Covering Radius of Some Codes

Ferruh Özbudak[i]
(joint work with Minjia Shi and Tor Helleseth)

[i]Middle East Technical University, Ankara, Turkey

Cognac
C.I.R.M.
Luminy
February 16, 2023
France

Outline I

Definitions and Main Results

- Covering radius of codes is one of the four fundamental parameters of a code
- Let $\mathbb{F}_{q_0}$ denote a finite field with q_0 elements, where q_0 is a prime power
- Let n be a positive integer. Let $\mathcal{C}$ be an $\mathbb{F}_{q_0}$-linear code of length n. Let w_H denote the Hamming weight in $\mathbb{F}_{q_0}^n$
- If $x \in \mathbb{F}_{q_0}^n$, then the Hamming distance of x to $\mathcal{C}$ is $d(x, \mathcal{C}) = \min\{w_H(x - c) : c \in \mathcal{C}\}$
- The *covering radius* of $\mathcal{C}$ is the integer given by

$$\max\left\{d(x, \mathcal{C}) : x \in \mathbb{F}_{q_0}^n\right\}.$$

Definitions and Main Results

- $s \geq 1$: an integer
- Put $q = q_0^s$ and $n = q + 1$
- H: the subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = n$
- $\{h_1, \ldots, h_n\}$: an enumeration of H
- The generalized Zetterberg code $\mathcal{C}_s(q_0)$ of length $n = q_0^s + 1$ over $\mathbb{F}_{q_0}$ is the $\mathbb{F}_{q_0}$-linear code with the parity check matrix

$$P = [h_1 \ h_2 \cdots h_n] .$$

Definitions and Main Results

Main Results:

We assume that $q_0^s \not\equiv 7 \mod 8$. We also assume that q_0 is odd.

(i). For each such q_0 and any integer $s \geq 1$, the covering radius of $\mathcal{C}_s(q_0)$ is either 2 or 3.

(ii). If $s = 1$, then the covering radius of $\mathcal{C}_s(q_0)$ is 2.

(iii). If $s \geq 2$ is an even integer, then the covering radius of $\mathcal{C}_s(q_0)$ is 3.

(iv). For each such q_0, there exists an odd integer $N_1(q_0) \geq 3$ with the following property: If $s \geq N_1(q_0)$ is an odd integer, then the covering radius of $\mathcal{C}_s(q_0)$ is 3.

Definitions and Main Results

(v). For each such q_0, let $I(q_0)$ be the set consisting of odd integers $s \geq 3$ such that the covering radius of $\mathcal{C}_s(q_0)$ is 3. We show that $I(q_0)$ is very different from the case of even s in some cases. For example

$$I(q_0) = \{s\colon\ s \text{ is an odd integer with } s \geq 3\} \text{ if } q_0 \in \{3, 5, 9, 11, 13\}.$$

However we also have that

$$3 \notin I(q_0) \text{ if } q_0 \in \{17, 19, 25\}.$$

(vi). We extend the notion generalized Zetterberg code to *half* and *twisted half* generalized Zetterberg codes. If $q_0 = 3$, then half and twisted half generalized Zetterberg codes are quasi-perfect. We also determine the covering radii of half and twisted half generalized Zetterberg codes.

Proving the upper bound 3

The main result of this section:

Theorem

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$ and $n = q + 1$. Assume that $q_0^s \not\equiv 7 \mod 8$. Then the covering radius of the Zetterberg code over $\mathbb{F}_{q_0}$ of length n is at most 3.

The Theorem above is equivalent to the following statement: For $\alpha \in \mathbb{F}_{q^2}$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that

$$c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha. \tag{1}$$

An important technique of Gashkov and Sidelnikov

Theorem

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$ and $n = q + 1$. Assume that $q \not\equiv 7 \mod 8$. Let P1, P2, P3 and P4 be the properties defined depending on q_0 and s as follows. Note that P3 and P4 are defined only if $q \equiv 3 \mod 8$.

- **Property P1:**
  For each $\alpha \in \mathbb{F}_q^*$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that $c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha$.

- **Property P2:**
  For each $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $\alpha^q = -\alpha$, there exist $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ and $h_1, h_2, h_3 \in H$ such that $c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha$.

An important technique of Gashkov and Sidelnikov

Theorem (Theorem continues)

- **Property P3:**
  Assume $q \equiv 3 \mod 4$. *Let* $\theta \in \mathbb{F}_{q^2}$ *be a primitive* 4*-th root of* 1. *For each* $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *with* $\alpha^q = \theta\alpha$, *there exist* $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ *and* $h_1, h_2, h_3 \in H$ *such that* $c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha$.

- **Property P4:**
  We keep the assumption on q *and the notation on* θ *of P3 above. For each* $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *with* $\alpha^q = -\theta\alpha$, *there exist* $c_1, c_2, c_3 \in \mathbb{F}_{q_0}$ *and* $h_1, h_2, h_3 \in H$ *such that* $c_1 h_1 + c_2 h_2 + c_3 h_3 = \alpha$.

An important technique of Gashkov and Sidelnikov

Theorem (Theorem continues)

Then we have the following:

- **Case** $q \equiv 1 \mod 4$**:**
  The covering radius of $\mathcal{C}_s(q_0)$ *is at most* 3 *if both of the the properties P1 and P2 hold simultaneously.*

- **Case** $q \equiv 3 \mod 8$**:**
  The covering radius of $\mathcal{C}_s(q_0)$ *is at most* 3 *if all of the four properties P1, P2, P3 and P4 hold simultaneously.*

Remark

An important strength of the Theorem above is the following: If $q \equiv 1 \mod 4$, then using properties P1 and P2 we need to consider only α in the set

$$\left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \alpha\right\} \bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\alpha\right\}.$$

Here and throughout $\bigsqcup$ is the disjoint union. Assume $q \equiv 3 \mod 4$ and $\theta \in \mathbb{F}_{q^2}$ is a primitive 4-th root of 1. Then using properties P1, P2, P3 and P4 we need to consider only α in the set

$$\left\{\alpha \in \mathbb{F}_{q^2} : \alpha^q = \alpha\right\} \bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\alpha\right\} \bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = \theta\alpha\right\}$$
$$\bigsqcup \left\{\alpha \in \mathbb{F}_{q^2}^* : \alpha^q = -\theta\alpha\right\}.$$

Hence, if $q \equiv 1 \mod 4$, the number of α we need to consider is $2q-1$. Similarly if $q \equiv 3 \mod 4$, the number of α we need to consider is $4q-3$. In particular, if q is large, then

$$max\left\{2q-1, 4q-3\right\} \ll q^2.$$

Property P1

In this subsection we prove that Property P1 holds. Throughout this

subsection let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Let H be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q + 1$. Let $w \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $w + w^q = 1$. Put $D = (\frac{w - w^q}{2})^2$.

The main result of this subsection:

Theorem

Let $\alpha \in \mathbb{F}_q \setminus \{0, 1, -1\}$. There exist $h_1, h_2, h_3 \in H$ such that

$$h_1 + h_2 + h_3 = \alpha.$$

Property P1

Proposition

Let $\alpha \in \mathbb{F}_q \setminus \{0, 1, -1\}$. Then the Theorem above holds if and only if there exist $x_1, x_2, x_3, y_1, y_2, y_3 \in \mathbb{F}_q$ such that

$$\begin{aligned} x_1 + x_2 + x_3 &= \alpha, \\ y_1 + y_2 + y_3 &= 0, \\ x_1^2 - Dy_1^2 &= 1, \\ x_2^2 - Dy_2^2 &= 1, \quad \textit{and} \\ x_3^2 - Dy_3^2 &= 1. \end{aligned}$$

Property P1

Proposition

Let $\alpha \in \mathbb{F}_q \setminus \{0, 1, -1\}$. *Let* $a(x), b(x), c(x) \in \mathbb{F}_q[x]$ *be the polynomials given by*

$$a(x) = 2\alpha x - \alpha^2 - 1,$$
$$b(x) = 2\alpha x^2 + (-3\alpha^2 - 1)x + \alpha^3 + \alpha, \quad \textit{and}$$
$$c(x) = (-\alpha^2 - 1)x^2 + (\alpha^3 + \alpha)x - \frac{\alpha^4}{4} - \frac{\alpha^2}{2} + \frac{3}{4}.$$

Put

$$\Delta(x) = b(x)^2 - 4a(x)c(x) \in \mathbb{F}_q[x]. \tag{2}$$

Property P1

Proposition (Proposition continues)

Assume that there exists $x_1 \in \mathbb{F}_q$ such that

(i). $x_1^2 - 1$ is a nonsquare in $\mathbb{F}_q$,

(ii). $a(x_1) \neq 0$, *and*

(iii). $\Delta(x_1)$ is a nonzero square in $\mathbb{F}_q$.

Then the theorem above holds.

Property P1

Proposition

Let $\alpha \in \mathbb{F}_q \setminus \{0, 1, -1\}$. Let $\Delta(x) \in \mathbb{F}_q[x]$ be the polynomial defined in the Proposition above. Then there is no polynomial $f(x) \in \overline{\mathbb{F}}_q[x]$ such that

$$\Delta(x) = (f(x))^2 \in \mathbb{F}_q[x]. \tag{3}$$

Proof of the main theorem for Property 1

Using Weil's sum for the quadratic character and the previous propositions we obtain that if

$$q - 8q^{1/2} - 16 > 0,$$

then the main theorem of Subsection Property 1 holds. This holds for $q > 94$. The set of cardinalities q such that there exists a finite field $\mathbb{F}_q$

of characteristic odd and $q \leq 94$ is

$$\begin{aligned} S \quad = \quad & \{3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, \\ & 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 79, 81, 83, 89\}. \end{aligned}$$

For each $q \in S$, using Magma and a direct search method we show that the theorem holds.

Finalizing the proof of the upper bound 3

Recall the main theorem for the upper bound:

Theorem

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$ and $n = q + 1$. Assume that $q_0^s \not\equiv 7 \mod 8$. Then the covering radius of the Zetterberg code over $\mathbb{F}_{q_0}$ of length n is at most 3.

The theorem above is reduced to Properties P1, P2, P3 and P4. We prove the corresponding statements for Properties P2, P3 and P4 analogous to the case of Property 1. Some further arithmetic techniques are needed in their proofs.

When is the covering radius 3?

In this section we determine the exact covering radius of generalized Zetterberg codes.
Let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q+1$ over $\mathbb{F}_{q_0}$.
Recall that $H \subseteq \mathbb{F}_{q^2}^*$ is the subgroup with $|H| = q+1$. Put $m = \frac{q_0-1}{2}$. Let $H_m \subseteq \mathbb{F}_{q^2}^*$ be the subgroup with $|H_m| = m(q+1)$.

Lemma

The covering radius of $\mathcal{C}_s(q_0)$ is at least 2. The covering radius of $\mathcal{C}_s(q_0)$ is at least 3 if and only if there exists $\alpha \in \mathbb{F}_{q^2}$ such that the equation

$$h_1 + h_2 = \alpha$$

is not solvable with $h_1, h_2 \in H_m$.

Properties NP1, NP2, NP3, NP4

Theorem

- *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. For an integer $s \geq 1$, let $q = q_0^s$.*
- *Assume that $q \not\equiv 7 \mod 8$. Let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q+1$ over $\mathbb{F}_{q_0}$. Recall that $m = \frac{q_0-1}{2}$ and $H_m \subseteq \mathbb{F}_{q^2}^*$ is the subgroup with $|H_m| = m(q+1)$.*
- *Let NP1, NP2, NP3 and NP4 be the properties defined depending on q_0 and s as follows. Note that NP3 and NP4 are defined only if $q \equiv 3 \mod 8$.*

Properties NP1, NP2, NP3, NP4

Theorem (Theorem continues)

- **Property NP1:**
  There exists $\alpha \in \mathbb{F}_q^*$ *such that the equation*

$$h_1 + h_2 = \alpha$$

  has no solution with $h_1, h_2 \in H_m$.

- **Property NP2:**
  There exists $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *with* $\alpha^q = -\alpha$ *such that the equation*

$$h_1 + h_2 = \alpha$$

  has no solution with $h_1, h_2 \in H_m$.

Properties NP1, NP2, NP3, NP4

Theorem (Theorem continues)

- **Property NP3:** *Assume that* $q \equiv 3 \mod 8$. *Let* $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *be a primitive* 4*-th root of* 1. *There exists* $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *with* $\alpha^q = \theta\alpha$ *such that the equation*

$$h_1 + h_2 = \alpha$$

has no solution with $h_1, h_2 \in H_m$.

- **Property NP4:** *Assume that* $q \equiv 3 \mod 8$. *Let* $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *be a primitive* 4*-th root of* 1. *There exists* $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ *with* $\alpha^q = -\theta\alpha$ *such that the equation*

$$h_1 + h_2 = \alpha$$

has no solution with $h_1, h_2 \in H_m$.

Properties NP1, NP2, NP3, NP4

Theorem (Theorem continues)

Then we have the following:

- **Case** $q \equiv 1 \mod 4$**:**
  The covering radius of $\mathcal{C}_s(q_0)$ *is* 3 *if and only if at least one of the two properties NP1 and NP2 holds. Otherwise the covering radius of* $\mathcal{C}_s(q_0)$ *is* 2*.*

- **Case** $q \equiv 3 \mod 8$**:**
  The covering radius of $\mathcal{C}_s(q_0)$ *is* 3 *if and only if at least one of the four properties NP1, NP2, NP3 and NP4 holds. Otherwise the covering radius of* $\mathcal{C}_s(q_0)$ *is* 2*.*

An equivalent formulation and a connection to algebraic curves over finite fields

Theorem

- *Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. For an integer $s \geq 1$, let $q = q_0^s$. Assume that $q \not\equiv 7 \mod 8$. Let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q+1$ over $\mathbb{F}_{q_0}$.*
- *Put $m = \frac{q_0-1}{2}$. Note that the number of nonzero squares in $\mathbb{F}_{q_0}$ is m.*
- *Let $\{\alpha_1, \ldots, \alpha_m\}$ be an enumerated set consisting of the nonzero square elements in $\mathbb{F}_{q_0}$.*
- *Let $w \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with $w + w^q = 1$. Put $D = \frac{1}{4} - w^{q+1}$. Recall that $D \in \mathbb{F}_q^*$ and D is not a square in $\mathbb{F}_q$.*
- *Let PP1, PP2 and PP3 be the properties defined depending on q_0 and s as follows.*

Properties PP1, PP2 and PP3

Theorem (Theorem continues)

- **Property PP1:**
  For $1 \leq i \leq m$, *let* $f_i(x) \in \mathbb{F}_q[x]$ *be the polynomial given by*

$$f_i(x) = x^2 - \alpha_i.$$

  There exists $a \in \mathbb{F}_q^*$ *such that* $f_i(a)$ *is a nonzero square in* $\mathbb{F}_q$ *for each* $1 \leq i \leq m$.

- **Property PP2:**
  For $1 \leq i \leq m$, *let* $f_i(x) \in \mathbb{F}_q[x]$ *be the polynomial given by*

$$f_i(x) = x^2 + \frac{\alpha_i}{D}.$$

  There exists $a \in \mathbb{F}_q^*$ *such that* $f_i(a)$ *is a nonzero square in* $\mathbb{F}_q$ *for each* $1 \leq i \leq m$.

Properties PP1, PP2 and PP3

Theorem (Theorem continues)

- **Property PP3:** *For* $1 \leq i \leq m$, *let* $f_i(x) \in \mathbb{F}_q[x]$ *be the polynomial given by*

$$f_i(x) = x^2 - 2\alpha_i.$$

There exists $a \in \mathbb{F}_q^*$ *such that* $f_i(a)$ *is a nonzero square in* $\mathbb{F}_q$ *for each* $1 \leq i \leq m$.

Properties PP1, PP2 and PP3

Theorem (Theorem continues)

Then we have the following:

- **Case** $q \equiv 1 \mod 4$**:**
  The covering radius of $\mathcal{C}_s(q_0)$ *is* 3 *if and only if at least one of the two properties PP1 and PP2 holds. Otherwise the covering radius of* $\mathcal{C}_s(q_0)$ *is* 2*.*

- **Case** $q \equiv 3 \mod 8$**:**
  The covering radius of $\mathcal{C}_s(q_0)$ *is* 3 *if and only if at least one of the three properties PP1, PP2 and PP3 holds. Otherwise the covering radius of* $\mathcal{C}_s(q_0)$ *is* 2*.*

Case s is even

The next corollary shows that the covering radius is always 3 if $s \geq 2$ is an **even** integer, independent of q_0.

Corollary

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Let $s \geq 2$ be an **even** *integer. Let $\mathcal{C}_s(q_0)_s$ be the generalized Zetterberg code of length $q_0^s + 1$ over $\mathbb{F}_{q_0}$. Then the covering radius of $\mathcal{C}_s(q_0)_s$ is 3.*

It is rather surprising that there exists a finite field $\mathbb{F}_{q_0}$ of odd characteristic and odd integer $s \geq 3$ such that $q_0 \not\equiv 7 \mod 8$ and the covering radius of the generalized Zetterberg code of length $q_0^s + 1$ over $\mathbb{F}_{q_0}$ is 2, not 3 as in the case of even integers $s \geq 2$ as proved in the Corollary above.

Curve χ_1 corresponding to Property PP1

The following theorem is related to Property PP1.

Theorem

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Assume that $q_0 > 3$. Let $m = \frac{q_0-1}{2}$ and $\{\alpha_1, \ldots, \alpha_m\}$ be an enumerated set consisting of the nonzero squares in $\mathbb{F}_{q_0}$. Let $s \geq 3$ be an odd integer and put $q = q_0^s$. Let χ_1 be the fibre product of the projective lines over $\mathbb{F}_q$ given by

$$\chi_1 : \begin{cases} y_1^2 &= x^2 - \alpha_1, \\ y_2^2 &= x^2 - \alpha_2, \\ &\vdots \\ y_m^2 &= x^2 - \alpha_m. \end{cases}$$

Curve χ_1 corresponding to Property PP1

Theorem (Theorem continues)

Let P_∞ be the pole of x in $\mathbb{F}_q(x)$. For $\alpha \in \mathbb{F}_q$, let P_α be the zero of $(x-\alpha)$ in $\mathbb{F}_q(x)$. We have the following:

(i). *The genus g of χ_1 is*

$$g = 1 + 2^{m-1}(m-2).$$

(ii). *There are exactly 2^m $\mathbb{F}_q$-rational points of χ_1 over P_∞.*

(iii). *If $q \equiv 1 \mod 4$, then there are exactly 2^m $\mathbb{F}_q$-rational points of χ_1 over P_0.*
If $q \equiv 3 \mod 4$, then there is no $\mathbb{F}_q$-rational point of χ_1 over P_0.

Curve χ_1 corresponding to Property PP1

Theorem (Theorem continues)

(iv). *If $\alpha \in \mathbb{F}_q^*$, then there are exactly 2^m $\mathbb{F}_q$-rational points of χ_1 over P_α if and only if*

$$f_i(\alpha) \text{ is a nonzero square in } \mathbb{F}_q \tag{4}$$

for each $1 \leq i \leq m$, where $f_i(x) = x^2 - \alpha_i \in \mathbb{F}_q[x]$.
If (4) does not hold, then there is no $\mathbb{F}_q$-rational point of χ_1 over P_α.

Using Hasse-Weil Inequality for Properties PP1, PP2 and PP3

There are analogous curves χ_2 for Property PP2 and χ_3 for Property PP3. We also have analogous rational point distribution results for χ_2 and χ_3 related to properties PP2 and PP3.
Using these and Hasse-Weil Inequality we obtain the following.

Theorem

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Assume that $q_0 > 3$ and $q_0 \not\equiv 7 \mod 8$. Put $m = \frac{q_0-1}{2}$.
Let s_1^* be the smallest odd integer with $s_1^* \geq 3$ such that

$$q_0^{s_1^*} + 1 - 2\left(1 + 2^{m-1}(m-2)\right) q_0^{s_1^*/2} > 2^m.$$

If s is an odd integer with $s \geq s_1^*$, then the generalized Zetterberg code $\mathcal{C}_s(q_0)$ over $\mathbb{F}_{q_0}$ of length $q_0^s + 1$ has covering radius 3.

Regions for Covering Radius 3

Definition

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Assume that $q_0 > 3$ and $q_0 \not\equiv 7 \mod 8$. Let $N_1(q_0)$ be the smallest odd integer with $s_1 \geq 3$ such that if s is an odd integer satisfying $s \geq s_1$, then the generalized Zetterberg code over $\mathbb{F}_{q_0}$ of length $q_0^s + 1$ has covering radius 3.

Numerical values on $N_1(q_0)$ easily for small q_0:

$$\begin{aligned} q_0 = 5: &\quad N_1(5) \leq 3; \\ q_0 = 9: &\quad N_1(9) \leq 5; \\ q_0 = 11: &\quad N_1(11) \leq 5; \\ q_0 = 13: &\quad N_1(13) \leq 5; \\ q_0 = 17: &\quad N_1(17) \leq 7; \\ q_0 = 19: &\quad N_1(19) \leq 7; \\ q_0 = 25: &\quad N_1(25) \leq 7. \end{aligned} \tag{5}$$

Refined Regions for Covering Radius 3

The following definition is a refinement of the definition of $N_1(q_0)$.

Definition

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic. Assume that $q_0 \not\equiv 7 \mod 8$. For an odd integer $s \geq 3$, let $\mathcal{C}_s(q_0)$ be the generalized Zetterberg code of length $q_0^s + 1$ over $\mathbb{F}_{q_0}$.
Let $I(q_0)$ be the set of odd integers given by

$$I(q_0) = \{s \geq 3 : s \text{ is odd and } \mathcal{C}_s(q_0) \text{ has covering radius } 3\}.$$

Refined Regions for Covering Radius 3

It follows immediately from definitions above that we have the following:

$$\{s : s \geq N_1(q_0) \text{ and } s \text{ is odd}\} \subseteq I(q_0).$$

The following proposition is also useful in determining $I(q_0)$.

Proposition

Let $\mathbb{F}_{q_0}$ be a finite field of odd characteristic with $q_0 > 3$. Assume that $q_0 \not\equiv 7 \mod 8$. If $s \in I(q_0)$ and $t \geq 1$ is an odd integer, then $st \in I(q_0)$.

Exact covering radius for some small q_0

Example

Let $q_0 = 3$. We obtain $I(3) = \{s : s \geq 3 \text{ is an odd integer}\}$.

Example

Let $q_0 = 5$. We obtain $I(5) = \{s : s \geq 3 \text{ is an odd integer}\}$.

The next example gives the smallest value of q_0 such that there exists a finite field $\mathbb{F}_{q_0}$ of odd characteristic with $q_0 \not\equiv 7 \mod 8$ such that $I(q_0) \neq \{s : s \geq 3 \text{ is an odd integer}\}$.

Example

Let $q_0 = 17$. We obtain $I(17) = \{s : s \geq 5 \text{ is an odd integer}\}$.

Half Generalized Zetterberg Code

Definition

Let $\mathbb{F}_{q_0}$ be an arbitrary finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Assume that $q \equiv 1 \mod 4$. Let H be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q + 1$. Let H_2 be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H_2| = \frac{q+1}{2}$. Note that $-1 \in H \setminus H_2$ and

$$H = H_2 \sqcup -H_2.$$

Here $-H_2 = \{-x : x \in H_2\}$. Let $h_2 \in H_2$ be a generator of H_2. Put $n = \frac{q+1}{2}$. We define the *half generalized Zettenberg code* $\mathcal{C}_s^{(2)}(q_0)$ *of length* n *over* $\mathbb{F}_{q_0}$ as the linear code over $\mathbb{F}_{q_0}$ with the parity check matrix

$$\begin{bmatrix} 1 & h_2 & h_2^2 & \cdots & h_2^{n-1} \end{bmatrix}.$$

Twisted Half Generalized Zetterberg Code

Definition

Let $\mathbb{F}_{q_0}$ be an arbitrary finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Assume that $q \equiv 3 \mod 4$. Let H be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q + 1$. Let H_4 be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H_4| = \frac{q+1}{4}$. Let $\theta \in \mathbb{F}_{q^2}$ be a primitive 4-th root of 1. Note that

$$H = (H_4 \sqcup \theta H_4) \sqcup -(H_4 \sqcup \theta H_4)$$

and $\theta \notin \mathbb{F}_{q_0}$. Here $-(H_4 \sqcup \theta H_4) = \{-x : x \in (H_4 \sqcup \theta H_4)\}$. Let $h_4 \in H_4$ be a generator of H_4. Put $n = \frac{q+1}{2}$.

Twisted Half Generalized Zetterberg Code

Definition (Definition continues)

Note that $H_4 \sqcup \theta H_4$ is a subset of H with $|H_4 \sqcup \theta H_4| = n$ and $H_4 \sqcup \theta H_4$ is not the subgroup of H with n elements, for example $-1 \notin (H_4 \sqcup \theta H_4)$. We define the *twisted half generalized Zettenberg code* $\mathcal{C}_s^{(2,t)}(q_0)$ *of length* n *over* $\mathbb{F}_{q_0}$ as the linear code over $\mathbb{F}_{q_0}$ with the parity check matrix

$$\left[\begin{array}{ccccccccc} 1 & h_4 & h_4^2 & \cdots & h_4^{n/2-1}\theta & \theta h_4 & \theta h_4^2 & \cdots & \theta h_4^{n/2-1} \end{array} \right].$$

In particular we define

- an half generalized Zettenberg code if $q \equiv 1 \mod 4$, and
- a twisted half generalized Zettenberg code if $q \equiv 3 \mod 4$.

Covering radius of Half Generalized Zetterberg Code

Theorem

Let $\mathbb{F}_{q_0}$ be an arbitrary finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Assume that $q \equiv 1 \mod 4$. Let $\mathcal{C}_s(q_0)$ be the generalized Zettenberg code of length $q+1$ over $\mathbb{F}_{q_0}$. Let $\mathcal{C}_s^{(2)}(q_0)$ be the half generalized Zettenberg code of length $\frac{q+1}{2}$ over $\mathbb{F}_{q_0}$. Then the covering radius of $\mathcal{C}_s(q_0)$ is equal to the covering radius of $\mathcal{C}_s^{(2)}(q_0)$.

Covering radius of Half Generalized Zetterberg Code

Theorem

Let $\mathbb{F}_{q_0}$ be an arbitrary finite field of odd characteristic. Let $s \geq 1$ be an integer. Put $q = q_0^s$. Assume that $q \equiv 3 \mod 4$. Let $\mathcal{C}_s(q_0)$ be the generalized Zettenberg code of length $q+1$ over $\mathbb{F}_{q_0}$. Let $\mathcal{C}_s^{(2,t)}(q_0)$ be the twisted half generalized Zettenberg code of length $\frac{q+1}{2}$ over $\mathbb{F}_{q_0}$. Then the covering radius of $\mathcal{C}_s(q_0)$ is equal to the covering radius of $\mathcal{C}_s^{(2,t)}(q_0)$.

Thank you.