Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 11-15*

Goppa codes for correcting nonuniform distributed errors

Sergey Bezzateev bsv@aanet.ru
Natalia Shekhunova sna@delfa.net
Saint Petersburg State University of Airspace Instrumentation
B. Morskaya 67, 190000, St. Petersburg, Russia

Abstract. Generalized Goppa codes with a locator set L consisting of rational functions with denominators of different degrees are considered. It is shown these codes can be used for correcting nonuniform distributed errors. Parameters and examples of these codes are presented.

1 Introduction

Most results of coding theory deal with the situation where the error probability in any position of an error vector is the same. It means that we have uniform error distribution on the code word length. However in practice there are many cases where the error probability depends on position of code word [1,2,3]. It means that error distribution on the code word is not uniform. Such type of error model is known as unequal error probability model. There are several approaches of using error correcting codes for such models:

- At first transmitted information is divided in two (or more) parts - more significant (MS) and less significant (LS) information. So called unequal error control [4] and unequal error protection codes[5,6,7,8] are used for such multilevel information. These codes have a property that its error-correction capability is described in terms of correcting errors in specific digits of a code word even though other digits in the code word may be decoded incorrectly. To each digit of the code words an error protection level t_i is assigned. Then if t errors occur in the reception of a code word, all digits which have protection t_i, where t_i is equal or greater than t will be decoded correctly even though the entire code word may not be decoded correctly.

- Construction of the codes with error correcting capability nonuniformly distributed on a code word length [9]. For such codes the number of correctable errors depends on positions where these errors take place. We will call these codes "codes for correcting nonuniform distributed errors".

- Construction of the codes with a property that different code words can correct different number of errors [10]. It means that different code words of the code can correct different error vectors. We will call these codes "codes with nonuniform error correcting capability".

In this paper we consider the class of linear block codes for correction of nonuniformly distributed errors based on the construction of generalized Goppa codes which represent (L,G) -codes with locator set L consisting of rational fractions with denominators of different degrees[11,12].

2 Code construction

Definition 1. Generalized Goppa code is the (L, G)- code with locator set L consisting of rational functions $\frac{v_i(x)}{u_i(x)}$, where $v_i(x), u_i(x)$ - are polynomials with coefficients from $GF(q^m), degv_i(x) < degu_i(x)$ and $GCD(u_i(x), u_j(x)) = 1, GCD(u_i(x), G(x)) = 1$ for any $i \neq j$ and $G(x)$ - is irreducible polynomial with coefficients from $GF(q^m)$. The vector

$$a = (a_1 a_2 \dots a_n)$$

is the code word of generalized Goppa code with length n if

$$\sum_{i=1}^{n} a_i \frac{v_i(x)}{u_i(x)} = 0 \ modG(x).$$

Let us consider situation when on the length of n symbols there are l parts $\{A_1, A_2, \dots, A_l\}$ with lengths $\{n_1, n_2, \dots, n_l\}, n = n_1 + n_2 + \dots + n_l$ and with error (erasure) probabilities $\{p_1, p_2, \dots, p_l\}$ (for example in [8] authors describe VHM system with $l = 4$ and erasure probabilities $\{0.1k, 0.25k, 0.5k, 0.95k\}$ where k is constant). In such cases we can describe the generalized Goppa code for correcting nonuniform distributed errors. For each part j $(j = 1, .., l)$ of code word length n we will use locator polynomials $u_i^j(x)$ with appropriate degree - $degu_i^j(x) = s_j$. Let us denote by $S = \{s_1, s_2, \dots, s_l\}$ the set of degrees of polynomials $u_i^j(x)$ in locator set L.
Definition 2.
The $(n_1/s_1, n_2/s_2, \dots, n_l/s_l, k, d)$ is a linear block code for correcting errors with nonuniform distribution of length $n = n_1 + n_2 + \dots, n_l$, dimension k and with minimal distance d. Where $s_1, s_2, \dots, s_l$ are weight coefficients corresponding to parts of codeword $n_1, n_2, \dots, n_l$ such that $(n_1/s_1, n_2/s_2, \dots, n_l/s_l, k, d)$ -code can correct at least T errors:

$$t = t_1 s_1 + t_2 s_2 + \dots + t_j s_j + \dots + t_l s_l,$$

where

- t_1 is the number of errors on the first n_1 positions of code word,
- t_2 is the number of errors on the second n_2 positions of code word,
- $\ldots$,
- t_l is the number of errors on the last n_l positions of code word.

Lemma 1 [12] The generalized Goppa code for correcting nonuniform distributed errors can correct any t errors

$$t = t_1 + t_2 + \ldots + t_j + \ldots + t_l$$

from the set $\{t_1, t_2, \ldots, t_l\}$ which satisfy the inequality

$$\frac{degG(x)}{2} \geq t_1 s_1 + t_2 s_2 + \ldots + t_j s_j + \ldots + t_l s_l,$$

where t_j is the number of errors on the length n_j.
For binary generalized Goppa code with separable Goppa polynomial $G(x)$ and $v_i^j(x) = u_i^{'j}(x)$ (where $u_i^{'j}(x)$ is formal derivative of $u_i^j(x)$)we have

$$degG(x) \geq t_1 s_1 + t_2 s_2 + \ldots + t_j s_j + \ldots + t_l s_l,$$

The dimension of such generalized Goppa code is

$$k \geq n - mdegG(x).$$

Lemma 2. The number n_j of different locator polynomials $u_i^j(x)$ for locator set L can be more or equal to the number of irreducible polynomials of degree s_j with coefficients from $GF(q^m)$. In case $j = 1, s_1 = 1, u_i^1(x) = x - \alpha^i$, where α is primitive element of $GF(q^m)$ and therefore $n_1 \leq q^m$.

For decoding procedure of these codes it is possible to use ordinary Berlekamp-Massey or Extended Euclidean algorithm[13].

3 Examples of code parameters

Example 1: (16/1,120/2,120,5) is the generalized Goppa code with the length n =136 for correcting nonuniform distributed errors with $n_1 = 16, s_1 = 1$ and $n_2 = 120, s_2 = 2$. The Goppa polynomial of this code can be any irreducible polynomial of degree 4 with coefficients from $GF(2^4)$.

$n_1 = 16$	$n_2 = 120$	$n = 136$
$s_1 = 1$	$s_2 = 2$	
t_1	t_2	$t = t_1 + t_2$
0	≤ 2	≤ 2
≤ 3	≤ 1	≤ 4
≤ 4	0	≤ 4

The nearest the best known linear codes for uniform distributed errors have parameters (136,121,5), (136,120,6) and (136,114,7)[14].

Example 2: (8/1,28/2,168/3,186,5) is the generalized Goppa code with length n =204, K = 186 and d = 5 for correction nonuniform distributed errors with $n_1 = 8, s_1 = 1$, $n_2 = 28, s_2 = 2$ and $n_3 = 168, s_3 = 3$. Goppa polynomial of this code can be any irreducible polynomial of degree 6 with the coefficients from $GF(2^3)$.

$n_1 = 8$	$n_2 = 28$	$n_3 = 168$	$n = 204$
$s_1 = 1$	$s_2 = 2$	$s_3 = 4$	
t_1	t_2	t_3	$t = t_1 + t_2 + t_3$
0	0	≤ 2	≤ 2
≤ 1	≤ 1	≤ 1	≤ 3
≤ 3	0	≤ 1	≤ 4
0	≤ 3	0	≤ 3
≤ 2	≤ 2	0	≤ 4
≤ 4	≤ 1	0	≤ 5
≤ 6	0	0	≤ 6

The nearest the best known linear codes for uniform distributed errors have parameters (204,188,5), (204,186,6) and (204,180,7)[14].

References

[1] L. Litwin, M. Pugel, The Principles of OFDM, RF. Design, Jan., 2001, 30-48.

[2] W. Chou, M. A. Neifeld, Interleaving and error correction in volume holographic memory systems, *Appl. Opt.* 37, 1998, 6951-6968.

[3] M. Sehlstedt, J. P. LeBlanc, Nonuniform bit-energy distribution in wireless video frames, Second Finnish Wireless Commun. Workshop, (Tampere, Finland), Oct. 2001, 13-18.

[4] H. Kaneko, E. Fujiwara, Optimal two-level q-ary unequal error control codes, Proc. 2003 IEEE Int. Symp. Inform. Theory, June 2003, 215.

[5] B. Masnick, J. Wolf, On linear unequal error protection codes, *IEEE Trans. Inform. Theory* 13, 1967, 600-607.

[6] I. M. Boyarinov, Constructing linear unequal error protection codes, *Probl. Pered. Inform.* 16(2), 1980, 103-107, (in Russian).

[7] R. H. Morelos-Zaragoza, Shu Lin, On a class of optimal nonbinary linear unequal-error-protection codes for two sets of message, *IEEE Trans. Inform. Theory* 40, 1994, 196-200.

[8] E. Kuriata, Creation of unequal error protection codes for two groups of symbols, *Int. J. Appl. Math. Comput. Sci.* 18, 2008, 251-257.

[9] H. Pishro-Nik, N. Rahnavard, F. Fekri, Nonuniform error correction using low-density parity-check codes, *IEEE Trans. Inform. Theory* 52, 2006, 292-300.

[10] M. A. Bernard, B. D. Sharma, Linear codes with non-uniform error correction capability *Des., Codes Crypt.* 10, 1997, 315-323.

[11] S. V. Bezzateev, N. A. Shekhunova, Class of the block codes with unequal error-correcting capability on length, VI Joint Russian-Swedish Intern. Workshop on Inform. Theory, Moscow, 1993, 54-60.

[12] S. V. Bezzateev, N. A. Shekhunova, Generalized Goppa codes for correcting localized errors, Proc. ISIT-98, Boston, USA, 1998, 377.

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

[14] Code Tables: Bounds on the parameters of various types of codes http://www.codetables.de/