BOUNDS ON MINIMUM DISTANCE IN CONSTACYCLIC CODES

DIANA RADKOVA, A. J. VAN ZANTEN

“St. Kl. Ohridski" University of Sofia,
Faculty of Mathematics and Informatics
Department of Algebra
5 James Bouchier Blvd., 1164 Sofia, Bulgaria

Delft University of Technology,
Faculty of Information Technology and Systems
Department of Mathematics,
P.O. Box 5031, 2600 GA Delft, The Netherlands

18.06.2008

Definition

Let a be a nonzero element of $F = \mathrm{GF}(q)$. A code C of length n over F is called constacyclic with respect to a, if whenever $\mathbf{x} = (c_1, c_2, \ldots, c_n)$ is in C, so is $\mathbf{y} = (ac_n, c_1, \ldots, c_{n-1})$.

Definition

Let a be a nonzero element of $F = \mathrm{GF}(q)$. A code C of length n over F is called constacyclic with respect to a, if whenever $\mathbf{x} = (c_1, c_2, \ldots, c_n)$ is in C, so is $\mathbf{y} = (ac_n, c_1, \ldots, c_{n-1})$.

- Let $0 \neq a \in F$ and let

$$\psi_a : \begin{cases} F^n \to F^n \\ (x_1, x_2, \ldots, x_n) \mapsto (ax_n, x_1, \ldots, x_{n-1}) \end{cases}.$$

Definition

Let a be a nonzero element of $F = \mathrm{GF}(q)$. A code C of length n over F is called constacyclic with respect to a, if whenever $\mathbf{x} = (c_1, c_2, \ldots, c_n)$ is in C, so is $\mathbf{y} = (ac_n, c_1, \ldots, c_{n-1})$.

- Let $0 \neq a \in F$ and let

$$\psi_a : \begin{cases} F^n \to F^n \\ (x_1, x_2, \ldots, x_n) \mapsto (ax_n, x_1, \ldots, x_{n-1}) \end{cases}.$$

- Then $\psi_a \in \mathrm{Hom}\, F^n$ and it has the following matrix

$$A(n,a) = A = \begin{pmatrix} 0 & 0 & 0 & \ldots & a \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

with respect to the standard basis $e = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$.

- The characteristic polynomial of A is

  $$f_A(x) = (-1)^n(x^n - a) = f(x).$$

- The characteristic polynomial of A is

  $$f_A(x) = (-1)^n(x^n - a) = f(x).$$

- Let $f(x) = (-1)^n f_1(x) \dots f_t(x)$ be the factorization of $f(x)$ into irreducible factors over F.

- The characteristic polynomial of A is

  $$f_A(x) = (-1)^n(x^n - a) = f(x).$$

- Let $f(x) = (-1)^n f_1(x) \dots f_t(x)$ be the factorization of $f(x)$ into irreducible factors over F.

- $U_i = \mathrm{Ker}\, f_i(\psi_a),\ i = 1, \dots, t.$

Theorem

Let C be a linear constacyclic code of length n over F. Then the following facts hold:

Theorem

Let C be a linear constacyclic code of length n over F. Then the following facts hold:

1) C is a constacyclic code iff C is a ψ_a-invariant subspace of F^n;

Theorem

Let C be a linear constacyclic code of length n over F. Then the following facts hold:

1) C is a constacyclic code iff C is a ψ_a-invariant subspace of F^n;

2) $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ for some minimal ψ_a-invariant subspaces U_{i_r} of F^n and $k := \dim_F C = k_{i_1} + \cdots + k_{i_s}$;

Theorem

Let C be a linear constacyclic code of length n over F. Then the following facts hold:

1) C is a constacyclic code iff C is a ψ_a-invariant subspace of F^n;

2) $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ for some minimal ψ_a-invariant subspaces U_{i_r} of F^n and $k := \dim_F C = k_{i_1} + \cdots + k_{i_s}$;

3) $f_{\psi_a|_C}(x) = (-1)^k f_{i_1}(x) \ldots f_{i_s}(x) = g(x)$;

Theorem

Let C be a linear constacyclic code of length n over F. Then the following facts hold:

1) C is a constacyclic code iff C is a ψ_a-invariant subspace of F^n;

2) $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ for some minimal ψ_a-invariant subspaces U_{i_r} of F^n and $k := \dim_F C = k_{i_1} + \cdots + k_{i_s}$;

3) $f_{\psi_a|_C}(x) = (-1)^k f_{i_1}(x) \ldots f_{i_s}(x) = g(x)$;

4) $\mathbf{c} \in C$ iff $g(A)\mathbf{c} = \mathbf{0}$;

Theorem

Let C be a linear constacyclic code of length n over F. Then the following facts hold:

1) C is a constacyclic code iff C is a ψ_a-invariant subspace of F^n;

2) $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ for some minimal ψ_a-invariant subspaces U_{i_r} of F^n and $k := \dim_F C = k_{i_1} + \cdots + k_{i_s}$;

3) $f_{\psi_a|_C}(x) = (-1)^k f_{i_1}(x) \ldots f_{i_s}(x) = g(x)$;

4) $\mathbf{c} \in C$ iff $g(A)\mathbf{c} = \mathbf{0}$;

5) the polynomial $g(x)$ has the smallest degree with respect to property 4);

Theorem

Let C be a linear constacyclic code of length n over F. Then the following facts hold:

1) C is a constacyclic code iff C is a ψ_a-invariant subspace of F^n;

2) $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ for some minimal ψ_a-invariant subspaces U_{i_r} of F^n and $k := \dim_F C = k_{i_1} + \cdots + k_{i_s}$;

3) $f_{\psi_a|_C}(x) = (-1)^k f_{i_1}(x) \ldots f_{i_s}(x) = g(x)$;

4) $\mathbf{c} \in C$ iff $g(A)\mathbf{c} = \mathbf{0}$;

5) the polynomial $g(x)$ has the smallest degree with respect to property 4);

6) $\operatorname{rank}(g(A)) = n - k$.

Theorem

Let C be a linear constacyclic code of length n over F. Then the following facts hold:

1) C is a constacyclic code iff C is a ψ_a-invariant subspace of F^n;

2) $C = U_{i_1} \oplus \cdots \oplus U_{i_s}$ for some minimal ψ_a-invariant subspaces U_{i_r} of F^n and $k := \dim_F C = k_{i_1} + \cdots + k_{i_s}$;

3) $f_{\psi_a|_C}(x) = (-1)^k f_{i_1}(x) \dots f_{i_s}(x) = g(x)$;

4) $\mathbf{c} \in C$ iff $g(A)\mathbf{c} = \mathbf{0}$;

5) the polynomial $g(x)$ has the smallest degree with respect to property 4);

6) $\operatorname{rank}(g(A)) = n - k$.

7) The matrix H, the rows of which are an arbitrary set of $n-k$ linearly independent rows of $g(A)$, is a parity check matrix of C.

- Let $K = \mathrm{GF}(q^m)$ be the splitting field of the polynomial $f(x) = (-1)^n(x^n - a)$ over F and let the eigenvalues of ψ_a be $\alpha_1, \ldots, \alpha_n$, where $\alpha_i = \sqrt[n]{a}\alpha^i$.

- Let $K = \mathrm{GF}(q^m)$ be the splitting field of the polynomial $f(x) = (-1)^n(x^n - a)$ over F and let the eigenvalues of ψ_a be $\alpha_1, \ldots, \alpha_n$, where $\alpha_i = \sqrt[n]{a}\alpha^i$.

Theorem

Let C be a linear constacyclic code of length n over F, $g(x) = f_{\psi_a|C}(x)$ and $h(x) = \frac{f(x)}{g(x)}$. Let for some integers $b \geq 1$, and $\delta \geq 1$ the following equalities

$$h(\alpha_b) = h(\alpha_{b+1}) = \cdots = h(\alpha_{b+\delta-2}) = 0$$

hold. Then the minimum distance of the code C is at least δ.

Definition

A set $M = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_l}\}$ of zeros of the polynomial $x^n - a$ in K will be called a consecutive set of length l if a primitive $n-$th root of unity β and an exponent i exist such that $M = \{\beta_i, \beta_{i+1}, \ldots, \beta_{i+l-1}\}$, with $\beta_s = \sqrt[n]{a}\beta^s$.

Definition

A set $M = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_l}\}$ of zeros of the polynomial $x^n - a$ in K will be called a consecutive set of length l if a primitive $n-$th root of unity β and an exponent i exist such that $M = \{\beta_i, \beta_{i+1}, \ldots, \beta_{i+l-1}\}$, with $\beta_s = \sqrt[n]{a}\beta^s$.

Corollary

Let C be a linear constacyclic code of length n over F and let

$$\alpha_b, \alpha_{b+s}, \ldots, \alpha_{b+(\delta-2)s}$$

are zeros of $h(x)$, where $(s, n) = 1$. Then the minimum distance of C is at least δ.

Theorem

Let C be a constacyclic code of length n over the field F, $g(x) = f_{\psi_a|_C}(x), h(x) = \frac{f(x)}{g(x)}$, and let α be a primitive n-th root of unity in K. Assume that there exist integers s, b, c_1 and c_2 where $s \geq 0$, $b \geq 0$, $(n, c_1) = 1$ and $(n, c_2) < \delta$, such that

$$h(\alpha_{b+i_1c_1+i_2c_2}) = 0, \quad 0 \leq i_1 \leq \delta - 2,\ 0 \leq i_2 \leq s.$$

Then the minimum distance d of C satisfies $d \geq \delta + s$.

Theorem

Let C be a constacyclic code of length n over the field F, $g(x) = f_{\psi_a|_C}(x), h(x) = \frac{f(x)}{g(x)}$, and let α be a primitive n-th root of unity in K. Assume that there exist integers s, b, c_1 and c_2 where $s \geq 0$, $b \geq 0$, $(n, c_1) = 1$ and $(n, c_2) < \delta$, such that

$$h(\alpha_{b+i_1c_1+i_2c_2}) = 0, \quad 0 \leq i_1 \leq \delta - 2,\ 0 \leq i_2 \leq s.$$

Then the minimum distance d of C satisfies $d \geq \delta + s$.

Definition

If $N = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_t}\}$ is a set of zeros of the polynomial $x^n - a$, we denote by U_N the matrix of size t by n over K that has $(\alpha_{i_l}, \alpha_{i_l}^2, \ldots, \alpha_{i_l}^n)$ as its $l-$th row, that is,

$$U_N = \begin{pmatrix} \alpha_{i_1} & \alpha_{i_1}^2 & \ldots & \alpha_{i_1}^n \\ \alpha_{i_2} & \alpha_{i_2}^2 & \ldots & \alpha_{i_2}^n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i_t} & \alpha_{i_t}^2 & \ldots & \alpha_{i_t}^n \end{pmatrix}.$$

Definition

If $N = \{\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_t}\}$ is a set of zeros of the polynomial $x^n - a$, we denote by U_N the matrix of size t by n over K that has $(\alpha_{i_l}, \alpha_{i_l}^2, \ldots, \alpha_{i_l}^n)$ as its $l-$th row, that is,

$$U_N = \begin{pmatrix} \alpha_{i_1} & \alpha_{i_1}^2 & \ldots & \alpha_{i_1}^n \\ \alpha_{i_2} & \alpha_{i_2}^2 & \ldots & \alpha_{i_2}^n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i_t} & \alpha_{i_t}^2 & \ldots & \alpha_{i_t}^n \end{pmatrix}.$$

- U_N is a parity check matrix for the constacyclic code C over F having N as a set of zeros of $h(x)$.

Definition

If $N = \{\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_t}\}$ is a set of zeros of the polynomial $x^n - a$, we denote by U_N the matrix of size t by n over K that has $(\alpha_{i_l}, \alpha_{i_l}^2, \dots, \alpha_{i_l}^n)$ as its $l-$th row, that is,

$$U_N = \begin{pmatrix} \alpha_{i_1} & \alpha_{i_1}^2 & \dots & \alpha_{i_1}^n \\ \alpha_{i_2} & \alpha_{i_2}^2 & \dots & \alpha_{i_2}^n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i_t} & \alpha_{i_t}^2 & \dots & \alpha_{i_t}^n \end{pmatrix}.$$

- U_N is a parity check matrix for the constacyclic code C over F having N as a set of zeros of $h(x)$.
- Let C_N be the constacyclic code over K with U_N as parity check matrix, and let this code has minimum distance d_N.

Theorem

If N is a nonempty set of zeros of the polynomial $x^n - a$ and if M is a set of $n-$th roots of unity such that $|\overline{M}| \leq |M| + d_N - 2$ for some consecutive set $\overline{M}$ containing M, then $d_{MN} \geq d_N + |M| - 1$.

Theorem

If N is a nonempty set of zeros of the polynomial $x^n - a$ and if M is a set of $n-$th roots of unity such that $|\overline{M}| \leq |M| + d_N - 2$ for some consecutive set $\overline{M}$ containing M, then $d_{MN} \geq d_N + |M| - 1$.

Corollary

Let N, M and $\overline{M}$ be as in the previous theorem, with N consecutive. Then $|\overline{M}| < |M| + |N|$ implies $d_{MN} \geq |M| + |N|$.

Example

Take $n = 25$, $q = 7$, $a = -1$ and let μ be a primitive 50−th root of unity. Then μ is a zero of the polynomial $x^{25} + 1$. Let the zeros of $h(x)$ be μ^i with $i \in C_1 \cup C_5 \cup C_{17}$, where

$$C_1 = \{1, 7, 49, 43\},\ C_5 = \{5, 35, 45, 15\},\ C_{17} = \{17, 19, 33, 31\}.$$

Since μ is a primitive 50−th root of unity, it follows that $\alpha := \mu^2$ is a primitive 25−th root of unity. In terms of α_i the zeros of $h(x)$ can be written as

$$\alpha_2, \alpha_3;\ \alpha_7, \alpha_8, \alpha_9;\ \alpha_{15}, \alpha_{16}, \alpha_{17};\ \alpha_{21}, \alpha_{22};\ \alpha_{24}, \alpha_{25}.$$

Example

Take $n = 25$, $q = 7$, $a = -1$ and let μ be a primitive 50−th root of unity. Then μ is a zero of the polynomial $x^{25} + 1$. Let the zeros of $h(x)$ be μ^i with $i \in C_1 \cup C_5 \cup C_{17}$, where

$$C_1 = \{1, 7, 49, 43\},\ C_5 = \{5, 35, 45, 15\},\ C_{17} = \{17, 19, 33, 31\}.$$

Since μ is a primitive 50−th root of unity, it follows that $\alpha := \mu^2$ is a primitive 25−th root of unity. In terms of α_i the zeros of $h(x)$ can be written as

$$\alpha_2, \alpha_3;\ \alpha_7, \alpha_8, \alpha_9;\ \alpha_{15}, \alpha_{16}, \alpha_{17};\ \alpha_{21}, \alpha_{22};\ \alpha_{24}, \alpha_{25}.$$

Take $N = \{\alpha_i \mid i = 15, 16\}$ and $M = \{\beta^j \mid j = 0, 2, 3, 4\}$ with $\beta = \alpha^3$. Then the elements of MN are zeros of $h(x)$. Since $d_N = 3$ and $|\overline{M}| = 5 \leq |M| + d_N - 2 = 4 + 3 - 2$, the last bound implies that $d \geq d_{MN} \geq |M| + d_N - 1 = 6$.

THANK YOU FOR
YOUR ATTENTION