199300711

475083

3p

59-64

[illegible]

P-3

More Box Codes

G. Solomon
Communications Systems Research Section

A new investigation shows that, starting from the BCH (21,15;3) code represented as a 7 × 3 matrix and adding a row and column to add even parity, one obtains an 8 × 4 matrix (32,15;8) code. An additional dimension is obtained by specifying odd parity on the rows and even parity on the columns, i.e., adjoining to the 8 × 4 matrix, the matrix, which is zero except for the fourth column (of all ones). Furthermore, any seven rows and three columns will form the BCH (21,15;3) code. This box code has the same weight structure as the quadratic residue and BCH codes of the same dimensions. Whether there exists an algebraic isomorphism to either code is as yet unknown.

I. Constructions

A box (32,16;8) code with the weight distribution of the BCH or quadratic codes of the same length is constructed here in a manner similar to the way in which the extended Golay (24,12;8) code was constructed [1]. The extended Golay (24,12;8) code was generated as a 6 × 4 binary matrix from the BCH-Hamming (15,11;3) code, represented as a 5 × 3 matrix, by adding a row and a column that are both of odd or even parity. The odd-parity case gave the additional twelfth dimension. Furthermore, any three columns and five rows of the 6 × 4 Golay code form a BCH-Hamming (15,11;3) code. The construction parallels [1] without going through the details. The original article contains the proofs.

The (32,16;8) code in 8 × 4 matrix form is obtained from the BCH-Hamming (21,15;3) code by adjoining row and column even parity. The BCH code is expressed here as a 7 × 3 matrix with entries in the $(i,\ j)$ positions, $0 \leq i \leq 6,\ 0 \leq j \leq 2$, corresponding to the coordinates $7i + 3j$ mod 21 of the code.

Let $\mathbf{A}$ be the BCH-Hamming (21,15;3) code. The Mattson-Solomon polynomial for a codeword $\mathbf{a} \in \mathbf{A} = (a_i,\ i = 0 \ldots 20)$ is given by

$$P_{\mathbf{a}}(z) = C_0 + \mathrm{Tr}\ Cz + \mathrm{Tr}'\ Dz^3 + \mathrm{Tr}'\ Gz^{-3} + Ez^7 + E^2 z^{14}$$

where $C \in GF(64)$, G and $D \in GF(8)$, $E \in GF(4)$, and $C_0 \in GF(2)$.

Here, $P_{\mathbf{a}}(\beta^i) = a_i$, for β as a primitive 21st root of unity. Tr denotes the linear operator Trace in $GF(64)$, i.e., $\mathrm{Tr}\ a = a + a^2 + a^4 + a^8 + a^{16} + a^{32}$. Tr′ denotes the linear operator Trace in $GF(8)$, i.e., $\mathrm{Tr}'\ a = a + a^2 + a^4$.

C-2

The parity check polynomial for the code is $(z+1)f_1(z)f_3(z)f_7(z)f_{-3}(z)$, where $f_i(z)$ is the irreducible polynomial over $GF(2)$ with β^i as a root

$$f_1(z) = z^6 + z^4 + z^2 + z + 1$$

$$f_3(z) = z^3 + z^2 + 1$$

$$f_{-3}(z) = z^3 + z + 1$$

$$f_7(z) = z^2 + z + 1$$

The weight, $w(\mathbf{a})$ mod 4 for even-weight words $\mathbf{a}(C_0 = 0)$, is given by $w \bmod 4 = 2\Gamma_2(P_{\mathbf{a}}(x))$, where $\Gamma_2(P_{\mathbf{a}}(x)) = DG + (DG)^2 + (DG)^4 + E^3$ [2].

Now place the codewords in 7×3 matrices (b_{ij}), $0 \leq i \leq 6$ and $0 \leq j \leq 2$, corresponding to their values $7i + 3j$ mod 21. The ith coordinate is entered thusly,

$$\begin{pmatrix} 0 & 7 & 14 \\ 3 & 10 & 17 \\ 6 & 13 & 20 \\ 9 & 16 & 2 \\ 12 & 19 & 5 \\ 15 & 1 & 8 \\ 18 & 4 & 11 \end{pmatrix}$$

The MS polynomial expressed in the 7×3 setting, indexing each row by y in terms of the independent variable x, becomes

$$\mathrm{Tr}\ Dy^3 + \mathrm{Tr}\ Gy^{-3} + \mathrm{Tr}'\ (E' + Cy + C^4y^4 + c^{16}y^2)x,\ E' = E^2$$

Note again that in the MS polynomials of each row, the Trace is defined over $GF(4)$ as $\mathrm{Tr}'\ a = a + a^2$ for $a \in GF(4)$, and is defined over $GF(8)$ as $\mathrm{Tr}\ Dy^3 = (Dy^3) + (Dy^3)^2 + (Dy^3)^4$ and $\mathrm{Tr}\ Gy^{-3} = (Gy^{-3}) + (Gy^{-3})^2 + (Gy^{-3})^4$.

Form the sum over the rows to give an eighth row with an MS polynomial of $\mathrm{Tr}'\ E'x$. Form the parity sum over the columns to obtain an 8×1 column that is, of course, $\mathrm{Tr}\ Dy^3 + \mathrm{Tr}\ Gy^{-3}; y^8 = y$. The bottom row is indexed by $y = 0$, and the parity column corresponds to $x = 0$.

Note that the coefficient of x, $E' + Cy + (Cy)^4 + (Cy)^{16}$, is the MS polynomial for an (8,4;4) code indexed by $y^8 = y$ over $GF(4)$. Note that the constant term in each row varies and is a binary (7,6;2) code. The constant term contributes the same values to the fourth parity column. Thus, if one started with a BCH subcode of dimension 14 of even-weight w with $w \bmod 4 = 2\Gamma_2$, where $\Gamma_2 = TrDG + E^3$, when one adjoins the parity rows and columns, one is adjoining row and column codewords whose weight modulo 4, $w \bmod 4 = TrDG + E^3$. So the total new weight $w' = 0 \bmod 4$.

This proves that $w' \geq 8$. For if $w = 4$ originally, now either $E^3 = 1$ and Tr $DG = 1$, adding weight 4, or $E = 0$ and TR $DG = 0$, adding a column of weight 4.

One could also show easily that $w' \geq 8$ by noting that the coefficient of x is now an (8,4;4) code over $GF(4)$, having adjoined an even-parity row. Thus, there are at least four rows each of weight 2. The addition of the even-parity column ensures that $w \geq 8$ when the coefficient of $x = 0$. The new codewords have weights of 8, 12, 16, 20, 24, and 32 in the 8×4 matrix code that was generated. Complementing these new codewords still gives words with weights of 8, 12, and 16, which accounts for the odd-weight BCH codewords adding up to dimension 15.

The 16th dimension of the constructed code is achieved by adding an odd-parity row and an even-parity column to the BCH words.

II. A Startling Property

Theorem. Consider the 8×4 binary matrix and consider any 7×3 submatrix obtained by removing one column and one row. This is the BCH (21,15;3) code.

Proof. Consider the 8×4 matrix with the top row deleted. Using the bottom parity check row and considering the first three columns, one can now show a permuted 7×3 BCH code where the rows have been interchanged.

The coefficient of x, the (8,4;4) code over $GF(4)$, gives rise to the (32,8;8) portion of the code. The map of $y \rightarrow (1+y)$ is a permutation of this code that interchanges the top and bottom rows, corresponding to $y = \beta^0 = 1$ and $y = 0$.

The remaining five dimensions, which are functions of C_0 and D in the BCH-Hamming code, are easily manipulated so that the weights stay the same. Since the code is clearly invariant under cyclic row permutations, this takes care of all subcodes with the first three columns fixed.

Now interchange the first column with the fourth rightmost parity column, and the second column with the third column, in order to obtain a BCH code like the one above in the top seven rows. This interchange of columns is given by $x \rightarrow x+1$.

This map takes the row indexed by y, Tr $Dy+\text{Tr}'\ (E'+Cy+(Cy)^4)x$ into a permuted row indexed by y, where $D \in GF(16)$ has been augmented. $\text{Tr}'\ (E'+Cy+(Cy)^4)+\text{Tr}\ Dy+\text{Tr}'\ (E'+Cy+(Cy)^4)x$. There clearly exists a value of D', such that $D' = \text{Tr}'\ (E'+Cy+(Cy)^4)+\text{Tr}\ Dy$ for all values of y. Now, clearly, every three columns that occurred in the leftmost 5 × 3 matrix now occur in the newly formed 5 × 3 matrix. As the code is invariant under cyclic column permutation, the proof is completed.

References

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

[2] G. Solomon and R. J. McEliece, "Weights of Cyclic Codes," *Journal of Combinatorial Theory*, vol. 1, no. 4, pp. 459–475, December 1966.