On the Second Generalized Covering Radius of Binary Primitive Triple-Error-Correcting BCH Codes[1]

Ferruh Özbudak

Sabancı University - Faculty of Engineering and Natural Sciences
(joint work with İlknur Öztürk)

5th Pythagorean Conference
Kalamata, Greece, June 1-6, 2025
June 02, 2025

[1]This study is funded by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under Grant Number 223N065.

Definition

Let q be a prime power and $n \in \mathbb{N}$. A q-ary block code is any non-empty subset

$$\mathcal{C} \subseteq \mathbb{F}_q^n,$$

where $\mathbb{F}_q$ denotes the finite field with q elements and $\mathbb{F}_q^n$ is equipped with the Hamming metric

$$d_H(x, y) = \left|\{ i \mid 1 \leq i \leq n,\ x_i \neq y_i \}\right|.$$

Moreover, define Hamming weight

$$w_H(x) = \left|\{ i : x_i \neq 0 \}\right| \quad \text{where} \quad x \in \mathbb{F}_q^n,$$

then

$$d_H(x, y) = w_H(x - y).$$

Definition

- The packing radius $t(\mathcal{C})$ of $\mathcal{C}$ is defined by $t(\mathcal{C}) = \left\lfloor \frac{d-1}{2} \right\rfloor$ where d is the minimum weight of $\mathcal{C}$.
- The covering radius of $\mathcal{C}$, denoted by $R(\mathcal{C})$, is the smallest integer r such that the Hamming balls of radius r centered at the codewords of $\mathcal{C}$ cover the complete space $\mathbb{F}_q^n$, namely

$$\mathbb{F}_{q_0}^n = \bigcup_{\mathbf{c} \in C} B(\mathbf{c}; r),$$

  where $B(\mathbf{c}; r) = \left\{ \mathbf{x} \in \mathbb{F}_{q_0}^n : w_H(\mathbf{x} - \mathbf{c}) \leq r \right\}$.
- It is well-known that for any code $\mathcal{C}$, $t(\mathcal{C}) \leq R(\mathcal{C})$, and $\mathcal{C}$ is called perfect if $t(\mathcal{C}) = R(\mathcal{C})$, and quasi-perfect if $t(\mathcal{C}) + 1 = R(\mathcal{C})$.

Definition

Here is a small example to explain this definition.

Example

Let $\mathcal{C} = \{\mathbf{c}_0 = 000, \mathbf{c}_1 = 111\}$ be a binary linear $[3, 1, 3]$ code. Its packing radius $t(\mathcal{C}) = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$. It is obvious that

$$\bigcup_{\mathbf{c} \in \mathcal{C}} B(\mathbf{c}; 0) = \mathcal{C} \neq \mathbb{F}_2^3.$$

It follows that $R(\mathcal{C}) \geq 1$.

Definition

Example

Note that
$B(\mathbf{c}_0; 1) = \{000, 100, 010, 001\}$ and $B(\mathbf{c}_1; 1) = \{111, 110, 011, 101\}$.
It follows that

$$\mathbb{F}_2^3 = \bigcup_{\mathbf{c} \in \mathcal{C}} B(\mathbf{c}; 1).$$

Hence, its covering radius $R(\mathcal{C}) = 1$. This implies that the code $\mathcal{C}$ is a perfect code since $t(\mathcal{C}) = R(\mathcal{C}) = 1$.

Definition

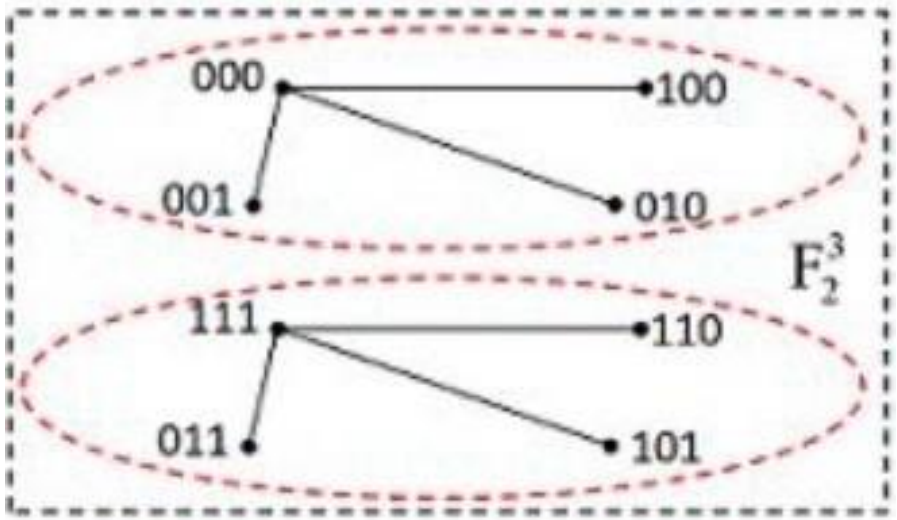


Figure: Diagram of the example above

Definition

Let q be a prime power and $\mathbb{F}_q$ denote the finite field with q elements. A q-ary linear code $\mathcal{C}$ of length n dimension k, and d is the minimum weight of $\mathcal{C}$ written as

$$[n, k, d]_q,$$

is a k-dimensional subspace of $\mathbb{F}_q^n$, i.e.

$$\mathcal{C} \subseteq \mathbb{F}_q^n.$$

Definition

Let C be an $[n, k, d]_q$ linear code. A matrix

$$H \in \mathbb{F}_q^{(n-k)\times n}$$

is called a parity–check matrix of $\mathcal{C}$ such that

$$\mathcal{C} = \{\ c \in \mathbb{F}_q^n \mid Hc^{\mathsf{T}} = \mathbf{0}\}.$$

Namely, $\mathcal{C} = \mathrm{Ker}\ H$.

Definition

Let $\mathcal{C}$ be a q-ary $[n, k, d]_q$ linear code with parity-check matrix

$$H = \left(h_1^{\mathsf{T}} \,\middle|\, h_2^{\mathsf{T}} \,\middle|\, \ldots \,\middle|\, h_n^{\mathsf{T}}\right) \in \mathbb{F}_q^{(n-k)\times n},$$

where h_i^{T} denotes the i-th column. For $t \geq 0$, the t-order generalized covering radius denoted as

$$R_t(\mathcal{C})$$

is the smallest non-negative integer r such that for $s_1^{\mathsf{T}}, \ldots, s_t^{\mathsf{T}} \in \mathbb{F}_q^{n-k}$ there exist indices $i_1, \ldots, i_r$ such that $\{ s_1^{\mathsf{T}}, \ldots, s_t^{\mathsf{T}} \} \subseteq \left\langle h_{i_1}^{\mathsf{T}}, \ldots, h_{i_r}^{\mathsf{T}} \right\rangle$.

Definition

Let q be a prime power and $\mathbb{F}_q$ denote the finite field with q elements. Let $m \geq 1$ an integer. Let α be a primitive element of order $n = q^m - 1$. The Melas code $M(m, q) \subseteq \mathbb{F}_q^n$ is the linear code with parity-check matrix

$$P = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^{-1} & \alpha^{-2} & \dots & \alpha^{-(n-1)} \end{pmatrix} \in \mathbb{F}_q^{2\times n}.$$

Except for the degenerate cases $M(1, 2)$ and $M(1, 3)$, $\dim M(m, q) = n - 2m$.

Melas Codes

Here the representation of the parity check matrix is in short. In fact, each column $\begin{bmatrix} \alpha^i \\ \alpha^{-i} \end{bmatrix}$ in P is considered as $\phi(\begin{bmatrix} \alpha^i \\ \alpha^{-i} \end{bmatrix}) \in \mathbb{F}_q^{2m}$, where ϕ is any $\mathbb{F}_q$-linear bijective map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^m$.

The Radius of Melas Codes

So far, the radius of Melas codes under some special conditions has been found, and the results are listed in the table below.

Table 2. The radius of $M(m, q)$ over $\mathbb{F}_q$ that have been discovered

Conditions	Radius
$m = 1, q = 2$	1
$m \geq 2,\ q = 2$	3
$m \geq 1,\ q > 2$, char $\mathbb{F}_q$ is 2	2
$m = 1,\ q = 3$	1
$m = 2,\ q = 3$	4
$m \geq 3,\ q = 3$	3
$m \geq 1,\ q \geq 5$, char $\mathbb{F}_q$ is odd	2

Zetterberg Codes

Let q_0 be an odd prime power and $s \geq 1$. Put

$$q = q_0^s, \qquad n = q + 1.$$

Let $H \subset \mathbb{F}_{q^2}^*$ be the unique subgroup of order n with enumeration $H = \{h_1, \ldots, h_n\}$. The generalized Zetterberg code

$$\mathcal{C}_s(q_0) \subset \mathbb{F}_{q_0}^n$$

is the q_0-ary linear code whose parity-check matrix is

$$P = \begin{bmatrix} h_1 & h_2 & \ldots & h_n \end{bmatrix} \in \mathbb{F}_{q_0}^{2s \times n}.$$

It has parameters $[n, n-2s, d]$ with $d \geq 3$ and $\dim C_s(q_0) = n - 2s$.

The Covering Radius of Zetterberg Codes

Let $\ell \geq 3$ and let the base field $\mathbb{F}_{q_0}$ satisfy $q_0 \equiv 2^\ell - 1 \pmod{2^{\ell+1}}$. Denote by $\mathcal{C}_s(q_0)$ the generalized Zetterberg code of odd characteristic.
First, we introduce some notation.

- Assume that $q = q_0^s \equiv 2^\ell - 1 \pmod{2^{\ell+1}}$.
- Let θ be a primitive 2^ℓ-th root of 1 in $\mathbb{F}_{q^2}^*$.
- Let H be the multiplicative subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q + 1$.
- Put $m = (q_0 - 1)/2$. Let H_m be the multiplicative subgroup of $\mathbb{F}_{q^2}^*$ with $|H_m| = m(q + 1)$.
- Clearly, $H_m = \mathbb{F}_{q_0}^* \cdot H$.

Definition

For index $0 \leq i \leq 2^\ell - 1$, let Property NPi be the property defined as follows: There exists $\gamma \in \mathbb{F}_{q^2}^*$ such that $\gamma^q = \theta^i \gamma$ and the equation

$$h_1 + h_2 = \gamma$$

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

The Covering Radius of Zetterberg Codes

According to the definition of covering radius, we obtain the following theorem.

Theorem

Let $\mathbb{F}_{q_0}$ be a finite field such that

$$q_0^s \equiv 2^\ell - 1 \pmod{2^{\ell+1}}.$$

Then the covering radius of $\mathcal{C}_s(q_0)$ is 3 if and only if there exists an index $0 \leq i \leq 2^\ell - 1$ such that Property NPi holds. Otherwise, the covering radius is 2.

We first consider Property NPi if i is even.

Theorem

Assume that $0 \leq i \leq 2^\ell - 1$ is an even integer. Let $\alpha_1, \ldots, \alpha_m$ be an enumeration of all nonzero squares in $\mathbb{F}_{q_0}$. Then Property NPi is equivalent to the following: The system

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

is solvable with $x, y_1, y_2, \ldots, y_m \in \mathbb{F}_q^*$.

We next consider Property NPi if i is odd.

Theorem

Assume that $0 \leq i \leq 2^\ell - 1$ is an odd integer. Let $\beta_1, \ldots, \beta_m$ be an enumeration of all nonzero non-squares in $\mathbb{F}_{q_0}$. Then Property NPi is equivalent to the following: The system

$$\begin{aligned} y_1^2 &= x^2 - \beta_1, \\ y_2^2 &= x^2 - \beta_2, \\ &\vdots \\ y_m^2 &= x^2 - \beta_m, \end{aligned}$$

is solvable with $x, y_1, y_2, \ldots, y_m \in \mathbb{F}_q^*$.

The Covering Radius of Zetterberg Codes

Using the previous theorems, the following corollaries are obtained.

Corollary

The covering radius of $\mathcal{C}_s(q_0)$ is 2 if $s = 1$.

Corollary

The covering radius of $\mathcal{C}_s(q_0)$ is 3 if s is even.

It remains to consider s is odd with $s \geq 3$.

The Covering Radius of Zetterberg Codes

Using the arithmetic of the fibre product of Kummer curves over finite fields and Hasse-Weil inequality, we determine that the covering radius of $\mathcal{C}_s(q_0)$ is 3 for all sufficiently large odd s.

Theorem

Recall that $m = (q_0 - 1)/2$. Let s^* be the smallest odd integer such that $s^* \geq 3$ and

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

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

The Covering Radius of Zetterberg Codes

We do not know the finite initial interval corresponding to the case that the covering radius of generalized Zetterberg code is 2.
We define the set

$$I(q_0) := \left\{ \text{odd } s \geq 3 \ : \ R(\mathcal{C}_s(q_0)) = 3 \right\}$$

collects precisely those odd exponents for which the covering radius of generalized Zetterberg code, $R(C_s(q_0)) = 3$. If s is odd, $s \geq 3$ and $s \notin I(q_0)$, then $R(C_s(q_0)) = 2$.

The last theorem implies that $\{\text{odd} \ \ s \geq 3\} \setminus I(q_0)$ is finite.

We determine $I(q_0)$ for certain small q_0. They produce some new quasi-perfect codes.

Binary Primitive Double-Error-Correcting BCH Code

Definition

Let $m \geq 2$ and $n = 2^m - 1$. The binary primitive double-error-correcting BCH code $BCH(2, m)$ is the $[n, k, d]$-code defined by

$$n = 2^m - 1, \quad k \geq n - 2m - 1, \quad d \geq 5,$$

Fix a primitive element $w \in \mathbb{F}_{2^m}^*$ and form the $2 \times n$ matrix over $\mathbb{F}_{2^m}$

$$H(2, m) = \begin{bmatrix} 1 & w & w^2 & \cdots & w^{n-1} \\ 1 & w^3 & w^6 & \cdots & w^{3(n-1)} \end{bmatrix}.$$

Choosing a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ and expanding each entry yields a binary $2m \times n$ parity-check matrix $\bar{H}(2, m)$, and

$$BCH(2, m) = \left\{ x \in \mathbb{F}_2^n \mid \bar{H}(2, m)\, x^{\mathsf{T}} = 0 \right\}.$$

Index the columns of the BCH parity-check matrix by elements $x \in \mathbb{F}_{2^m}^*$.

Then any target syndrome $\begin{bmatrix}\beta_1\\ \beta_2\end{bmatrix} \in \mathbb{F}_{2^m}^2$ such that

$$\bar{H}x^{\mathsf{T}} = \begin{bmatrix}\beta_1\\ \beta_2\end{bmatrix}$$

can be realized as the span of three columns corresponding to $x_1, x_2, x_3 \in \mathbb{F}_{2^m}^*$ satisfying

$$x_1 + x_2 + x_3 = \beta_1,$$
$$x_1^3 + x_2^3 + x_3^3 = \beta_2.$$

Covering Radius of $BCH(2, m)$

For all $m \geq 3$, the covering radius $R_1(BCH(2, m))$ of $BCH(2, m)$ determined as

$$R_1(BCH(2, m)) = 3,$$

i.e., every syndrome in $\mathbb{F}_{2^m}^2$ lies in the span of at most three columns of the parity-check matrix.

Second Generalized Covering Radius of $BCH(2, m)$

Definition

Let q be a prime power and $\mathbb{F}_q$ denote the finite field with q elements. For an $[n, k, d]$-code $\mathcal{C} \subseteq \mathbb{F}_q^n$, the second generalized covering radius denoted

$$R_2(\mathcal{C})$$

is the least integer r such that any two syndromes in $\mathbb{F}_q^{n-k}$ can be generated by at most r columns of a parity-check matrix of $\mathcal{C}$.

Second Generalized Covering Radius of $BCH(2, m)$

Using detailed methods of arithmetic and coding theory, recently L. Yohananov and M. Schwartz (2024) determined the second generalized covering radius the binary primitive double-error-correcting BCH code $BCH(2, m)$ as their main result, which is

$$R_2(BCH(2, m)) = \begin{cases} 5, & m \neq 4, \\ 6, & m = 4. \end{cases}$$

Third Generalized Covering Radius of $BCH(2, m)$

Using some methods derived from the theory of algebraic curves over finite fields, later F.Ö. and İ.Öztürk (2025) obtained the third generalized covering radius of $BCH(2, m)$.

Theorem

$$R_3\big(BCH(2,m)\big) = \begin{cases} 7, & m \geq 8 \text{ even}, \\ 6 \text{ or } 7, & m \geq 9 \text{ odd}. \end{cases}$$

Upper Bound on $R_3(BCH(2, m))$

Let $m \geq 8$ and choose $\beta_1, \ldots, \beta_6 \in \mathbb{F}_{2^m}^*$ with

$$\beta_1 \neq \beta_3, \quad \beta_1 \neq \beta_5, \quad \beta_3 \neq \beta_5, \quad \beta_1^3 \neq \beta_2, \quad \beta_3^3 \neq \beta_4, \quad \beta_5^3 \neq \beta_6.$$

Then there exist $\theta_1, \theta_2, \theta_3 \in \mathbb{F}_{2^m}^*$ with $\mathrm{Tr}(\theta_i) = 0$ and an $x \in \mathbb{F}_{2^m}^*$ satisfying the system of three Artin–Schreier equations

$$y_1^2 + y_1 = \frac{\beta_1^3 + \beta_2}{x^3}, \quad y_2^2 + y_2 = \frac{\beta_3^3 + \beta_4}{(x + \beta_1 + \beta_3)^3}, \quad y_3^2 + y_3 = \frac{\beta_5^3 + \beta_6}{(x + \beta_1 + \beta_5)^3}.$$

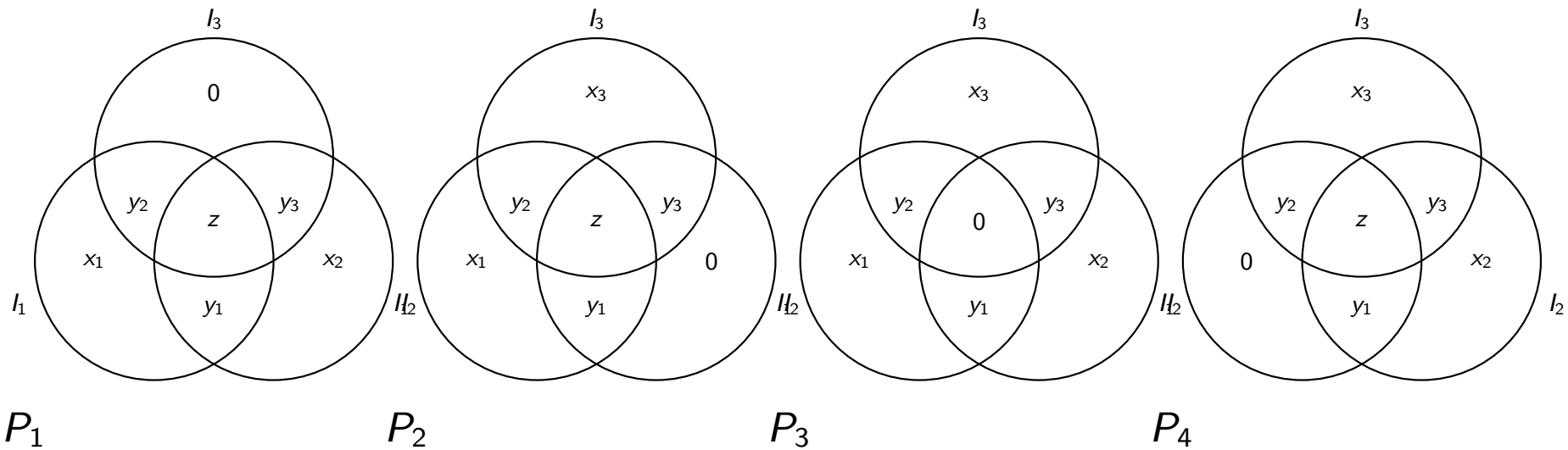
A genus-7 curve argument shows a suitable solution exists, forcing the following theorem.

Theorem

For all $m \geq 8$, $R_3(BCH(2, m)) \leq 7$.

Lower Bound on $R_3(BCH(2, m))$: Particular Patterns

$p_1 : (1, 1, 1, 1, 1, 1, 0)$, $p_2 : (1, 1, 0, 1, 1, 1, 1)$, $p_3 : (1, 1, 1, 0, 1, 1, 1)$, $p_4 : (0, 1, 1, 1, 1,$



P_1 P_2 P_3 P_4

Lower Bound on Third Generalized Covering Radius of $BCH(2, m)$

	p_1	p_2	p_3	p_4
α_1	$\beta_2 + \beta_3$	$\beta_2 + \beta_3$	β_1	β_1
α_2	$\beta_1 + \beta_3$	β_2	β_2	$\beta_1 + \beta_3$
α_3	β_3	$\beta_1 + \beta_2$	β_3	$\beta_1 + \beta_2$

In each column, the three values cannot simultaneously satisfy the necessary consistency conditions for the corresponding system of equations. Therefore, no solution exists under the assumption $R_3(BCH(2, m) \leq 6$, where m is even. This contradiction yields the desired lower bound.

Theorem

For all even integers $m \geq 4$, we have

$$R_3(BCH(2, m)) \geq 7.$$

Lower Bound on Third Generalized Covering Radius of $BCH(2, m)$

For odd m, a parallel analysis shows that any five or fewer columns also fails.

Theorem

For all odd integers $m \geq 5$, we have

$$R_3(BCH(2, m)) \geq 6.$$

Covering Radius of Triple Error Correcting BCH Codes $BCH(3, m)$

- $R_1(BCH(3, m)) = 5$ for large m.
- Put $q = 2^m$ and assume m is large enough.
- This means that for every vector

$$\begin{bmatrix} a_1 \\ a_3 \\ a_5 \end{bmatrix} \in \mathbb{F}_q^3,$$

there exist $x_1, x_2, x_3, x_4, x_5 \in \mathbb{F}_q^*$ such that:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 &= a_1, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 &= a_3, \\ x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5 &= a_5. \end{aligned}$$

Covering Radius of Triple Error Correcting BCH Codes $BCH(3, m)$

It is equivalent to the following: We can assume that $a_1 = 0$ without loss of generality. Hence, given

$$\begin{bmatrix} 0 \\ a_3 \\ a_5 \end{bmatrix} \in \mathbb{F}_q^3,$$

there exist $x_1, x_2, x_3, x_4, x_5 \in \mathbb{F}_q^*$ such that

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 &= 0, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 &= a_3, \\ x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5 &= a_5. \end{aligned}$$

Covering Radius of Triple Error Correcting BCH Codes $BCH(3, m)$

We obtain a result in the direction of the second generalized covering radius of the triple error correcting code $BCH(3, m)$ as follows:

As $R_1(BCH(3, m)) = 5$, it is immediate that:

Given

$$\begin{bmatrix} a_1 \\ a_3 \\ a_5 \end{bmatrix}, \quad \begin{bmatrix} b_1 \\ b_3 \\ b_5 \end{bmatrix} \in \mathbb{F}_q^3,$$

there exist $x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3, y_4, y_5 \in \mathbb{F}_q^*$ such that

Covering Radius of Triple Error Correcting BCH Codes $BCH(3, m)$

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 &= a_1, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 &= a_3, \\ x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5 &= a_5. \end{aligned} \quad \text{and} \quad \begin{aligned} y_1 + y_2 + y_3 + y_4 + y_5 &= b_1, \\ y_1^3 + y_2^3 + y_3^3 + y_4^3 + y_5^3 &= b_3, \\ y_1^5 + y_2^5 + y_3^5 + y_4^5 + y_5^5 &= b_5. \end{aligned}$$

Hence, $R_2(BCH(3, m)) \leq 10$ for sufficiently large m.

We obtain an improved upper bound 9 under some conditions.

Covering Radius of Triple Error Correcting BCH Codes $BCH(3, m)$

Theorem

Let $q = 2^m$ with m sufficiently large. Assume further that m is even.

Given

$$\begin{bmatrix} 0 \\ a_3 \\ a_5 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ b_3 \\ b_5 \end{bmatrix} \in \mathbb{F}_q^3,$$

there exist $x_1, x_2, x_3, y_1, y_2, y_3, \alpha, \beta, \gamma \in \mathbb{F}_q^*$ such that

Covering Radius of Triple Error Correcting BCH Codes $BCH(3, m)$

Theorem (continued)

$$\begin{aligned} x_1 + x_2 + x_3 + \alpha + \beta &= 0, \\ x_1^3 + x_2^3 + x_3^3 + \alpha^3 + \beta^3 &= a_3, \\ x_1^5 + x_2^5 + x_3^5 + \alpha^5 + \beta^5 &= a_5. \end{aligned}$$

and

$$\begin{aligned} y_1 + y_2 + y_3 + \gamma + \beta &= 0, \\ y_1^3 + y_2^3 + y_3^3 + \gamma^3 + \beta^3 &= b_3, \\ y_1^5 + y_2^5 + y_3^5 + \gamma^5 + \beta^5 &= b_5 \end{aligned}$$

and hence the "weak" second generalized covering radius $R_2(BCH(3, m))$ *of* $BCH(3, m)$ *is at most 9.*

Covering Radius of Triple Error Correcting BCH Codes $BCH(3, m)$

Remark

Note that the classical covering radius problem R_1 is known to be equivalent to the "weak" one. We hope to extend this to the case of second generalized covering radius.

Remark

It seems the case m is odd requires additional techniques. We plan to consider them as well using further detailed techniques.

Sketch of the Proof

Put $f(T) = (T + x_1)(T + x_2)(T + x_3)$ and $g(T) = (T + y_1)(T + y_2)(T + y_3)$. Aim to choose $x = \beta$ such that for suitable α and γ of the corresponding conditions are satisfied if

$$T^3 + T + A(a_2, a_3, \alpha, x)$$

and

$$T^3 + T + B(b_2, b_3, \gamma, x)$$

both split.

Sketch of the Proof (continued)

Here, $A(a_3, a_5, \alpha, x)$ and $B(b_3, b_5, \gamma, x)$ are rational functions depending on the syndromes

$$\begin{bmatrix} 0 \\ a_3 \\ a_5 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ b_3 \\ b_5 \end{bmatrix},$$

and the structure of the code $BCH(3, m)$.

The proof uses:

- properties of certain Dickson polynomials, and also
- algebraic curves over finite fields to show the existence of the corresponding solutions.

Thank you very much for your attention.