A Lower Bound of the Covering Radius of Irreducible Goppa Codes

Sergey Bezzateev and Natalia Shekhunova
bsv@aanet.ru sna@delfa.net
Saint Petersburg University of Aerospace Instrumentation
Russia

ACCT 2016: Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18 - 24, 2016, Albena, Bulgaria

Covering radius

The covering radius of a linear code C with a length n is defined as the least integer $\mathcal{R}(C)$ such that for any vector $\mathbf{x}$ of an n- dimensional space that does not belong to code C, a codeword $\mathbf{c} \in C$ is found that is located at a distance not exceeding $\mathcal{R}(C)$.

$$\mathcal{R}(C) = max\left\{min\left\{wt(\mathbf{x}+\mathbf{c}), \mathbf{c} \in C\right\}, \mathbf{x} \in Z_q^n\right\}.$$

Goppa codes: definitions

Goppa codes defined by a Goppa polynomial

$$G(x) \in \mathbb{F}_{q^m}[x], \deg G(x) = t$$

and location set of codeword positions

$$L = \{\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_i \in GF(q^m), G(\alpha_i) \neq 0\}.$$

Definition 1 *A q-ary vector $\mathbf{a} = (a_1 a_2 \ldots a_n)$ is a codeword of $\Gamma(L, G)$-code if the following congruence is satisfied*

$$\sum_{i=1}^{n} a_i \frac{1}{x - \alpha_i} \equiv 0 \ \ mod\, G(x).$$

Irreducible Goppa codes

Definition 2 *The $\Gamma(L, G)$ - code is called an **irreducible** one if the Goppa polynomial $G(x)$ is irreducible over $GF(q^m)$. The length of this code is equal to $n = q^m$.*

In the general case, the lower bound of the covering radius of Goppa codes is known for reducible separable Goppa codes only. It was proved by A. Tietavainen (1987) by using so-called the "Supercode Lemma".

Lemma 1 (The Supercode Lemma) *Let C_1 and C_2 be linear codes and $C_1 \subset C_2$. Then*

$$\mathcal{R}(C_1) \geq min\{wt(\mathbf{x}), \mathbf{x} \in C_2 \setminus C_1\} = d(C_2),$$

where $d(C_2)$ is the minimum distance of the code C_2.

Definition of $\Gamma(L, G)$-code as generalized (L, G)-code

Definition 3 (E.T.Mironchikov and N.A.Shekhunova, 1981) *A q-ary block code with a polynomial $G(x)$ of a degree τ and location set*

$$L = \{U_i(x)\}_{i=1}^{n}$$

where $U_i(x) = \frac{1}{x-\alpha_i}, \alpha_i \in GF(q^m), \alpha_i \neq \alpha_j$ and $G(\alpha_i) \neq 0$

is called a (L, G)-code if any q-ary vector $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ satisfying the equation

$$\sum_{i=1}^{n} a_i U_i(x) \equiv 0 \mod G(x)$$

is a codeword of this code.

Parameters of the irreducible $\Gamma(L, G)$-code

It is known that the irreducible $\Gamma(L, G)$-code has the following parameters:

$$n = |L| = q^m, \quad k \geq n - \tau m, \quad d \geq \tau + 1.$$

Extended $\Gamma(L, G)$-code

The $\Gamma(L, G)$-code can be extended by the addition of a parity check for all symbols of a codeword of $\Gamma(L, G)$-code. [E.R.Berlekamp, O.Moreno, 1973]

Definition 4 *The extension by a parity check of a code C of length n over $GF(q)$ is the code $\widehat{C}$ of length $n+1$ defined by:*

$$\widehat{C} = \left\{ \widehat{\boldsymbol{a}} = (a_1 \dots a_{n+1}) | \boldsymbol{a} = (a_1 \dots a_n) \in C \text{ and } \sum_{i=1}^{n+1} a_i = 0 \right\}.$$

Therefore, the location set $L_1 = L \cup \{1\}$ for the code $\widehat{C}$ has all the possible unitary polynomials from $F_{q^m}[x]$ of degree less or equal 1 as denominators of rational fractions.

Locator set of extended $\Gamma(L, G)$-code

$$\sum_{i=1}^{q^m+1} a_i U_i(x)) \equiv 0 \mod G(x)$$

$$U_i(x) = \frac{1}{x-\alpha_i}, \alpha_i \in GF(q^m), i = 1, \ldots, q^m,$$

$$U_{q^m+1}(x) = 1.$$

A q-ary $\Gamma_1(L_1, G)$-code with the location set $L_1 = \{U_i(x)\}_{i=1}^{q^m+1}$ and parameters:

$$n_1 = q^m + 1, \quad k_1 \geq n_1 - \tau m, \quad d_1 \geq \tau + 1.$$

The parity check matrix of the $\Gamma_1(L_1, G)$-code is

$$H_1 = \begin{pmatrix} G^{-1}(\alpha_1) & G^{-1}(\alpha_2) & \ldots & G^{-1}(\alpha_{n-1}) & G^{-1}(0) & 0 \\ \alpha_1 G^{-1}(\alpha_1) & \alpha_2 G^{-1}(\alpha_2) & \ldots & \alpha_{n-1} G^{-1}(\alpha_{n-1}) & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \alpha_1^{r-1} G^{-1}(\alpha_1) & \alpha_2^{r-1} G^{-1}(\alpha_2) & \ldots & \alpha_{n-1}^{r-1} G^{-1}(\alpha_{n-1}) & 0 & \frac{1}{g_r} \end{pmatrix}$$

$\Gamma(L, G)$-code extended by nominators

According to the V.D.Goppa extension [V.D. Goppa,1972], we obtain a q-ary $\Gamma_2(L_2, G)$-code with the location set:

$$L_2 = \left\{ \left\{ \frac{\lambda_j}{x - \alpha_i} \right\}_{j=1,m} \right\}_{i=1,n}, \tag{1}$$

where $\{\lambda_1, \lambda_2, \ldots, \lambda_m\}$ is the basis of $GF(q^m)$ over the field $GF(q)$ and with the following parameters :

$$n_2 = mq^m, \quad k_2 \geq n_2 - \tau m, \quad d_2 \geq \tau + 1.$$

Extended $\Gamma(L, G)$-code by nominators

A q-ary vector $\boldsymbol{c} = (c_{11}c_{12}\ldots c_{1m}c_{21}\ldots c_{nm})$ will be a codeword of the $\Gamma_2(L_2, G)$-code iff the following equality is satisfied:

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{c_{ij}\lambda_j}{x-\alpha_i} \equiv 0 \mod G(x).$$

Remark 1 *This code is an error-block correcting code [K. Feng, L. Xu, F.J. Hickernell,2006] with a partition* $\pi = [m]^{q^m}$.

$\Gamma(L, G)$-code extended by location set

Using both previous methods for extending $\Gamma(L, G)$-code we obtain a q-ary $\Gamma_3(L_3, G)$-code with the following parameters:

$$n_3 = mq^m + m, \quad k_3 \leq n_3 - \tau m, \quad d_3 \geq \tau + 1.$$

The location set is:

$$L_3 = L_2 \cup \{\lambda_1, \lambda_2, \ldots, \lambda_m\}.$$

Remark 2 *It is easy to see that, at the same time, this code according to [K. Feng, L. Xu, F.J. Hickernell, 2006], is an error-block correcting code with the partition* $\pi = [m]^{q^m+1}$.

Example:q-ary Hamming code as extended $\Gamma(L,G)$-code

The location set is:

$$L_3 = L_2 \cup \{\lambda_1, \lambda_2, \ldots, \lambda_{\frac{q^m-1}{q-1}}\}.$$

where

$$L_2 = \left\{ \left\{ \frac{\lambda_j}{x-\alpha_i} \right\}_{j=1,\frac{q^m-1}{q-1}} \right\}_{i=1,q^m},$$

and

$$\{\lambda_1 = 1, \lambda_2 = \alpha^{q-1}, \ldots, \lambda_i = \lambda_1 \alpha^{(i-1)(q-1)}, \ldots\}$$

is the multiplicative group in $GF(q^m)$. α ia a primitive element in $GF(q^m)$. $G(x)$ is any irreducible polynomial of degree 2.
We obtain a q-ary $\Gamma_3(L_3,G)$-code with the following parameters:

$$n_3 = \frac{q^m-1}{q-1}q^m + \frac{q^m-1}{q-1} = \frac{q^{2m}-1}{q-1}, \quad k_3 = n_3 - 2m, \quad d_3 = 3.$$

Error vectors and syndromes for $\Gamma(L, G)$-code

Let $\boldsymbol{e} = (e_1 e_2 \dots e_n), e_i \in GF(q)$ be an error vector.

$$S(x) \equiv \sum_{i=1}^{n} \frac{e_i}{x - \alpha_i} \equiv \frac{\sigma(x)}{\omega(x)} \mod G(x).$$

Rational fraction $\frac{\sigma(x)}{\omega(x)}, \deg \omega(x) = 1, \deg \sigma(x) = 0$ for the location set $L = GF(q^m)$ can be obtained if

$$wt(\boldsymbol{e}) = 1 \text{ and } \omega(x) = x - \alpha_i, \sigma(x) = e_i \in GF(q) \setminus \{0\}.$$

It is also exist another $q^m(q^m - q)$ different syndromes S_{ij}

$$S_{ij} \equiv \frac{b_{ij}}{x - \alpha_i} \mod G(x), \quad \begin{array}{l} \alpha_i \in GF(q^m), \\ b_{ij} \in GF(q^m) \setminus GF(q) \end{array}$$

that can not be obtained by any error vector $\boldsymbol{e}$ of weight 1.

Covering radius of irreducible $\Gamma(L, G)$-code

Let $\boldsymbol{e}$ be a coset leader of the $\Gamma(L, G)$-code and S_{ij} be its syndrome.

$$\sum_{i=1}^{n} \frac{e_i}{x-\alpha_i} \equiv \frac{\phi(x)}{\psi(x)} \equiv S_{ij}(x) \equiv \frac{b_{ij}}{x-\alpha_i} \equiv \frac{\sigma(x)}{\omega(x)} \mod G(x),$$
$$\deg \phi(x) < \deg \psi(x) = wt(\boldsymbol{e}), b_{ij} \in GF(q^m) \setminus GF(q)$$

so we have

$$\frac{\phi(x)}{\psi(x)} \equiv \frac{\sigma(x)}{\omega(x)} \mod G(x).$$

This equality will be fulfilled if and only if
$\max(\deg \psi(x), \deg \psi(x) - 1 + \deg \omega(x)) \geq \deg G(x)$,
i.e., $wt(\boldsymbol{e}) \geq \deg G(x)$.
Hence, we have the lower bound of the covering radius of the $\Gamma(L, G)$-code:

$$\mathcal{R}(\Gamma(L, G)) \geq \deg G(x).$$

Covering radius of irreducible $\Gamma_1(L_1, G)$ -code

$$L_1 = L \cup \{1\}.$$

We have $q^m(q^m - q)$ different syndromes S_{ij} corresponding to rational fractions:

$$S_{ij} \equiv \frac{b_{ij}}{x - \alpha_i} \mod G(x), \quad \alpha_i \in GF(q^m), \quad b_{ij} \in GF(q^m) \setminus GF(q)$$

same as for L. Same as for $\Gamma(L, G)$-code these syndromes can not obtained for any error vector of weight 1. Therefore same as for $\Gamma(L, G)$ code we obtain the following lower bound of the covering radius:

$$\mathcal{R}(\Gamma_1(L_1, G)) \geq \deg G(x).$$

Covering radius of irreducible $\Gamma_2(L_2, G)$-code

$$L_2 = \left\{ \left\{ \frac{\lambda_j}{x - \alpha_i} \right\}_{j=1,\frac{q^m-1}{q-1}} \right\}_{i=1,n}.$$

We have q^m different syndromes S_j corresponding to

$$S_j \equiv b_j \mod G(x), \quad b_i \in GF(q^m) \setminus \{0\}.$$

These syndromes can not obtained for any error vector of weight 1. Therefore same as for $\Gamma(L, G)$ and $\Gamma_1(L_1, G)$- codes we obtain the following lower bound of the covering radius:

$$\mathcal{R}(\Gamma_2(L_2, G)) \geq \deg G(x).$$

Error vectors and syndromes for $\Gamma_3(L_3, G)$-code

Let

$$\boldsymbol{e} = (e_{11}e_{12}\dots e_{1m}e_{21}\dots e_{nm}e_{01}e_{02}\dots e_{0m}), e_{ij} \in GF(q).$$

$$S(x) \equiv \sum_{i=1}^{n}\sum_{j=1}^{m}\frac{e_{ij}\lambda_j}{x-\alpha_i} + \sum_{j=1}^{m} e_{0j}\lambda_j \mod G(x).$$

For location set L_3 and the error vector $\boldsymbol{e}$ with $wt_\pi(\boldsymbol{e}) = 1$ we can obtain $S(x)$ as a rational fraction

$$\frac{\sigma(x)}{\omega(x)}, \deg\omega(x) = 1, \deg\sigma(x) = 0,$$

where $\omega(x) = x - \alpha_i,\ \alpha_i \in GF(q^m)$,

$$\sigma(x) = \sum_{j=1}^{m} e_{ij}\lambda_j = \sigma_0, \sigma_0 \in GF(q^m)\setminus\{0\}$$

or as an element $\sum_{j=1}^{m} e_{0j}\lambda_j \in GF(q^m)$.

Lemma about syndromes

We use here generalization for nonbinary case of Lemma about number of different syndromes and fractions [S.Bezzateev, Shekhunova , 2015].

Lemma 2 *The number of different nonzero syndromes* $S_{ij}(x) \in \mathbb{F}_{q^m}[x]$, $\deg S_{ij}(x) < \deg G(x)$ *such that*

$$\frac{a_{ij}}{\varphi_i(x)} = S_{ij}(x) \; mod \; G(x)$$

is equal to $q^{m\tau} - 1$,
where $G(x)$ *is a unitary separable polynomial from* $\mathbb{F}_{q^m}[x]$,
$\deg G(x) = \tau$,
$\varphi_i(x)$ *is a unitary polynomial from* $\mathbb{F}_{q^m}[x]$,
$0 \leq \deg \varphi_i(x) \leq \tau - 1$, $a_{ij} \in GF(q^m) \setminus \{0\}$.

General case: Covering radius of irreducible $\Gamma_3(L_3, G)$-code

From Lemma we obtain that for any irreducible polynomial $\varphi_i(x)$ of the second degree, a corresponding error vector $\boldsymbol{e}$ should exist. Let us define a coset leader $\boldsymbol{e}$ of $\Gamma_3(L_3, G)$-code and let $S_{ij} \equiv \frac{a_{ij}}{\varphi_i(x)} \mod G(x)$ be its syndrome.

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{e_{ij}\lambda_j}{x-\alpha_i} + \sum_{j=1}^{m} e_{0j}\lambda_j \equiv \frac{\phi(x)}{\psi(x)} \equiv S_{ij}(x) \equiv \frac{a_{ij}}{\varphi_i(x)} \mod G(x),$$

$\deg\phi(x) < \deg\psi(x) = wt_\pi(\boldsymbol{e}) \le wt(\boldsymbol{e})$, or

$\frac{\phi(x)}{\psi(x)} \equiv \frac{a_{ij}}{\varphi_i(x)} \mod G(x)$.

$\max(\deg\psi(x), \deg\phi(x)+2) \ge \deg G(x)$, i.e.

$wt(\boldsymbol{e}) \ge wt_\pi(\boldsymbol{e}) \ge \tau - 1$.

The lower bound of the covering radius of the irreducible $\Gamma_3(L_3, G)$-code:

$$\mathcal{R}(\Gamma_3(L_3, G)) \ge \tau - 1.$$

Example: Covering radius for q-ary Hamming code as $\Gamma_3(L_3, G)$-code

q-ary $\Gamma_3(L_3, G)$-code with the following parameters:

$$n_3 = \frac{q^m-1}{q-1}q^m + \frac{q^m-1}{q-1} = \frac{q^{2m}-1}{q-1}, \quad k_3 = n_3 - 2m, \quad d_3 = 3.$$

$$\tau = \deg G(x) = 2$$

and

$$L_3 = L_2 \cup \{\lambda_1, \lambda_2, \ldots, \lambda_m\}$$

where

$$L_2 = \left\{ \left\{ \frac{\lambda_j}{x - \alpha_i} \right\}_{j=1,\frac{q^m-1}{q-1}} \right\}_{i=1,n}.$$

Covering radius:

$$\mathcal{R}(\Gamma_3(L_3, G)) \geq \tau - 1 = 1.$$

Research Problem (12.3): What other extended Goppa codes are cyclic?

- Covering radius
- Goppa codes: definitions
- Error vectors and syndromes for $\Gamma(L, G)$-code
- Covering radius of irreducible $\Gamma(L, G)$-code
- Covering radius of irreducible $\Gamma_1(L_1, G)$ -code
- Covering radius of irreducible $\Gamma_2(L_2, G)$-code
- Error vectors and syndromes for $\Gamma_3(L_3, G)$-code
- Lemma about syndromes
- General case: Covering radius of irreducible $\Gamma_3(L_3, G)$-code

p.357, MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Amsterdam, Netherlands, North-Holland (1977)

Questions

- Covering radius
- Goppa codes: definitions
- Error vectors and syndromes for $\Gamma(L, G)$-code
- Covering radius of irreducible $\Gamma(L, G)$-code
- Covering radius of irreducible $\Gamma_1(L_1, G)$ -code
- Covering radius of irreducible $\Gamma_2(L_2, G)$-code
- Error vectors and syndromes for $\Gamma_3(L_3, G)$-code
- Lemma about syndromes
- General case: Covering radius of irreducible $\Gamma_3(L_3, G)$-code

THANK YOU !