Self-Dual (48,24;12) Codes

G. Solomon
Communications Systems Research Section

Two self-dual (48,24;12) codes are constructed as 6 × 8 matrices whose columns add up to form an extended BCH-Hamming (8,4;4) code and whose rows sum to odd or even parity. The codes constructed have the identical weight structure of the extended quadratic residue code of length 48. Algebraic isomorphisms may exist between pairs of these three codes. However, because of their matrix form, the newly constructed codes are easily correctable for all five-error and many six-error patterns. The first code comes from restricting a binary cyclic (63,18;36) code to a 6 × 7 matrix and then adjoining six dimensions to the extended 6 × 8 matrix. These six dimensions are generated by linear combinations of row permutations of a 6 × 8 matrix of weight 12, whose sums of rows and columns add to one. The second code comes from a slight modification in the parity (eighth) dimension of the Reed-Solomon (8,4;5) code over GF(64). Error correction in both codes uses the row sum parity information to detect errors in the correction algorithm.

I. The Code Constructions

The two constructed codes are similar in their final six dimensions. The first 18 dimensions of the constructed (48,24;12) codes are basically (42,18;12) codes represented as 6 × 7 matrices. An additional eighth row of all zeros is adjoined to give a (48,18;12) code. The last six dimensions are constructed the same way, although the encoding algorithm for the second (modified Reed-Solomon) code is direct and systematic. Decoding the two codes uses basically the same techniques as discussed in the second code description.

II. A Self-Dual (48,24;12) Code

Consider the BCH (63,18;24) code of length 63 generated by the recursion polynomial $f_1(z)f_3(z)f_{-1}(z)$, where $f_1(z) = z^6+z+1$, where β is a root that is a primitive generator of the 63 roots of unity in $GF(64)$. The polynomials $f_3(z)$ and $f_{-1}(z)$ contain β^3 and β^{-1} as roots, respectively. Restrict the values of the code to the coordinates $9i + 7j$ for $0 \leq i \leq 6$, $j = 1, 2, 4, 5, 7, 8$. The constructed code is a (42,18;12) code. To prove this, one examines the matrix in a Mattson-Solomon (MS) polynomial formulation over the rows.

Let $z = xy$, where $x^7 = 1$, $y^9 = 1$, $x = \beta^{9i}$, and $y = \beta^{7j}$. Indexing the rows by y, the MS polynomial for each row y is $P_y(x) = \text{Tr}\,(C_1y + (C_1y)^8)x + (C_3y^3 + C_3^8y^6)x^3 + (C_1y^1 + C_1^8y^1)x^5$, which becomes, in the Solomon-McEliece Γ_2 formulation, $P_y(x) = \text{Tr}\,(C_1y + (C_1y)^8)x + (C_3^2y^6 + C_3^{16}y^3 + C_1^4y^1 + C_1^8y^8)x^6$. Thus, the coefficient of x is seen to be a (6,2;5) code over $GF(8)$, while the coefficient of x^6 is a (6,4;3) code over $GF(8)$. The minimum binary weight of the six rows is ≥ 10. The sum Γ_2 over the rows gives zero, showing that the weights are multiples of 4 and proving that the minimum distance of the code is ≥ 12. Note that the sum over the rows is the (7,3;4) codeword given by Tr $(C_3 + C_3^8)x^6$.

Adjoin an eighth column of all zeros to this 7×6 matrix. Then, add six more dimensions by forming linear combinations of all cyclic row permutations of the single matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

The newly constructed code of length 48 and dimension 24 has a minimum distance of 12. The code of dimension 23 coming from sums of pairs of rows with weights of 24 is easily seen to have a distance of 12 and has row sums equal to zero. For the 24th dimension, whose row sums are odd, one need only check that certain weight patterns in the dimension 18 code do not exist.

To verify the results, one notes that if $\sum_j \Gamma_2 = 0$, $j = 1, 2, 4, 5, 7, 8$, one need only investigate the weight forms in any row permutation (6, 6, 6, 6, 6, 6), (6, 6, 6, 6, 2, 2), (6, 6, 6, 6, 4, 0), (2, 2, 2, 2, 2, 2), etc., to verify that this addition does not alter the basic minimum distance and self-orthogonality. This works. This is Code A.

III. A Modified Reed-Solomon (8,4;5) Code Over $GF(64)$

This code, Code B, while resembling Code A above, is easier to encode and decode. The idea emerged from the well-known result that the Reed-Solomon extended (8,4;5) code over $GF(8)$ represented in binary form in a normal basis is isomorphic to the extended Golay (24,12;8) code. The idea in its simpler form was first presented in [1]. This article presents a newer form with a proof; the proof relies heavily on [1].

IV. The Reed-Solomon (8,4;5) Code Over $GF(8)$ is the Golay Code

Let β be a root of the polynomial $g(x) = x^3 + x^2 + 1$. Express the elements of $GF(8)$ in terms of the root β^i, $i = 1, 2, 4$, of $g(x)$. This is a normal basis of the field. Consider the extended Reed-Solomon (8,4;5) code over $GF(8)$ given by the check recursion polynomial $f(x) = \prod_{i=0}^{3}(x + \beta^i)$. The MS polynomial for codeword **a** is given by

$$P_{\mathbf{a}}(x) = C_0 + C_1x + C_2x^2 + C_3x^3$$

$$x \in GF(8), \quad x = 1,\ \beta,\ \beta^2,\ \beta^3,\ \beta^4,\ \beta^5,\ \beta^6,\ 0$$

$$C_i \in GF(8), 0 \leq i \leq 3$$

Writing the codewords in binary, using the normal basis above, three codewords of length eight emerge as Tr $P(x)\beta^j$, $j = 1, 2, 4$, where Tr denotes the value in $GF(2)$ given by the Trace of an element $a \in GF(8)$, where Tr $a = a + a^2 + a^4$. Note that Tr $\beta^i = 1$, $i = 0, 1, 2, 4$, and Tr $\beta^i = 0$, $i = 3, 5, 6$.

It is easy to show, using the Γ_2 formula of [1], that the total weight of the three binary codewords is a multiple of 4, with a minimum weight equal to 8.

Proof. Set $C_0 = 0$. The binary polynomials may be written as Tr $P(x)\beta^j = \text{Tr}\,(C_1\beta^j + (C_2\beta^j)^4)x + (C_3\beta^j)^2x^6$. The expressions for $\Gamma_2(\text{Tr}\ P(x)\beta^j)$, $j = 1, 2, 4$, are

$$\Gamma_2(\text{Tr}\ P(x)\beta) = \text{Tr}\,(C_1C_3\beta^3 + C_2^4\beta^6)$$

$$= \text{Tr}\,(C_1C_3\beta^3 + C_2^4\beta^6)$$

$$\Gamma_2(\text{Tr}\ P(x)\beta^2) = \text{Tr}\,(C_1C_3\beta^6 + C_2^4\beta^5)$$

$$\Gamma_2(\text{Tr}\ P(x)\beta^4 = \text{Tr}\,(C_1C_3\beta^5 + C_2^4\beta^3)$$

Summing over all three binary codewords Tr $P(x)\beta^j$, $j = 1, 2, 4$, one obtains $\sum_j \Gamma_2(\text{Tr}\ P(x)\beta^j) = 0$. This implies that the binary weight of the above Reed-Solomon codeword is a multiple of 4. Since the minimum symbol weight is 5, the binary code is a (24,12;8) code. Furthermore, this stamps the code as a Golay code, by virtue of the uniqueness of the Golay code.

To decode this, simply use the decomposition of Tr $P(x)\beta^j$, $j = 1, 2, 4$, and test eight values for C_3 and decode the (8,4;4) BCH-Hamming code that remains. Note

that the parity of each Tr $P(x)\beta^j$, $j = 1, 2, 4$, is zero, which yields additional information to detect single errors and thus reduce the search for C_3. Use each of these eight trials to soft decode or maximum-likely decode three BCH-Hamming codes.

V. Code B via the Reed-Solomon Code

Using techniques similar to those above, if one starts with a Reed-Solomon (8,4;5) code over $GF(64)$, and represents the code in binary using a particular normal basis with the special property defined below, one can generate a code of length 48 and dimension 24 with weights that are multiples of 4.

The binary representation of the usual Reed-Solomon (8,4;5) code over $GF(64)$, yields six (8,7;2) codewords whose decomposition into two cyclic code components and a constant component looks like Reed-Solomon (6,4;3) and (6,2;5) codes over $GF(8)$ and a binary (6,6;1) code, respectively. However, Code B is constructed by modifying the extended coding rule for the parity symbol.

In particular, let γ be a root of the polynomial $f(x) = x^6 + x^5 + x^4 + x + 1$, where γ is a primitive generator of the 63 roots of unity. Represent the elements of $GF(64)$ in the normal representation using the roots of $f(x)$. The roots are γ^j, $j \in J$, $J = \{1, 2, 4, 8, 16, 32\}$.

Note that for this particular choice of $f(x)$,

$$\text{Tr } \gamma^j = 1; \quad j \in J; \quad J = 1, 2, 4, 8, 16, 32$$

$$\text{Tr } \gamma^i \gamma^k = 0; \quad i \neq k; \quad i, k \in J$$

Let β be a root of the polynomial $g(x) = x^3 + x^2 + 1$. Then, β is an element of $GF(8)$, a subfield of $GF(64)$, and $\beta = \gamma^9$.

Now use the recursion or check polynomial $h(x) = \prod_{i=0}^{3}(x + \beta^i)$ to generate a Reed-Solomon (7,4;4) code over $GF(64)$. This means that the initial shift register contains four elements in $GF(64)$ expressed as coefficients in the normal representation above. The cyclic portion of the code is of length seven, but the overall parity symbol, the eighth dimension, is defined differently. Representing the binary code as components Tr $P(x)\gamma^i$, $i = 1, 2, 4, 8, 16, 32$, extends the codes to the eighth coordinates by the rules. The binary value at the row indexed by the ith coordinate is achieved by Tr $C_0\gamma^i$ + Tr $\sum_{j \in J} C_0\gamma^i$.

Thus, for the constant term C_0 with Tr $C_0 = 0$, this behaves like the normal parity symbol, which is a sum over the values of the cyclic code coordinates. Note that this is equivalent to the way the additional six coordinates were defined in Code A above.

The general Mattson-Solomon polynomial of codeword **a**, similar to the Golay codeword over $GF(8)$, is $P_{\mathbf{a}}(x) = C_0 + C_1x + C_2x^2 + C_3x^3$, where $C_i \in GF(64)$ for $0 \leq i \leq 3$ and $x \in GF(8)$. Encode the codeword in its cyclic portion. The extended codeword **a** expressed in terms of the MS polynomial, is

$$\mathbf{a} = P_{\mathbf{a}}(\beta^i); \quad 0 \leq i \leq 6, \quad (P_{\mathbf{a}}(0))$$

Writing the codewords in binary, using the normal basis γ^j, where $j \in J$ above, there are six binary codewords of length eight

$$\text{Tr } P(x)\gamma^j; \quad j = 1, 2, 4, 8, 16, 32$$

where Tr a denotes the value in $GF(2)$ given by the Trace of an element $a \in GF(64)$

$$\text{Tr } a = a + a^2 + a^4 + a^8 + a^{16} + a^{32}$$

Consider one of the six binary words in its Mattson-Solomon setting,

$$\text{Tr } P_{\mathbf{a}}(x)\gamma^j = \text{Tr } (C_0 + C_1x + C_2x^2 + C_3x^3)\gamma^j$$

$$= \text{Tr } C_0\gamma^j + \text{Tr }'[(C_1x + C_2x^2 + C_3x^3)\gamma^j$$

$$+ ((C_1x + C_2x^2 + C_3x^3)\gamma^j)^8]$$

$$\text{Tr }'a = a + a^2 + a^4; \quad a \in GF(8)$$

Set $C_0 = 0$ temporarily, as this does not affect the arguments to follow, and

$$\text{Tr } P(x)\gamma^j = \text{Tr }'(C_1\gamma^j + (C_1\gamma^j)^8 + (C_2\gamma^j)^{32}$$

$$+ (C_2\gamma^{32j})^8)x + \text{Tr }'((C_3\gamma^j)^2 + (C_3\gamma^j)^{16})x^6$$

Lemma. The coefficient of x is a (6,4;3) code over $GF(8)$. The coefficient of x^3 is a (6,2;5) code over $GF(8)$.

The code is indexed by the values of γ^j, $j \in J$, $J = \{1, 2, 4, 8, 16, 32\}$.

Proof. The set γ^j, $j \in J$, $J = \{1, 2, 4, 8, 16, 32\}$ is a linear independent set, and thus can only take zero values one less than the number of terms in the coefficients of x and x^6. The components Tr $C_0\gamma^j$ for Tr $C_0 = 0$ form a binary (6,5;2) code.

Theorem. The Reed-Solomon code determined by codewords with MS polynomials $P_{\mathbf{a}}(x)$, when Tr $C_0 = 0$, forms a binary (48,23;12) code with weights that are multiples of 4.

Proof. The property of the weights that are multiples of 4 follows from using the Solomon-McEliece Γ_2 formula

$$\text{Tr } P(x)\gamma = \text{Tr } ((C_1\gamma + (C_2\gamma)^4 + (C_3\gamma^2 x^6))$$

where Tr is defined in $GF(64)$. Now

$$\begin{aligned}\Gamma_2(\text{Tr } P(x)\gamma) = \text{Tr } [&C_1C_3^2\gamma^3 + C_1^8C_3^2\gamma^{10} + C_1C_3^{16}\gamma^{17} \\ &+ C_1^8C_3^{16}\gamma^{24} + C_2^{32}C_3^2\gamma^{34} + C_2^4C_3^2\gamma^6 \\ &+ C_2^{32}C_3^{16}\gamma^{48} + C_2^4C_3^{16}\gamma^{20}]\end{aligned}$$

for

$$\begin{aligned}\Gamma_2(\text{Tr } P(x)\gamma^2) = \text{Tr } [&C_1C_3^2\gamma^6 + C_1^8C_3^2\gamma^{20} + C_1C_3^{16}\gamma^{34} \\ &+ C_1^8C_3^{16}\gamma^{48} + C_2^{32}C_3^2\gamma^5 + C_2^4C_3^2\gamma^{12} \\ &+ C_2^{32}C_3^{16}\gamma^{33} + C_2^4C_3^{16}\gamma^{40}]\end{aligned}$$

Similarly,

$$\begin{aligned}\Gamma_2(\text{Tr } P(x)\gamma^4) = \text{Tr } [&C_1C_3^2\gamma^{12} + C_1^8C_3^2\gamma^{40} + C_1C_3^{16}\gamma^5 \\ &+ C_1^8C_3^{16}\gamma^{33} + C_2^{32}C_3^2\gamma^{10} + C_2^4C_3^2\gamma^{24} \\ &+ C_2^{32}C_3^{16}\gamma^3 + C_2^4C_3^{16}\gamma^{17}]\end{aligned}$$

and, therefore, $\sum_{j\in J}\Gamma_2(\text{Tr } P(x)\gamma^j) = 0$. Recall that the normal basis was chosen so that Tr $\gamma^j = 1$, $j \in J$, and Tr $\gamma^3 =$ Tr $\gamma^5 =$ Tr $\gamma^9 = 0$.

It has been demonstrated that the binary weight of any codeword in the Reed-Solomon code above is a multiple of 4. Since the symbol distance of the code is greater than 5, the weights have been narrowed down to 8, 12, 16, 20, ..., 40.

VI. Structure of the Code

An examination of the Reed-Solomon code in its cyclic components reveals that most code symbols weights are 3, 5, and 6. The code has weight 3 when $C_3 \neq 0$ and C_1 and $C_2 = 0$. Clearly, the binary weight of the code is ≥ 12, independent of the value of C_0. From above, it is clear that the dimension 18 portion of the code has a minimum distance of 12. In fact, the codewords have weights 12 through 36 in multiples of 4. Now, consider C_0 by itself when Tr $C_0 = 0$. Adding this to the dimension 18 code addressed above, the minimum distance is kept at 12. If the symbol weight of the Reed-Solomon code is 5 or 6, then the binary weight of the dimension 18 code is ≥ 12, and no complementing can reduce this weight. For symbols of weight 3, one must have three codewords of weight 4 each; again, complementing does not reduce the weight.

The extension parity rule for C_0 has been changed as follows: if, say, for $i = 1$, Tr $P(x)\gamma^i = 1$ and Tr $P(x)\gamma^i = 0$, $i \neq 1$, an eighth row of weight 5 is adjoined, e.g., 011111. The argument invoked in the first code above may be used to prove that the minimum code distance is 12 and all words have weight multiples of 4, i.e., the code is self-dual.

VII. Decoding Binary

To correct five or more errors, begin by trying 64 different values of C_3. This eliminates the cyclic component attached to x^6. Since each of the six binary codes is now an odd-error-detecting, single-error-correcting code, the parity information is used to correct single errors when they occur. In the case of a five binary error pattern, at least four correct values of C_1 and C_2 are available. Therefore, in $\binom{6}{2}$ trials, a total of at most $15 \times 64 = 1024 - 64 = 960$ candidates is available to find the most likely error pattern.

Note that five-error patterns occur in rows as 5, 4 1, 2 3, 1 2 2, 1 3 1, 1 1 1 2, and 1 1 1 1 1. Six-error patterns occur in rows as 6, 5 1, 4 2, 3 2 1, 3 3, 3 1 1 1, 2 2 2, 2 2 1 1, and 2 1 1 1 1. Using this technique, the only error pattern that would not emerge as a candidate would be the 2 2 2 case. This occurs in 560 patterns out of the

possible $\binom{48}{6}$ error patterns. The number of uncorrectable, but detectable, six-error patterns is given by $\binom{12}{6}$ times the number of codewords of weight 12.

A soft decoding using these techniques would perhaps add a few decibels to the hard-decision decoding performance.

Reference

[1] G. Solomon, "Golay and Other Box Codes," *TDA Progress Report 42-109*, vol. January–March 1992, pp. 130–135, May 15, 1992.