AN UPPER BOUND ON THE COVERING RADIUS OF A CLASS OF CYCLIC CODES

EVGENIYA VELIKOVA, ASEN BOJILOV

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

21.06.2008

- $F = \mathrm{GF}(q)$, $q = p^m$, $p = \mathrm{char}\, F$, $p \neq 2$, $F^* = \langle \beta \rangle$

- $F = \mathrm{GF}(q)$, $q = p^m$, $p = \operatorname{char} F$, $p \neq 2$, $F^* = \langle \beta \rangle$
- C is cyclic code of length n, $(n, p) = 1$ and generator polinomial $g(x) \in F[x]$, $\deg g(x) = s$

- $F = \mathrm{GF}(q)$, $q = p^m$, $p = \operatorname{char} F$, $p \neq 2$, $F^* = \langle \beta \rangle$
- C is cyclic code of length n, $(n, p) = 1$ and generator polinomial $g(x) \in F[x]$, $\deg g(x) = s$
- $\dim C = n - s$

- $F = \mathrm{GF}(q)$, $q = p^m$, $p = \operatorname{char} F$, $p \neq 2$, $F^* = \langle \beta \rangle$
- C is cyclic code of length n, $(n, p) = 1$ and generator polinomial $g(x) \in F[x]$, $\deg g(x) = s$
- $\dim C = n - s$
- $c(x) \in C$ iff $g(x) \mid c(x)$.

- $F = \mathrm{GF}(q)$, $q = p^m$, $p = \mathrm{char}\, F$, $p \neq 2$, $F^* = \langle \beta \rangle$
- C is cyclic code of length n, $(n, p) = 1$ and generator polinomial $g(x) \in F[x]$, $\deg g(x) = s$
- $\dim C = n - s$
- $c(x) \in C$ iff $g(x) \mid c(x)$.
- $g(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_s)$, $\alpha_i = \beta^{k_i} \in K > F$, $k_i \in \{0, 1, \ldots, q - 2\}$

- $F = \mathrm{GF}(q)$, $q = p^m$, $p = \mathrm{char}\, F$, $p \neq 2$, $F^* = \langle \beta \rangle$
- C is cyclic code of length n, $(n, p) = 1$ and generator polinomial $g(x) \in F[x]$, $\deg g(x) = s$
- $\dim C = n - s$
- $c(x) \in C$ iff $g(x) \mid c(x)$.
- $g(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_s)$, $\alpha_i = \beta^{k_i} \in K > F$, $k_i \in \{0, 1, \ldots, q - 2\}$
- $$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \ldots & \alpha_3^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha_s & \alpha_s^2 & \ldots & \alpha_s^{n-1} \end{pmatrix} = \begin{pmatrix} h_0 & h_1 & \ldots & h_{n-1} \end{pmatrix}$$

- $F = \mathrm{GF}(q)$, $q = p^m$, $p = \mathrm{char}\, F$, $p \neq 2$, $F^* = \langle \beta \rangle$
- C is cyclic code of length n, $(n, p) = 1$ and generator polinomial $g(x) \in F[x]$, $\deg g(x) = s$
- $\dim C = n - s$
- $c(x) \in C$ iff $g(x) \mid c(x)$.
- $g(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_s)$, $\alpha_i = \beta^{k_i} \in K > F$, $k_i \in \{0, 1, \dots, q-2\}$
- $$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_s & \alpha_s^2 & \dots & \alpha_s^{n-1} \end{pmatrix} = \begin{pmatrix} h_0 & h_1 & \dots & h_{n-1} \end{pmatrix}$$
- $Hc^t = (0, 0, \dots, 0)^t \in F^s \Leftrightarrow c \in C$

- $\mathbf{d}(v, C) = \min_{c \in C}\{\mathbf{d}(v, c)\}$

- $\mathbf{d}(v, C) = \min_{c \in C}\{\mathbf{d}(v, c)\}$
- $\rho = \max_{v \in F^n}\{d(v, C)\}$

- $\mathbf{d}(v, C) = \min_{c \in C} \{\mathbf{d}(v, c)\}$
- $\rho = \max_{v \in F^n} \{d(v, C)\}$
- $\mathrm{wt}(\mathrm{v} + \mathrm{C}) = \min_{\mathrm{c} \in \mathrm{C}} \{\mathrm{v} + \mathrm{c}\} = \mathbf{d}(\mathrm{v}, \mathrm{C})$, $\rho = \max_{v \in F^n} \{\mathrm{wt}(\mathrm{v} + \mathrm{C})\}$

- $\mathbf{d}(v, C) = \min_{c \in C}\{\mathbf{d}(v, c)\}$
- $\rho = \max_{v \in F^n}\{d(v, C)\}$
- $\mathrm{wt(v + C)} = \min_{\mathrm{c \in C}}\{\mathrm{v + c}\} = \mathbf{d}(\mathrm{v, C})$, $\rho = \max_{v \in F^n}\{\mathrm{wt(v + C)}\}$
- $u \in v + C$ is a leader $\Leftrightarrow \mathrm{wt(u) = wt(v + C)}$

- $\mathbf{d}(v, C) = \min_{c \in C}\{\mathbf{d}(v, c)\}$
- $\rho = \max_{v \in F^n}\{d(v, C)\}$
- $\mathrm{wt(v + C)} = \min_{\mathrm{c \in C}}\{\mathrm{v + c}\} = \mathbf{d}(\mathrm{v, C})$, $\rho = \max_{v \in F^n}\{\mathrm{wt(v + C)}\}$
- $u \in v + C$ is a leader $\Leftrightarrow \mathrm{wt(u) = wt(v + C)}$
- $s(v + C) = s(v + c) = s(u) = Hu^t \in F^s$, $c \in C$, $u \in v + C$ is a leader

- $\mathbf{d}(v, C) = \min_{c \in C}\{\mathbf{d}(v, c)\}$
- $\rho = \max_{v \in F^n}\{d(v, C)\}$
- $\mathrm{wt}(\mathrm{v} + \mathrm{C}) = \min_{\mathrm{c} \in \mathrm{C}}\{\mathrm{v} + \mathrm{c}\} = \mathbf{d}(\mathrm{v}, \mathrm{C})$, $\rho = \max_{v \in F^n}\{\mathrm{wt}(\mathrm{v} + \mathrm{C})\}$
- $u \in v + C$ is a leader $\Leftrightarrow \mathrm{wt}(\mathrm{u}) = \mathrm{wt}(\mathrm{v} + \mathrm{C})$
- $s(v + C) = s(v + c) = s(u) = Hu^t \in F^s$, $c \in C$, $u \in v + C$ is a leader
- $\mathrm{wt}(\mathrm{v} + \mathrm{C}) = \mathrm{l} \Leftrightarrow \mathrm{s}(\mathrm{v} + \mathrm{C}) = \mathrm{a}_{\mathrm{i}_1}\mathrm{h}_{\mathrm{i}_1} + \mathrm{a}_{\mathrm{i}_2}\mathrm{h}_{\mathrm{i}_2} + \cdots + \mathrm{a}_{\mathrm{i}_\mathrm{l}}\mathrm{h}_{\mathrm{i}_\mathrm{l}}$

- $\mathbf{d}(v, C) = \min_{c \in C}\{\mathbf{d}(v, c)\}$
- $\rho = \max_{v \in F^n}\{d(v, C)\}$
- $\mathrm{wt}(\mathrm{v} + \mathrm{C}) = \min_{\mathrm{c} \in \mathrm{C}}\{\mathrm{v} + \mathrm{c}\} = \mathbf{d}(\mathrm{v}, \mathrm{C})$, $\rho = \max_{v \in F^n}\{\mathrm{wt}(\mathrm{v} + \mathrm{C})\}$
- $u \in v + C$ is a leader $\Leftrightarrow \mathrm{wt}(\mathrm{u}) = \mathrm{wt}(\mathrm{v} + \mathrm{C})$
- $s(v + C) = s(v + c) = s(u) = Hu^t \in F^s$, $c \in C$, $u \in v + C$ is a leader
- $\mathrm{wt}(\mathrm{v} + \mathrm{C}) = \mathrm{l} \Leftrightarrow \mathrm{s}(\mathrm{v} + \mathrm{C}) = \mathrm{a}_{\mathrm{i}_1}\mathrm{h}_{\mathrm{i}_1} + \mathrm{a}_{\mathrm{i}_2}\mathrm{h}_{\mathrm{i}_2} + \cdots + \mathrm{a}_{\mathrm{i}_\mathrm{l}}\mathrm{h}_{\mathrm{i}_\mathrm{l}}$
- ρ is a minimal r, such that every nonzero vector from F^s is a linear combination over F of less or equal of r columns of H

- $f_a(x) \in \mathbb{Z}_p[x]$ is the minimal polynomial of $a \in F$

- $f_a(x) \in \mathbb{Z}_p[x]$ is the minimal polynomial of $a \in F$
- $[q-1, q-1-2m]$-code C with generator polynomial $g(x) = f_\beta(x).f_{\beta-1}(x)$, $\deg f_\beta = \deg f_{\beta-1} = m$

- $f_a(x) \in \mathbb{Z}_p[x]$ is the minimal polynomial of $a \in F$
- $[q-1, q-1-2m]$-code C with generator polynomial $g(x) = f_\beta(x).f_{\beta^{-1}}(x)$, $\deg f_\beta = \deg f_{\beta^{-1}} = m$
- $$H = \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{q-2} \\ 1 & \beta^{-1} & \beta^{-2} & \dots & \beta^{-(q-2)} \end{pmatrix}$$

- $f_a(x) \in \mathbb{Z}_p[x]$ is the minimal polynomial of $a \in F$
- $[q-1, q-1-2m]$-code C with generator polynomial $g(x) = f_\beta(x).f_{\beta^{-1}}(x)$, $\deg f_\beta = \deg f_{\beta^{-1}} = m$
- $$H = \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{q-2} \\ 1 & \beta^{-1} & \beta^{-2} & \dots & \beta^{-(q-2)} \end{pmatrix}$$
- $s = (a, b) \in F^2$, $(a, b) \neq (0, 0)$

- $f_a(x) \in \mathbb{Z}_p[x]$ is the minimal polynomial of $a \in F$
- $[q-1, q-1-2m]$-code C with generator polynomial $g(x) = f_\beta(x).f_{\beta^{-1}}(x)$, $\deg f_\beta = \deg f_{\beta^{-1}} = m$
- $$H = \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{q-2} \\ 1 & \beta^{-1} & \beta^{-2} & \dots & \beta^{-(q-2)} \end{pmatrix}$$
- $s = (a, b) \in F^2$, $(a, b) \neq (0, 0)$
- $$\left| \begin{aligned} a_1x_1 + a_2x_2 + \dots + a_jx_j &= a \\ a_1\frac{1}{x_1} + a_2\frac{1}{x_2} + \dots + a_j\frac{1}{x_j} &= b \end{aligned} \right.$$

- $f_a(x) \in \mathbb{Z}_p[x]$ is the minimal polynomial of $a \in F$
- $[q-1, q-1-2m]$-code C with generator polynomial $g(x) = f_\beta(x).f_{\beta^{-1}}(x)$, $\deg f_\beta = \deg f_{\beta^{-1}} = m$
- $$H = \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{q-2} \\ 1 & \beta^{-1} & \beta^{-2} & \dots & \beta^{-(q-2)} \end{pmatrix}$$
- $s = (a, b) \in F^2$, $(a, b) \neq (0, 0)$
- $$\left| \begin{aligned} a_1x_1 + a_2x_2 + \dots + a_jx_j &= a \\ a_1\frac{1}{x_1} + a_2\frac{1}{x_2} + \dots + a_j\frac{1}{x_j} &= b \end{aligned} \right.$$
- $a_1, a_2, \dots, a_j \in \mathbb{Z}_p$; $x_1, x_2, \dots, x_j \in F$; $j \leq 3$

- $$Q = \langle \beta^2 \rangle \cup \{0\} = \{a \in F \mid \exists b \in F \colon a = b^2\}$$

- $$Q = \langle \beta^2 \rangle \cup \{0\} = \{a \in F \mid \exists b \in F \colon a = b^2\}$$
- $$N = \beta \langle \beta^2 \rangle = F \backslash Q = \{a \in F \mid \exists b \in F \colon a = \beta b^2\}$$

- $$Q = \langle \beta^2 \rangle \cup \{0\} = \{a \in F \mid \exists b \in F \colon a = b^2\}$$
- $$N = \beta\langle \beta^2 \rangle = F \backslash Q = \{a \in F \mid \exists b \in F \colon a = \beta b^2\}$$
- $j = 1$
  the system has a solution iff $ab \in Q$, $ab \neq 0$

- $$Q = \langle \beta^2 \rangle \cup \{0\} = \{a \in F \mid \exists b \in F\colon a = b^2\}$$
- $$N = \beta\langle \beta^2 \rangle = F \backslash Q = \{a \in F \mid \exists b \in F\colon a = \beta b^2\}$$
- $j = 1$
  the system has a solution iff $ab \in Q$, $ab \neq 0$
- $$\left| \begin{aligned} x_1 + x_2 + x_3 &= a \\ \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} &= b \end{aligned} \right.$$
  $(a, b) \neq (0, 0)$ and $ab \neq 1$

- $$Q = \langle \beta^2 \rangle \cup \{0\} = \{a \in F \mid \exists b \in F \colon a = b^2\}$$
- $$N = \beta \langle \beta^2 \rangle = F \backslash Q = \{a \in F \mid \exists b \in F \colon a = \beta b^2\}$$
- $j = 1$
  the system has a solution iff $ab \in Q$, $ab \neq 0$
- $$\left| \begin{array}{l} x_1 + x_2 + x_3 = a \\ \dfrac{1}{x_1} + \dfrac{1}{x_2} + \dfrac{1}{x_3} = b \end{array} \right.$$
  $(a, b) \neq (0, 0)$ and $ab \neq 1$
- $b \neq 0$

- $$Q = \langle \beta^2 \rangle \cup \{0\} = \{a \in F \mid \exists b \in F \colon a = b^2\}$$
- $$N = \beta \langle \beta^2 \rangle = F \backslash Q = \{a \in F \mid \exists b \in F \colon a = \beta b^2\}$$
- $j = 1$
  the system has a solution iff $ab \in Q$, $ab \neq 0$
- $$\left| \begin{array}{l} x_1 + x_2 + x_3 = a \\ \dfrac{1}{x_1} + \dfrac{1}{x_2} + \dfrac{1}{x_3} = b \end{array} \right.$$
  $(a, b) \neq (0, 0)$ and $ab \neq 1$
- $b \neq 0$
- If the system has a solution for every $(a, b) \neq (0, 0)$, then $\rho \leq 3$

- $$x_1 = \frac{a + y}{1 + yb}$$

- $$x_1 = \frac{a+y}{1+yb}$$
- $$x_2 + x_3 = \frac{y(ab-1)}{yb+1}, \qquad x_2 x_3 = \frac{a+y}{yb+1} y$$

- $$x_1 = \frac{a+y}{1+yb}$$
- $$x_2 + x_3 = \frac{y(ab-1)}{yb+1}, \qquad x_2 x_3 = \frac{a+y}{yb+1} y$$
- $$t^2 - \frac{y(ab-1)}{yb+1} t + \frac{a+y}{yb+1} y = 0$$

- $$x_1 = \frac{a+y}{1+yb}$$
- $$x_2 + x_3 = \frac{y(ab-1)}{yb+1}, \qquad x_2 x_3 = \frac{a+y}{yb+1} y$$
- $$t^2 - \frac{y(ab-1)}{yb+1} t + \frac{a+y}{yb+1} y = 0$$
- $$(yb+1)^2 D = -y D_1, \qquad D_1(y) = 4by^2 + (-a^2b^2 + 6ab + 3)y + 4a$$

- $$x_1 = \frac{a+y}{1+yb}$$
- $$x_2 + x_3 = \frac{y(ab-1)}{yb+1}, \qquad x_2 x_3 = \frac{a+y}{yb+1} y$$
- $$t^2 - \frac{y(ab-1)}{yb+1} t + \frac{a+y}{yb+1} y = 0$$
- $$(yb+1)^2 D = -yD_1, \qquad D_1(y) = 4by^2 + (-a^2 b^2 + 6ab + 3)y + 4a$$
- $$x_2 = \frac{(ab-1)y + \sqrt{-yD_1}}{2(1+yb)}, \qquad x_3 = \frac{(ab-1)y - \sqrt{-yD_1}}{2(1+yb)}.$$

- $$\left(\frac{a}{q}\right) = \begin{cases} 0, & \text{if } \ a = 0, \\ 1, & \text{if } \ a \in Q, \ a \neq 0, \\ -1, & \text{if } \ a \in N \end{cases}$$

- $$\left(\frac{a}{q}\right) = \begin{cases} 0, & \text{if } \ a = 0, \\ 1, & \text{if } \ a \in Q, \ a \neq 0, \\ -1, & \text{if } \ a \in N \end{cases}$$

Lemma

Let M be the set of the solutions (x, y) of the equation $Ax^2 + By^2 = C$ in the finite field F with q elements and let $D = AB \neq 0$. Then the following fact holds

$$|M| = \begin{cases} q - \left(\frac{-D}{q}\right), & \textit{if } \ C \neq 0, \\ q + \left(\frac{-D}{q}\right)(q-1), & \textit{if } \ C = 0, \end{cases}$$

Lemma

Let $f(x) = Ax^2 + Bx + C \in F[x]$, $A \neq 0$, $B \neq 0$, *and let*

$$M = \{x^2 \mid x \in F,\ f(x^2) = f(\gamma x^2) \text{ for some } \gamma \in N\}.$$

Then

$$|M| = \left\lfloor \frac{q+3}{4} \right\rfloor$$

Lemma

Let $f(x) = Ax^2 + Bx + C \in F[x]$, $A \neq 0$, $B \neq 0$, *and let*

$$M = \{x^2 \mid x \in F,\ f(x^2) = f(\gamma x^2) \text{ for some } \gamma \in N\}.$$

Then

$$|M| = \left\lfloor \frac{q+3}{4} \right\rfloor$$

- $\mathrm{D}_1(y) = 4by^2 + (-a^2b^2 + 6ab + 3)y + 4a$

- $\mathrm{D}_1(y) = 4by^2 + (-a^2b^2 + 6ab + 3)y + 4a$
- $-a^2b^2 + 6ab + 3 \neq 0 \Rightarrow D_1(c^2) = D_1(\gamma c^2)$, $c \in F$ and $\gamma \in N$

- $\mathrm{D}_1(y) = 4by^2 + (-a^2b^2 + 6ab + 3)y + 4a$
- $-a^2b^2 + 6ab + 3 \neq 0 \Rightarrow D_1(c^2) = D_1(\gamma c^2)$, $c \in F$ and $\gamma \in N$
- $y = c^2$ or $y = \gamma c^2$: $D = -yD_1(y) \in Q$

- $\mathrm{D}_1(y) = 4by^2 + (-a^2b^2 + 6ab + 3)y + 4a$
- $-a^2b^2 + 6ab + 3 \neq 0 \Rightarrow D_1(c^2) = D_1(\gamma c^2)$, $c \in F$ and $\gamma \in N$
- $y = c^2$ or $y = \gamma c^2$: $D = -yD_1(y) \in Q$
- $-a^2b^2 + 6ab + 3 = 0$

$$\left| \begin{array}{l} x_1 + x_2 + x_3 = \dfrac{a}{2} \\ \dfrac{1}{x_1} + \dfrac{1}{x_2} + \dfrac{1}{x_3} = \dfrac{b}{2} \end{array} \right.$$

Theorem

The $[p^m - 1, p^m - 1 - 2m]$*-code* C *defined above has covering radius at most 3 for* $p \neq 2$ *and* $q > 36$.

Theorem

The $[p^m - 1, p^m - 1 - 2m]$-code C defined above has covering radius at most 3 for $p \neq 2$ and $q > 36$.

THANK YOU FOR YOUR ATTENTION