the method presented in Reference 2 which considers the temporary correction of two errors and hence takes a large can be employed if the different weights of received error patterns can be distinguished by the receiver. In this letter, a double-error-correcting perfect code since the minimum distance of a code 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.  

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

M. M. TAHERI 15th June 1989
Department of Electronic Systems Engineering
University of Essex
Wivenhoe Park, Colchester CO4 4SQ. United Kingdom

References
1 OOGUCHI, Y.: Radio Sci., 1980, 16, pp. 691-730
3 OLMWORTH, I. D.: IEE Colloquium on cross polar cancellation techniques, Digest No. 111, December 1985

COMPLETE DECODING ALGORITHM OF (11, 6, 5) GOLOY 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. The (11, 6, 5) Golay code is a double-error-correcting perfect code since the minimum distance of this code is equal to 5. 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. 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 \( g(x) = x^5 + x^4 + x^3 + x^2 + 1 \). The codewords of this code can be simply generated in systematic form by \( K(x)g(x) = \text{Mod}(K(x)x^5g(x)) \), where \( K(x) \) is the information polynomial of degree 5 and \( \text{Mod}(K(x)x^5g(x)) \) indicates the remainder polynomial of \( K(x)x^5 \) divided by \( g(x) \). The roots of this generator polynomial are given by \( \beta, \beta', \beta'', \beta''' \), where \( \beta \) is the primitive 11th root of unity.2,3 Letting \( \alpha \) be the primitive element in GF(3), it is found that \( \beta = \alpha^2 \) and therefore the arithmetic computation of this code can be performed in GF(3). Furthermore, since \{0, 1, 2\} are the elements of GF(3), the addition of any two elements in GF(3) 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 \( \alpha^2 + 2\alpha + 1 \).

Complete decoding algorithm: If the received polynomial is expressed as \( r(x) = r_6 + r_5x + \ldots + r_1x^5 + r_0x^6 \), by choosing two roots \( \beta \) and \( \beta' \), the syndrome values \( S_j \) and \( S_j' \) of \( r(x) \) can be obtained from

\[
S_j = \text{Mod}(r(x)/g(x)) \quad i = 1, 5
\]

\[
= \text{Mod}(r(x)/g(x))_{x=\alpha^2i} \quad i = 1, 5
\]

\[
= \sum_j Y_j X_j' \quad i = 1, 5(1)
\]

where \( Y_j \) is the error locator of \( j \)-th error symbol and \( X_j' \) 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

\[
(S_j) = (Y_j X_j') = Y_j X_j' = S_j
\]

It implies that \( T_1 = (S_j) = 2S_j = 0 \) if one error has occurred. Moreover, as confirmed by computer simulation, we found that \( T_1 \neq 0 \) if two or three errors have occurred. Clearly, \( S_j = T_1 = 0 \) 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 \( S_j = T_1 = 0 \)

(ii) if there is one error, then \( S_j \neq 0 \) and \( T_1 = 0 \)

(iii) if there are two or three errors, then \( S_j \neq 0 \) and \( T_1 \neq 0 \).

Furthermore, the syndrome values of a cyclic shift of \( r(x) \), \( S_j' \) and \( S_j'' \), can be simply obtained by shifting the syndrome generator of \( r(x) \) once with initial contents \( S_j \) (Reference 5, theorem 8.7). Thus,

\[
S_j'' = \text{Mod}(r(x)/g(x))_{x=\alpha^{2i}} \quad 0 \leq j \leq 11, i = 1, 5
\]

are the syndrome values of \( r(x) = r_6 + r_5x + \ldots + r_1x^5 + r_0x^6 \). Since the relationships between \( S_j' \) and \( S_j'' \) change only when the weight of the error pattern changes and are independent of the cyclic shift of \( r(x) \), a complete decoding algorithm of the (11, 6, 5) Golay code is then presented as follows:

(a) Calculate the syndrome values \( S_j \) and \( S_j' \). If \( S_j = 0 \) then read \( r(x) \) and end this algorithm; otherwise, calculate \( T_1 \).

(b) \( j = 1 \).

(c) Find \( S_j'' \), \( i = 1, 5 \).

(d) If \( T_1 = 0 \) then calculate \( Z_1 = (S_j'')^2 + Z_1 \) and \( Z_1'' = Z_1^2 \). If \( Z_1 = 0 \) then replace \( T_1 \) by \( T_1'' \), else if \( Z_1'' = 0 \) then replace \( T_1'' \) by \( T_1 \). Go to step (f).

(e) If \( T_1 \neq 0 \) then calculate \( Z_1 = (S_j'')^2 + 2(S_j'' + 1) \) and \( Z_1'' = (S_j'')^2 + 2S_j'' + 2S_j'' \). If \( Z_1 = 0 \) then replace \( T_1 \) by \( T_1'' \), else if \( Z_1'' = 0 \) then replace \( T_1'' \) by \( T_1 \). Go to step (f).

(f) If \( j = 0 \) then the decoding algorithm is completed; otherwise, \( j = j + 1 \) and go to step (c).
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 $S_2^1 + 2S_2$ in GF($2^3$), the algorithm can be easily implemented in hardware by employing ternary-state logic gates.

Acknowledgment: The work reported in this letter is supported by the National Science Council of Republic of China under Grant NSC.77-0040-E009-08.

C.-H. WEI
Institute of Electronics and Center for Telecommunications Research National Chiao Tung University Hsin Chou, Taiwan, Republic of China

15th June 1989

J USTE N E SCON 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.

Reducant residue codes[1] 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[2] 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 develop operations on polynomials modulo irreducible polynomials.

Let $a(x)$ be a polynomial of degree less than $mK$ with coefficients over a field $F$. Let $m(x), m_1(x), \ldots, m_{mK}(x)$ be $n$ relatively prime polynomials (the called) each of degree $m$, where $n \geq \deg(a(x)) + m$. Then the word or vector $c = [c_0(x), c_1(x), \ldots, c_{n-1}(x)]$ is a code word of a $(N, K, N-K+1)$ linear maximum distance separable code, where $r(x) = (a(x) \mod m(x))$. This code is called a redundant residue code since $r(x)$ is the residue of $a(x)$ modulo $m(x)$. The term redundant comes from the fact that $a(x)$ can be recovered from $c(x)$ by $K$ residues $r_0(x), r_1(x), \ldots, r_{K-1}(x)$ if $m(x) > \deg(a(x))$ by means of the Chinese remainder theorem. The residues $r_0(x), r_1(x), \ldots, r_{K-1}(x)$ are redundant residues which lead to the distance $N-K+1$ for this code. If $m(x) = x - \alpha$ where $\alpha$ are the elements of a finite field $GF(p^q)$, the code is a Reed-Solomon (RS) code where $a(x)$ is a polynomial over $GF(p^q)$ which carries the information.

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

$$b = [a_0(x), a_1(x), a_2(x), a_3(x), \ldots, a_{mK}(x)]$$

where $a(x) = a(x) \mod m(x)$ for $0 \leq i < N-1$, and where $v(x)$ is a polynomial of degree $m$ over $F$ so that the members of the set $m(x), m_1(x), \ldots, m_{mK}(x), v(x)$ are relatively prime. It is now shown that every nonzero pair of polynomials $[a(x), v(x)]$ where $v(x)$ is distinct, i.e. $[a(x), v(x)] \neq [a(x), v'(x)], v(x)$ for $r \neq 1$ and $a(x)$ and $v(x)$ both nonzero. For the converse, $[a(x), v(x)] = [a(x), v'(x)]$ then $a(x) = a(x)$ and $v(x) = v(x)$, which means that $a(x) \neq a(x) \mod m(x)$ since $\deg a(x) < mK$.

Now assume the redundant residue code $C$, composed of words such as in eqn. 1, is linear, if we assume two words generated by the information polynomials $a(x)$ and $v(x)$ are irreducible polynomials of degree $m$ over $F$ such that the distance $d = 2m$.

$C = [a_0(x) + c(x)] = [a_0(x) - c(x)]$.

Now assume the $m(x)$ are irreducible polynomials of degree $m$ over $F(2)$. The length of the resulting code (eqn. 1) will be determined by the number $l_{mK}$ of such polynomials where $l_{mK} = 2^{mK}$. Now let $f_0, f_1, f_2, \ldots, f_{mK}$ be a set of $M$ distinct binary vectors, each of length $2m$, and let $w_i$ be the Hamming weight of $y_i$. Let $p = (w_0 + \ldots + w_{mK})/2mK$. Then $\log M = 2mK$ (where $H_x$ is the binary entropy function). For the above redundant residue code $B$, $M = N - K + 1$ where $N = l_{mK}$, and each pair $y_j = [a_j(x), v_j(x)]$ has components of degree less than $m$ and length $2m$. The polynomial $a_j(x)$ can be of the form $t_j(x)/v_j(x)$, where $t_j(x)$ and $v_j(x)$ are irreducible and $\deg(t_j(x)) + \deg(v_j(x)) = m$. Thus all $\log M$ irreducible binary polynomials of degree $m$ can be used for the moduli $m(x)$. The rate $R$ of $B$ is $K/2N$, and since the distance of $C$ is $D = N - K + 1$, then $D/N = 1 - K/ N + 1/N > 1$ and $D/N = 1 - 2R$. Then the ratio of distance $d$ to length $2mN$ of code, in bits, is

$$d/2mN(2mN - N + 1)N(N + 1)/N \geq \left(1 - 2R/|H_x|\right) \log(N + 1)$$

$$\geq \left(1 - 2R/|H_x|\right) \log(N + 1)$$

$$\geq \left(1 - 2R/|H_x|\right) \log(1 - 2^{-mK - 1}) = \log(1 - 2R/|H_x|)$$

$$= \left(1 - 2R/|H_x|\right) \log(1 - 2^{-mK - 1})$$

$$= \left(1 - 2R/|H_x|\right) \log(1 - 2^{-mK - 1})$$

$$= \left(1 - 2R/|H_x|\right) \log(1 - 2^{-mK - 1})$$

$$= \left(1 - 2R/|H_x|\right)$$

Thus we get the same result as the Justesen codes using RS codes.