Journal of ELECTRICAL ENGINEERING, VOL. 55, NO. 3-4, 2004, 89–94

DOUBLE ERROR CORRECTING CODES WITH IMPROVED CODE RATES

Martin Rakús — Peter Farkaš *

In [1] a new family of error detection codes called Weighted Sum Codes were proposed. In [2] it was noted that these codes are equivalent to lengthened Reed Solomon Codes, and shortened versions of lengthened Reed Solomon codes, respectively, constructed over $GF(2^{(h/2)})$. It was also shown that it is possible to use these codes for correction of one error in each codeword over $GF(2^{(h/2)})$. In [3] a class of modified Generalized Weighted Sum Codes for single error and conditionally double error correction were presented. In this paper we present a new family of double error – correcting codes with code distance $d_m = 5$. The weight spectrum for [59,49,5] code constructed over $GF(8)$ which is an example of the new codes was obtained by computer using its dual [4]. The code rates of the new codes are higher than the code rate of ordinary Reed Solomon codes constructed over the same finite fields

K e y w o r d s: linear block code, finite field, Reed Solomon codes, code rate, code distance, error control code

1 INTRODUCTION

The next generation of commercial optical fiber transmission systems will be capable of single-fiber WDM transmission supporting hundreds of wavelengths at 10 Gb/s per wavelength and experiments demonstrated already 10 Tb/s transmission per fiber [5]. In most communication networks , data are organized in units of fixed length, the so-called packets. Because of channel impairment the transmitted packet can be received in error or might be completely lost. Error control codes can be used to protect the transmitted information. Taking into account that the expected communication speeds are of the same order of magnitude as the main memory bus speeds of current workstations it becomes obvious that the decoding complexity of error control codes for high speed networks will be the limiting factor for their application. This is the main motivation for the development of the error control codes presented in this paper.

2 KNOWN MODIFIED GENERALIZED WEIGHTED SUM CODES

A family of codes that use polynomial arithmetics and process $h/2$ bit symbols was introduced in [1]. In [3] another family of codes were proposed — the so-called conditionally double error correcting codes, described with the following $\mathbf{H}$ matrix (1):

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}' & \mathbf{A}' & \cdots & \mathbf{A}' & \ldots & \mathbf{A}' & \\ & & & & & & \mathbf{I} \\ \boldsymbol{a}_0 & \boldsymbol{a}_1 & \cdots & \boldsymbol{a}_j & \cdots & \boldsymbol{a}_{q-2} & \\ \boldsymbol{a'}_0 & \boldsymbol{a'}_1 & \cdots & \boldsymbol{a'}_j & \cdots & \boldsymbol{a'}_{q-2} & \end{bmatrix} = [\mathbf{B}'\mathbf{I}] \quad (1)$$

where $\boldsymbol{a}_0 = (\alpha^0, \alpha^1, \ldots, \alpha^{q-2})$, $\boldsymbol{a}_i$ is the ith left cyclic shift of $\boldsymbol{a}_0$, $\boldsymbol{a'}_i$ is the ith right cyclic shift of $\boldsymbol{a}_0$ and:

$$\mathbf{A}' = \begin{bmatrix} 1 & \ldots & 1 & 1 & 1 & 1 \\ \alpha^{q-2} & \ldots & \alpha^3 & \alpha^2 & \alpha^1 & \alpha^0 \\ \alpha^{2(q-2)} & \ldots & \alpha^6 & \alpha^4 & \alpha^2 & \alpha^0 \\ \alpha^{3(q-2)} & \ldots & \alpha^9 & \alpha^6 & \alpha^3 & \alpha^0 \end{bmatrix} \quad (2)$$

N o t e . From the form of $\mathbf{H}$ in (1) we see that the information symbols are partitioned into $q-1$ blocks, each of length of $q-1$ symbols from $GF(q)$. i determines the position of the first error within its block and k fixes in which block it is located. Together, i and k fix the exact location of the first error. Similarly j and l locate the second error precisely.

It was also shown that the codes given by (1), if they are defined over finite fields with characteristic 2, can correct in most cases double errors in each codeword if both of the two errors occur in the information symbols of a received word. Since the system of control equations need not have a unique solution, the terminology *conditionally 2 - information - error - correcting* code was introduced in [3].

3 NEW CODES

In this section a new family of codes and one example from that family a [59,49,5] code constructed over $GF(8)$ will be presented as an attempt to improve the error correction capabilities of modified WSC. These codes could be constructed over any finite fields. They have a higher code rate than Reed Solomon codes if constructed over the same finite fields. In contrast to conditionally double error correcting codes defined by equation (1), the new codes have a code distances which allow to make exact conclusions about their error control capabilities.

* Slovak University of Technology, Faculty of Electrical Engineering and Information Technology, Department of Telecommunications, Ilkovičova 3, 812 19 Bratislava, Slovakia, E-mail: rakus@ktl.elf.stuba.sk, p.farkas@ieee.org

ISSN 1335-3632

$$\mathbf{H} = \left[\begin{array}{cccc|c|cccc|cccc} \multicolumn{4}{c|}{\mathbf{A}} & \cdots & \multicolumn{4}{c|}{\mathbf{A}} & \multicolumn{4}{c}{\mathbf{A}} \\ \alpha^{q-2} & \cdots & \alpha^{q-2} & \alpha^{q-2} & \cdots & \alpha^{1} & \cdots & \alpha^{1} & \alpha^{1} & \alpha^{0} & \cdots & \alpha^{0} & \alpha^{0} & \alpha^{0} \\ \alpha^{2(q-2)} & \cdots & \alpha^{2(q-2)} & \alpha^{2(q-2)} & \cdots & \alpha^{2} & \cdots & \alpha^{2} & \alpha^{2} & \alpha^{0} & \cdots & \alpha^{0} & \alpha^{0} & \alpha^{0} \\ \alpha^{3(q-2)} & \cdots & \alpha^{3(q-2)} & \alpha^{3(q-2)} & \cdots & \alpha^{3} & \cdots & \alpha^{3} & \alpha^{3} & \alpha^{0} & \cdots & \alpha^{0} & \alpha^{0} & \alpha^{0} \\ \alpha^{0} & \cdots & \alpha^{3} & \alpha^{2} & \cdots & \alpha^{q-3} & \cdots & \alpha^{1} & \alpha^{0} & \alpha^{q-2} & \cdots & \alpha^{2} & \alpha^{1} & \alpha^{0} \\ \alpha^{q-3} & \cdots & \alpha^{1} & \alpha^{0} & \cdots & \alpha^{0} & \cdots & \alpha^{3} & \alpha^{2} & \alpha^{1} & \cdots & \alpha^{2} & \alpha^{1} & \alpha^{0} \\ \alpha^{0} & \cdots & \alpha^{q-4} & \alpha^{q-3} & \cdots & \alpha^{2} & \cdots & \alpha^{q-2} & \alpha^{0} & \alpha^{1} & \cdots & \alpha^{q-3} & \alpha^{q-2} & \alpha^{0} \end{array}\right] = [\mathbf{BI}] \tag{3}$$

The new family of codes is defined by **H** matrix (3), where submatrix **A** has form:

$$\mathbf{A} = \begin{bmatrix} 1 & \cdots & 1 & 1 & 1 \\ \alpha^{q-2} & \cdots & \alpha^{2} & \alpha^{1} & \alpha^{0} \\ \alpha^{2(q-2)} & \cdots & \alpha^{4} & \alpha^{2} & \alpha^{0} \\ \alpha^{3(q-2)} & \cdots & \alpha^{6} & \alpha^{3} & \alpha^{0} \end{bmatrix} \tag{4}$$

For example over $GF(8)$ we get a [59,49,5] code with weight spectrum:

$$\begin{aligned} a_0 &= 1 \\ a_1 &= 0 \\ a_2 &= 0 \\ a_3 &= 0 \\ a_4 &= 0 \\ a_5 &= 2744 \\ a_6 &= 23667 \\ a_7 &= 391804 \\ a_8 &= 11373929 \\ a_9 &= 405888707 \\ &\vdots \end{aligned}$$

In this weight spectrum the first entry for non–zero codeword is $a_5 = 2744$, therefore the code distance of the new [59,49,5] code constructed over $GF(8)$ is 5. To show that such code distance is valid for all the codes defined by (3), it is necessary to clarify that such codes could correct all double errors. The complete decoding algorithm is described in the next section.

4 DECODING ALGORITHM

Decoding algorithm will be demonstrated on the example of [59,49,5] code constructed over $GF(8)$.

The first step is to calculate syndrome values based on the received symbols:
$\hat{Q}_{(q-1)^2-1}, \hat{Q}_{(q-1)^2-2}, \cdots, \hat{Q}_0, \hat{P}_9, \hat{P}_8, \cdots, \hat{P}_0$ by the following rules:

$$\begin{aligned} S_9 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \hat{Q}_i + \hat{P}_9 \\ S_8 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \alpha^{i} \hat{Q}_i + \hat{P}_8 \\ S_7 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \alpha^{2i} \hat{Q}_i + \hat{P}_7 \\ S_6 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \alpha^{3i} \hat{Q}_i + \hat{P}_6 \\ S_5 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \alpha^{(q-m)} \hat{Q}_i + \hat{P}_5 \\ S_4 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \alpha^{2(q-m)} \hat{Q}_i + \hat{P}_4 \\ S_3 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \alpha^{3(q-m)} \hat{Q}_i + \hat{P}_3 \\ S_2 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \alpha^{(i+m)-1} \hat{Q}_i + \hat{P}_2 \\ S_1 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \alpha^{(i-m)+1} \hat{Q}_i + \hat{P}_1 \\ S_0 &= \sum_{m=2}^{q} \sum_{i=u}^{v} \alpha^{1-(i+m)} \hat{Q}_i + \hat{P}_0 \,, \end{aligned} \tag{5}$$

where q denotes the number of elements of used finite field $GF(q)$; $m \in \langle 2, q \rangle$ denotes the location of the block; $m = q$ denotes the first block, $q-1$ symbols long, next to **I** in **H** matrix (3); i denotes symbol position within information part of the codeword, $i \in \langle 0, (q-1)^2 - 1 \rangle$; $i = 0$ denotes the first symbol next to **I** in **H** matrix (3). For the rest of the decoding procedure the error positions and the blocks are denoted in following way: i, j denotes the error position within the information part of the codeword, $i, j \in \langle 0, (q-1)^2 - 1 \rangle$; $i, j = 0$ denotes the first symbol next to **I** in **H** matrix (3); k, l denotes the block position within information part of the codeword, $k, l \in \langle 0, (q-2) \rangle$; $k, l = 0$ denotes the first block $q-1$ symbols long, next to **I** in **H** matrix (3).

Depending on the actual number and position of errors in the received vector it is necessary to create several sets of systems of equations covering all possible combinations of locations and number of correctable errors.

In order to determine the error location the following determinants are calculated:

$$\begin{aligned} D_1 &= \begin{vmatrix} S_6 & S_7 \\ S_7 & S_8 \end{vmatrix} \quad D_2 = \begin{vmatrix} S_7 & S_8 \\ S_8 & S_9 \end{vmatrix} \quad D_3 = \begin{vmatrix} S_6 & S_8 \\ S_7 & S_9 \end{vmatrix} \\ D_4 &= \begin{vmatrix} S_5 & S_9 \\ S_4 & S_5 \end{vmatrix} \quad D_5 = \begin{vmatrix} S_4 & S_5 \\ S_3 & S_4 \end{vmatrix} \quad D_6 = \begin{vmatrix} S_5 & S_9 \\ S_3 & S_4 \end{vmatrix} \end{aligned} \tag{6}$$

In the decoding algorithm variable ρ will denote the number of non-zero syndromes.

Decoding algorithm:

1.a If $\rho = 1$ then one error is in the parity part at the position i and the value of the error is:

$$Y_i = S_i \tag{7}$$

1.b If $\rho = 2$ two errors are in the parity part at the positions i, j and the values of the errors are:

$$\begin{aligned} Y_i &= S_i \\ Y_j &= S_j \end{aligned} \tag{8}$$

2 One error is located in the parity part and one in the information part. In such a case, depending on the value and location of the errors several options have to be analyzed:

2.a

$$D_1 = D_2 = D_3 = D_4 = D_5 = D_6 = 0 \tag{9}$$

If condition (9) is satisfied then location and value of the error in the information part are:

$$\begin{aligned} Y_1 &= S_9 \\ \alpha^i &= S_8/S_9 \\ \alpha^k &= S_5/S_9 \end{aligned} \tag{10}$$

In order to determine the location and the value of the error in the parity part it is necessary to perform the following search:

If $Y_1 + S_9 \neq 0$ then $Y_2 = Y_1 + S_9$ and the error is on the position P_9.

If $Y_1\alpha^i + S_8 \neq 0$ then $Y_2 = Y_1\alpha^i + S_8$ and the error is on the position P_8.

If $Y_1\alpha^{2i} + S_7 \neq 0$ then $Y_2 = Y_1\alpha^{2i} + S_7$ and the error is on the position P_7.

If $Y_1\alpha^{3i} + S_6 \neq 0$ then $Y_2 = Y_1\alpha^{3i} + S_6$ and the error is on the position P_6.

If $Y_1\alpha^k + S_5 \neq 0$ then $Y_2 = Y_1\alpha^k + S_5$ and the error is on the position P_5.

If $Y_1\alpha^{2k} + S_4 \neq 0$ then $Y_2 = Y_1\alpha^{2k} + S_4$ and the error is on the position P_4.

If $Y_1\alpha^{3k} + S_3 \neq 0$ then $Y_2 = Y_1\alpha^{3k} + S_3$ and the error is on the position P_3.

If $Y_1\alpha^{i-k} + S_2 \neq 0$ then $Y_2 = Y_1\alpha^{i-k} + S_2$ and the error is on the position P_2.

If $Y_1\alpha^{i+k} + S_1 \neq 0$ then $Y_2 = Y_1\alpha^{i+k} + S_1$ and the error is on the position P_1.

If $Y_1\alpha^{-(i-k)} + S_0 \neq 0$ then $Y_2 = Y_1\alpha^{-(i-k)} + S_0$ and the error is on the position P_0.

2.b

$$\begin{aligned} &D_1 = D_2 = D_3 = 0 \wedge \\ &\wedge D_4 \neq 0\,,\ D_5 \neq 0\,,\ D_6 \neq 0 \wedge \\ &\wedge S_9\alpha_p^i/S_2 = S_1/S_9\alpha_p^i = S_0\alpha_p^i/S_9\,, \end{aligned} \tag{11}$$

where $p = 1, 2, 3$ (the last row of condition (11) can be performed because: $D_1 = D_2 = D_3 = 0 \Rightarrow S_2, S_6, S_7, S_8, S_9 \neq 0$ since only one error can be in the parity part).

$$\begin{aligned} \alpha_1^i &= S_8/S_9 \\ \alpha_2^i &= S_7/S_8 \\ \alpha_3^i &= S_6/S_7 \end{aligned} \tag{12}$$

If condition (11) is satisfied for at least one member of α_p^i, then one error is in the information part and one in the parity part. Location and value of the error in the information part are:

$$\begin{aligned} Y_1 &= S_9 \\ \alpha^i &= S_8/S_9 \end{aligned} \tag{13}$$

α^k has to be determined from the following condition:

$$\text{If } \ S_5/S_9 = S_4/S_5 = S_3/S_4\,, \tag{14}$$

then $\alpha^k = S_5/S_9$, else $\alpha^k = S_8/S_2$. The value and the position of the error in the parity part is determined using the same search as in 2.a.

2.c

$$\begin{aligned} &D_1 \neq 0\,,\ D_2 \neq 0\,,\ D_3 \neq 0 \wedge \\ &\wedge D_4 = D_5 = D_6 = 0 \wedge \\ &\wedge S_2\alpha_p^k/S_9 = S_1/S_9\alpha_p^k = S_9\alpha_p^k/S_0\,, \end{aligned} \tag{15}$$

here $p = 1, 2, 3$ (the last row of condition (15) can be performed because: $D_4 = D_5 = D_6 = 0 \Rightarrow S_0, S_3, S_4, S_5, S_9 \neq 0$ since only one error can be in the parity part).

$$\begin{aligned} \alpha_1^k &= S_5/S_9 \\ \alpha_2^k &= S_4/S_5 \\ \alpha_3^k &= S_3/S_4 \end{aligned} \tag{16}$$

If condition (15) is satisfied for at least one member of α_p^k, then one error is in the information part and one in the parity part. Location and value of the error in the information part are:

$$\begin{aligned} Y_1 &= S_9 \\ \alpha^k &= S_5/S_9 \end{aligned} \tag{17}$$

α^i has to be determined from the following condition:

$$\text{If } \ S_8/S_9 = S_7/S_8 = S_6/S_7\,, \tag{18}$$

then $\alpha^i = S_8/S_9$, else $\alpha^i = S_1/S_5$. The value and the position of the error in the parity part is determined using the same search as in 2.a.

2.d

$$\begin{aligned} &D_1 = D_5 = 0 \wedge D_2 \neq 0 \wedge \\ &\wedge D_3 \neq 0\,,\ D_4 \neq 0\,,\ D_6 \neq 0 \end{aligned} \tag{19}$$

If condition (19) is satisfied then location and value of the error in the information part are:

$$\begin{aligned} Y_1 &= S_6{S_8}^3/{S_7}^3 \\ \alpha^i &= S_7/S_8 \\ \alpha^k &= S_4/S_5 \end{aligned} \tag{20}$$

The value and the position of the error in the parity part is determined using the same search as in 2.a.

2.e

$$\begin{aligned} &D_1 \neq 0\,,\ D_3 \neq 0 \wedge \\ &\wedge D_2 = D_4 = D_5 = D_6 = 0 \end{aligned} \tag{21}$$

If condition (21) is satisfied then location and value of the error in the information part are:

$$\begin{aligned} Y_1 &= S_9 \\ \alpha^k &= S_5/S_9 \end{aligned} \tag{22}$$

α^i has to be determined from the following condition:

$$\text{If } S_8/S_9 = S_7/S_8 = S_6/S_7 \tag{23}$$

then $\alpha^i = S_1/S_5$, else $\alpha^i = S_8/S_9$. The value and the position of the error in the parity part is determined using the same search as in 2.a.

2.f
$$D_1 = D_2 = D_3 = D_4 = 0 \wedge \\ \wedge D_5 \neq 0,\ D_6 \neq 0 \tag{24}$$

If condition (24) is satisfied then location and value of the error in the information part are:

$$Y_1 = S_9 \\ \alpha^i = S_8/S_9 \\ \alpha^k = S_5/S_9 \tag{25}$$

The value and the position of the error in the parity part is determined using the same search as in 2.a.

3
$$\rho = n - k \wedge S_7 = {S_8}^2/S_9 \wedge \\ \wedge S_6 = {S_8}^3/{S_9}^2 \wedge S_4 = {S_5}^2/S_9 \wedge \\ \wedge S_3 = {S_5}^3/{S_9}^2 \wedge S_2 = S_8S_9/S_5 \wedge \\ \wedge S_1 = S_5S_8/S_9 \wedge S_0 = S_5S_9/S_8 \tag{26}$$

n denotes the codeword length and k denotes the number of information symbols. If condition (26) is satisfied then one error is in the information part. Location and value of the error are:

$$Y_1 = S_9 \\ \alpha^i = S_8/S_9 \\ \alpha^k = S_5/S_9 \tag{27}$$

4 Two errors are located in the information part. In such a case it is necessary to consider several possibilities. Both errors can be the same or different: location-wise: within the block, or can also be placed in different blocks, value-wise: they can have the same or different values.

4.a Both error are different: value-wise, location-wise and block-wise:

$$Y_1 \neq Y_2,\ \alpha^i \neq \alpha^j,\ \alpha^k \neq \alpha^l \tag{28}$$

This situation occurs when:

4.a.1
$$D_1 \neq 0,\ D_2 \neq 0,\ D_3 \neq 0, \\ D_4 \neq 0,\ D_5 \neq 0,\ D_6 \neq 0 \tag{29}$$

If condition (29) is satisfied then solution can be found using classical method. $t = 2$, (t denotes the number of correctable errors), so error locator polynomial has quadratic form:

$$\sigma(x) = x^2 + \sigma_1 x + \sigma_2 \tag{30}$$

(30) leads to linear system of equations:

$$S_6 + S_7\sigma_1 + S_8\sigma_2 = 0 \\ S_7 + S_8\sigma_1 + S_9\sigma_2 = 0 \tag{31}$$

Then:

$$\sigma_2 = \frac{S_7^2 + S_6S_8}{S_8^2 + S_7S_9} \\ \sigma_1 = \frac{S_6 + S_8\sigma_2}{S_7} \tag{32}$$

Coefficients (32) σ_1, σ_2 of error locator polynomial enable by using Chien algorithm to determine locators of errors: α^i, α^j. By using rewritten syndrome equations:

$$S_9 = Y_1 + Y_2 \\ S_8 = Y_1X_1 + Y_2X_2, \tag{33}$$

where $X_1 = \alpha^i$, $X_2 = \alpha^j$, it is possible to find block locators α^k, α^l:

$$\alpha^k = \frac{S_1 + Y_2\alpha^j\alpha^l}{Y_1\alpha^i} \tag{34}$$

what leads to quadratic equation:

$$(\alpha^l)^2Y_2S_2\alpha^j + \alpha^l\big(S_1S_2 + Y_1^2(\alpha^i)^2 + Y_2^2(\alpha^j)^2\big) \\ + Y_2S_1\alpha^j = 0 \tag{35}$$

Roots of (35) α_1^l, α_2^l can be found using Chien algorithm. In order to use a right root for calculation of α^k, it is necessary to check if:

$$S_5 = Y_1\alpha^k + Y_2\alpha_i^l, \tag{36}$$

where $i = 1, 2$ and to pick that α_i^l for what condition (36) is true.

4.a.2
$$D_1 = D_2 = D_3 = 0 \wedge \\ \wedge D_4 \neq 0, D_5 \neq 0,\ D_6 \neq 0 \wedge \\ \wedge S_9\alpha_p^i/S_2 \neq S_1/S_9\alpha_p^i \neq S_0\alpha_p^i/S_9, \tag{37}$$

where $p = 1, 2, 3$ and:

$$\alpha_1^i = S_8/S_9 \\ \alpha_2^i = S_7/S_8 \\ \alpha_3^i = S_6/S_7 \tag{38}$$

If condition (37) is satisfied for at least one member of α_p^i, then Y_1, Y_2, α^i, α^j, α^k, α^l can be found exactly the same way as in 4.a.1.

4.a.3
$$D_1 \neq 0,\ D_2 \neq 0,\ D_3 \neq 0 \wedge \\ \wedge D_4 = D_5 = D_6 = 0 \wedge \\ \wedge S_2\alpha_p^k/S_9 \neq S_1/S_9\alpha_p^k \neq S_9\alpha_p^k/S_0, \tag{39}$$

where $p = 1, 2, 3$ and:

$$\alpha_1^k = S_5/S_9 \\ \alpha_2^k = S_4/S_5 \\ \alpha_3^k = S_3/S_4 \tag{40}$$

If condition (39) is satisfied for at least one member of α_p^k, then Y_1, Y_2, α^i, α^j, α^k, α^l can be found

the similar way as in 4.a.1 by using a different set of equations:

$$\begin{aligned} S_3 + S_4\sigma_1 + S_5\sigma_2 &= 0 \\ S_4 + S_5\sigma_1 + S_9\sigma_2 &= 0\,, \end{aligned} \tag{41}$$

where:

$$\begin{aligned} \sigma_2 &= \frac{S_4^2 + S_3S_5}{S_5^2 + S_4S_9} \\ \sigma_1 &= \frac{S_3 + S_5\sigma_2}{S_4} \end{aligned} \tag{42}$$

Coefficients (42) σ_1, σ_2 of error locator polynomial enables by using Chien algorithm to determine locators of blocks where errors are located: α^k, α^l. By using rewritten syndrome equations:

$$\begin{aligned} S_9 &= Y_1 + Y_2 \\ S_5 &= Y_1X_1' + Y_2X_2'\,, \end{aligned} \tag{43}$$

where $X_1' = \alpha^k$, $X_2' = \alpha^l$, it is possible to find error locators α^i, α^j:

$$\alpha^i = \frac{S_1 + Y_2\alpha^j\alpha^l}{Y_1\alpha^k} \tag{44}$$

$$\alpha^j = \frac{S_1\alpha^l + S_2\alpha^{2k}\alpha^{2l}}{Y_2\alpha^{2k}(\alpha^{2l} + 1)} \tag{45}$$

4.b Both errors are the same value-wise:

$$Y_1 = Y_2 \tag{46}$$

Depending of their location several possibilities can occur:

4.b.1

$$D_1 = D_2 = D_3 = 0 \wedge S_9 = 0 \tag{47}$$

If condition (47) is satisfied then both errors are positioned in different blocks and on different position within the blocks:

$$\alpha^k \neq \alpha^l \wedge \alpha^i \neq \alpha^j \tag{48}$$

Then:

$$\begin{aligned} S_6 + S_7\sigma_1 + S_8\sigma_2 &= 0 \\ S_7 + S_8\sigma_1 + 0 &= 0 \end{aligned} \tag{49}$$

and:

$$\begin{aligned} \sigma_2 &= \frac{S_7^2 + S_6S_8}{S_8^2} \\ \sigma_1 &= S_7/S_8 \end{aligned} \tag{50}$$

Coefficients (50) σ_1, σ_2 of error locator polynomial enables by using Chien algorithm to determine locators of errors: α^i, α^j.
By using rewritten syndrome equation:

$$S_8 = YX_1 + YX_2\,, \tag{51}$$

where $X_1 = \alpha^i$, $X_2 = \alpha^j$, it is possible to determine the value of errors:

$$Y = Y_1 = Y_2 = S_8/X_1 + X_2 \tag{52}$$

Block locators are determined from equations (53):

$$\begin{aligned} S_3 + S_4\sigma_1' + S_5\sigma_2' &= 0 \\ S_4 + S_5\sigma_1' + 0 &= 0 \end{aligned} \tag{53}$$

Then:

$$\begin{aligned} \sigma_2' &= \frac{S_4^2 + S_3S_5}{S_5^2} \\ \sigma_1' &= S_4/S_5 \end{aligned} \tag{54}$$

Coefficients (54) σ_1', σ_2' of error locator polynomial allow, by using Chien algorithm, to determine block locators: α^k, α^l.

4.b.2

$$\begin{aligned} S_9 = S_8 = S_7 = S_6 = 0 \wedge \\ S_{5-0} \neq 0 \end{aligned} \tag{55}$$

If condition (55) is satisfied, then both errors are positioned in different blocks and on the same position within the blocks:

$$\alpha^k \neq \alpha^l \wedge \alpha^i = \alpha^j \tag{56}$$

Then:

$$\begin{aligned} S_3 + S_4\sigma_1' + S_5\sigma_2' &= 0 \\ S_4 + S_5\sigma_1' + 0 &= 0 \end{aligned} \tag{57}$$

and:

$$\begin{aligned} \sigma_2' &= \frac{S_4^2 + S_3S_5}{S_5^2} \\ \sigma_1' &= S_4/S_5 \end{aligned} \tag{58}$$

Coefficients (58) σ_1', σ_2' of error locator polynomial enable by using Chien algorithm to determine block locators: α^k, α^l.
By using rewritten syndrome equation:

$$S_5 = YX_1' + YX_2'\,, \tag{59}$$

where $X_1' = \alpha^k$, $X_2' = \alpha^l$, it is possible to determine the value of errors:

$$Y = Y_1 = Y_2 = S_5/X_1' + X_2' \tag{60}$$

Error locators are determined from syndrome equation (61):

$$S_1 = Y\alpha^i(X_1' + X_2') \tag{61}$$

Then:

$$\alpha^i = S_1/S_5 \tag{62}$$

4.b.3

$$\begin{aligned} D_1 \neq 0\,,\ D_2 \neq 0\,,\ D_3 \neq 0 \wedge \\ S_9 = S_5 = S_4 = S_3 = 0 \end{aligned} \tag{63}$$

If condition (63) is satisfied then both errors are positioned in the same block and are on different positions within that block:

$$\alpha^k = \alpha^l \wedge \alpha^i \neq \alpha^j \tag{64}$$

Then:

$$\begin{aligned} S_6 + S_7\sigma_1 + S_8\sigma_2 &= 0 \\ S_7 + S_8\sigma_1 + 0 &= 0 \end{aligned} \tag{65}$$

and:

$$\sigma_2 = \frac{S_7^2 + S_6 S_8}{S_8^2}$$
$$\sigma_1 = S_7/S_8 \tag{66}$$

Coefficients (66) σ_1, σ_2 of error locator polynomial enable by using Chien algorithm to determine locators of errors: α^i, α^j.
By using rewritten syndrome equation:

$$S_8 = YX_1 + YX_2\,, \tag{67}$$

where $X_1 = \alpha^i$, $X_2 = \alpha^j$, it is possible to determine the value of errors:

$$Y = Y_1 = Y_2 = S_8/X_1 + X_2 \tag{68}$$

Block locator is determined from syndrome equation:

$$S_1 = Y\alpha^k(X_1 + X_2) \tag{69}$$

Then:

$$\alpha^k = S_1/S_8 \tag{70}$$

5 CONCLUSION

The double error correcting code presented in this paper has a higher code rate as well as $q-1$ times longer codeword than Reed Solomon codes if constructed over the same finite fields.

References

[1] McAULEY, A. J.: Weighted Sum Codes for Error Detection and their Comparison with Existing Codes, IEEE Trans. on Networking **2** No. 1 (1994), 16–22.

[2] FARKAŠ, P. Comments on "Weighted Sum Codes for Error Detection and their Comparison with Existing Codes": IEEE Trans. on Networking **3** No. 2 (1995), 129–130.

[3] FARKAŠ, P.—BAYLIS, J.: Modified Generalized Weighted Sum Codes for Error Control, Coding, Communications and Broadcasting, Research Studies Press LTD., Baldock, Hertfordshire, England, 2000, pp. 63–72.

[4] McWILLIAMS, F. J.—SLOANE, N. J. A.: The Theory of Error Correcting Codes, North-Holland, 1993.

[5] BLUMENTHAL, D. J. *et al*: Optical Signal Processing for Optical Packet Switching Networks, IEEE Optical Communications **1** (2003), 23–29.

Received 3 November 2003

Martin Rakús (Ing) graduated in radioelectronics from the Slovak University of Technology in 2001. Since 1995 he is with the Department of Telecommunications. Currently he works in the same dept. as an assistant professor. Since 2001 he has been a PhD student at the Dept. of Telecommunications. His primary research interests are error control coding and communication systems. He is a member of the IEEE.

Peter Farkaš (Prof, Ing, DrSc) received the Ing (MSc) degree from the Slovak Technical University in Bratislava, Slovakia, in 1980 and CSc (PhD) degree from Sanct Petersburg State University, Sanct Petersburg, Russia, in 1987. Since 1981 he has been with the Department of Telecommunications of the Faculty of Electrical Engineering and Information Technology of Slovak Technical University in Bratislava. He was responsible for three and was actively involved in many other research projects in the area of digital communications and telecommunication networks. His current research interests are connected with error control codes, image processing and SS/CDMA. His lecture activities are in information theory, digital communications. He is a member of the IEEE and of the Slovak Society for Computer Science. Currently he is a member of the executive committee of the Czech-Slovak Section of IEEE.