N89-27891

Decoding of 1/2-Rate (24,12) Golay Codes

T.-K. Truong
Communications Systems Research Section

I. S. Reed and X. Yin
Department of Electrical Engineering, University of Southern California

In this article, a decoding method for a (23,12) Golay code is extended to the important 1/2-rate (24,12) Golay code.

I. Introduction

The 23-bit Golay code is a very useful code, particularly for those applications where a parity bit is added to yield a 1/2-rate code. Recently a simplified procedure was developed for decoding this important (24,12) Golay code [1]. It is shown here that this procedure can be extended to any decoding method which can correct three errors in the (23,12) Golay code.

There are several known decoding procedures for correcting the three possible errors of (23,12) Golay code:

(1) The minimum-distance method [2]

(2) The standard-array method [2], [3]

(3) The majority-logic method, suggested by Goethals [4]

(4) Kasami's error-trapping algorithm [5]

(5) The shift-and-search procedure [1]

(6) Algebraic algorithms which include Berlekamp's method [2], [6] as well as the extended Bose-Chaudhuri-Hocquenghem (BCH) algorithm suggested recently by M. Elia in [7]

In this article, a simple method is given to extend any of these procedures to the 1/2-rate (24,12) Golay code so that three errors can be corrected and four errors can be detected.

II. Theorem for Close-Packed Error-Correcting Codes

The (23,12) Golay code is a close-packed error-correcting code for which the following theorem can be proved:

Theorem: Let $\mathbf{C}$ be the set of codewords of a Golay code. Also let $\mathbf{E}_i$ be the set of vectors of weight i. Then for any $\underline{c} \in \mathbf{C}$, and any $\underline{e}_4 \in \mathbf{E}_4$, there is a $\underline{c}' \in \mathbf{C}$ such that

$$\underline{c} + \underline{e}_4 = \underline{c}' + \underline{e}_3$$

where $\underline{e}_3 \in \mathbf{E}_3$.

Proof: See Appendix and [1].

III. The (24,12) Golay Code

A (24,12) Golay codeword can be formed by adding an even or odd parity-check bit to the (23,12) Golay codeword. It is well known that such a (24,12) Golay code has the minimum distance $d_{\min} = 8$. Thus any decoding algorithm can be extended to the (24,12) Golay code with the correction of three or fewer errors and the detection of four errors.

There is no loss in generality to assume that the parity of a (24,12) Golay codeword is even. That is, the sum of the 24 bits modulo 2 is equal to zero. Now assume during transmission that four errors are added to the codeword. There are two cases to consider:

(1) If the four errors occur in the first 23 bits, then by the Theorem in Section II, the addition of an error vector of Hamming weight 4 to a codeword produces a 23-bit vector that is equal to some other (23,12) Golay codeword plus an error vector of weight 3. Thus if one of the decoding algorithms in Section I is applied to the first 23 bits, an error vector of weight 3 is added to the received codeword. As a consequence the parity of the (24,12) codeword also is changed. Hence by checking the parity of the decoded codeword, the decoder detects the presence of four errors.

(2) On the other hand, if three errors occur in the first 23 bits, and one error occurs in the parity bit, the decoding algorithm corrects the three errors in the first 23 bits. The parity of the 23-bit decoded codeword now differs from the received parity bit. Hence the decoder detects the presence of four errors.

The extended decoding algorithm for the (24,12) Golay code is summarized as follows:

> Apply any decoding algorithm which can correct three errors to the first 23 bits. If the number of errors is less than three, the decoding procedure terminates normally. If the number of errors is greater than or equal to three, the parity of the decoded codeword is compared with the received parity bit. If they are different, the decoder detects four errors. The detailed flowchart of this decoding procedure is shown in Fig. 1.

IV. An Example of Implementation

A complete algebraic decoding algorithm for the (23,12) Golay code was found recently by M. Elia [7]. To illustrate this method, define

$$E(x) = e_{22}x^{22} + e_{21}x^{21} + \cdots + e_1 x + e_0$$

to be the error polynomial. Then the received codeword has the form

$$R(x) = C(x) + E(x) = q(x)\mathbf{g}(x) + E(x)$$

Suppose that three errors occur in the received code word $R(x)$ and assume that $2t \leqslant d - 1$. Since α, α^3, and α^9 are the roots of $\mathbf{g}(x)$, one has

$$s_1 = E(\alpha) = R(\alpha),\ s_3 = E(\alpha^3) = R(\alpha^3),\ s_9 = E(\alpha^9) = R(\alpha^9)$$

where s_1, s_3, and s_9 are called the syndromes of the code. Assume z_1, z_2, and z_3 are the positions of the three errors. Then the error-locator polynomial is defined by

$$\sigma(z) = \prod_{i=1}^{3} (z - z_i) = z^3 + \sigma_1 z^2 + \sigma_2 z + \sigma_3$$

where $\sigma_1 = z_1 + z_2 + z_3$, $\sigma_2 = z_1 z_2 + z_2 z_3 + z_1 z_3$, and $\sigma_3 = z_1 z_2 z_3$. Then from [7],

$$\sigma_1 = s_1$$

$$\sigma_2 = s_1^2 + D^{1/3}$$

$$\sigma_3 = s_3 + s_1 D^{1/3}$$

where

$$D = \frac{(s_1^3 + s_3)^2 + (s_1^9 + s_9)}{(s_1^3 + s_3)}$$

Hence under different conditions for the syndromes, the error location polynomial has the following forms:

$$\sigma(z) = \begin{cases} 1 & \text{If } s_1 = s_3 = s_9 = 0 \\ & \quad \text{then no error} \\ z + s_1 & \text{If } s_3 = s_1^3 \text{ and } s_3^3 = s_9 \\ & \quad \text{then one error} \\ z^2 + s_1 z & \text{If } s_1 \neq s_3 \text{ and } s_3 = s_1 D^{1/3} \\ \quad + (s_1^2 + D^{1/3}) & \quad \text{then two errors} \\ z^3 + s_1 z^2 & \text{Otherwise three errors} \\ \quad + (s_1^2 + D^{1/3}) z & \\ \quad + (s_3 + s_1 D^{1/3}) & \end{cases}$$

Note that the cube root $D^{1/3}$ is in $GF(2^{11})$ and can be computed recursively, i.e.,

$$D^{1/3} = D^{1365} = D^{2^{10}+2^8+2^6+2^4+2^2+2^0} =$$

$$D^{2^{10}}D^{2^8}D^{2^6}D^{2^4}D^{2^2}D$$

After using the Chien search to find the error locations, one can apply the decoding procedure in this article to decode the (24,12) Golay code as described in Fig. 2.

A shift-and-search procedure for decoding Golay codes is given in [1]. In a computer simulation, this procedure is compared with the Elia algebraic technique in terms of CPU time. For three and four errors this comparison shows that the algebraic method is more than twice as fast as the shift-and-search method in [1]. These results are shown in detail in Table 1.

V. Conclusion

The procedure given in this article extends the decoding of the (23,12) Golay code to the (24,12) Golay code. This extension generalizes to any close-packed error-correcting code. However, since there is only one other nontrivial multiple-error-correcting perfect code – the (11,6) Golay code over $GF(3)$ – such a generality may be somewhat academic.

Acknowledgment

The authors thank Professor Van Lint, presently visiting at Caltech, for bringing M. Elia's paper to our attention.

References

[1] T.-K. Truong, J. K. Holmes, I. S. Reed, and X. Yin, "A Simplified Procedure for Decoding the (23,12) and (24,12) Golay Codes," *TDA Progress Report 42-96*, vol. October–December 1988, Jet Propulsion Laboratory, Pasadena, California, pp. 49–58, February 15, 1989.

[2] J. H. van Lint, *Introduction to Coding Theory*, New York: Springer-Verlag, 1982.

[3] R. McEliece, *The Theory of Information and Coding*, Reading, Massachusetts: Addison-Wesley, 1977.

[4] J. J. MacWilliams and W. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.

[5] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*, Englewood Cliffs, New Jersey: Prentice-Hall, 1983.

[6] E. R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw-Hill, 1968.

[7] M. Elia, "Algebraic Decoding of the (23,12) Golay Code," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 150–151, January 1987.

Table 1. Computer CPU time for decoder simulations

	Number of errors				
CPU time, ms	0	1	2	3	4
Algebraic method	15.5	16	20	21	22
Shift-and-search method	15	15.5	20	44.5	47

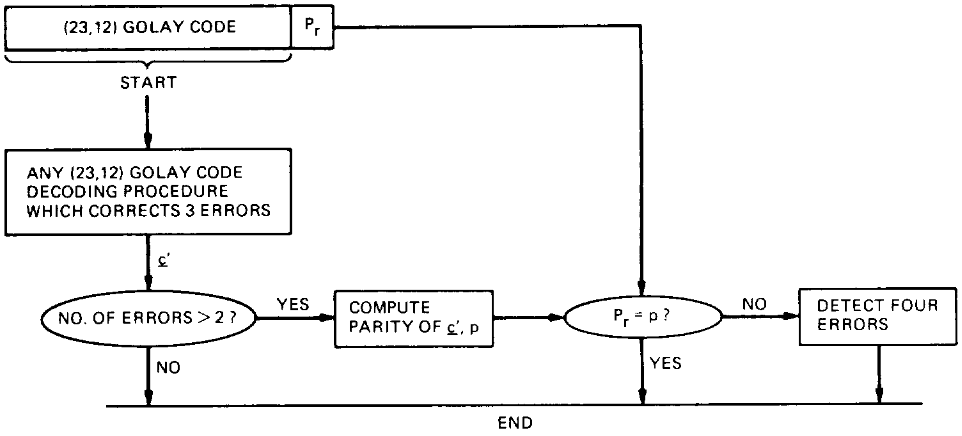

Fig. 1. Flowchart for decoding (24,12) Golay codes.

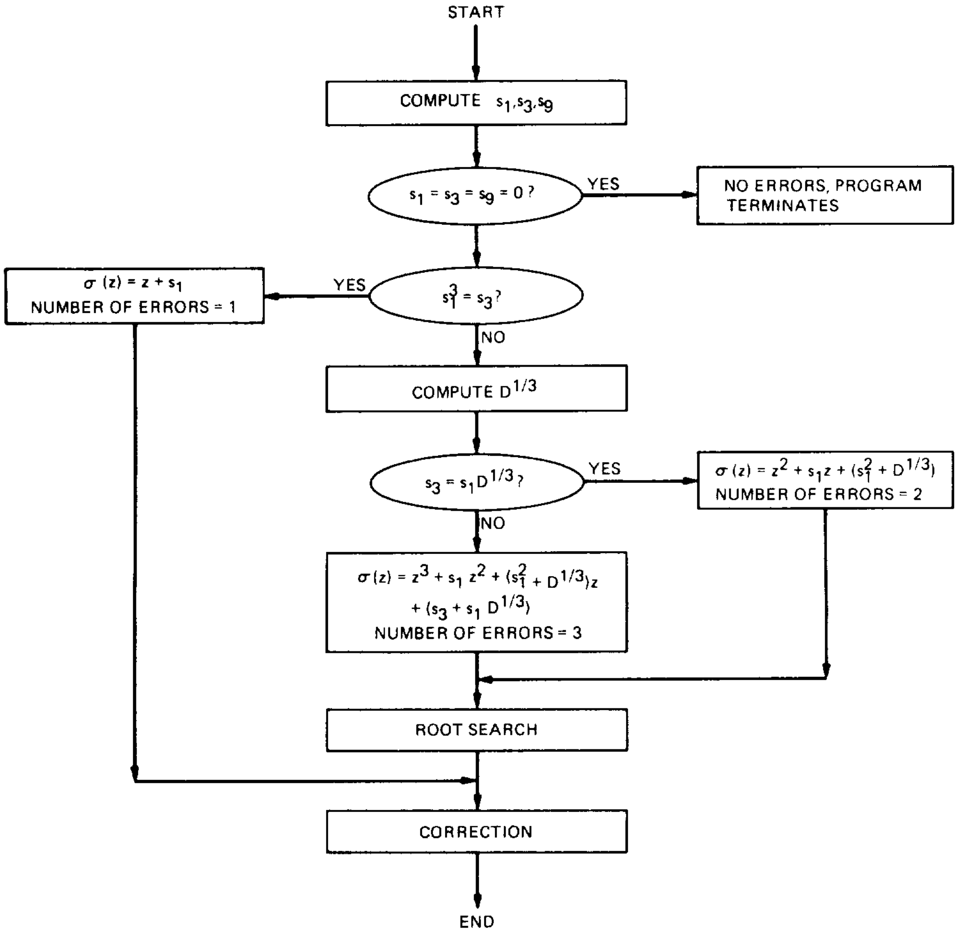

Fig. 2. Flowchart of Elia's algebraic procedure.

Appendix

Proof of Theorem

It is well known that the (23,12) Golay code is a close-packed code, i.e., the following equation holds:

$$2^{23} = \left[1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}\right] 2^{12}$$

Let $\mathbf{C}$ be the set of codewords of the Golay code. Also let $\mathbf{E}_i$ be the set of vectors of weight i. Therefore, for any $\underline{c} \in \mathbf{C}$, and any $\underline{e}_4 \in \mathbf{E}_4$, then $\underline{x} = \underline{c} + \underline{e}_4 = \underline{c}' + \underline{e}$ where weight of $\underline{e}$ satisfies $w(\underline{e}) \leqslant 3$. Hence $\underline{e} = \underline{x} + \underline{c}'$ so that by property $w(x + y) \geqslant |w(x) - w(y)|$ one has the inequality

$$w(\underline{e}) = w(\underline{c} + \underline{c}' + \underline{e}_4) \geqslant |\, w(\underline{c} + \underline{c}') - w(\underline{e}_4)|$$

where $w(\underline{c} + \underline{c}') = dis(\underline{c}, \underline{c}')$. Since minimum distance of the code is $d_{\min} = 7$, one has finally that $w(\underline{e}) \geqslant 3$, and the theorem is proved.

Appendix

Proof of Theorem

It is well known that the (23,12) Golay code is a close-packed code, i.e., the following equation holds:

$$2^{23} = \left[1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}\right] 2^{12}$$

Let **C** be the set of codewords of the Golay code. Also let $\mathbf{E}_i$ be the set of vectors of weight i. Therefore, for any $\underline{c} \in \mathbf{C}$, and any $\underline{e}_4 \in \mathbf{E}_4$, then $\underline{x} = \underline{c} + \underline{e}_4 = \underline{c}' + \underline{e}$ where weight of $\underline{e}$ satisfies $w(\underline{e}) \leqslant 3$. Hence $\underline{e} = \underline{x} + \underline{c}'$ so that by property $w(x+y) \geqslant |w(x) - w(y)|$ one has the inequality

$$w(\underline{e}) = w(\underline{c} + \underline{c}' + \underline{e}_4) \geqslant |\,w(\underline{c} + \underline{c}') - w(\underline{e}_4)|$$

where $w(\underline{c} + \underline{c}') = dis(\underline{c}, \underline{c}')$. Since minimum distance of the code is $d_{\text{min}} = 7$, one has finally that $w(\underline{e}) \geqslant 3$, and the theorem is proved.