

Lower bound of the covering radius of binary irreducible Goppa codes

Sergey Bezzateev, Natalia Shekhunova

▶ **To cite this version:**

Sergey Bezzateev, Natalia Shekhunova. Lower bound of the covering radius of binary irreducible Goppa codes. WCC2015 - 9th International Workshop on Coding and Cryptography 2015, Anne Canteaut, Gaëtan Leurent, Maria Naya-Plasencia, Apr 2015, Paris, France. hal-01276223

HAL Id: hal-01276223

https://inria.hal.science/hal-01276223

Submitted on 19 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Lower Bound of the Covering Radius of Binary Irreducible Goppa Codes

Sergey Bezzateev and Natalia Shekhunova

Saint Petersburg State University of Aerospace Instrumentation, Russia
bsv@aanet.ru, sna@delfa.net *

Abstract. The lower bound of the covering radius of binary irreducible Goppa codes is obtained.

1 Introduction

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 $\mathcal{R}(C)$. It follows from this definition that the covering radius $\mathcal{R}(C)$ of the binary linear code C can be written as:

$$\mathcal{R}(C) = max\left\{min\left\{wt(\mathbf{x} \oplus \mathbf{c}), \mathbf{c} \in C\right\}, \mathbf{x} \in Z_2^n\right\}.$$

It is known that the problem of finding the covering radius for different classes of block codes remains topical for a long time because it presents one of the versions of the classical problem of discrete mathematics: the covering of n - dimensional vector space with the least number of spheres of radius $\mathcal{R}(C)$ in Hamming metric so that every vector of the space belongs at least to one of the spheres. The upper and lower bounds of the covering radius for many classes of block codes were obtained and discussed in papers [1–6].

This paper presents the lower bound of the covering radius of binary irreducible Goppa codes.

Let us consider some definitions that we will use to prove the main result of this paper.

It is well-known that binary Goppa codes can be defined [7] by a Goppa polynomial $G(x) \in \mathbb{F}_{2^m}[x], \deg G(x) = t$ and set of numerators of codeword positions

$$L = \{\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_i \in GF(2^m), G(\alpha_i) \neq 0\}.$$

Definition 1. *[8] A binary vector* $\mathbf{a} = (a_1 a_2 \ldots a_n)$ *is a codeword of* $\Gamma(L, G)$*-code if the following congruence is satisfied*

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

* The research leading to these results has received funding from the Ministry of Education and Science of the Russian Federation according to the project part of the state funding assignment No. 2.2716.2014/, July 17th, 2014.

Definition 2. *[8] The Goppa code is called a separable code if its Goppa polynomial $G(x)$ has no multiple roots.*

Definition 3. *[8] The separable (L, G) - code with $L \subset GF(2^m)$ and $\deg G(x) = t$ is called a reducible one if all t roots of a polynomial $G(x)$ belong to $GF(2^m)$. The length of the code is equal to $n = 2^m - t$.*

Definition 4. *[8] The (L, G) - code is called an irreducible one if the Goppa polynomial $G(x)$ is irreducible over $GF(2^m)$. The length of this code is equal to $n = 2^m$.*

The known results on the covering radius of different classes of codes were extended in paper [9] and the upper bound of the covering radius of the irreducible Goppa codes was presented:

$$\mathcal{R}(C) \leq 2t + 1, \text{ if } 2^m \geq 4(t-1)^{4t+2} \left(\frac{2}{1 + \sqrt{1 - \frac{1}{(t-1)^{4t}}}} \right)^{4t+2}. \qquad (1)$$

O.Moreno [10] in 1981 proved that, when m is odd, the irreducible binary Goppa codes with parameters $(2^m, 2^m - 2m, 5)$ are quasi-perfect and hence the covering radius is equal to 3. Later G.L.Feng and K.K.Tzeng [11] showed that when m is even the covering radius is 4.

In 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 [12]. He used the "Supercode Lemma" for the proof of the lower bound of the covering radius of reducible separable Goppa codes.

Lemma 1. *(The Supercode Lemma from [1, 13]) 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.

It is obvious that for the reducible Goppa code C_1 with

$$G_1(x) = \prod_{i=1}^{t}(x - \alpha_{j_i}), L_1 = GF(2^m) \setminus \{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_t}\},$$

for example, Goppa code C_2 with

$$G_2(x) = \prod_{i=1}^{t-1}(x - \alpha_{j_i}), L_2 = L_1$$

can be chosen as a supercode. It means that in this case

$$\mathcal{R}(C_1) \geq d(C_2) \geq 2(t-1) + 1 = 2t - 1.$$

However, for the irreducible Goppa code C_1 with the Goppa polynomial $G_1(x) \in \mathbb{F}_{2^m}[x]$ and $L = GF(2^m)$ the supercode C_2 with $G_2(x) = \frac{G_1(x)}{x-\beta}$, $G_1(\beta) = 0$, $\beta \in GF(2^{mt}), L = GF(2^m)$ is the same as the code C_1, and hence it is impossible to use Lemma 1.

Therefore, "The Supercode Lemma" cannot be used for constructing the lower bound of the covering radius of irreducible Goppa codes. In general case for any binary code, a lower bound to the covering radius of the code is $\mathcal{R}(C)$, given by sphere-covering bound :

$$\sum_{i=0}^{\mathcal{R}(C)-1} \binom{n}{i} + \gamma_0 \binom{n}{\mathcal{R}(C)} = 2^{n-k}, \text{where } 0 < \gamma_0 \leq 1. \tag{2}$$

As far as we know, the nontrivial lower bound of the covering radius of irreducible Goppa codes has not been presented. The exhaustive algorithm for determining the coset leader weight distribution was presented in [14] and some results on covering radius for irreducible binary Goppa codes with lengths 32, 64 and 128 were obtained.

Below, we will prove that the lower bound of the covering radius of all binary irreducible Goppa codes of dimension $k = 2^m - mt, t = \deg G(x), L = GF(2^m)$ is defined by the following relation

$$\mathcal{R}(C) \geq 2t - 1. \tag{3}$$

In Section 3 we compare new bound (3) for covering radius and results obtained in [14].

2 Main result

We will use the results from [15, 16] for the proof of the lower bound of the covering radius of all binary irreducible Goppa codes.

Let us consider a binary irreducible Goppa code C of the length $n = 2^m$ and dimension $k = n - mt$, with the Goppa polynomial $G(x) \in \mathbb{F}_{2^m}[x], \deg G(x) = t$, and $L = GF(2^m)$.

Proposition 1. *(Lemma 2 from [16]) For every syndrome* $S_j(x) \equiv \sum_{i=1}^{n} e_{j_i} \frac{1}{x-\alpha_i} \mod G(x)$ *of a binary irreducible Goppa code C there exists its rational fraction* $\frac{\varphi_j'(x)}{\varphi_j(x)}$ *such that*

$$\frac{\varphi_j'(x)}{\varphi_j(x)} \equiv S_j(x) \mod G(x), \tag{4}$$

where $\varphi_j(x)$ is a separable polynomial with coefficients from $GF(2^m)$,
$\deg \varphi_j(x) \leq t$, $\varphi_j'(x)$ is a formal derivative of the polynomial $\varphi_j(x)$.
$\mathbf{e} = (e_1 e_2 \dots e_n)$ is an error vector, $wt(\mathbf{e}) \leq \mathcal{R}(C)$.

Theorem 1. *[8]*

The number of normalized polynomials of the degree ℓ irreducible over the field $GF(2^m)$ is determined by the value

$$I_{2^m}(\ell) = \frac{1}{\ell} \sum_{d|\ell} \mu(d) 2^{m\frac{\ell}{d}} \ ,$$

where $\mu(d)$ is the Möbius function:

$$\mu(d) = \begin{cases} 1 \ \text{ if } d = 1 \ ; \\ (-1)^r \text{ if } d \text{ is a product of } r \text{ different prime numbers;} \\ 0 \quad \text{in all other cases.} \end{cases}$$

Lemma 2. *[17]*

The number of unitary separable polynomials of degree $\ell > 1$ with coefficients from the field $GF(2^m)$ is $M_{2^m}^{\ell} = 2^{m\ell} - 2^{m(\ell-1)}$.

The number of different nonzero syndromes $S_j(x)$ is defined by the value $2^{mt} - 1$ and the number of different separable polynomials $\varphi_j(x)$ corresponding to these syndromes (4) is defined by $M - 1 = 2^{mt} - 1$. Where M is the number of all separable polynomials from $\mathbb{F}_{2^m}[x]$ of degree less or equal t [15, 16] :

$$\begin{array}{l} M = M_1 + M_2 + \ldots + M_t = 2^{mt}, \\ M_1 = 2^m, \\ \text{where } M_1 \text{ is the number of reducible separable polynomials} \\ \text{of the first degree,} \\ M_2 = \overline{M}_2 + \widetilde{M}_2 = M_{2^m}^2 = 2^{2m} - 2^m, \\ \text{where } \overline{M}_2 \text{ is the number of reducible separable polynomials} \\ \text{of the second degree,} \\ \widetilde{M}_2 \text{ is the number of irreducible over } GF(2^m) \text{ polynomials} \\ \text{of the second degree,} \\ \overline{M}_2 = \binom{2^m}{2} = 2^{2m-1} - 2^{m-1}, \widetilde{M}_2 = I_{2^m}(2) = \frac{2^{2m}-2^m}{2}, \\ \vdots \\ M_t = \overline{M}_t + \widetilde{M}_t = M_{2^m}^t = 2^{tm} - 2^{(t-1)m}, \\ \text{where } \overline{M}_t \text{ is the number of reducible separable polynomials} \\ \text{of degree } t, \\ \widetilde{M}_t \text{ is the number of irreducible over } GF(2^m) \text{ polynomials} \\ \text{of degree } t, \\ \widetilde{M}_t = I_{2^m}(t), \ \overline{M}_t = M_{2^m}^t - \widetilde{M}_t = 2^{tm} - 2^{(t-1)m} - I_{2^m}(t). \end{array} \tag{5}$$

Let us denote by T_i the number of different coset leaders of weight i of the code C. It is known that the following relations:

$$T_0 = 1, T_1 = n = 2^m, T_2 = \binom{n}{2}, T_t = \binom{n}{t}, \sum_{i=0}^{\mathcal{R}(C)} T_i = 2^{n-k}$$

are fulfilled for the code C.

Theorem 2. *For the binary irreducible Goppa code C of dimension $k = 2^m - mt$, Goppa polynomial $G(x), \deg G(x) = t$ and locator set $L = GF(2^m)$, the minimum weight τ of the coset leader $\mathbf{e} = (e_1 e_2 \dots e_n)$ corresponding to the syndrome*

$S(x) = \dfrac{\varphi^{'}(x)}{\varphi(x)}$, where $\varphi(x)$ is the irreducible polynomial of the second degree,

satisfies the relation

$$\tau \geq 2t - 1.$$

Proof. Let us consider the syndromes $S(x)$ satisfying the following relation:

$$\begin{array}{l} \frac{\varphi^{'}(x)}{\varphi(x)} \equiv S(x) \ \ mod\ G(x), \\ \varphi(x) \text{ is the irreducible polynomial}, \deg \varphi(x) = 2. \end{array} \tag{6}$$

Let the error vector $\mathbf{e} = (e_1 e_2 \dots e_n)$ be a coset leader of the code C corresponding to syndrome $S(x)$ that satisfies relation(6).

$$\begin{array}{l} S(x) \equiv \sum\limits_{i=1}^{n} e_i \frac{1}{x-\alpha_i} \equiv \frac{\sigma^{'}(x)}{\sigma(x)} \ \ mod\ G(x), wt(\mathbf{e}) = \tau \leq \mathcal{R}(C), \\ \sigma(x) = \prod\limits_{e_j \neq 0} (x - \alpha_j), \deg \sigma(x) = \tau. \end{array}$$

Then

$$\frac{\sigma^{'}(x)\varphi(x) + \varphi^{'}(x)\sigma(x)}{\sigma(x)\varphi(x)} \equiv 0 \ \ mod\ G(x).$$

Since the formal derivative is in the numerator, the relation can be rewritten as

$$\begin{array}{c} \frac{\sigma^{'}(x)\varphi(x)+\varphi^{'}(x)\sigma(x)}{\sigma(x)\varphi(x)} \equiv \frac{\omega^2(x)}{\psi(x)} \equiv 0 \ \ mod\ G(x), \\ \psi(x) = \sigma(x)\varphi(x), \omega^2(x) = \psi^{'}(x). \end{array}$$

$\deg \omega(x) \geq t$ and, therefore $\deg \psi^{'}(x) \geq 2t, \deg \psi(x) \geq \deg \psi^{'}(x) + 1 = 2t + 1.$

So, $\tau = \deg \sigma(x) = \deg \psi(x) - \deg \varphi(x) \geq 2t - 1.$

Remark 1. According to (5), there exist only $\widetilde{M}_2 = \frac{2^{2m}-2^m}{2}$ different syndromes $S(x)$ satisfying relation (6).

Corollary 1. *The lower bound of the covering radius $\mathcal{R}(C)$ of the binary irreducible Goppa code C of dimension $k = 2^m - mt$ with $G(x) \in \mathbb{F}_{2^m}[x], \deg G(x) = t$ and $L = GF(2^m)$ is defined by the inequality*

$$\mathcal{R}(C) \geq \tau \geq 2t - 1.$$

Corollary 2. *The lower bound of the number of coset leaders of the code C, with the weight not less than $2t - 1$ is defined by the number $\widetilde{M}_2$ of different syndromes $S(x)$ satisfying relation (6):*

$$\sum_{i=2t-1}^{\mathcal{R}(C)} T_i \geq \widetilde{M}_2 = \frac{2^{2m} - 2^m}{2}.$$

3 Examples

As examples we present Table 1 and Table 2 showing the values of the covering radius results for irreducible binary Goppa codes that were obtained in [14] by using algorithm to evaluate the coset leader weight distribution, sphere-covering bound (2) and new lower bound of covering radius (3) for some binary codes described in [14].

Table 1. The covering radius of $(32, k)$ irreducible binary Goppa codes.

Goppa code (n, k, d)	(32,22,5)	(32,17,7)	(32,11,9)	(32,6,11)
covering radius [14]	3	6	8	12
new lower bound (3)	3	5	7	9
sphere-covering bound (2)	3	4	6	7

Table 2. The covering radius of $(64, k)$ and $(128, 93)$ irreducible binary Goppa codes.

Goppa code (n, k, d)	(64,52,5)	(64,46,7)	(64,40,9)	(64,34,11)	(64,28,13)	(128,93,11)
covering radius [14]	4	5	7	9	12	9
new lower bound (3)	3	5	7	9	11	9
sphere-covering bound (2)	3	4	6	8	10	7

4 Conclusion

The lower bound of the covering radius of binary irreducible Goppa codes with the Goppa polynomial of degree t and $L = GF(2^m)$ is obtained:

$$\mathcal{R}(C) \geq \tau \geq 2t - 1 \text{ if the code dimension is } k = 2^m - mt.$$

It should be mentioned that to establish the bound it was convenient to adopt the method that we had used for designing the class of binary Goppa codes that are perfect in the weighted Hamming metric [15, 16].

5 Acknowledgments

The authors would like to thank the reviewers for comments and fruitful suggestions which helped to improve the presentation of this paper.

References

1. Cohen, G.D., Karpovsky, M.G., Mattson, H.F.,Jr., Schatz, J.R.: Covering radius survey and recent results, IEEE Trans. Inform. Theory, 31 , 328-343 (1985).
2. Cohen, G.D.,Lobstein, A.C., Sloane, N.J.A.: Further Results of the Covering radius of codes, IEEE Trans. Inform. Theory ,32 , 680-694 (1986).
3. Vladuts, S. G., Skorobogatov, A. N.: Covering radius for long BCH codes, Problemy Peredachi lnlormatsii, vol. 25, 38-45 (1989). Translated in: Problems of Inform. Transm., vol. 25, No. 1, 28-34 (1989).
4. Moreno, C. J. , Moreno, O.: Exponential sums and Goppa codes I, Proc. American Math. Sac., vol. 111, 523-531 (1991).
5. Cohen, G.D., Litsyn, S.N., Lobstein, A.C., Mattson, H.F., Jr.: Covering radius 1985 1994, Appl. Algebra Eng. Comm. Comp., 8 , 173-239 (1997).
6. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering codes. North-Holland, Amsterdam (1997).
7. Goppa, V.D.: A new class of linear error correcting codes, Probl. Inform.Transm. vol.6, no.3, 24-30 (1970).
8. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Amsterdam, Netherlands, North-Holland (1977).
9. Levy-dit-Vehel, F., Litsyn, S.: Parameters of Goppa codes revisited, IEEE Trans. Inform. Theory, 1811-1819 (1997).
10. Moreno, O.: Goppa codes related quasi-perfect double-error-correcting codes, in "Abstracts of Papers," IEEE Internat. Sympos. Inform. Theory, Santa Monica, Calif.,(1981).
11. Feng,G.L., Tzeng, K.K.: On Quasi-perfect property of double-error-correcting Goppa codes and their complete decoding, Information and Control, 61, 132-146 (1984).
12. Tietavainen,A.: Codes and character sums ,Lecture Notes in Computer Science 388, Codes theory and Applications, 3-12 (1987).
13. Cohen, G., Frankl, P.: Good coverings of Hamming spaces with spheres, Discrete Mathematics, 56, 125-131 (1985).
14. Grassl,M.,Tomlinson, M. , Tjhai, C.J., Jibril,M., Ahmed, M.Z.:Results On The Covering Radius Of Some Best Known Binary Codes,(unpublished)
15. Bezzateev, S.V., Shekhunova, N.A.: Class of binary generalized Goppa codes perfect in weighted Hamming metric, Proc. of WCC-2011, Paris, 233-242 (2011).
16. Bezzateev, S., Shekhunova, N.: Class of generalized Goppa codes perfect in weighted Hamming metric, Designs, Codes and Cryptography, v.66, n.1-3, 391-399 (2013).
17. Carlitz L.: The arithmetic of polynomials in a Galois field. Am. J. Math. 54, 39-50 (1932).