}_q^n$  be a cyclic code with defining set  $T_C = T_D \setminus (T \cup T^{-1})$ , where  $T = \{-t \pmod n \mid t \in T\}$ . Then there exists a subsystem code with parameters  $[[n, n - k - r, r, d^\perp]]_q$ , where  $k = 2|T_{D^\perp}|$  and  $r = |T \cup T^{-1}|$ .

## Subsystem Codes based on RS Codes

Constructed a family of subsystem codes based on RS Codes.  
The idea is to establish conditions to transfer stabilizer codes to subsystem codes.

### Definition: RS Codes

- \* Let  $n = q - 1$ , a Reed-Solomon code (RS) over a finite field  $\mathbb{F}_q$  is a BCH code with length  $n$  and designed distance  $2 \leq d < n$ .
- \* RS codes are maximal distance separable (MDS) codes with parameters  $[q - 1, q - d, d]_q$ .
- \* RS with length  $n = q - 1$  and designed distance  $\delta$  is a type of cyclic code with defining set  $S = C_1 \cup C_2 \cup \dots \cup C_{\delta-1}$  and generator polynomial

$$g(x) = \prod_{i \in S} (x - \alpha^i)$$

where  $\alpha$  is a primitive root in  $F_q$ , and  $C_i$  is a cyclotomic coset.

## Reed-Solomon Subsystem Codes:

- We have defined the CSS Euclidean and Hermitian constructions for subsystem codes.
- We show that if the designed distance of a RS code is bound by  $0 \leq \delta < (q-1)/2$ , then immediately, there will be a subsystem code.

### Lemma

*Let  $q$  be power of a prime. The following family of subsystem codes is derived from RS codes.*

- If  $0 \leq \delta < (q-1)/2$  there exist subsystem codes with parameters  $[[q-1, q-2\delta-1-r, r, \delta+1]]_q$  and  $[[q, q-2\delta-2-r, r, \delta+2]]_q$ .*
- If  $0 \leq \delta < q-1$  there exist subsystem codes with parameters  $[[q^2-1, q^2-2\delta-1-r, r, \delta+1]]_q$  and  $[[q^2, q^2-2\delta-2-r, r, \delta+2]]_q$ .*

## Example

Let  $C$  be a RS code with length  $n = q - 1 = 6$  over  $\mathbf{F}_q$ .

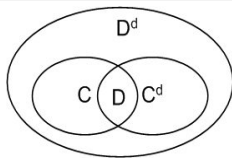
Define  $N = \{0, 1, 2, 3, 4, 5\}$ . We can construct subsystem code from RS codes with parameters  $[6, 4, 3]_7$ . This code is a subcode-subfield in BCH codes with designed distance  $\delta = 3$ .

So,  $T_D^\perp = \{1, 2\}$ ,  $T_D = \{0, 1, 2, 3\}$ ,  $T_C = \{1, 2, 3\}$  and  $T_C^\perp = \{0, 1, 2\}$ . The generator polynomial is given by  $k = n - \deg(g(x))$

We notice that  $T_D = T_C \cup T_C^\perp$  and  $\dim C = 3$ ,  $\dim D = 2$  and  $\dim D^\perp = 4$ .

Therefore, we have  $k=4-3=1$  and  $r=3-2=1$ .

Consequently, there exists a subsystem code with parameters  $[6, 1, 1, 3]$  over  $\mathbf{F}_7$



# Short Subsystem Codes $[[8, 1, 2, 3]]_2$ and $[[6, 2, 3]]_3$

QEC07,  
USC,  
12/20/2007

1. Subsys.  
Codes

2. Bounds

3. Subsys.  
construction

4. RS & MDS

5. Conclusion

$$C_S = \begin{bmatrix} X & I & Y & I & Z & Y & X & Z \\ Y & I & Y & X & I & Z & Z & X \\ I & X & Y & Y & Z & X & Z & I \\ I & Y & I & Z & Y & X & X & Z \\ I & I & X & Z & X & Y & Z & Y \\ \hline Y & I & I & I & I & Y & X & X \\ I & X & I & I & I & Y & Y & X \end{bmatrix}$$

$$C_S^\perp = \begin{bmatrix} X & I & Y & I & Z & Y & X & Z \\ Y & I & Y & X & I & Z & Z & X \\ I & X & Y & Y & Z & X & Z & I \\ I & Y & I & Z & Y & X & X & Z \\ I & I & X & Z & X & Y & Z & Y \\ \hline X & I & I & I & I & I & Z & Y \\ I & I & I & Y & I & Y & Y & Y \end{bmatrix}$$

$$D_S = \begin{bmatrix} X & I & Y & I & Z & Y & X & Z \\ Y & I & Y & X & I & Z & Z & X \\ I & X & Y & Y & Z & X & Z & I \\ I & Y & I & Z & Y & X & X & Z \\ I & I & X & Z & X & Y & Z & Y \end{bmatrix}$$

$$D_S^\perp = \begin{bmatrix} X & I & I & I & I & I & Z & Y \\ Y & I & I & I & I & Y & X & X \\ I & X & I & I & I & Y & Y & X \\ I & Y & I & I & I & I & X & Z \\ I & I & X & I & I & Y & Z & I \\ I & I & Y & I & I & I & Z & X \\ I & I & I & X & I & Y & I & Z \\ I & I & I & Y & I & Y & Y & Y \\ I & I & I & I & X & I & Y & Z \\ I & I & I & I & Y & Y & Z & Z \\ I & I & I & I & I & Z & X & Y \end{bmatrix}$$

There exist  $[[8, 2, 1, 3]]_2$  and  $[[8, 1, 2, 3]]_2$  subsystem codes.

No nontrivial  $[[7, 1, 1, 3]]_2$  exists.

# Optimal Pure Subsystem Codes

Subsystem Codes	Parent Code (RS Code)
$[[8, 1, 5, 2]]_3$ $[[8, 4, 2, 2]]_3$ $[[8, 5, 1, 2]]_3$ $[[9, 1, 4, 3]]_3$ $[[9, 4, 1, 3]]_3$	$[8, 6, 3]_{3^2}$ $[8, 3, 6]_{3^2}$ $[8, 2, 7]_{3^2}$ $[9, 6, 4]_{3^2}^\dagger, \delta = 3$ $[9, 3, 7]_{3^2}^\dagger, \delta = 6$
$[[15, 1, 10, 3]]_4$ $[[15, 9, 2, 3]]_4$ $[[15, 10, 1, 3]]_4$ $[[16, 1, 9, 4]]_4$	$[15, 12, 4]_{4^2}$ $[15, 4, 12]_{4^2}$ $[15, 3, 13]_{4^2}$ $[16, 12, 5]_{4^2}^\dagger, \delta = 4$
$[[24, 1, 17, 4]]_5$ $[[24, 16, 2, 4]]_5$ $[[24, 17, 1, 4]]_5$ $[[24, 19, 1, 3]]_5$ $[[24, 21, 1, 2]]_5$ $[[23, 1, 18, 3]]_5$ $[[23, 16, 3, 3]]_5$	$[24, 20, 5]_{5^2}$ $[24, 5, 20]_{5^2}$ $[24, 4, 21]_{5^2}$ $[24, 3, 22]_{5^2}$ $[24, 2, 23]_{5^2}$ $[23, 20, 4]_{5^2}^*, \delta = 5$ $[23, 5, 19]_{5^2}^*, \delta = 20$
$[[48, 1, 37, 6]]_7$	$[48, 42, 7]_{7^2}$

\* Punctured code

† Extended code

QEC07,  
USC,  
12/20/2007

1. Subsys.  
Codes

2. Bounds

3. Subsys.  
construction

4. RS & MDS

5. Conclusion

Table: BCH subsystem codes

Subsystem Code	Parent BCH Code	Designed distance
$[[15, 1, 2, 5]]_2$	$[15, 8, 6]_{2^2}$	6
$[[15, 5, 2, 3]]_2$	$[15, 6, 7]_{2^2}$	7
$[[17, 8, 1, 4]]_2$	$[17, 5, 9]_{2^2}$	4
$[[21, 6, 3, 3]]_2$	$[21, 9, 7]_{2^2}$	6
$[[21, 7, 2, 3]]_2$	$[21, 8, 9]_{2^2}$	8
$[[31, 10, 1, 5]]_2$	$[31, 11, 11]_{2^2}$	8
$[[31, 20, 1, 3]]_2$	$[31, 6, 15]_{2^2}$	12

1. Subsys.  
Codes

2. Bounds

3. Subsys.  
construction

4. RS & MDS

5. Conclusion

# Linear programming bound with $q = 2$

n/k	k=1	k=2	k=3	k=4	k=5	k=6	k=7	k=8	k=9	k=10	k=11	k=12
n=5	(3,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)								
n=6	(1,3), (4,2), (5,1)	(3,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)							
n=7	(3,3), (5,2), (6,1)	(4,2), (5,1)	(3,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)						
n=8	(4,3), (6,2), (7,1)	(3,3), (5,2), (6,1)	(4,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)					
n=9	(2,4), (6,3), (7,2), (8,1)	(4,3), (6,2), (7,1)	(2,3), (5,2), (6,1)	(4,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)				
n=10	(4,4), (7,3), (8,2), (9,1)	(2,4), (6,3), (7,2), (8,1)	(4,3), (6,2), (7,1)	(1,3), (5,2), (6,1)	(4,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)			
n=11	(2,5), (5,4), (8,3), (9,2), (10,1)	(4,4), (7,3), (8,2), (9,1)	(2,4), (5,3), (7,2), (8,1)	(3,3), (6,2), (7,1)	(1,3), (5,2), (6,1)	(3,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)		
n=12	(3,5), (7,4), (9,3), (10,2), (11,1)	(1,5), (6,4), (8,3), (9,2), (10,1)	(4,4), (7,3), (8,2), (9,1)	(1,4), (5,3), (7,2), (8,1)	(3,3), (6,2), (7,1)	(1,3), (5,2), (6,1)	(3,2), (5,1)	(2,2), (4,1)	(1,2), (3,1)	(2,1)	(1,1)	

- Subsystem codes can be constructed from classical codes without the need for self-orthogonal conditions. Many families are shown.
- Syndrome measurements: Stabilizer codes need  $n - k$  syndrome measurements while subsystem codes need  $n - k - r$  for fixed  $n$  and  $d$ . Fault tolerance operations of a family of subsystem codes, future direction.
- All classes of stabilizer codes (impure and pure) are also subsystem codes. All pure subsys. codes are also stabilizer codes.
- Impure subsystem codes are superior. They do not obey Hamming bound. Some of them are not stabilizer codes.

Impure  $[[9, 1, 4, 3]]_2$  subsys. code can not be  $[[9, 1 + 4, 3]]_2 = [[9, 5, 3]]_2$  stabilizer code from the linear programming bound.

## Thank you

- S.A. Aly and A. Klappenecker, Subsystem Code Constructions, IEEE Transaction on Information Theory, on submission 2007.
- S.A. Aly, A. Klappenecker, and P.K. Sarvepalli, Subsystem codes, Proceedings of the 45th Allerton Conference on Communication, Control, and Computing, Urbana, IL, September 2006.

1. Subsys.  
Codes

2. Bounds

3. Subsys.  
construction

4. RS & MDS

5. Conclusion