Quasi-cyclic Codes from Cyclic-Structured Designs with Good Properties

Dimitris E. Simos[1] Christos Koukouvinos[1]

[1]Department of Mathematics
National Technical University of Athens, Greece

Algebraic Combinatorics and Applications (ALCOMA10)
Designs and Codes
April 12, Thurnau, Germany

Outline of the Talk

1. Introduction
   - Preliminaries
   - Motivation
   - Contribution

Outline of the Talk

1. Introduction
   - Preliminaries
   - Motivation
   - Contribution
2. Construction of QC Codes from Cyclic-Structured Designs
   - Supersaturated Designs
   - A Construction Method for QC Codes from Supersaturated Designs
   - A Link between Optimal Supersaturated Designs and LCD QC Codes

Outline of the Talk

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(q)$ is a k-dimensional vector subspace of $GF(q)^n$, where $GF(q)$ is the Galois field with q elements.

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(q)$ is a k-dimensional vector subspace of $GF(q)^n$, where $GF(q)$ is the Galois field with q elements.

- We consider the case where $q = 2$.

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(q)$ is a k-dimensional vector subspace of $GF(q)^n$, where $GF(q)$ is the Galois field with q elements.

- We consider the case where $q = 2$.
- The elements of C are called codewords and the (Hamming) weight $wt(x)$ of a codeword x is the number of non-zero coordinates in x.

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(q)$ is a k-dimensional vector subspace of $GF(q)^n$, where $GF(q)$ is the Galois field with q elements.

- We consider the case where $q = 2$.
- The elements of C are called codewords and the (Hamming) weight $wt(x)$ of a codeword x is the number of non-zero coordinates in x.

Definition

- The minimum weight of C is defined as $\min\{wt(x) \mid 0 \neq x \in C\}$.
- An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d.

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(q)$ is a k-dimensional vector subspace of $GF(q)^n$, where $GF(q)$ is the Galois field with q elements.

- We consider the case where $q = 2$.
- The elements of C are called codewords and the (Hamming) weight $wt(x)$ of a codeword x is the number of non-zero coordinates in x.

Definition

- The minimum weight of C is defined as $\min\{wt(x) \mid 0 \neq x \in C\}$.
- An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d.

- A matrix whose rows are linearly independent and generate the code C is called a generator matrix of C.

Quasi-Cyclic Codes

Quasi-Cyclic Codes

- A code C is said to be *quasi-cyclic* (QC or p-QC or QC of index p) if a cyclic shift of a codeword by p positions results in another codeword
- A cyclic shift of an m-tuple $(x_0, x_1, \ldots, x_{m-1})$ is the m-tuple $(x_{m-1}, x_0, \ldots, x_{m-2})$
- Cyclic code: a QC code with $p = 1$.
- The length n of a p-QC code is a multiple of p so that $n = pm$

Quasi-Cyclic Codes

Quasi-Cyclic Codes

- A code C is said to be *quasi-cyclic* (QC or p-QC or QC of index p) if a cyclic shift of a codeword by p positions results in another codeword
- A cyclic shift of an m-tuple $(x_0, x_1, \ldots, x_{m-1})$ is the m-tuple $(x_{m-1}, x_0, \ldots, x_{m-2})$
- Cyclic code: a QC code with $p = 1$.
- The length n of a p-QC code is a multiple of p so that $n = pm$

Rate r of an $[n, k]$ code

$$r = \frac{k}{n}$$

the number of information symbols per codeword

Circulant Matrices

- $circ(b_0, b_1, \ldots, b_{m-1})$: A circulant matrix with first row $(b_0, b_1, \ldots, b_{m-1})$

Example

$$\begin{bmatrix} b_0 & b_1 & b_2 & \ldots & b_{m-2} & b_{m-1} \\ b_{m-1} & b_0 & b_1 & \ldots & b_{m-3} & b_{m-2} \\ b_{m-2} & b_{m-1} & b_0 & \ldots & b_{m-4} & b_{m-3} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ b_1 & b_2 & b_3 & \ldots & b_{m-1} & b_0 \end{bmatrix}$$

Generator Matrix of a QC Code

1-Generator QC Codes

- QC codes can be constructed from $m \times m$ circulant matrices
- In this case, the generator matrix G of a p-QC code can be represented as
$$G = [B_1 \ B_2 \ \ldots \ B_p].$$
where B_i, $i = 1, \ldots, p$ is a circulant matrix
- A p-QC code over $GF(q)$ of length $n = pm$ can be viewed as a $GF(q)[x]/(x^m - 1)$ submodule of $(GF(q)[x]/(x^m - 1))^p$

Why Interested in Quasi-Cyclic Codes?

1. QC codes meet a modified version of the Gilbert-Varshamov bound (Kasami, 1974)
2. Some of the best quadratic residue codes and Pless symmetry codes are QC codes (MacWilliams and Sloane, 1977)
3. A large number of record-breaking (and optimal) codes are QC codes (Grassl Tables, online)
4. There is a link between QC codes and convolutional codes (Solomon and Tilborg, 1979)
5. Their decoding complexity is manageable (Karlin, 1970), and many QC codes are majority logic decodable (Gulliver and Bhargava, 1993)
6. Their algebraic structure is thoroughly investigated (Ling and Solé, 2001, 2003, 2005 and Ling et. al., 2006)

Linear Codes with Complementary Duals

Definition

The dual code $C^{\perp}$ of C is defined as
$C^{\perp} = \{x \in \mathrm{GF}(q)^n \mid x \cdot y = 0 \text{ for all } y \in C\}$.

- A linear code with a complementary dual (an *LCD code*) is a code C whose dual code $C^{\perp}$ satisfies $C \cap C^{\perp} = \{\mathbf{0}\}$ (Massey, 1992)
- A few classes of LCD quasi-cyclic codes are identified so far (Esmaeilli and Yari, 2009)

An Important Property

LCD codes meet the asymptotic Gilbert Varshamov bound (Sendrier, 2004)

Exploring LCD QC Codes over $GF(2)$

Characterization of LCD Codes

If G is a generator matrix for an $[n, k]$ linear code C, then C is an LCD code if and only if the $k \times k$ matrix GG^T is nonsingular

Exploring LCD QC Codes over $GF(2)$

Characterization of LCD Codes

If G is a generator matrix for an $[n, k]$ linear code C, then C is an LCD code if and only if the $k \times k$ matrix GG^T is nonsingular

- We consider systematic *QC* codes of rate $1/p$ with generator matrix $G = [I_m \; B_2 \; \ldots \; B_p]$ which has full dimension m
- $GG^T = I_m + \sum_{i=2}^{m} B_i B_i^T$ is a circulant symmetric matrix since circulant matrices form a commutative algebra
- We focus on the set of $(0, 1)$ invertible circulant matrices with determinant equal to 1
- These matrices form the special linear group $SL(m, GF(2))$
- We aim to decide the nonsingularity of GG^T with little effort

Our Results on QC Codes

Our Goal

We are interested in the construction of good binary QC codes and the (possible) interaction of the later codes with Design Theory

1. We gave a construction method for QC codes from cyclic-structured designs

Our Results on QC Codes

Our Goal

We are interested in the construction of good binary QC codes and the (possible) interaction of the later codes with Design Theory

1. We gave a construction method for QC codes from cyclic-structured designs
2. We established a link between LCD QC codes and optimal designs
3. We constructed new QC codes belonging to the class of LCD QC codes

Our Results on QC Codes

Our Goal

We are interested in the construction of good binary QC codes and the (possible) interaction of the later codes with Design Theory

1. We gave a construction method for QC codes from cyclic-structured designs
2. We established a link between LCD QC codes and optimal designs
3. We constructed new QC codes belonging to the class of LCD QC codes
4. We constructed some good QC codes
   - of rate $1/4$
   - of rate $1/5$
   - of rate $1/6$

   via a heuristic search

Supersaturated Designs

- Supersaturated design (SSD): A two-level design in which the number of experimental runs (rows) n is lower than the number of factors (columns) m, that is $n \leq m$.
- Levels: Two possible settings for each factor coded as ± 1
- Treatment combination: Any combination of the levels of all factors
- Design matrix: $\mathbf{X} = [\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m]$
  1. rows: represent the n treatment combinations
  2. columns: give the sequence of factor levels

Balanced Designs

Designs with the equal occurence property, i.e. all columns consist of $\frac{n}{2}$ elements equal to 1 and $\frac{n}{2}$ elements equal to -1, when n is even

k-Circulant Supersaturated Designs

Cyclic-Structured Class of SSDs

- k-circulant SSD: Cycling the elements of a generator k elements at a time (Liu and Dean, 2004)
- Generator: The first row of the design matrix $\mathbf{X}$

Necessary and Sufficient Conditions for Balanced Designs

Let a k-circulant SSD with n runs and m factors with generator $(g_1, g_2, \ldots, g_m)$

1. $n = 2t$, $m = (2t-1)k$, for some positive integer t;
2. the generator contains exactly kt elements equal to -1 and $(kt-k)$ elements equal to $+1$;
3. $\sum_{u=0}^{2t-2} g_{uk+j} + 1 = 0, \; i = 1, \ldots, k.$

k-Circulant Supersaturated Designs (Cont.)

Example

A 2-circulant design for $m = 22$ factors in $n = 12$ runs can be obtained from the following generator.

$$(- + - - + - + + + - - - + + - - + - - + - +)$$

by repeatedly cycling elements 2 positions to the right and moving the last two elements to the first two positions.

$$\mathbf{x} = \left[\begin{array}{c}
- + - - + - + + + - - - + + - - + - - + - + \\
\hline
- + - + - - + - + + + - - - + + - - + - - + \\
- + - + - + - - + - + + + - - - + + - - + - \\
+ - - + - + - + - - + - + + + - - - + + - - \\
- - + - - + - + - + - - + - + + + - - - + + \\
+ + - - + - - + - + - + - - + - + + + - - - \\
- - + + - - + - - + - + - + - - + - + + + - \\
+ - - - + + - - + - - + - + - + - - + - + + \\
+ + + - - - + + - - + - - + - + - + - - + - \\
+ - + + + - - - + + - - + - - + - + - + - - \\
- - + - + + + - - - + + - - + - - + - + - + \\
+ +
\end{array}\right]$$

Supersaturated Designs in Coding Theory

Supersaturated Designs over $GF(2)$

- Transformation of $\mathbf{X}_{(-1,1)}$ to $\mathbf{X}_{(1,0)}$
- $g = (g_1, g_2, \ldots, g_m) \rightarrow g' = (g'_1, g'_2, \ldots, g'_m)$ where $g'_i = (1 - g_i)/2$, for $i = 1, \ldots, m$
- All arithmetic on $\mathbf{X}_{(1,0)}$ is performed over $GF(2)$

A $[33, 11]$ QC Code derived from a 2-Circulant Design

- Selection of odd and even factors of $\mathbf{X}_{(1,0)}$
- Generator Matrix: $G = [I_{11} \;\; B_1 \;\; B_2]$ or $G = [I_{11} \; \overline{\mathbf{X}}_{(1,0)}]$
  1. $B_1 = circ(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$
  2. $B_2 = circ(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$
- $GG^T = I_{11} \Rightarrow$ nonsingular over $GF(2) \Rightarrow G$ generates an LCD QC code

Construction of QC Codes from k-Circulant SSDs

Construction Method for Binary QC Codes from Cyclic SSDs

Let $\mathbf{X}_{(-1,1)}$ be a k-circulant SSD with n rows and $m = k(n-1)$ columns.

1. Transform $\mathbf{X}_{(-1,1)}$ to $\mathbf{X}_{(1,0)}$
2. Form k circulant $(n-1) \times (n-1)$ matrices as

$$B_j = circ(\bigcup_{l=0}^{n-2} \{g'_{kl+j}\}), \ j = 1, \ldots, k$$

3. Then, the generator matrix $G = [I_{n-1} \ \overline{\mathbf{X}}_{(1,0)}]$ where $\overline{\mathbf{X}}_{(1,0)} = [B_1 \ B_2 \ \ldots \ B_k]$ generates a binary QC code of rate $1/(k+1)$ with parameters $[(k+1)(n-1), n-1]$

Some Properties of derived QC Codes

An Upper Bound on the Minimum Distance

Let a binary $[(k+1)(n-1), n-1]$ QC code constructed from a k-circulant SSD. Then its minimum distance d is upper bounded by $\frac{kn}{2}+1$, i.e. $d \leq \frac{kn}{2}+1$.

Equivalence of Supersaturated Designs

Two supersaturated designs are equivalent if one can be transformed into the other by a series of row or column:

- permutations
- negations

Equivalence of QC Codes

Equivalent k-circulant supersaturated designs produce equivalent binary *QC* codes

$E(s^2)$-Optimal Supersaturated Designs

- An experimenter is interested to find designs as near orthogonal as possible.

$E(s^2)$-Criterion

Consider s_{ij} to be the element in the i-th row and j-th column of the information matrix $\mathbf{X}^T_{(-1,1)}\mathbf{X}_{(-1,1)}$. Booth and Cox (1962) proposed as a criterion for comparing designs the minimization of average of s_{ij}^2, denoted by $E(s^2)$, where $E(s^2) = \sum_{1\leq i<j\leq m} s_{ij}^2 / \begin{pmatrix} m \\ 2 \end{pmatrix}$

- $E(s^2)$-Optimal SSD: If the sum of squares of the elements of $\mathbf{X}_{(-1,1)}\mathbf{X}^T_{(-1,1)}$ and $\mathbf{X}^T_{(-1,1)}\mathbf{X}_{(-1,1)}$ reach the minimum.

$E(s^2)$-Optimal Supersaturated Designs over $GF(2)$

Theorem

Let a k-circulant supersaturated design with $(n-1)$ rows and $k(n-1)$ columns with design matrix $\mathbf{X}_{(1,0)}$. Then, it is $E(s^2)$-optimal over $GF(2)$ if

$$D = \mathbf{X}_{(1,0)}\mathbf{X}_{(1,0)}^T = \begin{bmatrix} \frac{kn}{2} & \frac{kn}{4} & \frac{kn}{4} & \cdots & \frac{kn}{4} & \frac{kn}{4} \\ \frac{kn}{4} & \frac{kn}{2} & \frac{kn}{4} & \cdots & \frac{kn}{4} & \frac{kn}{4} \\ \frac{kn}{4} & \frac{kn}{4} & \frac{kn}{2} & \cdots & \frac{kn}{4} & \frac{kn}{4} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \frac{kn}{4} & \frac{kn}{4} & \frac{kn}{4} & \cdots & \frac{kn}{4} & \frac{kn}{2} \end{bmatrix} = \frac{kn}{4}\mathbf{I}_{n-1} + \frac{kn}{4}\mathbf{J}_{n-1}$$

Necessary Condition for Optimality

kn must be divisible by 4, i.e. $kn \equiv 0 \mod 4$

LCD QC Codes from $E(s^2)$-Optimal SSDs

Theorem

Let an $E(s^2)$ optimal k-circulant SSD with n rows and $k(n-1)$ columns with design matrix $\mathbf{X}_{(-1,1)}$. Then the binary $[(k+1)(n-1), n-1]$ QC code constructed by our method is LCD if:

(i) $n \equiv 0(mod 4)$ and k is even.

(ii) $n \equiv 0(mod 8)$ and k is odd.

(iii) $n \equiv 2(mod 4)$ and $k \equiv 0(mod 4)$.

LCD QC Codes from $E(s^2)$-Optimal SSDs (Cont.)

- There exist $E(s^2)$-optimal k-circulant SSDs with n runs and $m = k(n-1)$ factors for $(n, m) \in M$ where $M = \{(8, 14), (8, 21), (8, 28), (8, 35), (10, 36), (12, 22), (12, 44), (12, 66), (12, 88), (14, 52), (16, 30), (16, 45), (16, 60), (16, 75), (20, 38)\}$

LCD QC Codes from $E(s^2)$-Optimal SSDs (Cont.)

- There exist $E(s^2)$-optimal k-circulant SSDs with n runs and $m = k(n-1)$ factors for $(n, m) \in M$ where $M = \{(8,14), (8,21), (8,28), (8,35), (10,36), (12,22), (12,44), (12,66), (12,88), (14,52), (16,30), (16,45), (16,60), (16,75), (20,38)\}$

Some new LCD QC Codes

There exist LCD QC codes with parameters,

(i) $[21, 7], [33, 11], [45, 15], [57, 19]$ of rate $1/3$.

(ii) $[28, 7], [60, 15]$ of rate $1/4$.

(iii) $[35, 7], [45, 9], [55, 11], [65, 13], [75, 15]$ of rate $1/5$.

(iv) $[42, 7], [90, 15]$ of rate $1/6$.

(v) $[77, 11]$ of rate $1/7$.

(vi) $[99, 11]$ of rate $1/9$.

Formulation of the Genetic Algorithm

1. Chromosome Representation: A binary string of length pm corresponding to the first row of the generator matrix of a $[pm, m]$ QC Code
2. Initial Population: Random samples of k-circulant SSDs
   - **Sample** 100000000000000; 110010001111010; 110101111000100 for a $1/3$ rate QC code
3. Objective Function (OF): Maximize

$$OF = \frac{d_C + (p-1) \cdot d_{C^\perp}}{p}$$

   - **Optimal Solution** when d_C attains the current d_{LB} of linear codes
4. Genetic operators: Standard reproduction, crossover and mutation

Bounds on the Minimum Distance of QC Codes

- Best Code: Achieves the maximum possible minimum distance for a given class of linear codes
- Good Code: Attains the known lower bound on the minimum distance of a linear code
- Optimal Code: Achieves the maximum possible minimum distance for a linear code with the same parameters

Bounds on the Minimum Distance of QC Codes

- Best Code: Achieves the maximum possible minimum distance for a given class of linear codes
- Good Code: Attains the known lower bound on the minimum distance of a linear code
- Optimal Code: Achieves the maximum possible minimum distance for a linear code with the same parameters

Bounds on the Minimum distance of linear codes

`www.codetables.de` maintained by Marcus Grassl.

Bounds on the Minimum distance of binary QC codes

"Web Database of Binary QC Codes" maintained by E. Z. Chen.

Bounds on the Minimum distance of binary QC codes (Cont.)

- All computations on the minimum distance d_{QC} and code equivalence have been performed in MAGMA
- d_{LB}: The current lower bound on the minimum distance of QC and linear codes retrieved by Chen and Grassl Tables
- d_{UB}: The theoretical upper bound
- All good or best QC codes we have found are inequivalent when compared to the respective QC or linear codes with the same parameters (except for two cases)

Binary QC codes of rate $1/4$

A good $[44, 11, 16]$ LCD code

```
[ 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1 ]
[ 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1 ]
[ 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0 ]
```

Code	d_{QC}	$[d_{Lb}, d_{Ub}]$
$[20, 5]$	9	9
$[28, 7]$	12	12
$[36, 9]$	14	14
$[44, 11]$	16	16-17
$[52, 13]$	19	19-20
$[76, 19]$	24	24-28

Table: Minimum distances of binary QC codes of rate $1/4$

Binary QC codes of rate $1/5$

A good $[45, 9, 18]$ LCD code

```
[ 1, 0, 0, 1, 0, 1, 0, 1, 0 ]
[ 1, 0, 1, 0, 1, 0, 0, 0, 1 ]
[ 0, 0, 1, 1, 0, 1, 1, 0, 1 ]
[ 0, 1, 1, 1, 1, 1, 0, 0, 0 ]
```

Code	d_{QC}	$[d_{Lb}, d_{Ub}]$
$[25, 5]$	12	12
$[35, 7]$	16	16
$[45, 9]$	18	18-19
$[55, 11]$	21	22-23

Table: Minimum distances of binary QC codes of rate $1/5$

Binary QC codes of rate $1/6$

A best $[42, 7, 19]$ code

```
[ 0, 1, 0, 0, 1, 0, 1 ]
[ 0, 0, 1, 0, 1, 1, 0 ]
[ 0, 1, 1, 0, 0, 1, 1 ]
[ 1, 0, 0, 0, 1, 1, 0 ]
[ 1, 1, 1, 0, 1, 0, 1 ]
```

Code	d_{QC}	$[d_{Lb}, d_{Ub}]$
$[30, 5]$	15	15
$[42, 7]$	19	19
$[54, 9]$	23	23-24

Table: Minimum distances of binary QC codes of rate $1/6$

Conclusion

1. We gave a construction method for QC codes from cyclic-structured designs

Conclusion

1. We gave a construction method for QC codes from cyclic-structured designs
2. We established a link between LCD QC codes and optimal designs

Conclusion

1. We gave a construction method for QC codes from cyclic-structured designs
2. We established a link between LCD QC codes and optimal designs
3. We constructed some good QC codes via a heuristic search

Conclusion

1. We gave a construction method for QC codes from cyclic-structured designs
2. We established a link between LCD QC codes and optimal designs
3. We constructed some good QC codes via a heuristic search

Future Work

- Explore the structure of supersaturated designs over $GF(q)$ and derive analoque QC Codes

Conclusion

1. We gave a construction method for QC codes from cyclic-structured designs
2. We established a link between LCD QC codes and optimal designs
3. We constructed some good QC codes via a heuristic search

Future Work

- Explore the structure of supersaturated designs over $GF(q)$ and derive analoque QC Codes
- Find new QC Codes over $GF(q)$

References

- Ling, S, Solé, P.: On the algebraic structure of quasi-cyclic codes I: finite fields, *IEEE Transactions on Information Theory*, **47** (2001), 2751–2760.
- Liu, Y., Dean, A.: *k*-circulant supersaturated designs, *Technometrics*, **46** (2004), 32–46.
- Massey, J.L.: Linear codes with complementary duals, *Discrete Math.*, **106/107** (1992), 337–342.
- Sendrier, N.: Linear codes with complementary duals meet the Gilbert-Varshamov bound, *Discrete Math.*, **285** (2004), 345–347.
- Vaessens, R.J.M., Aarts, E.H.L., van Lint, J.H.: Genetic algorithms in coding theory - a table for $A_3(n, d)$, *Discrete Appl. Math.*, **45** (1993), 71–87.