much lesser extent on the size distribution. The relationship between the differential attenuation and the phase allows the propagation analysis to be simplified because this analysis will depend mainly on one parameter. The importance of this simplification is apparent in the adaptive cancellation of cross-polarisation. For dual linearly polarised links, in the case where differential phase shift is the dominant cause of cross-polarisation, it is proposed to perform adaptive cancellation of the cross-polarisation by means of a simplified network with only one variable parameter.

Acknowledgments: It is a pleasure to acknowledge the help and co-operation of Dr. A. R. Holt of the Mathematics Department at Essex in providing the computed scattering amplitudes.

M. M. TAHERI

Department of Electronic Systems Engineering
University of Essex
Wivenhoe Park, Colchester CO3 4SQ, United Kingdom

13th June 1989

References

1 OGUCHI, T.: *Radio Sci.*, 1980, **16**, pp. 691–730
2 HOLT, A. R.: *Acoustic, Electromagnetic and Elastic Wave Scattering*, 1980, pp. 225–268
3 DILWORTH, I. J.: IEE colloquium on cross polar cancellation techniques, Digest No. 111, December 1985
4 HARDEN, W., NORBURY, J. R., and WHITE, W.: 'Radio attenuation studies'. IEE/URSI International Conference on Antennas and Propagation, pp. 87–91, 1978
5 MORRISON, J. A., and CROSS, M. J.: *Bell Syst. Tech. J.*, 1974, **53**, (4), pp. 955–1019
6 GODDARD, J. W. F., and CHERRY, S.: U.R.S.I., open symposium, Bournemouth, UK, pp. 161–167, 1982
7 OLALERE AJAYI, G.: 'Waves using a tropical raindrop size distribution', *Int. J. Infrared Millim. Waves*, 1985, pp. 771–806
8 UPTON, S. A. J.: Ph.D. thesis, University of Essex, 1984
9 MCEWAN, N. J., GUNES, M., and MAHMOUD, M. S.: 'RF methods for adaptive cancellation of cross-polarisation in microwave satellite systems'. *IEE Conf. Publ. 195*, 1981, Pt. 2, pp. 188–192
10 ROGERS, D. V., and ALLNUTT, J. E.: 'Some practical considerations for depolarisation compensation in 14/11 and 14/12 GHz communications satellite systems', *Electron. Lett.*, 1985, **21**, pp. 1093–1094

COMPLETE DECODING ALGORITHM OF (11, 6, 5) GOLAY CODE

Indexing terms: Codes, Error-correction codes, Decoding, Algorithms

A simple complete decoding algorithm for the (11, 6, 5) perfect ternary Golay code is presented. This algorithm is based on a step-by-step method and requires only 17 shift operations for decoding one received word.

Introduction: The three known perfect codes are the (7, 4, 3) Hamming code, the (23, 12, 7) binary Golay code and the (11, 6, 5) ternary Golay code.[1] The (11, 6, 5) Golay code is a double-error-correcting perfect code since the minimum distance of this code is confirmed to be 5.[2] Therefore, a complete decoding algorithm can be easily achieved if any combination of two or fewer errors can be corrected. Since the (11, 6, 5) Golay code is a cyclic code, the step-by-step decoding method can be employed if the different weights of received error patterns can be distinguished by the receiver.[3] In this letter, a simple algebraic step-by-step decoding algorithm of the (11, 6, 5) Golay code is presented. This method is much faster than the method presented in Reference 2 which considers the temporary correction of two errors and hence takes a large amount of shift operations to complete the correction process.

(11, 6, 5) Golay code: Consider the (11, 6, 5) Golay code with generator polynomial $g(x) = x^5 + x^4 + 2x^3 + x^2 + 2$, the encoded codeword $c(x)$ can be simply generated in systematic form by $K(x)x^6 - \text{Mod}\ \{K(x)x^6/g(x)\}$, where $K(x)$ is the information polynomial of degree 5 and Mod $\{K(x)x^6/g(x)\}$ indicates the remainder polynomial of $K(x)x^6$ divided by $g(x)$. The roots of this generator polynomial are confirmed to be (β, β^3, β^4, β^5, β^9), where β is the primitive 11th root of unity.[1,2] Letting α be the primitive element in GF (3^5), it is found that $\beta = \alpha^{22}$ and therefore the arithmetic computation of this code can be performed in GF (3^5). Furthermore, since $\{0, 1, 2\}$ are the elements of GF (3), the addition of any two elements in GF (3^5) is accomplished by adding the corresponding polynomial term by term using modulo-3 addition. The multiplication of nonzero elements may be done by multiplication of the corresponding polynomials and reduction of the product modulo $\alpha^5 + 2\alpha + 1$.[4]

Complete decoding algorithm: If the received polynomial is expressed as $\tau(x) = \tau_0 + \tau_1 x + \ldots + \tau_{10}x^{10}$, by choosing two roots β and β^5, the syndrome values S_1 and S_5 of $\tau(x)$ can be obtained from

$$\begin{aligned} S_i &= \tau(\beta^i) && i = 1, 5 \\ &= \text{Mod}\ \{\tau(x)/g(x)\}_{|x=\alpha^{22i}} && i = 1, 5 \\ &= \sum_{j=1}^{2} Y_j X_j^i && i = 1, 5 \quad (1) \end{aligned}$$

where X_j is the error locator of jth error symbol and Y_j is the corresponding error value. Since Y_j can only be 0, 1 or 2, it is found that if only one error has occurred, then

$$(S_1)^5 = (Y_1 X_1)^5 = Y_1 X_1^5 = S_5 \quad (2)$$

It implies that $T_5 = (S_1)^5 + 2S_5 = 0$ if one error has occurred. Moreover, as confirmed by computer simulation, we found that $T_5 \neq 0$ if two or three errors have occurred. Clearly, $S_1 = T_5 = 0$, if no error occurs. Thus, the relationships of the syndrome values for various weights of error patterns can be concluded as follows:

(i) if there is no error, then $S_1 = T_5 = 0$

(ii) if there is one error, then $S_1 \neq 0$ and $T_5 = 0$

(iii) if there are two or three errors, then $S_1 \neq 0$ and $T_5 \neq 0$.

Furthermore, the syndrome values of a cyclic shift of $\tau(x)$, $S_1^{(1)}$ and $S_5^{(1)}$, can be simply obtained by shifting the syndrome generator of $g(x)$ once with initial contents S_i (Reference 5, theorem 8.7). Thus,

$$S_i^{(j)} = \text{Mod}\ \{\tau^{(j)}(x)/g(x)\}_{|x=\alpha^{22i}} \qquad 0 < j \leq 11,\ i = 1, 5 \quad (3)$$

are the syndrome values of $\tau^{(j)}(x) = \tau_{11-j} + \tau_{12-j}x + \ldots + \tau_0 x^j + \ldots + \tau_{10-j}x^{10}$. Since the relationships between $S_1^{(j)}$ and $S_5^{(j)}$ change only when the weight of the error pattern changes and are independent of the cyclic shift of $\tau(x)$, a complete decoding algorithm of the (11, 6, 5) Golay code is then presented as follows:

(*a*) Calculate the syndrome values S_1 and S_5. If $S_1 = 0$ then read out $\tau(x)$ and end this algorithm; otherwise, calculate T_5.

(*b*) $j = 1$.

(*c*) Find $S_i^{(j)}$, $i = 1, 5$.

(*d*) If $T_5 = 0$ then calculate $Z_1^1 = S_1^{(j)} + 1$ and $Z_1^2 = S_1^{(j)} + 2$. If $Z_1^1 = 0$ then replace τ_{11-j} with $\tau_{11-j} + 1$; if $Z_1^2 = 0$ then replace τ_{11-j} with $\tau_{11-j} + 2$. Go to step (*f*).

(*e*) If $T_5 \neq 0$ then calculate $Z_5^1 = (S_1^{(j)} + 1)^5 + 2(S_5^{(j)} + 1)$ and $Z_5^2 = (S_1^{(j)} + 2)^5 + 2(S_5^{(j)} + 2)$. If $Z_5^1 = 0$ then replace τ_{11-j} by $\tau_{11-j} + 1$; if $Z_5^2 = 0$ then replace τ_{11-j} by $\tau_{11-j} + 2$.

(*f*) If $j = 6$ then the decoding algorithm is completed; otherwise, $j = j + 1$ and go to step (*c*).

This step-by-step decoding algorithm needs only 17 shift operations to decode one received word, where 11 shift operations are used for calculating the syndrome values S_1 and S_5 in step (*a*) and the other 6 shift operations are used for correcting the errors in the information part.

Conclusions: A simple algebraic step-by-step decoding algorithm of (11, 6, 5) Golay code in systematic form has been presented. This decoding algorithm requires only 17 shift operations to decode one received word. Since the decoding algorithm makes use of the cyclic properties of the code and requires only the calculation of the value of $(S_1)^5 + 2S_5$ in GF (3^5), the algorithm can be easily implemented in hardware by employing ternary-state logic gates.

Acknowledgement: The work reported in this letter is supported by the National Science Council of Republic of China under Grant NSC.77-0404-E009-08.

S.-W. WEI
C.-H. WEI

Institute of Electronics and Center for Telecommunications Research
National Chiao Tung University
Hsin Chu, Taiwan, Republic of China

13th June 1989

References

1 MACWILLIAMS, F. J., and SLONE, N. J. A.: 'The theory of error correcting code' (North-Holland Mathematical Library, 1978)
2 CHIEN, R. T., and LUM, V.: 'On Golay's perfect codes and step-by-step decoding', *IEEE Trans.*, 1966, **IT-12**, pp. 403–404
3 HARTMANN, C. R. P.: 'A note on the decoding of double-error-correcting binary BCH codes of primitive length', *IEEE Trans.*, 1971, **IT-17**, pp. 765–766
4 MICHELSON, A. M., and LEVESQUE, A. H.: 'Error-control techniques for digital communication' (John Wiley & Sons, Inc., 1985)
5 PETERSON, W. W., and WELDON, E. J., JR.: 'Error-correcting codes' (2nd ed., MIT press, Cambridge, 1972)

JUSTESEN CONSTRUCTION FOR POLYNOMIAL REDUNDANT RESIDUE CODES

Indexing terms: Codes, Information theory, Error-correction codes, Polynomials

The Justesen construction for asymptotically good codes is described in terms of polynomial redundant residue codes by constructive methods using polynomial operations. Irreducible polynomials of higher degree give asymptotic limits equivalent to RS codes. A different construction gives higher rate codes with asymptotic results similar to the punctured Justesen codes.

Redundant residue codes[2] are a general class of linear maximum distance separable codes. In a certain sense, they can be said to contain Reed–Solomon (RS), Goppa and alternant codes. The Justesen codes[1] were constructed with RS codes as the outer codes in a concatenated scheme. In this letter it is shown how redundant residue codes, instead of RS codes, can be used in a similar construction. The construction and proofs involve operations on polynomials modulo irreducible polynomials.

Let $u(x)$ be a polynomial of degree less than mK with coefficients over a field F. Let $m_0(x), m_1(x), m_2(x), \ldots, m_{N-1}(x)$ be N relatively prime polynomials (called the moduli) each of degree m, where $N \geq [\deg u(x)]/m$ and $N > K$. Then the word or vector $c = [r_0(x), r_1(x), r_2(x), \ldots, r_{N-1}(x)]$ is a code word of a $(N, K, N - K + 1)$ linear maximum distance separable code, where $r_i(x) = u(x) \bmod m_i(x)$. This code is called a redundant residue code since $r_i(x)$ is the residue of $u(x)$ modulo $m_i(x)$. The term redundant comes from the fact that $u(x)$ can be recovered from c by K residues $r_0(x), r_1(x), \ldots, r_{K-1}(x)$ if $mK > \deg u(x)$ by means of the Chinese remainder theorem. The residues $r_K(x), r_{K+1}(x), \ldots, r_{N-1}(x)$ are redundant residues which lead to the distance $N - K + 1$ for this code. If $m(x) = x - \alpha^i$ where α^i are the elements of a finite field $GF(q^h)$, the code is a Reed-Solomon (RS) code where $u(x)$ is a polynomial over $GF(q^h)$ which carries the information.

Let C be a $(N, K, N - K + 1)$ redundant residue code over a field F where $a = [a_0(x), a_1(x), \ldots, a_{N-1}(x)]$ is a codeword of C, and $a_i(x) = u(x) \bmod m_i(x)$ for $\deg u(x) < mK$. Let b be the vector

$$b = [a_0(x), v_0(x); a_1(x), v_1(x); \ldots; a_{N-1}(x), v_{N-1}(x)] \quad (1)$$

where $v_i(x) = a_i(x)v(x) \bmod m_i(x)$ for $0 \leq i \leq N - 1$, and where $v(x)$ is a polynomial of degree m over F so that the members of the set $m_0(x), m_1(x), \ldots, m_{N-1}(x), v(x)$ are relatively prime. It is now shown that every nonzero pair of polynomials $[a_i(x), v_i(x)]$ is distinct, i.e. $[a_i(x), v_i(x)] \neq [a_j(x), v_j(x)]$ for $i \neq j$ and $a_i(x)$ and $a_j(x)$ both nonzero. For the obverse, $[a_i(x), v_i(x)] = [a_j(x), v_j(x)]$. Then $a_i(x) = a_j(x)$ and $v_i(x) = v_j(x)$, which means that $a_i(x)v(x) \bmod m_i(x) \equiv a_i(x)v(x) \bmod m_j(x)$. Since $\deg a_i(x)v(x) \geq m$, then

$$a_i(x)v(x) - c_i(x)m_i(x) = a_i(x)v(x) - c_j(x)m_j(x) \quad (2)$$

where $c_i(x), c_j(x) \neq 0$. Therefore $c_i(x)m_i(x) = c_j(x)m_j(x)$. Since $m_i(x), m_j(x)$ are relatively prime, then it is necessary that $c_j(x) = e_i(x)m_i(x)$, $c_i(x) = e_j(x)m_j(x)$, where $e_i(x)$ and $e_j(x)$ are both nonzero. As a result, $\deg c_i(x) \geq m$ and $\deg c_j(x) \geq m$, whereas $\deg a_i(x)v(x) \leq 2m - 1$, so that eqn. 2 is not a polynomial of degree less than m. This gives a contradiction since $v_i(x)$ must have degree less than m. If in eqn. 1, $a_i(x) \neq 0$, then $v_i(x) \neq 0$ since $m_i(x)$ and $v(x)$ are relatively prime. Since the code C has distance $N - K + 1$, then there are at least $N - K + 1$ distinct pairs $[a_i(x), v_i(x)]$ in eqn. 1.

The redundant residue code B, composed of words such as eqn. 1, is linear, if we assume two code words generated by the information polynomials $u(x)$ and $u'(x)$. Then the sum of coordinate pairs $[a_i(x), v_i(x)]$ and $[a'_i(x), v'_i(x)]$ is $[a_i(x) + a'_i(x), v_i(x) + v'_i(x)] = [[(u(x) + u'(x)] \bmod m_i(x), [a_i(x) + a'_i(x)]v(x) \bmod m_i(x)]$. This code can be considered a concatenated code for the same reasons as for the Justesen code using RS codes as the outer codes, and has length $2mN$ symbols from F and mK information symbols, giving a rate of $K/2N$. If $m_i(x) = x - \alpha^i$, $0 \leq i \leq q^h - 1$, where α is a primitive element of $GF(q^h)$ and $v(x) = x$, then this construction yields the original Justesen construction.[1] This is because $a_i(x) = u(x) \bmod x - \alpha^i = u(\alpha^i)$ and $x \bmod x - \alpha^i = \alpha^i$, so that $a_i(x)v(x) \bmod m_i(x) \equiv [a_i(x)][v(x) \bmod m_i(x)] = \alpha^i u(\alpha^i)$.

Now assume the $m_i(x)$ are irreducible polynomials of degree m over $GF(2)$. The length of the resulting code (eqn. 1) will be determined by the number I_m of such polynomials where $\lim I_m/(2^m/m) = 1$, as $m \to \infty$. Now let $y_0, y_1, y_2, \ldots, y_{M-1}$ be a set of M distinct binary vectors, each of length $2m$, and let w_i be the Hamming weight of y_i. Let $p = (w_0 + \ldots + w_{M-1})/2mM$. Then[3] $\log M \leq 2mH_2(p)$ where H_2 is the binary entropy function. For the above redundant residue code B, $M = N - K + 1$ where $N = I_m$, and each pair $y_j = [a_j(x), v_j(x)]$ has components of degree less than m and length $2m$. The polynomial $v(x)$ can be of the form $t_1(x)t_2(x)$, where $t_1(x)$ and $t_2(x)$ are irreducible and $\deg t_1(x) + \deg t_2(x) = m$. Thus all I_m irreducible binary polynomials of degree m can be used for the moduli $m_i(x)$. The rate R of B is $K/2N$, and since the distance of C is $D = N - K + 1$, then $D/N = 1 - K/N + 1/N > 1 - K/N = 1 - 2R$. Then the ratio of distance d to length $2mN$ of code, in bits, is

$$\begin{aligned}
&d/2mN[d/2m(N - K + 1)][(N - K + 1)/N] \\
&\quad \geq [(N - K + 1)/N]H_2^{-1}[(1/2m) \log (N - K + 1)] \\
&\quad \geq (1 - 2R)H_2^{-1}[(1/2m) \log N(1 - 2R)] \\
&\quad \geq (1 - 2R)H_2^{-1}\{(1/2m) \log [(2^m/m)(1 - 2^{-m/2+1})(1 - 2R)]\} \\
&= (1 - 2R)H_2^{-1}\{(m/2m) + (1/2m)[\log (1 - 2^{-m/2+1}) \\
&\quad + \log (1 - 2R) - \log m]\} \\
&\quad \to (1 - 2R)H_2^{-1}\{(1/2) + (1/2m)[\log (1 - 2R) - \log m]\} \\
&\quad \to (1 - 2R)H_2^{-1}(1/2)
\end{aligned}$$

as $m \to \infty$, since $\log (1 - 2^{-m/2+1}) = -2^{-m/2+1} + 0(2^{-m+2})$ which tends to zero as $m \to \infty$. Also, $(\log m)/m \to 0$ as $m \to \infty$. Thus we get the same asymptotic result as the Justesen codes using RS codes.