496113 S3-61 146833 P- 2

N93-24662

Soft Decoding a Self-Dual (48,24;12) Code

G. Solomon[1]
Communications Systems Research Section

A self-dual (48,24;12) code comes from restricting a binary cyclic (63,18;36) code to a 6 × 7 matrix, adding an eighth all-zero column, and then adjoining six dimensions to this 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. A soft decoding using these properties and approximating maximum likelihood is presented here. This is preliminary to a possible soft decoding of the box (72,36;15) code that promises a 7.7-dB theoretical coding under maximum likelihood.

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

Consider the BCH (63,18;24) code of length 63 generated by the recursion polynomial $f_1(x)f_3(x)f_{-1}(x)$, where $f_1(x) = x^6 + x + 1$ with a root β that is a primitive generator of the 63rd roots of unity in $GF(64)$. Here $f_3(x)f_{_1}(x)$ contains β^3 and β^{-1} as roots, respectively. Restrict the values of the code to the coordinates $9i + 7j$ for $0 \leq i \leq 6$, $j = 1, 2, 4, 5, 7, 8$. Thus, a (42,18;12) code has been constructed. To prove this, one examines the matrix in a Mattson-Solomon (MS) polynomial formulation over the rows.

For $z = xy$, 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 is $P_y(x) = \mathrm{Tr}\ (C_1 y + (C_1 y)^8)x + (C_3 y^3 + C_3^8 y^6)x^3 + (C_{_1} y^{_1} + C_{_1}^8 y^{_1})x^5$. This polynomial becomes, in the Solomon-McEliece Γ_2 Formulation, $P_y(x) = \mathrm{Tr}\ (C_1 y + (C_1 y)^8)x + (C_3^2 y^6 + C_3^{16} y^3 + C_{_1}^4 y^1 + C_{_1}^8 y^8)x^6$.

Thus, the coefficient in 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 $\geq$10. Now, summing Γ_2 over the rows, one can see that this adds to 0, yielding weights that are multiples of 4, and thus proving that the minimum distance of the code is $\geq$12. Note that the sum of the rows is the (7,3;4) codeword given by Tr $(C_3 + C_3^8)x^6$.

Adjoin an eighth column to this 7 × 6 matrix. Now 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 dimension 23 code coming from pairs of rows with weight 24 is easily seen to have distance 12 and row sums equal to zero. For the 24th dimension, whose row sums are odd, one need only check

[1] Consultant.

that certain weight patterns in the dimension 18 code did not exist.

To verify the results, note that $\sum_j \Gamma_2 = 0, j = 1, 2, 4, 5, 7, 8$, and 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.

II. Soft Decoding This Code

To decode this code using soft-decision information, first assume that the rows are of even parity. There are six (8,7;2) binary codes with the coefficients of x forming a (6,2;5) code over $GF(8)$. There are 64 such possibilities, and these are stored as six (8,3;4) codes that are cyclic extensions of the maximal length shift register codes Tr cx, $x = \beta^i$, where $0 \leq i \leq 6$. Adding these six codewords to a received word, six extended BCH-Hamming (8,4;4) words are left to maximum likely decode. These words must have coefficients of x^6 that form a (6,4;3) pseudocode. Conducting fifteen trials where four words are assumed correct and generating the rest of the words will give a set of soft-decoded values. Thus, in 64 x 15 trials a candidate emerges for maximum likelihood decoding. This technique will correct all hard-decision five-error patterns, and almost all six-error patterns. Assuming an odd parity in the eighth column, one uses 2 x 64 x 15 total examinations (2020 trials) in total. How close this is to maximum likelihood is a yet unanswered question.

The 64 words are generated by taking the recursion x^6+x+1 to generate six linearly independent words, placing the word in the 9 x 7 matrix as prescribed, and then limiting each codeword to the rows 1, 2, 4, 5, 7, and 8. This will give six generators of the (6,2;5) code and so will yield 64 words. For the (6,4;3) code, generate the cyclic code formed by $(x^6+x^4+x^2+x+1)(x^6+x^5+1)$. Generate 12 linearly independent words as above and limit each codeword to the rows 1, 2, 4, 5, 7, and 8 to give 12 generators of the (6,4;3) code over $GF(8)$. This is the form desired.

III. Analysis of Performance

How close is this to maximum likelihood performance? Performance here consists of maximum likelihood decoding of the six BCH-Hamming (8,4;4) codes and assumes at least four rows are correct. This clearly will not work if three or more of the decoded rows are incorrect. This is the key factor to decoding correctly. If p is the decoding error under the maximum likelihood of the (8,4;4) code, then the decoding error is $\sum_{i=3}^{6} p^i(1-p)^{6-i}$. This is roughly $20p^3$ for the entire code.

IV. Soft Decoding the (72,36;15) Code

To decode the code in [1] using soft-decision information, first assume that the rows are of even parity. There are nine binary (8,7;2) codes with coefficients of x^6 forming a maximal-distance-separable (MDS) (9,3;7) code over $GF(8)$. There are 128 such possibilities, and these are stored as nine (8,3;4) codes that are cyclic extensions of the maximal length shift register codes Tr cx^6, $x = \beta^i$, where $0 \leq i \leq 6$. Adding these six codewords to a received word, nine extended BCH-Hamming (8,4;4) words are left to maximum likely decode. These decoded words are now symbols that are coefficients of x that form a (9,6;4) code over $GF(8)$. Eighty-four trials, where six symbols are assumed correct to generate the rest of the symbols, will give a set of values for soft decoding. Thus, in $128 \times 84 = 10,752$ trials, there emerges a candidate for maximum likelihood decoding. This technique will correct all hard-decision, seven-error patterns and almost all eight-error patterns. Assuming an odd parity in the eighth column, there have been $2 \times 10,752 = 21,504$ total examinations.

Reference

[1] G. Solomon, "Self-Dual (48,24;12) Codes," *The Telecommunications and Data Acquisition Progress Report 42-111, vol. July–September*, pp. 75–79, November 15, 1992.