Further Results on Finite-State Codes

F. Pollara and K.-M. Cheung
Communications Systems Research Section

R. J. McEliece
California Institute of Technology

A general construction for finite-state (FS) codes is applied to some well-known block codes. New subcodes of the (24,12) Golay code are used to generate two optimal FS codes with $\mathrm{d}_{free} = 12$ *and 16. A partition of the (16,8) Nordstrom–Robinson code yields a* $\mathrm{d}_{free} = 10$ *FS code. Simulation results are shown and decoding algorithms are briefly discussed.*

I. Introduction

Future deep-space communication systems will take advantage of powerful error-correcting coding schemes to keep power and antenna size requirements within acceptable bounds. Such codes can be found by computer search or, as considered in this article, by constructions based on known codes.

In a previous article [1] it was shown how some optimal Finite-State (FS) codes can be constructed from known block codes. This article considers new FS codes based on other block codes and describes performance results obtained by simulation.

II. Codes Derived From the (24,12) Golay Code

The basic idea developed in [1] consists in choosing an (n, k_1) block code C_1 with minimum distance d_1, and then decomposing C_1 into the disjoint union of cosets generated by an (n, k_2) subcode C_2 of C_1, with minimum distance d_2. By properly assigning these cosets to the edges of a 2^m-state completely connected graph, it is possible to construct an (n, k, m) FS code, with $k = m + k_2$ and $d_{\text{free}} \geqslant \min(d_2, 2d_1)$.

The (24,12) Golay code could be an interesting candidate for this construction provided that it contains a subcode with minimum distance d_2 larger than $d_1 = 8$. The following theorem shows that such a subcode does indeed exist.

Theorem 1. The (24,12) Golay code has a (24,5) subcode with minimum distance 12.

Proof: The proof is based on the Turyn construction of the Golay code (p. 587 of [2]). Let A be the (7,3) code with code words consisting of (0,0,0,0,0,0,0) and the seven cyclic shifts of (1,1,0,1,0,0,0). Then the (7,4) code $H = A \cup \bar{A}$, where the bar denotes the complemented code words, is the (7,4) Hamming code. Similarly, consider the code A^* obtained by reversing the order of symbols in A, and the code $H^* = A^* \cup \bar{A}^*$. Let

Table 1. Transfer function matrix to generate a completely connected state diagram with 8 states and 16 labels

	1	0	D	1	
$G(D)$ =	D	1	0	0	d_f = 2 branches
	0	D	1	0	

Table 2. Transfer function matrix to generate a non-completely connected state diagram with 64 states and 16 labels

	$1+D$	0	D^2	1	
$G(D)$ =	D^2	$1+D$	0	0	d_f = 3 branches
	0	D^2	$1+D$	0	

C and C^* be (8,4) codes obtained by adding a parity check bit to H and H^*. Then C and C^* have $d_{\min} = 4$, and the code G consisting of all vectors

$$|a+x|b+x|a+b+x|, \quad a,b \in C, \quad x \in C^* \qquad (1)$$

is the (24,12) binary Golay code with $d_{\min} = 8$.

Let B be the subcode of C consisting of the two code words (0,0,0,0,0,0,0,0) and (1,1,1,1,1,1,1,1). Then the construction in (1) with a, $b \in B$ and $x \in A^*$ generates code words of the form

$$|x|x|x|, \quad |x|\overline{x}|\overline{x}|, \quad |\overline{x}|x|\overline{x}|, \quad |\overline{x}|\overline{x}|x| \qquad (2)$$

Code words taken from two distinct subcodes of the four subcodes above are at minimum distance 8 + 8 = 16 for fixed x, and at distance 4 X 3 = 12 for $x \neq y \in A^*$. Code words in the same subcode are at minimum distance 4 X 3 = 12. Therefore, by using all 8 possible choices for x, we have constructed a (24,5) subcode of the Golay code with $d_{\min} = 12$. ■

Previously known (24,5) subcodes of the Golay code have $d_{\min} = 8$ [3], [4]. The (24,5) subcode just described can be represented on a trellis as shown in Fig. 1, where each edge x or $\bar{x}$ corresponds to eight bits. Figure 1 consists of the union of 8 cosets D_i, $i = 0, 1, \ldots, 7$, given by (2) with $x \in A^*$. Each coset has 4 code words and is represented by a trellis as shown in Fig. 2. This observation leads to the following result.

Corollary 1. The (24,12) Golay code has a (24,2) subcode with minimum distance equal to 16.

Proof: This follows directly from Expression (2) with x = (0,0,0,0,0,0,0,0). Figure 2 shows the trellis representing the (24,2) subcode with 4 code words. ■

Since there are 128 (24,5) cosets in the Golay code, it is possible to construct a non-catastrophic [1] FS code with up to 64 states on a completely connected graph. By this construction we obtain a (24,11,6) FS code with $d_{\text{free}} = \min(12, 2 \times 8) = 12$. For this code, since d_2 is strictly smaller than $2d_1$, it is also possible to say that there are exactly 30 error events at distance 12, the number of code words of the (24,5) subcode of weight 12. Similarly, by using the 2^{10} (24,2) cosets, we can construct a (24,11,9) FS code with $d_{\text{free}} = \min(16, 2 \times 8) = 16$. These new codes are both optimal in the sense that they achieve the largest possible free distance, as predicted by the Plotkin bound for FS codes [1].

III. Codes Derived From the Nordstrom–Robinson Code

In [1] a (16,7,2) FS code was constructed starting from the nonlinear (16,8) Nordstrom–Robinson code with $d_{\min} = 6$, which is the union of 8 particular cosets of the (16,5) first-order Reed–Müller code with $d_{\min} = 8$.

Given that the Nordstrom–Robinson code has many pairs of code words at distance 10 and that a $(16,k)$ code may have $d_{\min} = 10$ only if $k \leqslant 2$ (by the Plotkin bound), it is interesting to see if the Nordstrom–Robinson code can be split into 64 sets of 4 code words, each with $d_{\min} = 10$. The following theorem proves that this is true.

Theorem 2. The (16,8) Nordstrom–Robinson code can be partitioned into 64 sets, each having $d_{\min} = 10$.

Proof: The Nordstrom–Robinson code is the union of 8 cosets of the (16,5) first-order Reed–Müller code. Let the 8 coset leaders be denoted by a_i and b_i, $i = 0,1,2,3$. Then $a_0 = 0$ and the other coset leaders can be taken to be the following seven *bent*[1] functions of four Boolean variables x_1,x_2,x_3,x_4 (problem 21, p. 476 of [2]),

$$a_1 = x_1x_2 + x_1x_3 + x_2x_3 + x_2x_4$$
$$a_2 = x_1x_2 + x_3x_4$$
$$a_3 = x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$
$$b_0 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4$$
$$b_1 = x_1x_2 + x_1x_4 + x_2x_3$$
$$b_2 = x_1x_3 + x_2x_4 + x_3x_4$$
$$b_3 = x_1x_3 + x_1x_4 + x_2x_3 + x_3x_4$$

If instead the coset leaders are taken to be:

$$A_0 = 0$$
$$A_1 = a_1 + x_3 + 1$$
$$A_2 = a_2 + x_2 + x_4 + 1$$
$$A_3 = a_3 + x_1 + x_2 + 1$$
$$B_0 = b_0 + x_2 + x_3 + x_4$$
$$B_1 = b_1 + x_1 + x_4$$
$$B_2 = b_2 + x_3 + x_4 + 1$$
$$B_3 = b_3 + x_1 + x_2 + x_3 + 1$$

[1] These Boolean functions are so called because they are in some sense furthest away from linear functions.

then dist $(A_i, A_j) = 10$, dist $(B_i, B_j) = 10$, and dist $(A_i, B_j) = 6$ for all i and j, $i \neq j$. Then, for each word w in the (16,5) first-order Reed-Müller code $(A_0 + w, A_1 + w, A_2 + w, A_3 + w)$ and $(B_0 + w, B_1 + w, B_2 + w, B_3 + w)$ are subsets of the Nordstrom-Robinson code with distance 10. There are 64 such subsets and they exhaust the Nordstrom-Robinson code. ■

Table 1 shows the code words of the (16,5) first-order Reed-Müller code and the 8 coset leaders that generate the 64 subsets used for the FS code construction. By assigning the 64 subsets to the edges of a 32-state completely connected graph a (16,7,5) FS code can be constructed. This code has $d_{\text{free}} = \min(2 \times 6, 10) = 10$, which meets the Plotkin bound.

IV. Simulation Results and Decoding Algorithms

An existing software simulation for FS codes has been adapted to the newly found codes. Simulation results showing the probability of bit error versus E_b/N_0 are given in Fig. 3. The (24,11,6) FS code with $d_{\text{free}} = 12$ and the (16,7,5) FS code with $d_{\text{free}} = 10$ are compared for reference to the (2,1,6) Voyager convolutional code.

These results are obtained by a soft, maximum-likelihood decoder based on the Viterbi algorithm. The decoder performs two basic steps:

(1) Each received word (24 or 16 symbols) is compared to the code words in each coset (128 or 64) and the closest code word in each coset is stored together with its distance.

(2) At each state, the decoder further selects the closest code word among those chosen in step 1 for the cosets assigned to branches reaching that state.

For the (24,11,6) code, the total number of bit operations per decoded bit involved in the decoding process is $(24/11)\,2^{12}$, where 2^{12} is the total number of branches in one stage of the decoder trellis. It is interesting to note that the same number for the Golay code is $(24/12)\,2^{12}$, which is very close, but the FS code has $d_{\text{free}} = 12$ compared to a $d_{\text{free}} = 8$ of the Golay code. Similarly, the decoding of the (16,7,5) code involves $(16/7)\,2^{10}$ bits per decoded bit.

V. Conclusion

In this article we have described FS codes based on partitions of the Golay and Nordstrom-Robinson codes, which did not appear in the literature.

The comparison of these new codes to known codes, block and convolutional, is complicated by the fact that both the performance and the decoding complexity must be taken into account, and the complexity is intimately related to the particular hardware architecture used for the decoder. We feel that the proposed codes may take greater advantage of parallel VLSI architectures than conventional convolutional codes with no structure. Also, the trellis representation of cosets as in Figs. 1 and 2 can be used to reduce the number of comparisons to select the closest code word with methods similar to those described in [3].

Figure 4 summarizes the present knowledge on FS codes by showing the Plotkin or Hamming bound (whichever is tighter) on the free distance achievable for a given encoder memory and for two classes of FS codes, the $(24,11,m)$ and the $(16,7,m)$ classes. The (16,7,2) code has been reported in [1]. The Voyager code is also shown for comparison as a member of the $(2,1,m)$ class of convolutional codes. More work needs to be done in constructing yet more powerful FS codes, especially those based on graphs that are not completely connected.

References

[1] F. Pollara, R. J. McEliece, and K. Abdel-Ghaffar, "Constructions for Finite-State Codes," *TDA Progress Report 42-90*, April–June 1987, Jet Propulsion Laboratory, Pasadena, California, pp. 42–49, August 15, 1987.

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1978.

[3] J. H. Conway and N. J. A. Sloane, "Soft Decoding Techniques for Codes and Lattices," *IEEE Trans. Information Theory*, vol. IT-32, January 1986.

[4] G. D. Forney, "Coset Codes I and II," *IEEE Trans. Information Theory*, to be published in 1988.

Table 1. Code words of (16,5) first-order Reed–Müller code and coset leaders

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	w_0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	w_1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	w_2
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	w_3
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	w_4
1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	w_5
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	w_6
1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	w_7
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	w_8
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	w_9
0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	w_{10}
1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	w_{11}
0	0	1	1	0	0	1	1	1	1	0	0	1	1	0	0	w_{12}
1	1	0	0	1	1	0	0	0	0	1	1	0	0	1	1	w_{13}
0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	w_{14}
1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	w_{15}
1	1	0	0	0	0	1	1	0	0	1	1	1	1	0	0	w_{16}
0	0	1	1	1	1	0	0	1	1	0	0	0	0	1	1	w_{17}
0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	w_{18}
1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	w_{19}
0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	w_{20}
1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	w_{21}
1	0	1	0	0	1	0	1	0	1	0	1	1	0	1	0	w_{22}
0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1	w_{23}
0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	w_{24}
1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	w_{25}
0	1	1	0	0	1	1	0	1	0	0	1	1	0	0	1	w_{26}
1	0	0	1	1	0	0	1	0	1	1	0	0	1	1	0	w_{27}
1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	w_{28}
0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	w_{29}
1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	w_{30}
0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	w_{31}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	A_0
1	1	0	0	1	0	1	0	1	1	1	1	0	1	1	0	A_1
1	0	1	1	0	1	0	0	1	0	1	1	1	0	1	1	A_2
1	1	1	0	0	1	1	1	0	1	0	0	1	1	0	1	A_3
0	1	1	0	1	1	0	0	0	0	0	0	0	1	0	1	B_0
0	1	0	1	0	1	1	0	1	1	1	1	0	0	1	1	B_1
1	0	0	0	1	1	0	1	1	0	1	1	1	1	1	0	B_2
1	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	B_3

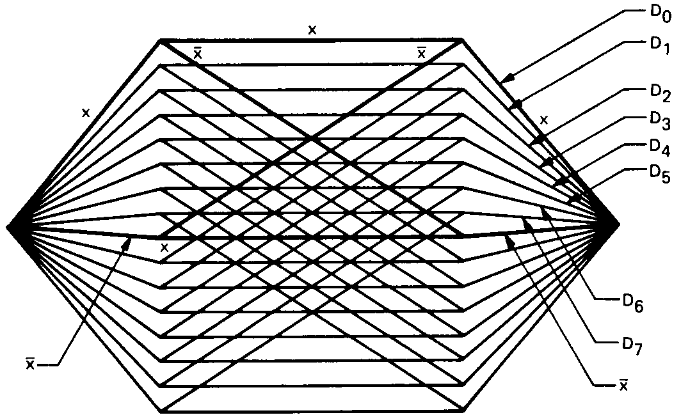

Fig. 1. The (24,5) subcode, x ∈ A*

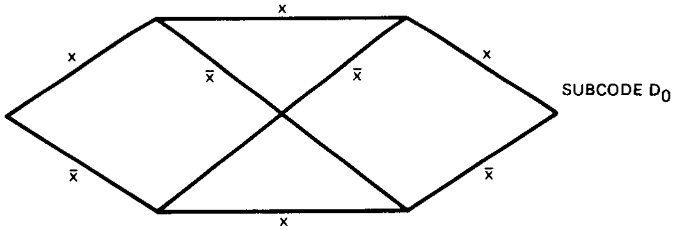

Fig. 2. The (24,2) subcode, x = (0,0,0,0,0,0,0,0)

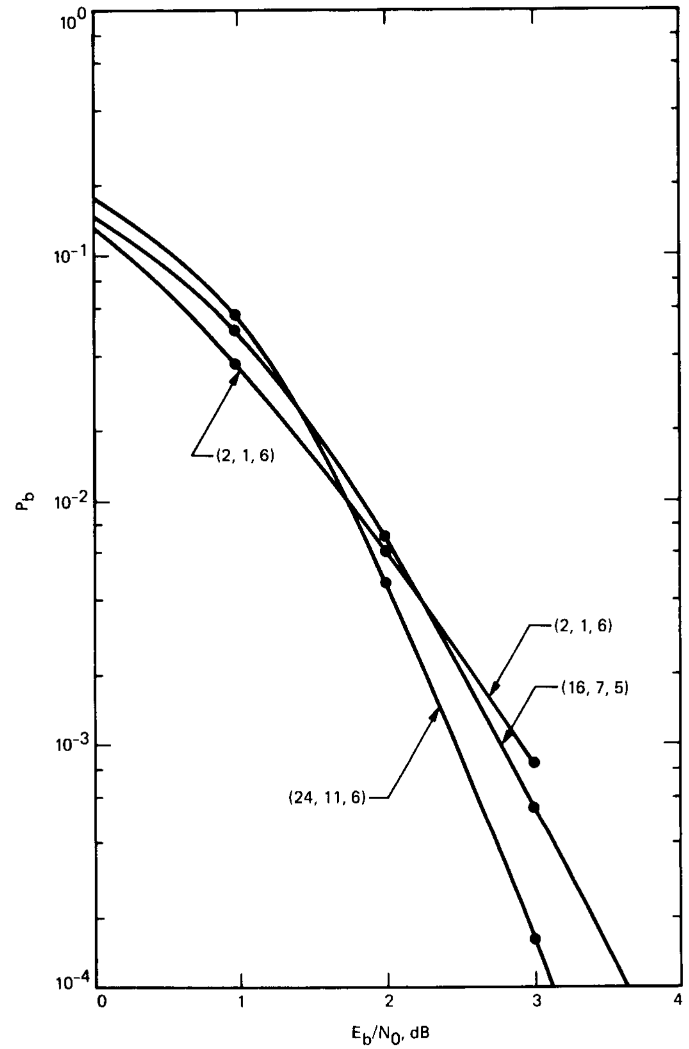

Fig. 3. Bit error probability of two new FS codes

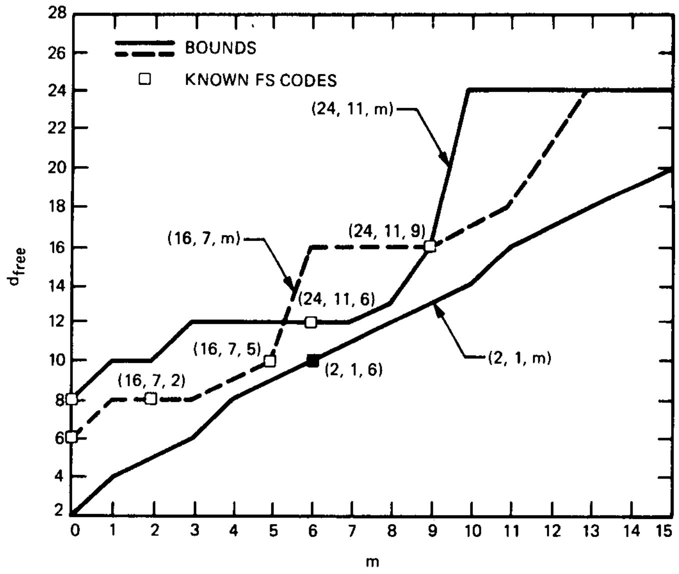

Fig. 4. Free distance bounds for two classes of FS codes compared to (2,1,*m*) convolutional codes