SOME NEW QUASI-CYCLIC SELF-DUAL CODES

Pınar Çomak, J-L. Kim, F. Özbudak

Institute of Applied Mathematics
Middle East Technical University, Ankara, Turkey

June 21, 2016
15th International Workshop on ACCT,
Albena, Bulgaria

Outline

1. Introduction

Outline

1. Introduction
2. Quasi-Cyclic Codes

Outline

Outline

Outline

1. Introduction
2. Quasi-Cyclic Codes
3. Construction of Quasi-Cyclic Self-Dual Codes
4. New Codes
5. Conclusion

Linear codes

Definition

A q-ary linear code $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$. If $\mathcal{C}$ has dimension k and minimum distance d then $\mathcal{C}$ is called an $[n, k, d]$ linear code.

Linear codes

Definition

A q-ary linear code $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$. If $\mathcal{C}$ has dimension k and minimum distance d then $\mathcal{C}$ is called an $[n, k, d]$ linear code.

- the minimum Hamming distance $d(\mathcal{C})$ is the minimum number of distinct coordinates between any pair of distinct codewords.
- the weight $w(c)$ of a codeword c in $\mathbb{F}_q^n$ is defined to be the number of non-zero entries of c.

Linear codes

Definition

A q-ary linear code $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$. If $\mathcal{C}$ has dimension k and minimum distance d then $\mathcal{C}$ is called an $[n, k, d]$ linear code.

- the minimum Hamming distance $d(\mathcal{C})$ is the minimum number of distinct coordinates between any pair of distinct codewords.
- the weight $w(c)$ of a codeword c in $\mathbb{F}_q^n$ is defined to be the number of non-zero entries of c.

For a linear code, the minimum distance is equal to the smallest weight of the nonzero codewords. i.e.
$d(\mathcal{C}) = w(c - c') \geq w(\mathcal{C}) = w(c) = d(c, \mathbf{0}) \geq d(\mathcal{C})$

Weight enumerators

The number of codewords of $\mathcal{C}$ having Hamming weight equal to i by A_i. The Hamming weight enumerator of the code $\mathcal{C}$ is defined as

$$W_{\mathcal{C}}(y) = \sum_{c \in \mathcal{C}} y^{wt(c)} = \sum_{i=0}^{n} A_i y^i.$$

Inner products

The Euclidean inner product is defined on $\mathbb{F}_q^{\ell m}$ as

$$(a, b) = a \cdot b = \sum_{i=0}^{m-1} \sum_{j=0}^{\ell-1} a_{ij} b_{ij}$$

for

$$a = (a_{0,0}, a_{0,1}, \ldots, a_{0,\ell-1}, a_{1,0}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1})$$

and

$$b = (b_{0,0}, b_{0,1}, \ldots, b_{0,\ell-1}, b_{1,0}, \ldots, b_{1,\ell-1}, \ldots, b_{m-1,0}, \ldots, b_{m-1,\ell-1})$$

Inner products

The Hermitian inner product is defined on $\mathcal{R}^\ell = \mathbb{F}_q[Y]^\ell/(Y^m - 1)$ as

$$(x, y) = \langle x, y \rangle = \sum_{j=0}^{\ell-1} x_j \overline{y_j}$$

for

$$x = (x_0, x_1, \ldots, x_{\ell-1}) \quad and \quad y = (y_0, y_1, \ldots, y_{\ell-1})$$

Inner products

The Hermitian inner product is defined on $\mathcal{R}^\ell = \mathbb{F}_q[Y]^\ell/(Y^m - 1)$ as

$$(x, y) = \langle x, y \rangle = \sum_{j=0}^{\ell-1} x_j \overline{y_j}$$

for

$$x = (x_0, x_1, \ldots, x_{\ell-1}) \quad and \quad y = (y_0, y_1, \ldots, y_{\ell-1})$$

Here the conjugation map $^-$ on $\mathcal{R}$ is a map sending Y to $Y^{-1} = Y^{m-1}$ and it acts as the identity map on $\mathbb{F}_q$.

Duality

Dual codes

The dual of a code $\mathcal{C}$ is $\mathcal{C}^{\perp} = \{u \in \mathbb{F}^n : (u, v) = 0 \text{ for all } v \in \mathcal{C}\}$.

Suppose $\mathcal{C}$ is an $[n, k]$ code over $\mathbb{F}_q$. Then the dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is a linear $[n, n-k]$ code.

Duality

Dual codes

The dual of a code $\mathcal{C}$ is $\mathcal{C}^\perp = \{u \in \mathbb{F}^n : (u, v) = 0 \text{ for all } v \in \mathcal{C}\}$.

Suppose $\mathcal{C}$ is an $[n, k]$ code over $\mathbb{F}_q$. Then the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$ is a linear $[n, n-k]$ code.

A code $\mathcal{C}$ is said to be self-dual if $\mathcal{C} = \mathcal{C}^\perp$. Note that self-dual codes are of the form $[n, n/2]$.

Duality

Dual codes

The dual of a code $\mathcal{C}$ is $\mathcal{C}^{\perp} = \{u \in \mathbb{F}^n : (u, v) = 0 \text{ for all } v \in \mathcal{C}\}$.

Suppose $\mathcal{C}$ is an $[n, k]$ code over $\mathbb{F}_q$. Then the dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is a linear $[n, n-k]$ code.

A code $\mathcal{C}$ is said to be self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$. Note that self-dual codes are of the form $[n, n/2]$.

If the weight of each codeword is divisible by 4 then the self-dual codes are called Type II. Otherwise, they are called Type I self-dual codes.

Cyclic codes

Definition

An $[n, k]$ linear code $\mathcal{C}$ is said to be cyclic if for every codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then there is the corresponding codeword $c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.

Cyclic codes

Definition

An $[n, k]$ linear code $\mathcal{C}$ is said to be cyclic if for every codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then there is the corresponding codeword $c' = (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$.

Polynomial representation

The codeword

$$c = (c_0, c_1, \ldots, c_{n-1})$$

can be represented by the polynomial

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}.$$

Cyclic shift

With polynomial representation, a cyclic shift can be represented as follows:

$$xc(x) = c_0x + c_1x^2 + c_2x^3 + \cdots + c_{n-1}x^n$$

in *mod* $(x^n - 1)$ is

$$xc(x) \quad mod\ (x^n - 1) = c_{n-1} + c_0x + c_1x^2 + c_2x^3 + \cdots + c_{n-2}x^{n-1}.$$

Quasi-cyclic codes

Let $\mathbb{F}_q$ be a finite field and m be a positive integer coprime with the characteristic of $\mathbb{F}_q$.

Quasi-cyclic codes

Let $\mathbb{F}_q$ be a finite field and m be a positive integer coprime with the characteristic of $\mathbb{F}_q$.

Definition

A linear code $\mathcal{C}$ of length ℓm over $\mathbb{F}_q$ is called ℓ-quasi-cyclic code if the codeword

$$(c_{0,0}, \ldots, c_{0,\ell-1}, c_{1,0}, \ldots, c_{1,\ell-1}, \ldots, c_{m-1,0}, \ldots, c_{m-1,\ell-1}) \in \mathcal{C}$$

then

$$(c_{m-1,0}, \ldots, c_{m-1,\ell-1}, c_{0,0}, \ldots, c_{0,\ell-1}, \ldots, c_{m-2,0}, \ldots, c_{m-2,\ell-1}) \in \mathcal{C}.$$

1-1 correspondence

Let $\mathcal{R} = \mathbb{F}_q[Y]/(Y^m - 1)$. Define a map $\phi : \mathbb{F}_q^{\ell m} \to \mathcal{R}^\ell$ by

$$\phi(c) = (c_0(Y), c_1(Y), \ldots, c_{\ell-1}(Y)) \in \mathcal{R}^\ell$$

1-1 correspondence

Let $\mathcal{R} = \mathbb{F}_q[Y]/(Y^m - 1)$. Define a map $\phi : \mathbb{F}_q^{\ell m} \to \mathcal{R}^\ell$ by

$$\phi(c) = (c_0(Y), c_1(Y), \ldots, c_{\ell-1}(Y)) \in \mathcal{R}^\ell$$

where $c_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in \mathcal{R}, \quad j = 0, \ldots, \ell - 1.$

1-1 correspondence

Let $\mathcal{R} = \mathbb{F}_q[Y]/(Y^m - 1)$. Define a map $\phi : \mathbb{F}_q^{\ell m} \to \mathcal{R}^\ell$ by

$$\phi(c) = (c_0(Y), c_1(Y), \ldots, c_{\ell-1}(Y)) \in \mathcal{R}^\ell$$

where $c_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in \mathcal{R}, \quad j = 0, \ldots, \ell - 1.$

The map ϕ gives a one-to-one correspondence between ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of length ℓm and linear codes over $\mathcal{R}$ of length ℓ.

1-1 correspondence

Let $\mathcal{R} = \mathbb{F}_q[Y]/(Y^m - 1)$. Define a map $\phi : \mathbb{F}_q^{\ell m} \to \mathcal{R}^\ell$ by

$$\phi(c) = (c_0(Y), c_1(Y), \ldots, c_{\ell-1}(Y)) \in \mathcal{R}^\ell$$

where $c_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in \mathcal{R}, \quad j = 0, \ldots, \ell - 1.$

The map ϕ gives a one-to-one correspondence between ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of length ℓm and linear codes over $\mathcal{R}$ of length ℓ.

$$(T^{\ell k}(a)) \cdot b = 0 \Leftrightarrow \langle \phi(a), \phi(b) \rangle = 0$$

for $a, b \in \mathbb{F}_q^{\ell m}$, $\forall k \in \{0, \cdots, m-1\}$.

1-1 correspondence

Let $\mathcal{R} = \mathbb{F}_q[Y]/(Y^m - 1)$. Define a map $\phi : \mathbb{F}_q^{\ell m} \to \mathcal{R}^\ell$ by

$$\phi(c) = (c_0(Y), c_1(Y), \ldots, c_{\ell-1}(Y)) \in \mathcal{R}^\ell$$

where $c_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in \mathcal{R}, \quad j = 0, \ldots, \ell - 1.$

The map ϕ gives a one-to-one correspondence between ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of length ℓm and linear codes over $\mathcal{R}$ of length ℓ.

$$(T^{\ell k}(a)) \cdot b = 0 \Leftrightarrow \langle \phi(a), \phi(b) \rangle = 0$$

for $a, b \in \mathbb{F}_q^{\ell m}$, $\forall k \in \{0, \cdots, m-1\}$.

It follows $\phi(\mathcal{C})^\perp = \phi(\mathcal{C}^\perp)$, where the dual in $\mathbb{F}_q^{\ell m}$ is taken w.r.t. the Euclidean inner product, while the dual in $\mathcal{R}^\ell$ is taken w.r.t. the Hermitian inner product.

Ring Decomposition

The polynomial $Y^m - 1$ factors completely into distinct irreducible factors in $\mathbb{F}_q[Y]$ as $Y^m - 1 = \delta g_1 \ldots g_s h_1 h_1^* \ldots h_t h_t^*$ where δ is nonzero in $\mathbb{F}_q$, $g_1 \ldots g_s$ are the polynomials which are self-reciprocal, and h_i^*'s are reciprocals of h_i's, for all $1 \leq i \leq t$.

Ring Decomposition

The polynomial $Y^m - 1$ factors completely into distinct irreducible factors in $\mathbb{F}_q[Y]$ as $Y^m - 1 = \delta g_1 \dots g_s h_1 h_1^* \dots h_t h_t^*$ where δ is nonzero in $\mathbb{F}_q$, $g_1 \dots g_s$ are the polynomials which are self-reciprocal, and h_i^*'s are reciprocals of h_i's, for all $1 \leq i \leq t$. The ring $\mathcal{R}$ can be decomposed as

$$\mathcal{R} = \frac{F_q[Y]}{(Y^m - 1)} = \left(\bigoplus_{i=1}^{s} \frac{F_q[Y]}{(g_i)} \right) \oplus \left(\bigoplus_{j=1}^{t} \left(\frac{F_q[Y]}{(h_j)} \oplus \frac{F_q[Y]}{(h_j^*)} \right) \right)$$

by Chinese Remainder Theorem.

Ring Decomposition

By CRT, every $\mathcal{R}$-linear code $\mathcal{C}$ of length ℓ can be decomposed as the direct sum

$$\mathcal{C} = \left(\bigoplus_{i=1}^{s} \mathcal{C}_i \right) \oplus \left(\bigoplus_{j=1}^{t} \left(\mathcal{C}_j' \oplus \mathcal{C}_j'' \right) \right)$$

where $\mathcal{C}_i$, $\mathcal{C}_j'$ and $\mathcal{C}_j''$ are linear codes over $F_q[Y]/(g_i)$, $F_q[Y]/(h_j)$ and $F_q[Y]/(h_j^*)$, respectively, all of length ℓ for each $1 \leq i \leq s$, and for each $1 \leq j \leq t$.

Ring Decomposition

Theorem

An ℓ-quasi-cyclic code $\mathcal{C}$ of length ℓm over $\mathbb{F}_q$, is self-dual if and only if

$$\mathcal{C} = \left(\bigoplus_{i=1}^{s} \mathcal{C}_i \right) \oplus \left(\bigoplus_{j=1}^{t} \left(\mathcal{C}_j' \oplus (\mathcal{C}_j')^{\perp} \right) \right)$$

where, for $1 \leq i \leq s$, $\mathcal{C}_i$ is a self-dual code of length ℓ w.r.t. the Hermitian inner product and for $1 \leq j \leq t$, $\mathcal{C}_j'$ is a linear code of length ℓ and $(\mathcal{C}')^{\perp}$ is its dual w.r.t. the Euclidean inner product.

Existence of Self-Dual Codes

Let $\mathcal{R} = \mathcal{R}(\mathbb{F}_q, m) = \mathbb{F}_q[Y]/(Y^m - 1)$.

Proposition

If $char(\mathbb{F}_q) = 2$, then there exists a self-dual code of length ℓ over $\mathcal{R}$ if and only if $2 \mid \ell$.

Existence of Self-Dual Codes

Let $\mathcal{R} = \mathcal{R}(\mathbb{F}_q, m) = \mathbb{F}_q[Y]/(Y^m - 1)$.

Proposition

If $char(\mathbb{F}_q) = 2$, then there exists a self-dual code of length ℓ over $\mathcal{R}$ if and only if $2 \mid \ell$.

The following lemma helps us to complete the classification of quasi-cyclic self-dual codes.

Lemma

Let $\mathcal{C}$ be a binary ℓ-quasi-cyclic self-dual code of length $m\ell$ with m prime. If m does not divide the weight i, then m must divide A_i.

Binary Cubic Codes

Let $q = 2$ and $m = 3$.

Binary Cubic Codes

Let $q = 2$ and $m = 3$. $Y^3 - 1 = (Y - 1)(Y^2 + Y + 1)$ over $\mathbb{F}_2$.

Binary Cubic Codes

Let $q = 2$ and $m = 3$. $Y^3 - 1 = (Y - 1)(Y^2 + Y + 1)$ over $\mathbb{F}_2$.

Then,

$$\mathcal{R} = \frac{\mathbb{F}_2[Y]}{(Y^3-1)} = \mathbb{F}_2 \oplus \mathbb{F}_{2^2}.$$

Binary Cubic Codes

Let $q = 2$ and $m = 3$. $Y^3 - 1 = (Y - 1)(Y^2 + Y + 1)$ over $\mathbb{F}_2$.

Then,

$$\mathcal{R} = \frac{\mathbb{F}_2[Y]}{(Y^3-1)} = \mathbb{F}_2 \oplus \mathbb{F}_{2^2}.$$

Remark that

Cubic binary codes of length 3ℓ are viewed as codes of length ℓ over the ring $\mathbb{F}_2 \times \mathbb{F}_4$.

Binary Cubic Codes

Cubic Construction

$\mathcal{C}$ is constructed by *Cubic Construction* as

$\mathcal{C} = \{ \ (\ x + b \mid x + a \mid x + a + b \ ) \mid x \in \mathcal{C}_1, \ a + \omega b \in \mathcal{C}_2 \}$,

where $\omega^2 + \omega + 1 = 0$.

Binary Cubic Codes

Cubic Construction

$\mathcal{C}$ is constructed by *Cubic Construction* as
$\mathcal{C} = \{ \ (\ x + b \mid x + a \mid x + a + b \ ) \mid x \in \mathcal{C}_1, \ a + \omega b \in \mathcal{C}_2 \}$,
where $\omega^2 + \omega + 1 = 0$.

This gives a correspondence between the self-dual ℓ-quasi-cyclic codes $\mathcal{C}$ of length 3ℓ over $\mathbb{F}_2$ and a pair $(\mathcal{C}_1, \mathcal{C}_2)$, where $\mathcal{C}_1$ is a self-dual linear code w.r.t. Euclidean inner product over $\mathbb{F}_2$ of length ℓ and $\mathcal{C}_2$ is a self-dual linear code w.r.t. Hermitian inner product over F_{2^2} of length ℓ.

The Complete Classification

Theorem

Up to permutation equivalence the numbers of cubic self-dual codes of lengths up to 48 are as follows:
There is/are
for $\ell = 2$, unique binary cubic self-dual code of length 6,
for $\ell = 4$, 2 binary cubic self-dual codes of length 12,
for $\ell = 6$, 3 binary cubic self-dual codes of length 18,
for $\ell = 8$, 16 binary cubic self-dual codes of length 24,
for $\ell = 10$, 8 binary cubic self-dual codes of length 30,
for $\ell = 12$, 13 binary cubic self-dual codes of length 36,
for $\ell = 14$, 1569 binary cubic self-dual codes of length 42,
for $\ell = 16$, 264 binary cubic self-dual codes of length 48.

Construction of cubic self-dual codes of index 18

The shortest length of binary cubic self-dual codes for which the classification is not completed is $\ell = 18$.

Construction of cubic self-dual codes of index 18

The shortest length of binary cubic self-dual codes for which the classification is not completed is $\ell = 18$.

For self-dual $[54, 27, 10]$ codes, there are two *weight enumerators*:

$$W_1 = 1 + (351 - 8\beta)y^{10} + (5031 + 24\beta)y^{12} + \dots \quad 0 \leq \beta \leq 43$$
$$W_2 = 1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12} + \dots \quad 12 \leq \beta \leq 43.$$

Construction of cubic self-dual codes of index 18

Previous results

Before our work, it was known that seven inequivalent codes with W_1 for $\beta = 0, 3, 6, 9, 12, 15, 18$ and six inequivalent codes with W_2 for $\beta = 12, 15, 18, 21, 24, 27$ were found.

Construction of cubic self-dual codes of index 18

Previous results

Before our work, it was known that seven inequivalent codes with W_1 for $\beta = 0, 3, 6, 9, 12, 15, 18$ and six inequivalent codes with W_2 for $\beta = 12, 15, 18, 21, 24, 27$ were found.

Our results

We improve the results by finding eight $[54, 27, 10]$ codes with W_1 for $\beta = 0, 3, 6, 9, 12, 15, 18, 21$ and six $[54, 27, 10]$ codes with W_2 for $\beta = 12, 15, 18, 21, 24, 27$ by taking $\mathcal{C}_1$'s from extremal self-dual binary codes and $\mathcal{C}_2$'s from not extremal self-dual quaternary codes. For W_1, the value $\beta = 21$ is the new one.

Construction of cubic self-dual codes of index 18

Remark

These $[54, 27, 10]$ codes are of Type I 18-quasi-cyclic self-dual codes of length 54 since their binary components $\mathcal{C}_1$'s are of Type I and self-dual with respect to the Euclidean inner product.

Construction of cubic self-dual codes of index 18

Conjecture

Based on computational evidence, we conjecture that there is no other $[54, 27, 10]$ self-dual cubic code over $\mathbb{F}_2$.

Construction of cubic self-dual codes of index 18

Conjecture

Based on computational evidence, we conjecture that there is no other $[54, 27, 10]$ self-dual cubic code over $\mathbb{F}_2$.

Our computational results are listed above:

	Possible values	Found values	Conjecture
W_1	$0 \leq \beta \leq 43$	$\beta \in \{0, 3, 6, 9, 12, 15, 18, 21\}$	$\beta \notin \{24, \cdots, 42\}$
W_2	$12 \leq \beta \leq 43$	$\beta \in \{12, 15, 18, 21, 24, 27\}$	$\beta \notin \{30, \cdots, 42\}$

Future Work

This construction will be applied in order to find more binary self-dual codes of larger lengths.

THANK YOU!

References

J. Baylis, *Error Correcting Codes A Mathematical Introduction*, Chapman and Hall Mathematics, 1998.

R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company, 1984.

A. Bonnecaze, A.D. Bracco, S.T. Dougherty, L.R. Nochefranca, P. Solé, *Cubic self-dual binary codes*, IEEE Trans. Inform. Theory., vol. 49, no. 9, pp. 2253-2259, Sep. 2003.

S. Bouyuklieva, P.R.J. Östergård, *New constructions of optimal self-dual binary codes of length 54*, Des Codes Crypt. vol. 41, pp.101-109, 2006.

S. Bouyuklieva, N. Yankov, J.-L. Kim, *Classification of binary self-dual* $[48, 24, 10]$ *codes with an automorphism of odd prime order*, Finite Fields and Their Appl., vol. 18, no. 6, pp. 1104-1113, 2012.

References

S. Han, J.-L. Kim, H. Lee and Y. Lee, *Construction of quasi-cyclic self-dual codes*, Finite Fields and Their Appl., vol. 18, no. 3, pp. 613-633, 2012.

R. Hill, *A First Course in Coding Theory*, Clarendon Press, Oxford, 1986.

W.C. Huffman, V. Pless, *Fundamentals of Error-correcting Codes*, Cambridge University Press, Cambridge, 2003.

J.-L. Kim, Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields*, J. Combin. Theory Ser. A. vol. 105, pp. 79-95, 2004.

R. Lidl, H. Niederreiter, *Finite Fields*, Addison-Wesley Publishing Company, 1983.

References

S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes I, Finite fields* IEEE Trans. Inform. Theory. vol. 47, pp. 2751-2760, 2001.

F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands, North-Holland, 1977.

A.Munemasa, http://math.is.tohoku.ac.jp/~munemasa/research/codes/sd2.htm

V. Pless, *A classification of self-orthogonal codes over GF(2)*, Discrete Math., vol. 3, pp. 209-246, 1972.

E. Rains and N.J.A. Sloane, *Self-dual codes*, in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998.