Encoding and Decoding a Telecommunication Standard Command Code

B. Benjauthrit and T. K. Truong
TDA Engineering Office

This paper describes a simple encoder/decoder implementation scheme for the (63,56) BCH code which can be used to correct single errors and to detect any even-number of errors. The scheme is feasible for onboard-spacecraft implementation.

Recently, it was shown in Ref. 1 that a Bose Chaudhuri and Hocquenghem (BCH) code (Ref. 2) may be used to improve command coding for future planetary exploration missions. A block of command data of 64 bits is shown as follows:

I_0,I_1 I_{55}	$P_0,P_1,..P_6$	F_1
56 information bits	7 parity check bits	1 filler bit

The first 56 bits, I_0 through I_{55}, are command information, $P_0, P_1, \ldots, P_6$ are parity check bits of the (63,56) BCH code, and F_1=0 is a filler bit. This code (which may also be referred to as an extended Hamming code, Ref. 3) will be shown to give a single-error correcting, even-number-error detecting capability advantage over the uncoded scheme, and simple linear switching circuits can be used to improve the encoding and decoding efficiency of it.

In order to generate the parity-check matrix of the (63, 56) BCH code, it is necessary to find the generator polynomial $g'(x)$ for this code. By Ref. 2, Appendix C, an irreducible polynomial in $GF(2^6)$ is $g^*(x) = x^6 + x + 1$. However, since the reciprocal polynomial is also a primitive polynomial, the reciprocal of $g^*(x)$, $g(x) = x^6 g^* (1/x) = x^6 + x^5 + 1$, may also be used. Further, since the code requires 7 parity check bits, the parity check matrix generating polynomial $g(x) = x^6 + x^5 + 1$ will give one fewer parity check. To obtain one additional parity check, one must find $g'(x)$ of degree seven. One possible such $g'(x)$ is of the form:

$$g'(x) = (x + 1)(x^6 + x^5 + 1) = x^7 + x^5 + x + 1 \qquad (1)$$

Since the sequence generated from the equation

$$x^7 = x^5 + x + 1 \qquad (2)$$

has period 63[1], the period of the sequence generated from $g'(x)$, then the parity check matrix generated from Eq. (2) is given in Table 1. Note that α^j is obtained by substituting α for x in Eq. (2) and reducing modulo $\alpha^7 + \alpha^5 + \alpha + 1$. Also $\alpha^{63} = 1$.

The parity check matrix H generates a (63, 56) code which is capable of correcting single errors and detecting any even-number errors in a code block of 63 bits. To show this, let $C = (C_{62}, C_{61}, \cdots, C_0)$ denote the codeword. Then the syndrome of C is

$$S = HC^t = \sum_{i=0}^{62} C_{62-i}\,\alpha^i = 0, \text{ for all } \alpha^i \epsilon H,$$

where C^t designates the transpose of C. Let the received codeword with an error be

$$\begin{aligned} R &= (R_{62}, R_{61}, \cdots, R_{62-j}, \cdots, R_0) = C + E \\ &= (C_{62}, C_{61}, \cdots, C_{62-j}, \cdots, C_0) + (0, 0, \cdots, E_{62-j}, \cdots, 0) \end{aligned}$$

where E represents the error code word. Then the syndrome S_1 of R is

$$S_1 = E_{62-j}\,\alpha^j = \alpha^j$$

Hence j is the error location of the received codeword, and an error is corrected.

Now observe that every column of H contains an odd number of 1's.[2] If a double error occurs in locations i and j, then

$$S_1 = E_{62-i}\,\alpha^i + E_{62-j}\,\alpha^j = \alpha^i + \alpha^j = \alpha^k, \alpha^k \epsilon GF(2^7)$$

Since α^i and α^j each has an odd number of 1's, α^k must have an even number of 1's (i.e., $(2M + 1) + (2N + 1) = 2(M + N + 1)$) and is thus not contained in H. Hence, the double error is detected. In fact, any number of double errors can be detected by this code because the field element of the resulting syndrome contains the number of 1's equal to $(2N_1 + 1) + (2N_2 + 1) + (2M_1 + 1) + (2M_2 + 1) + \cdots = 2(N_1 + N_2 + 1 + M_1 + M_2 + 1 + \cdots)$, which is even. Therefore, any double errors or even number of errors are detectable by this code.

Once the desired parity check matrix generating polynomial is determined, the encoder/decoder implementation scheme is similar to that discussed by Berlekamp [Ref. 4, Chapter 5]. The encoder and decoder derived from $g'(x)$ in Eq. (2) for the code are depicted in Fig. 1. This indicates that only a 7-cell shift register and 3 modulo-two adders are required for the implementation of the encoder. To implement the decoder, a 77-cell shift register, 6 modulo-two adders and one OR gate are needed. Any double errors can be monitored at the output of the 7-input modulo-two adder.

The encoder operates this way: First, the shift register is initialized to zero, and the three switches are posed in the up positions. When the message source is turned on, a block of 56 information bits, $I_0, I_1, \ldots, I_{55}$, is shifted down the channel and into the feedback shift register. Then the three switches are placed in the down positions, but the shifting is continued eight more times to generate the 7 parity check bits and one filler bit (to make a 64-bit word). At this point, the feedback shift register contains all zeros. Finally, all the switches are toggled back up again, ready for encoding the next block of information bits. The decoder operates as follows: After the entire received codeword $R = (R_0, R_1, \ldots, R_{63})$ has been buffered into the top register, discarding the filler bit at the end, the middle register contains the syndrome S_1 of R. The field elements S_1 are then transferred to the bottom register, while the middle register is reset to zero as indicated by the dashed lines. This yields $S_1\alpha$ in the bottom register. (The contents of this register are multiplied by α for each shift). Hence the input leads to the OR gate carry $1 + S_1\alpha^i$ as the digit at location α^{-i} deserts the buffer, $i = 1, 2, \cdots, 63$. If $1 + S_1\alpha^i \neq 0$, then $S_1 \neq \alpha^{-i}$, so the digit at location α^{-i} leaves the buffer unchanged. However, if $1 + S_1\alpha^i = 0$, then $S_1 = \alpha^{-i}$, and

[1] To prove this, one first recalls from Theorem 2.3 of Golomb (Ref. 3) that the period of the sequence I generated from the characteristic polynomial $f(x)$ is the smallest positive integer p for which $f(x)|1 + x^p$ mod 2. Now let $f'(x) = (x + 1)\,f(x)$. We must show that the sequence generated by $f'(x)$ also has period p. It is evident that $x + 1|x^p + 1$. Since also $f(x)|x^p + 1$, then $lcm\ (x + 1, f(x))|\,x^p + 1$. Now since $gcd(x + 1, f(x)) = 1$ implies $lcm(x + 1, f(x)) = f'(x)$; hence $f'(x)|x^p + 1$. Further, assume that $f'(x)|x^r + 1$ for all positive integer $r < p$. This then implies that $x^r + 1 = f'(x)\,a(x) = f(x)\,b(x)$ and $f(x)|x^r + 1$. Hence $f'(x)|x^r + 1$ for $f(x)|x^r + 1$.

[2] This is because Eq. (2) has 3 terms (or, in general, an odd number of terms, say equal to $2M + 1$ terms) on the right-hand side. Hence any column in H generated from Eq. (1) contains the number of 1's of the form $(2L + 1) - 1 + (2M + 1) - 2N = 2\,(L + M - N) + 1$, which is always odd.

the error is corrected as it departs the buffer. To monitor the occurrence of an even number of errors, a 7-input modulo-two adder is connected to the output of the bottom register. Since an even number of errors will result in a field element syndrome having an even number of 1's, a zero appearing at the output of this modulo-two adder will indicate an uncorrectable error.

Since the implementation and its principle of operations suggested above are simple, the (63,56) code is feasible for onboard-spacecraft implementation. The code with the above implementation scheme is suitable for incorporation into the NASA telemetry command coding standard. This would result in gaining a single-error correcting, even-number error detecting capability advantage over the uncoded system.

Acknowledgement

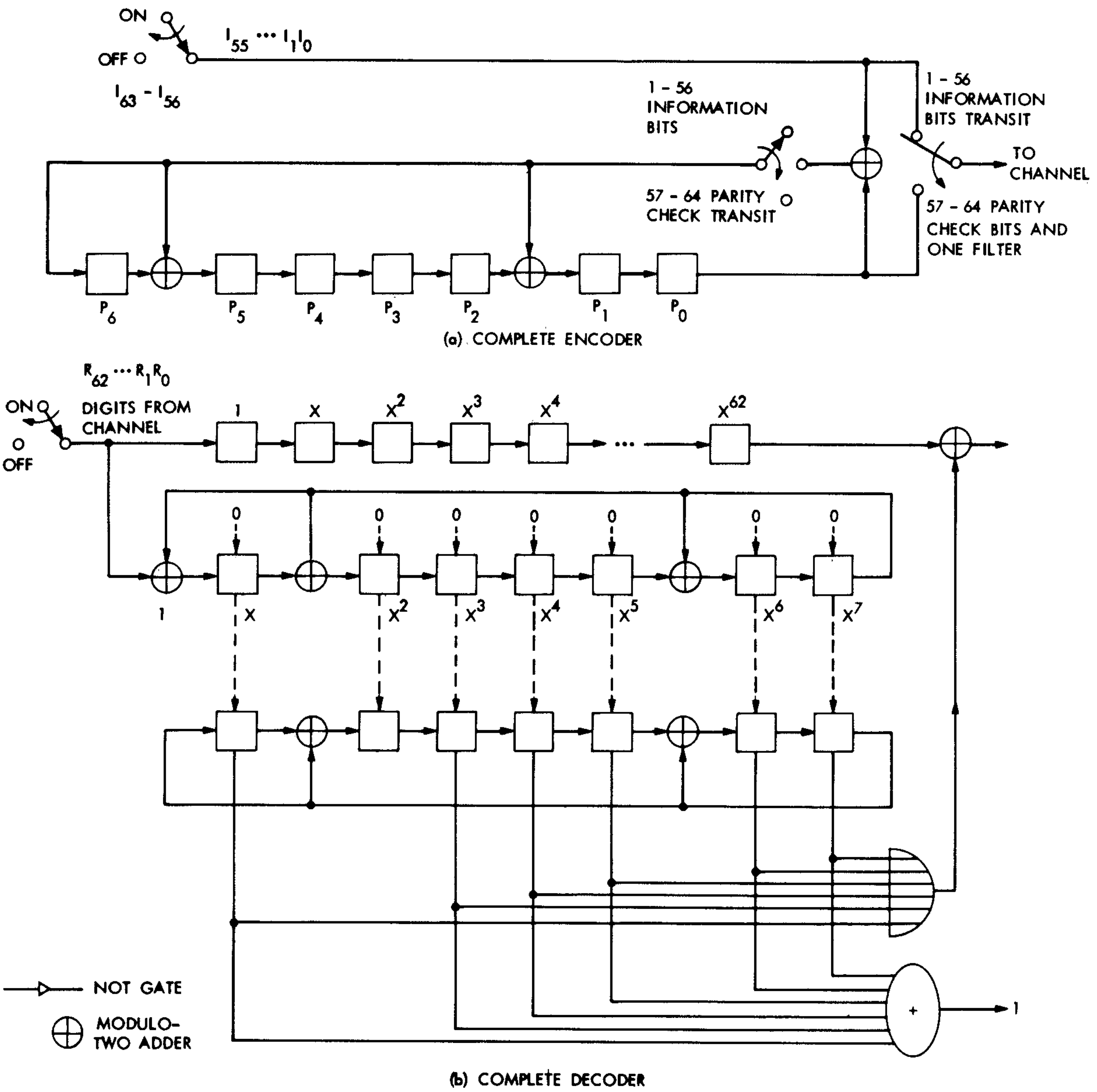
The authors express their thanks to B. D. L. Mulhall for first directing their attention to this coding problem and Prof. L. R. Welch of USC for his many helpful suggestions on the subject of coding.

References

1. Truszynski, G. M., and Hinners, N. W., "NASA Planetary Program Flight/Ground Telecommunications Standards – Command Coding Standard," Memorandum to distribution, NASA Headquarters, Sep. 20, 1976.
2. Peterson, W. W., and Weldon, E. J., Jr., *Error-Correcting Codes*, 2nd ed., MIT Press, Massachusetts Institute of Technology, 1972.
3. Golomb, S. W., *Shift Register Sequences*, Holden, Inc., 1967.
4. Berlekamp, E. R., *Algebraic Coding Theory*, McGraw-Hill, 1972.

Table 1. Parity check matrix generated from $x^7 = x^6 + x + 1$

$$\begin{array}{rcl}
 & \alpha^0\alpha^1\alpha^2\alpha^3\alpha^4\alpha^5\cdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \alpha^{61}\alpha^{62} & \\
 & 012345678901234567890123456789012345678901234567890123456789012 & \\
H = & \left[\begin{array}{c}
100000010101001100100010010110110001110100001101011100111101111\\
010000011111101010110011011101101001001110001011110010100011000\\
001000001111110101011001101110110100100111000101111001010001100\\
000100000111111010101100110111011010010011100010111100101000110\\
000010000011111101010110011011101101001001110001011110010100011\\
000001010100110010001001011011000111010000110101110011110111110\\
000000101010011001000100101101100011101000011010111001111011111
\end{array}\right] & \begin{array}{l}\alpha^0\\ \alpha^1\\ \alpha^2\\ \alpha^3\\ \alpha^4\\ \alpha^5\\ \alpha^6\end{array}
\end{array}$$



(a) COMPLETE ENCODER

(b) COMPLETE DECODER

Fig. 1. Encoder/decoder for (63, 56) extended Hamming codes