ulm university universität ulm

A New Error and Erasure Decoding Approach for Cyclic Codes

Alexander Zeh[1,2] and Sergey Bezzateev[3]

[1] Institute of Communications Engineering, Ulm University, Ulm, Germany
[2] INRIA-Saclay-Île de France/École Polytechnique, Paris, France
[3] Saint Petersburg State University of Airspace Instrumentation, St. Petersburg, Russia

June 16, 2012

13th Algebraic and Combinatorial Coding Theory (ACCT 2012), Pomorie, Bulgaria

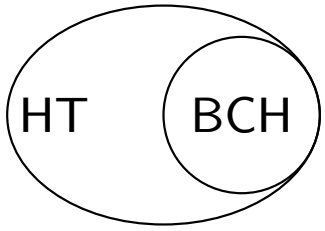
Bounds on the Minmium Distance of Cyclic Codes

[BCH] Bose, R.C., Chaudhuri, D.K.R.: *On a class of error correcting binary group codes*, Information and Control 3(1), 68–79 (1960)
Hocquenghem, A.: *Codes Correcteurs d'Erreurs*, Chiffres (Paris) 2, 147–156 (1959)

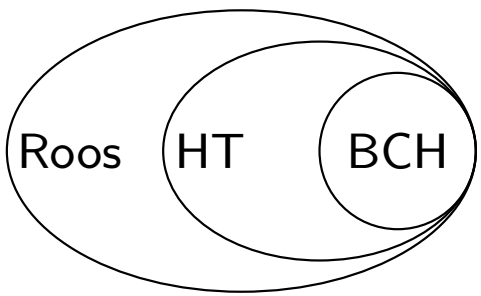
Bounds on the Minmium Distance of Cyclic Codes

[BCH] Bose, R.C., Chaudhuri, D.K.R.: *On a class of error correcting binary group codes*, Information and Control 3(1), 68–79 (1960)
Hocquenghem, A.: *Codes Correcteurs d'Erreurs*, Chiffres (Paris) 2, 147–156 (1959)

[HT] Hartmann, C., Tzeng, K.: *Generalizations of the BCH bound*, Information and Control 20(5), 489–498 (1972)



Bounds on the Minmium Distance of Cyclic Codes

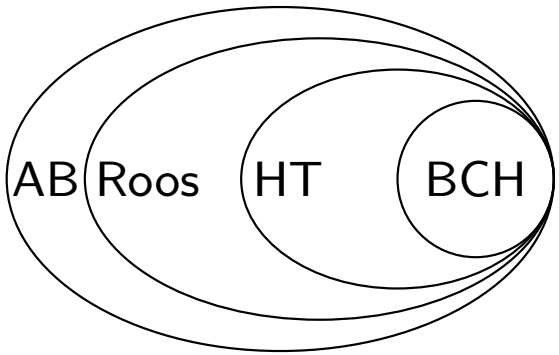


[BCH] Bose, R.C., Chaudhuri, D.K.R.: *On a class of error correcting binary group codes*, Information and Control 3(1), 68–79 (1960)
Hocquenghem, A.: *Codes Correcteurs d'Erreurs*, Chiffres (Paris) 2, 147–156 (1959)

[HT] Hartmann, C., Tzeng, K.: *Generalizations of the BCH bound*, Information and Control 20(5), 489–498 (1972)

[Roos] Roos, C.: *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound*, Journal of Combinatorial Theory, Series A 33(2), 229–232 (1982)

Bounds on the Minmium Distance of Cyclic Codes



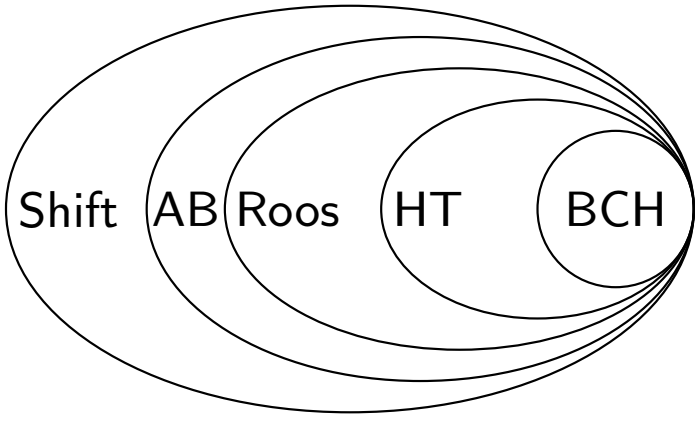
[BCH] Bose, R.C., Chaudhuri, D.K.R.: *On a class of error correcting binary group codes*, Information and Control 3(1), 68–79 (1960)
Hocquenghem, A.: *Codes Correcteurs d'Erreurs*, Chiffres (Paris) 2, 147–156 (1959)

[HT] Hartmann, C., Tzeng, K.: *Generalizations of the BCH bound*, Information and Control 20(5), 489–498 (1972)

[Roos] Roos, C.: *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound*, Journal of Combinatorial Theory, Series A 33(2), 229–232 (1982)

[AB] van Lint, J., Wilson, R.: *On the Minimum Distance of Cyclic Codes*, IEEE Transactions on Information Theory 32(1), 23–40 (1986)

Bounds on the Minmium Distance of Cyclic Codes



[BCH] Bose, R.C., Chaudhuri, D.K.R.: *On a class of error correcting binary group codes*, Information and Control 3(1), 68–79 (1960)
Hocquenghem, A.: *Codes Correcteurs d'Erreurs*, Chiffres (Paris) 2, 147–156 (1959)

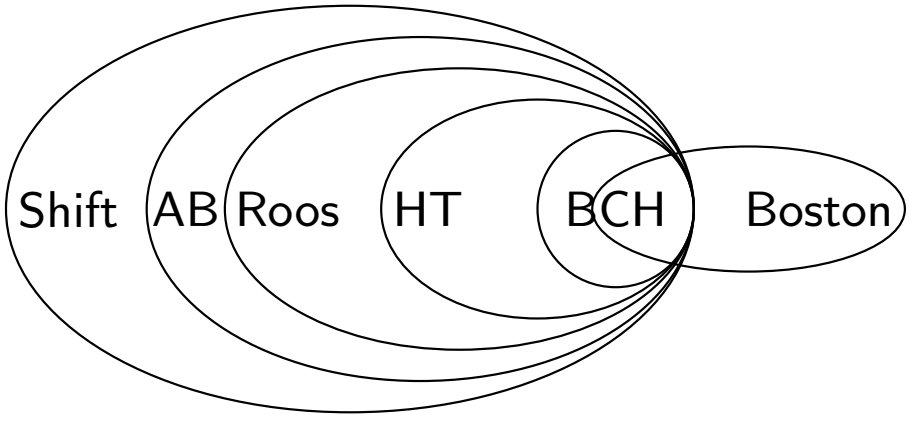
[HT] Hartmann, C., Tzeng, K.: *Generalizations of the BCH bound*, Information and Control 20(5), 489–498 (1972)

[Roos] Roos, C.: *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound*, Journal of Combinatorial Theory, Series A 33(2), 229–232 (1982)

[AB] van Lint, J., Wilson, R.: *On the Minimum Distance of Cyclic Codes*, IEEE Transactions on Information Theory 32(1), 23–40 (1986)

[Shift] Pellikaan R.: *The shift bound for cyclic Reed-Muller and geometric Goppa codes*, In Walter de Gruyter & Co pp. 155-174 (1996)

Bounds on the Minmium Distance of Cyclic Codes



[BCH] Bose, R.C., Chaudhuri, D.K.R.: *On a class of error correcting binary group codes*, Information and Control 3(1), 68–79 (1960)
Hocquenghem, A.: *Codes Correcteurs d'Erreurs*, Chiffres (Paris) 2, 147–156 (1959)

[HT] Hartmann, C., Tzeng, K.: *Generalizations of the BCH bound*, Information and Control 20(5), 489–498 (1972)

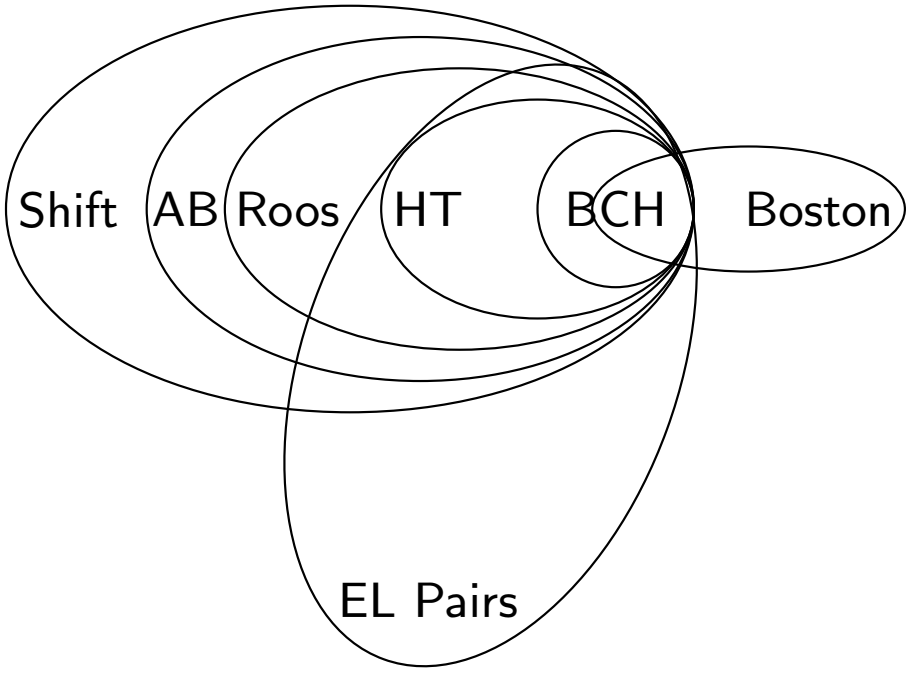
[Roos] Roos, C.: *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound*, Journal of Combinatorial Theory, Series A 33(2), 229–232 (1982)

[AB] van Lint, J., Wilson, R.: *On the Minimum Distance of Cyclic Codes*, IEEE Transactions on Information Theory 32(1), 23–40 (1986)

[Shift] Pellikaan R.: *The shift bound for cyclic Reed-Muller and geometric Goppa codes*, In Walter de Gruyter & Co pp. 155-174 (1996)

[Boston] Boston N.: *Bounding minimum distances of cyclic codes using algebraic geometry*, Electronic Notes in Discrete Mathematics, 6 , pp. 385-394 (2001)

Bounds on the Minmium Distance of Cyclic Codes



[BCH] Bose, R.C., Chaudhuri, D.K.R.: *On a class of error correcting binary group codes*, Information and Control 3(1), 68–79 (1960)
Hocquenghem, A.: *Codes Correcteurs d'Erreurs*, Chiffres (Paris) 2, 147–156 (1959)

[HT] Hartmann, C., Tzeng, K.: *Generalizations of the BCH bound*, Information and Control 20(5), 489–498 (1972)

[Roos] Roos, C.: *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound*, Journal of Combinatorial Theory, Series A 33(2), 229–232 (1982)

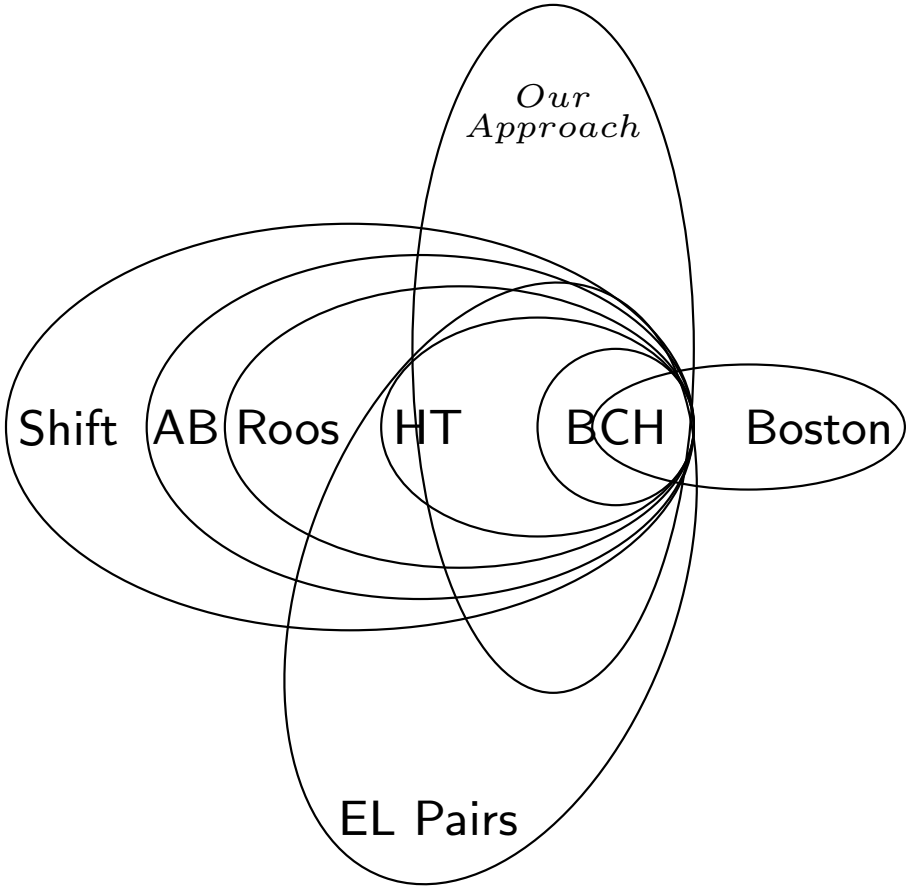
[AB] van Lint, J., Wilson, R.: *On the Minimum Distance of Cyclic Codes*, IEEE Transactions on Information Theory 32(1), 23–40 (1986)

[Shift] Pellikaan R.: *The shift bound for cyclic Reed-Muller and geometric Goppa codes*, In Walter de Gruyter & Co pp. 155-174 (1996)

[Boston] Boston N.: *Bounding minimum distances of cyclic codes using algebraic geometry*, Electronic Notes in Discrete Mathematics, 6 , pp. 385-394 (2001)

[EL Pairs] Duursma, I.M., Koetter, R.: *Error-locating pairs for cyclic codes*, IEEE Transactions on Information Theory 40(4), 1108–1121 (2002)

Bounds on the Minmium Distance of Cyclic Codes



[BCH] Bose, R.C., Chaudhuri, D.K.R.: *On a class of error correcting binary group codes*, Information and Control 3(1), 68–79 (1960)
Hocquenghem, A.: *Codes Correcteurs d'Erreurs*, Chiffres (Paris) 2, 147–156 (1959)

[HT] Hartmann, C., Tzeng, K.: *Generalizations of the BCH bound*, Information and Control 20(5), 489–498 (1972)

[Roos] Roos, C.: *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound*, Journal of Combinatorial Theory, Series A 33(2), 229–232 (1982)

[AB] van Lint, J., Wilson, R.: *On the Minimum Distance of Cyclic Codes*, IEEE Transactions on Information Theory 32(1), 23–40 (1986)

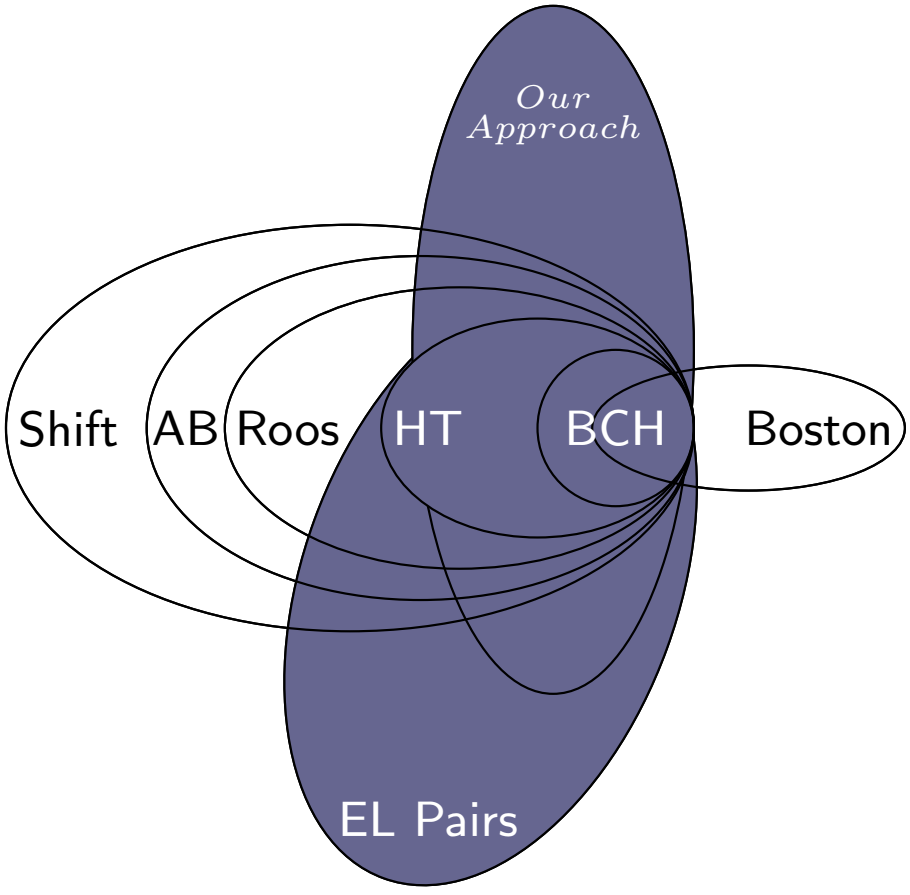
[Shift] Pellikaan R.: *The shift bound for cyclic Reed-Muller and geometric Goppa codes*, In Walter de Gruyter & Co pp. 155-174 (1996)

[Boston] Boston N.: *Bounding minimum distances of cyclic codes using algebraic geometry*, Electronic Notes in Discrete Mathematics, 6 , pp. 385-394 (2001)

[EL Pairs] Duursma, I.M., Koetter, R.: *Error-locating pairs for cyclic codes*, IEEE Transactions on Information Theory 40(4), 1108–1121 (2002)

[Our] Z., Bezzateev, S.: *A New Bound on the Minimum Distance of Cyclic Codes Using Small-Minimum-Distance Cyclic Codes*, 2012

Bounds on the Minmium Distance of Cyclic Codes



[BCH] Bose, R.C., Chaudhuri, D.K.R.: *On a class of error correcting binary group codes*, Information and Control 3(1), 68–79 (1960)
Hocquenghem, A.: *Codes Correcteurs d'Erreurs*, Chiffres (Paris) 2, 147–156 (1959)

[HT] Hartmann, C., Tzeng, K.: *Generalizations of the BCH bound*, Information and Control 20(5), 489–498 (1972)

[Roos] Roos, C.: *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound*, Journal of Combinatorial Theory, Series A 33(2), 229–232 (1982)

[AB] van Lint, J., Wilson, R.: *On the Minimum Distance of Cyclic Codes*, IEEE Transactions on Information Theory 32(1), 23–40 (1986)

[Shift] Pellikaan R.: *The shift bound for cyclic Reed-Muller and geometric Goppa codes*, In Walter de Gruyter & Co pp. 155-174 (1996)

[Boston] Boston N.: *Bounding minimum distances of cyclic codes using algebraic geometry*, Electronic Notes in Discrete Mathematics, 6 , pp. 385-394 (2001)

[EL Pairs] Duursma, I.M., Koetter, R.: *Error-locating pairs for cyclic codes*, IEEE Transactions on Information Theory 40(4), 1108–1121 (2002)

[Our] Z., Bezzateev, S.: *A New Bound on the Minimum Distance of Cyclic Codes Using Small-Minimum-Distance Cyclic Codes*, 2012

Outline

Outline

Preliminaries

дефиниция

A q-ary cyclic code over $\mathbb{F}_q$ of

- *length n,*
- *dimension k and*
- *minimum distance d*

is denoted by $\mathcal{C}(q; n, k, d) \subset \mathbb{F}_q^n$.
It is an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$ generated by $g(x)$.

Preliminaries

дефиниция

A q-ary cyclic code over $\mathbb{F}_q$ of

- *length n,*
- *dimension k and*
- *minimum distance d*

is denoted by $\mathcal{C}(q; n, k, d) \subset \mathbb{F}_q^n$.
It is an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$ generated by $g(x)$.

The cyclotomic coset $M_r^{(n)}$ modulo n over $\mathbb{F}_q$ is denoted by:

$$M_r^{(n)} = \{rq^j \bmod n \,|\, j = 0, 1, \ldots, n_r - 1\}.$$

Preliminaries

дефиниция

A q-ary cyclic code over $\mathbb{F}_q$ of

- *length n,*
- *dimension k and*
- *minimum distance d*

is denoted by $\mathcal{C}(q; n, k, d) \subset \mathbb{F}_q^n$.
It is an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$ generated by $g(x)$.

The cyclotomic coset $M_r^{(n)}$ modulo n over $\mathbb{F}_q$ is denoted by:

$$M_r^{(n)} = \{rq^j \bmod n \,|\, j = 0, 1, \ldots, n_r - 1\}.$$

Defining set $D_{\mathcal{C}}$ of $\mathcal{C}$ is:

$$D_{\mathcal{C}} = \{0 \leq i \leq n-1 \,|\, g(\alpha^i) = 0\} = M_{r_1}^{(n)} \cup M_{r_2}^{(n)} \cup \ldots.$$

Known Bounds on the Minimium Distance

Теорема (Hartmann–Tzeng (HT) Bound)

Given $\mathcal{C}$ with minimum distance d with $D_{\mathcal{C}}$.
Suppose there exist the integers b_1, m_1 and m_2 with $\gcd(n, m_1) = 1$ *and* $\gcd(n, m_2) = 1$ *such that*

$$\{b_1 + i_1 m_1 + i_2 m_2 \mid 0 \leq i_1 \leq d_0 - 2,\ 0 \leq i_2 \leq \nu\} \subseteq D_{\mathcal{C}}.$$

Then $d \geq d_0 + \nu$.

Known Bounds on the Minimium Distance

теорема (Hartmann–Tzeng (HT) Bound)

Given $\mathcal{C}$ with minimum distance d with $D_{\mathcal{C}}$.
Suppose there exist the integers b_1, m_1 and m_2 with $\gcd(n, m_1) = 1$ *and* $\gcd(n, m_2) = 1$ *such that*

$$\{b_1 + i_1 m_1 + i_2 m_2 \mid 0 \leq i_1 \leq d_0 - 2,\ 0 \leq i_2 \leq \nu\} \subseteq D_{\mathcal{C}}.$$

Then $d \geq d_0 + \nu$.

пример: Binary Cyclic Code of Length 17

The defining set for the binary cyclic code $\mathcal{C}(2; 17, 9, 5)$ of length $n = 17$ is:

$$D_{\mathcal{C}} = M_1^{(17)} = \{1, 2, 4, 8, 9, 13, 15, 16\} \equiv \{1, 2, 4, 8, -8, -4, -2, -1\}.$$

Then, we have $d \geq 5,$ with $b_1 = 1, m_1 = 7, m_2 = 1, d_0 = 3, \nu = 1.$

Known Bounds on the Minimium Distance

теорема (Hartmann–Tzeng (HT) Bound)

Given $\mathcal{C}$ with minimum distance d with $D_{\mathcal{C}}$.
Suppose there exist the integers b_1, m_1 and m_2 with $\gcd(n, m_1) = 1$ *and* $\gcd(n, m_2) = 1$ *such that*

$$\{b_1 + i_1 m_1 + i_2 m_2 \mid 0 \le i_1 \le d_0 - 2,\ 0 \le i_2 \le \nu\} \subseteq D_{\mathcal{C}}.$$

Then $d \ge d_0 + \nu$.

пример: Binary Cyclic Code of Length 17

The defining set for the binary cyclic code $\mathcal{C}(2; 17, 9, 5)$ of length $n = 17$ is:

$$D_{\mathcal{C}} = M_1^{(17)} = \{1, 2, 4, 8, 9, 13, 15, 16\} \equiv \{1, 2, 4, 8, -8, -4, -2, -1\}.$$

Then, we have $d \ge 5,$ with $b_1 = 1, m_1 = 7, m_2 = 1, d_0 = 3, \nu = 1.$

$D_{\mathcal{C}}$	13	□	15	16	□	1	2	□	4
$D_{\mathcal{C}}$	-4	□	-2	-1	□	1	2	□	4

Outline

The Non-Zero-Locator Code (i)

дефиниция (Non-Zero-Locator Code)

Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$ and

The Non-Zero-Locator Code (i)

дефиниция (Non-Zero-Locator Code)

Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$ and

- *$\mathbb{F}_{q^s}$ contain the nth roots of unity and α be a primitive element of order n*

The Non-Zero-Locator Code (i)

дефиниция (Non-Zero-Locator Code)

Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$ and

- $\mathbb{F}_{q^s}$ *contain the nth roots of unity and α be a primitive element of order n*
- $\gcd(n, n_\ell) = 1$ *and* $\mathbb{F}_{q_\ell} = \mathbb{F}_{q^u}$

The Non-Zero-Locator Code (i)

дефиниция (Non-Zero-Locator Code)

Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$ and

- *$\mathbb{F}_{q^s}$ contain the nth roots of unity and α be a primitive element of order n*
- *$\gcd(n, n_\ell) = 1$ and $\mathbb{F}_{q_\ell} = \mathbb{F}_{q^u}$*
- *$\mathbb{F}_{q_\ell^{s_\ell}}$ contain the n_ℓth roots of unity and β be a primitive element of order n_ℓ*

be given.

The Non-Zero-Locator Code (i)

дефиниция (Non-Zero-Locator Code)

Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$ and

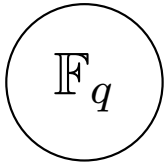
- *$\mathbb{F}_{q^s}$ contain the nth roots of unity and α be a primitive element of order n*
- *$\gcd(n, n_\ell) = 1$ and $\mathbb{F}_{q_\ell} = \mathbb{F}_{q^u}$*
- *$\mathbb{F}_{q_\ell^{s_\ell}}$ contain the n_ℓth roots of unity and β be a primitive element of order n_ℓ*

be given.
Then $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ is a non-zero-locator code of $\mathcal{C}$ if there exists a $\mu \geq 2$ and an integer e, such that $\forall\, a(x) \in \mathcal{L}$ and $\forall\, c(x) \in \mathcal{C}$:

$$\sum_{j=0}^{\infty} c(\alpha^{j+e}) a(\beta^j) x^j \equiv 0 \bmod x^{\mu-1}, \tag{1}$$

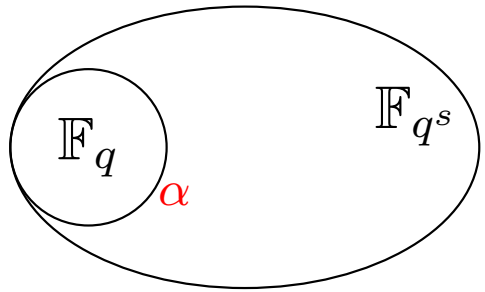
holds.

The Non-Zero-Locator Code (ii)



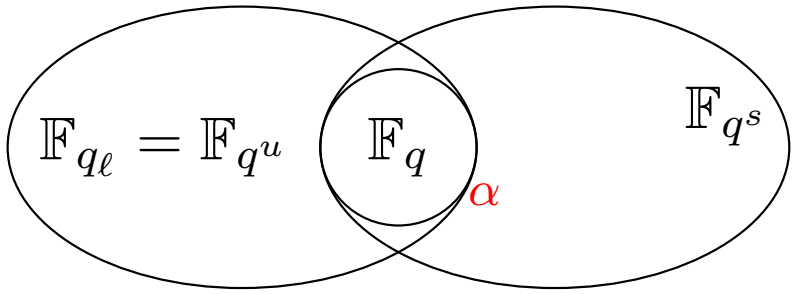
Let $r = \mathrm{lcm}(s, u \cdot s_\ell)$ and let γ be a primitive element in $\mathbb{F}_{q^r}$. Then $\gamma^{(q^r-1)/n}$ and $\gamma^{(q^r-1)/n_\ell}$ are elements of order n and n_ℓ.

The Non-Zero-Locator Code (ii)



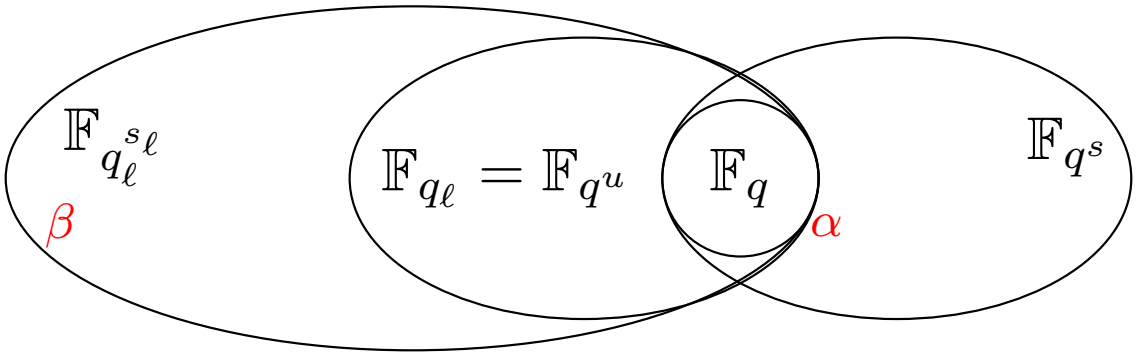
Let $r = \mathrm{lcm}(s, u \cdot s_\ell)$ and let γ be a primitive element in $\mathbb{F}_{q^r}$. Then $\gamma^{(q^r-1)/n}$ and $\gamma^{(q^r-1)/n_\ell}$ are elements of order n and n_ℓ.

The Non-Zero-Locator Code (ii)



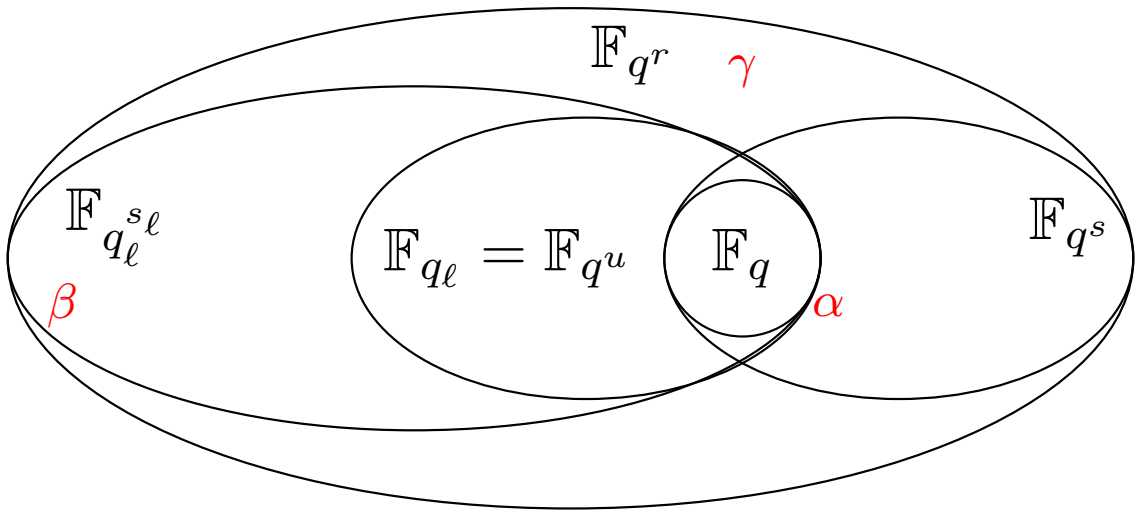
Let $r = \mathrm{lcm}(s, u \cdot s_\ell)$ and let γ be a primitive element in $\mathbb{F}_{q^r}$. Then $\gamma^{(q^r-1)/n}$ and $\gamma^{(q^r-1)/n_\ell}$ are elements of order n and n_ℓ.

The Non-Zero-Locator Code (ii)



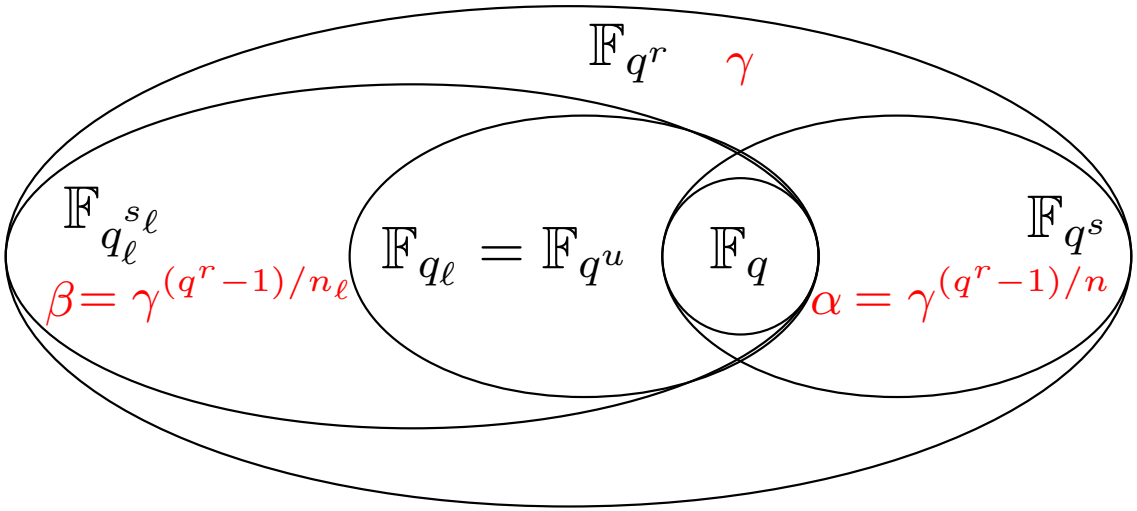
Let $r = \mathrm{lcm}(s, u \cdot s_\ell)$ and let γ be a primitive element in $\mathbb{F}_{q^r}$. Then $\gamma^{(q^r-1)/n}$ and $\gamma^{(q^r-1)/n_\ell}$ are elements of order n and n_ℓ.

The Non-Zero-Locator Code (ii)



Let $r = \mathrm{lcm}(s, u \cdot s_\ell)$ and let γ be a primitive element in $\mathbb{F}_{q^r}$. Then $\gamma^{(q^r-1)/n}$ and $\gamma^{(q^r-1)/n_\ell}$ are elements of order n and n_ℓ.

The Non-Zero-Locator Code (ii)



Let $r = \mathrm{lcm}(s, u \cdot s_\ell)$ and let γ be a primitive element in $\mathbb{F}_{q^r}$. Then $\gamma^{(q^r-1)/n}$ and $\gamma^{(q^r-1)/n_\ell}$ are elements of order n and n_ℓ.

The Non-Zero-Locator Code (iii)

We rewrite (1).
We search the "longest" sequence:

$$c(\alpha^e)a(\beta^0), c(\alpha^{e+1})a(\beta^1), \ldots, c(\alpha^{e+\mu-2})a(\beta^{\mu-2}),$$

that results in a zero-sequence of length $\mu - 1$.

пример: Binary Cyclic Code of Length 17

$D_{\mathcal{C}}$	-4	□	-2	-1	□	1	2	□	4
$D_{\mathcal{P}}$	□	3	□	□	3	□	□	3	□

Theorem on the Minimum Distance

теорема (Minimum Distance)

Let

- *q-ary cyclic code $\mathcal{C}(q; n, k, d)$ and*
- *non-zero-locator code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$*
- *with $\gcd(n, n_\ell) = 1$ and the integer μ be given.*

Then:

$$d \geq d^* \stackrel{\text{def}}{=} \left\lceil \frac{\mu}{d_\ell} \right\rceil .$$

Theorem on the Minimum Distance

Теорема (Minimum Distance)

Let

- *q-ary cyclic code $\mathcal{C}(q; n, k, d)$ and*
- *non-zero-locator code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$*
- *with $\gcd(n, n_\ell) = 1$ and the integer μ be given.*

Then:

$$d \geq d^* \stackrel{\text{def}}{=} \left\lceil \frac{\mu}{d_\ell} \right\rceil .$$

Let $a(x) = 1$ be the low-weight codeword $\in \mathcal{L}(q_\ell; n_\ell, n_\ell, 1)$. Then,

$$\sum_{j=0}^{\infty} c(\alpha^{j+e}) a(\beta^j) x^j \equiv 0 \bmod x^{\mu-1},$$

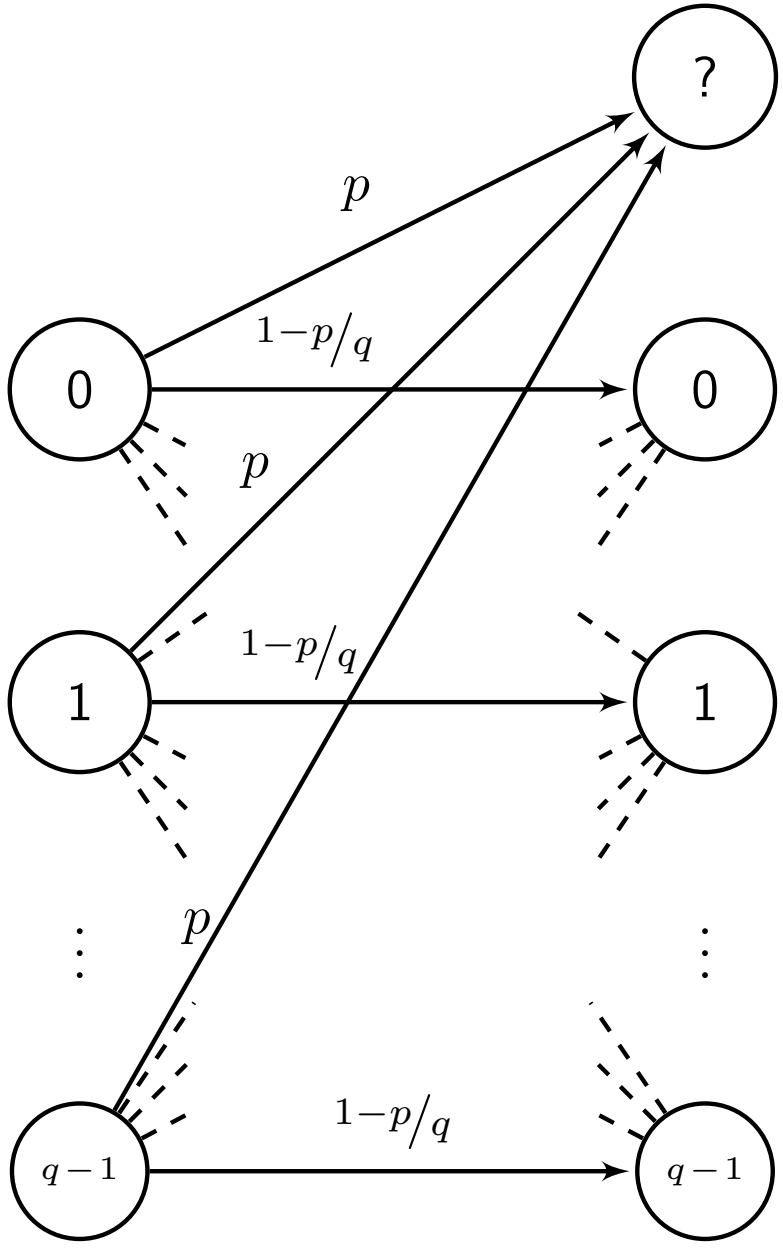
becomes

$$c(\alpha^{j+e}) 1 = 0, \quad \forall j = 0, \ldots, \mu - 1.$$

$\Longrightarrow$ BCH Bound!

Outline

Erasure Channel



Channel Model

- Input: q-ary alphabet
- Output: $(q+1)$-ary alphabet

Erasure probability is p.

Erasures and Received Word

Let:

- the set $\mathcal{E} = \{i_0, i_1, \ldots, i_{\varepsilon-1}\}$ with $|\mathcal{E}| = \varepsilon$ be the set of erroneous positions and
- the polynomial $e(x) = \sum_{i \in \mathcal{E}} e_i x^i$ and
- "?" mark an erasure and
- set $\mathcal{D} = \{j_0, j_1, \ldots, j_{\delta-1}\}$ with $|\mathcal{D}| = \delta$ be the set of erased positions

Erasures and Received Word

Let:

- the set $\mathcal{E} = \{i_0, i_1, \ldots, i_{\varepsilon-1}\}$ with $|\mathcal{E}| = \varepsilon$ be the set of erroneous positions and
- the polynomial $e(x) = \sum_{i \in \mathcal{E}} e_i x^i$ and
- "?" mark an erasure and
- set $\mathcal{D} = \{j_0, j_1, \ldots, j_{\delta-1}\}$ with $|\mathcal{D}| = \delta$ be the set of erased positions

and we have the received polynomial:

$$\widetilde{r}(x) = \sum_{i=0}^{n-1} \widetilde{r}_i x^i \quad \text{with} \quad \widetilde{r}_i \in \mathbb{F}_q \cup \{?\}.$$

Erasure Polynomial and Modified Received Word

Substitution of ? by an arbitrary element from $\mathbb{F}_q$ (zero).
We define the erasure polynomial:

$$d(x) = \sum_{i \in \mathcal{D}} d_i x^i,$$

such that $\widetilde{r}_i + d_i = c_i + d_i = 0, \ \forall i \in \mathcal{D}$.

Erasure Polynomial and Modified Received Word

Substitution of ? by an arbitrary element from $\mathbb{F}_q$ (zero).
We define the erasure polynomial:

$$d(x) = \sum_{i \in \mathcal{D}} d_i x^i,$$

such that $\widetilde{r}_i + d_i = c_i + d_i = 0, \ \forall i \in \mathcal{D}$.
Let the modified received polynomial $r(x) \in \mathbb{F}_q[x]$ be

$$r(x) = \sum_{i=0}^{n-1} r_i x^i = c(x) + d(x) + e(x).$$

Syndromes and Erasure-Locator Polynomial

Let a low-weight codeword:

$$a(x) = \prod_{j \in \mathcal{Z}} a_j x^j,$$

with $|\mathcal{Z}| = d_\ell$ be given.
We define a syndrome polynomial $S(x) \in \mathbb{F}_{q^r}[x]$ as follows:

$$S(x) \stackrel{\text{def}}{\equiv} \sum_{j=0}^{\infty} r(\alpha^{j+e}) a(\beta^j) x^j \mod x^{\mu-1}.$$

Syndromes and Erasure-Locator Polynomial

Let a low-weight codeword:

$$a(x) = \prod_{j \in \mathcal{Z}} a_j x^j,$$

with $|\mathcal{Z}| = d_\ell$ be given.
We define a syndrome polynomial $S(x) \in \mathbb{F}_{q^r}[x]$ as follows:

$$S(x) \stackrel{\text{def}}{=} \sum_{j=0}^{\infty} r(\alpha^{j+e}) a(\beta^j) x^j \mod x^{\mu-1}.$$

The corresponding erasure-locator polynomial $\Psi(x) \in \mathbb{F}_{q^r}[x]$ and error-locator polynomial $\Lambda(x) \in \mathbb{F}_{q^r}[x]$ are:

$$\Psi(x) \stackrel{\text{def}}{=} \prod_{i \in \mathcal{D}} \Big(\prod_{j \in \mathcal{Z}} \big(1 - x\alpha^i \beta^j\big) \Big)$$

$$\Lambda(x) \stackrel{\text{def}}{=} \prod_{i \in \mathcal{E}} \Big(\prod_{j \in \mathcal{Z}} \big(1 - x\alpha^i \beta^j\big) \Big).$$

Key Equation

With

$$\widetilde{S}(x) \stackrel{\text{def}}{\equiv} \Psi(x) \cdot S(x) \mod x^{\mu-1}$$

we obtain the following **Key Equation:**

Key Equation

With

$$\widetilde{S}(x) \stackrel{\text{def}}{\equiv} \Psi(x) \cdot S(x) \mod x^{\mu-1}$$

we obtain the following **Key Equation:**

$$\widetilde{S}(x) \equiv \frac{\widetilde{\Omega}(x)}{\Lambda(x)} \mod x^{\mu-1}$$

with

$$\begin{aligned} \deg \Lambda(x) &= \varepsilon \cdot d_\ell \\ \deg \widetilde{\Omega}(x) &\leq (\varepsilon + \delta) \cdot d_\ell - 1. \end{aligned}$$

Decoding up to the New Bound

Error/Erasure Decoding

Input: Received Word $\widetilde{r}(x)$, Low-weight Codeword $a(x) = \sum_{j \in \mathcal{Z}} a_j x^j \in \mathcal{L}$, Integers e and μ

Prepr.: Calculate one root γ_i of each $\prod_{j \in \mathcal{Z}} \left(1 - x\alpha^i \beta^j\right)$ with $\gamma_i = \beta^{-\kappa} \alpha^{-i}$, where $\kappa \in \mathcal{Z}$

1. Remove erasures from $\widetilde{r}(x) \Rightarrow r(x)$
2. Calculate erasure-polynomial $\Psi(x)$
3. Calculate $S(x)$ and $\widetilde{S}(x)$
4. Obtain $\Lambda(x)$, $\widetilde{\Omega}(x)$ from $\texttt{EEA}\left(x^{\mu-1}, \widetilde{S}(x)\right)$
5. Find all i for which $\Lambda(\gamma_i) = 0$
6. Save them as $\widehat{\mathcal{E}} = \{i_0, i_1, \ldots, i_{\varepsilon-1}\}$ and $\widehat{\mathcal{D}} = \{i_0, i_1, \ldots, i_{\delta-1}\}$
7. Determine Error/Erasure values $e_{i_0}, e_{i_1}, \ldots, e_{i_{\varepsilon-1}}$ and $d_{i_0}, d_{i_1}, \ldots, d_{i_{\delta-1}}$
8. $\widehat{e}(x) \leftarrow \sum_{i \in \widehat{\mathcal{E}}} e_i x^i$ and $\widehat{d}(x) \leftarrow \sum_{i \in \widehat{\mathcal{D}}} d_i x^i$
9. $\widehat{c}(x) \leftarrow r(x) - \widehat{e}(x) - \widehat{d}(x)$

Output: Estimated codeword $\widehat{c}(x)$

Outline

Conclusion and Outlook

Results

The concept of the non-zero-locator code was extended to combined error/erasure decoding:

- A modified **Key Equation** was derived and
- The EEA can be used to solve it.

Conclusion and Outlook

Results

The concept of the non-zero-locator code was extended to combined error/erasure decoding:

- A modified **Key Equation** was derived and
- The EEA can be used to solve it.

Outlook

- Further investigation of "good" non-zero-locator codes.
- Adaption to non-cyclic block codes.
- Sub-quadratic-time modification of the EEA.

Thank you

Благодаря ви за вниманието!