Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 54–59*

A lower bound of the covering radius of irreducible Goppa codes

Sergey V. Bezzateev bsv@aanet.ru
Natalia A. Shekhunova sna@delfa.net
Saint Petersburg State University of Aerospace Instrumentation, Bolshaya Morskaya, 67, Saint Petersburg, 190000, Russia

A lower bound of the covering radius of non-binary irreducible Goppa codes is obtained.

1 Introduction

Problem of finding the covering radius(CR) of different classes of block codes remains topical for a long time. The known results of the CR of many classes of block codes were extended in [1–4]. In particular, the upper bound of irreducible Goppa codes was presented in [4]. The lower bound for the CR of binary irreducible Goppa codes was presented by authors in [5]. Let us give some definitions which are necessary for the explanation of the results presented in this paper.

Definition 1. *[6] A q-ary block code with a polynomial $G(x)$ of a degree τ and location set*

$$L = \{U_i(x)\}_{i=1}^{n} \ \text{ where } U_i(x) = \frac{1}{x-\alpha_i}, \alpha_i \in GF(q^m), \alpha_i \neq \alpha_j \tag{1}$$

and $G(\alpha_i) \neq 0$ is called a $\Gamma(L,G)$-code(Goppa code) if any q-ary vector $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ satisfying the following equation

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

is a codeword of this code.

It is known [7] that the $\Gamma(L,G)$-code has the following parameters:

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

Definition 2. *[7] The $\Gamma(L,G)$-code is called an irreducible one if polynomial $G(x)$ is irreducible over $GF(q^m)$.*

It is clear that a length of this code is equal to $n = q^m$. The class of Goppa codes is a subclass of extended RS-codes (alternant codes) [7]. A parity-check matrix of $\Gamma(L, G)$-code with $G(x) = G(x) = g_r x^r + g_{r-1}x^{r-1} + \ldots + g_1 x + g_0$ can be written in the following form [7]:

$$H = \begin{pmatrix} G^{-1}(\alpha_1) & G^{-1}(\alpha_2) & \ldots & G^{-1}(\alpha_{n-1}) & G^{-1}(0) \\ \alpha_1 G^{-1}(\alpha_1) & \alpha_2 G^{-1}(\alpha_2) & \ldots & \alpha_{n-1} G^{-1}(\alpha_{n-1}) & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{r-1} G^{-1}(\alpha_1) & \alpha_2^{r-1} G^{-1}(\alpha_2) & \ldots & \alpha_{n-1}^{r-1} G^{-1}(\alpha_{n-1}) & 0 \end{pmatrix}. \tag{2}$$

The $\Gamma(L, G)$-code can be extended by the addition of parity check for all symbols of a codeword of $\Gamma(L, G)$-code [9–13].

Definition 3. *[7] The extension by parity check of a code C of length n over $GF(q)$ is the code $\widehat{C}$ of length $n + 1$ defined by*

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

Therefore, the location set $L_1 = L \cup \{1\}$ for the code $\widehat{C}$ has all possible unitary polynomials from $F_{q^m}[x]$ of degree less or equal 1 as denominators of rational fractions. It is obvious that we can make the same extension without overall parity check and obtain a q-ary $\Gamma_1(L_1, G)$-code with the location set L_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 can be written in the following form:

$$H_1 = \begin{pmatrix} G^{-1}(\alpha_1) & G^{-1}(\alpha_2) & \ldots & G^{-1}(\alpha_{n-1}) & G^{-1}(0) & 0 \\ \alpha_1 G^{-1}(\alpha_1) & \alpha_2 G^{-1}(\alpha_2) & \ldots & \alpha_{n-1} G^{-1}(\alpha_{n-1}) & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \alpha_1^{r-1} G^{-1}(\alpha_1) & \alpha_2^{r-1} G^{-1}(\alpha_2) & \ldots & \alpha_{n-1}^{r-1} G^{-1}(\alpha_{n-1}) & 0 & \frac{1}{g_r} \end{pmatrix}, \tag{3}$$

Now let us use an extension of an irreducible q-ary Goppa code that was presented by V.D.Goppa in [15]. According to the Goppa extension, we obtain a q-ary $\Gamma_2(L_2, G)$-code with the location set

$$L_2 = \left\{ \left\{ \frac{\lambda_j}{x - \alpha_i} \right\}_{j=1,m} \right\}_{i=1,n}, \tag{4}$$

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

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

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

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

This code is an error-block correcting code [14] with a partition $\pi = [m]^{q^m}$. It means that codeword of the $\Gamma_2(L_2, G)$-code can be represented as a vector

$$\boldsymbol{c} = (c_{11}c_{12}\dots c_{1m}c_{21}\dots c_{nm}) = (\boldsymbol{u}_1\boldsymbol{u}_2\dots\boldsymbol{u}_n),\ \boldsymbol{u}_i = (e_{i1}e_{i2}\dots e_{im}).$$

It is known [14] that the minimum distance between two vectors $\boldsymbol{c} = (\boldsymbol{u}_1\boldsymbol{u}_2\dots\boldsymbol{u}_n)$ and $\boldsymbol{b} = (\boldsymbol{v}_1\boldsymbol{v}_2\dots\boldsymbol{v}_n)$ in the $\pi-$ metric is defined as

$$d_\pi(\boldsymbol{c}, \boldsymbol{b}) = wt_\pi(\boldsymbol{c} - \boldsymbol{b}) = \sharp\{i | 1 \le i \le n, \boldsymbol{u}_i \ne \boldsymbol{v}_i\}.$$

Using the technique considered above for the transformation of the $\Gamma(L, G)$-code in the $\Gamma_1(L_1, G)$-code and extending it by the basis of the field $GF(q^m)$ over $GF(q)$ we obtain a q-ary $\Gamma_3(L_3, G)$-code with the following parameters:

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

The location set

$$L_3 = L_2 \cup \{\lambda_1, \lambda_2, \dots, \lambda_m\}. \tag{5}$$

It is easy to see that at the same time this code according to [14] is an error-block correcting code with partition $\pi = [m]^{q^m+1}$.

2 Main result

First of all, let us consider the $\Gamma(L, G)$-code with $n = q^m$. Let $\boldsymbol{e} = (e_1e_2\dots e_n), e_i \in GF(q)$ be an error vector and we can write a syndrome $S(x)$ associated with this $\boldsymbol{e}$ as

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

It is clear that a rational fraction $\frac{\sigma(x)}{\omega(x)}, \deg\omega(x) = 1, \deg\sigma(x) = 0$ for the location set (1) can be obtained if

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

Then there exist $q^m(q^m - q)$ different syndromes S_{ij} corresponding to such different rational fractions:

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

and these syndromes can not be obtained for any error vector of weight 1. It is obvious that every such syndrome corresponds to its own error vector $\boldsymbol{e}$. Let an error vector $\boldsymbol{e}$ be a coset leader of the $\Gamma(L, G)$-code and S_{ij} be its syndrome. Then the following relation has to be satisfied:

$$\begin{array}{l}\sum\limits_{i=1}^{n} \frac{e_i}{x-\alpha_i} \equiv \frac{\phi(x)}{\psi(x)} \equiv S_{ij}(x) \equiv \frac{b_{ij}}{x-\alpha_i} \equiv \frac{\sigma(x)}{\omega(x)} \mod G(x), \\ \deg \phi(x) < \deg \psi(x) = wt(\boldsymbol{e}),\end{array}$$

have that is

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

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., $wt(\boldsymbol{e}) \geq \tau$. Hence, we have the lower bound of the covering radius of the $\Gamma(L, G)$-code:

$$\rho \geq \tau. \tag{6}$$

It is clear that the $\Gamma_2(L_2, G)$-code has the same lower bound. Finally, let us obtain the lower bound of the covering radius of irreducible $\Gamma_3(L_3, G)$-codes with the location set(5) and $n_3 = mq^m + m$. Let

$$\boldsymbol{e} = (e_{11}e_{12} \dots e_{1m}e_{21} \dots e_{nm}e_{01}e_{02} \dots e_{0m}), e_{ij} \in GF(q) \tag{7}$$

be an error vector. Then, for the $\Gamma_3(L_3, G)$-code the syndrome $S(x)$ corresponding to this error vector is defined by the following relation:

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

In this case, for location set (5) and the error vector $\boldsymbol{e}$ with $wt_\pi(\boldsymbol{e}) = 1$ we can obtain or a rational fraction:

$$\frac{\sigma(x)}{\omega(x)}, \deg \omega(x) = 1, \deg \sigma(x) = 0, \tag{8}$$

or an element

$$\sum_{j=1}^{m} e_{0j}\lambda_j \in GF(q^m), \tag{9}$$

where

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

In other words, a possible error vector of weight 1 in π-metric is defined by a syndrome corresponding to any rational fraction (8) or to any element (9).
Now, for the proof of the lower bound of the covering radius of the $\Gamma_3(L_3, G)$-code we use Lemma 1 similar to Lemma 3 from [5] .

Lemma 1. *The number of different nonzero syndromes* $S_{ij}(x) \in \mathbb{F}_{q^m}[x]$, $\deg S_{ij}(x) < \deg G(x)$ *such that*

$$\frac{a_{ij}}{\varphi_i(x)} = S_{ij}(x) \; mod \; G(x) \tag{10}$$

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

There exists an unique rational fraction of the form (10) that is, for every $q^{m\tau} - 1$ possible nonzero syndrome S_{ij} (10). Thus, there exists an irreducible polynomial $\varphi_i(x)$ of the second degree and an element $a_{ij} \in GF(q^m)$ such that relation (10) from Lemma 1 is fulfilled. For any such polynomial $\varphi_i(x)$ of the second degree, a corresponding error vector should exist. Let us define a coset leader $\boldsymbol{e}$ of $\Gamma_3(L_3, G)$-code and $S_{ij} \equiv \frac{a_{ij}}{\varphi_i(x)} \mod G(x)$ be its syndrome. Obviously, for vector $\boldsymbol{e}$, the following equality has to be fulfilled:

$$\begin{array}{l} \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{m} \frac{e_{ij}\lambda_j}{x-\alpha_i} + \sum\limits_{j=1}^{m} e_{0j}\lambda_j \equiv \frac{\phi(x)}{\psi(x)} \equiv S_{ij}(x) \equiv \frac{a_{ij}}{\varphi_i(x)} \mod G(x), \\ \deg \phi(x) < \deg \psi(x) = wt_\pi(\boldsymbol{e}) \leq wt(\boldsymbol{e}), \end{array}$$

or

$$\frac{\phi(x)}{\psi(x)} \equiv \frac{a_{ij}}{\varphi_i(x)} \mod G(x). \tag{11}$$

It is clear that relation (11) will be fulfilled if $\max(\deg \psi(x), \deg \phi(x) + 2) \geq \deg G(x)$ only, i.e. $wt(\boldsymbol{e}) \geq wt_\pi(\boldsymbol{e}) \geq \tau - 1$. Now, we immediately obtain the lower bound of the covering radius of the irreducible $\Gamma_3(L_3, G)$-code:

$$\rho \geq \tau - 1. \tag{12}$$

3 Conclusion

The lower bounds of the covering radius for all classes of q-ary irreducible Goppa codes (classical and extended) are presented.

References

[1] G.D.Cohen, S.N. Litsyn, A.C. Lobstein, H.F.Jr. Mattson, Covering radius 1985–1994, *Appl. Algebra Eng. Comm. Comp.*, 8, pp.173–239, 1997.

[2] G.D.Cohen, I. Honkala, S.N. Litsyn, A.C. Lobstein, *Covering codes*, North-Holland, Amsterdam, 1997.

[3] G.D. Cohen,M.G. Karpovsky, H. F. Mattson,Jr.,J.R. Schatz,Covering Radius- Survey and Recent Results,*IEEE Trans. Inform. Theory*, v. 31, n. 3, pp.328-343, 1985.

[4] F. Levy-dit-Vehel, S. Litsyn, Parameters of Goppa codes revisited, *IEEE Trans. Inform. Theory*, pp.1811-1819, 1997.

[5] S.V. Bezzateev, N.A. Shekhunova, Lower bound of the covering radius of binary irreducible Goppa codes. Pascale Charpin, Nicolas Sendrier, Jean-Pierre Tillich. WCC2015 - 9th International Workshop on Coding and Cryptography 2015, Apr 2015, Paris, France. 2016, Proceedings of the 9th International Workshop on Coding and Cryptography 2015 WCC2015. $< wcc2015.inria.f > . < hal - 01276223 >$

[6] N.A. Shechunova, E.T. Mironchikov, Cyclic (L, G)- codes, *Probl. Peredachi Inform.*, n.3, pp.3-10, 1981(in Russian).

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[8] V.D. Goppa, A new class of linear error-correcting codes, (in Russian), *Probl. Peredachi Inform.*, vol. 6, no. 3, pp.24-30, 1970.

[9] E.R.Berlekamp, O.Moreno, Extended Double-Error-Gorrecting Binary Goppa Codes Are Cyclic, *IEEE Trans. Inform. Theory*, v. 19, n. 6, pp.817-818, 1973.

[10] K.K.Tzeng, K.Zimmermann, On Extending Goppa Codes to Cyclic Codes, *IEEE Trans. Inform. Theory*, v. 21, n. 6, pp. 712-716, 1975.

[11] O.Moreno, Symmetries of Binary Goppa Codes, *IEEE Trans. Inform. Theory*, v. 25, n. 5, pp. 609-612, 1979.

[12] A.L.Vishnevetskii, Cyclicity of extended Goppa codes, *Probl. Peredachi Inform.* vol 18, n.3, pp. 14-18, 1982. Springer-Verlag, New York/ Berlin, 1985.

[13] H.Stichtenoth, Which extended Goppa codes are cyclic?, *J.Comb Theory*, vol. A 51, pp.205-220, 1989.

[14] K. Feng, L. Xu, F.J. Hickernell, Linear error-block codes, *Finite Fields Appl.*, vol. 12, pp. 638-652, 2006.

[15] V.D. Goppa, Some codes constructed on the basis of (L,g) codes, (in Russian), *Probl. Peredachi Inform.*, vol. 8, no. 2, pp. 107–109 , 1972.