Algebraic Soft-Decision Techniques for Linear Block Codes

Valdemar C. da Rocha Jr. and Patrick G. Farrell

This paper presents a way of incorporating soft-decision information as an integral part of the process of decoding linear block codes which have an algebraic structure. The quantised demodulator output levels of a soft-decision communication system are represented by the elements of a Galois field. As a consequence it is then possible to define a soft syndrome, a soft standard array and a soft trellis for decoding linear block codes. This approach stands in opposition to deconding methods which combine hard-decisions with the digit reliability measures in an ad-hoc fashion. A soft version of an error-trapping decoder for cyclic codes is given as an application of the theory developed. The basic BCH (Bose-Chaudhuri-Hocquenghem) algebraic algorithm needs to be modified in order to benefit from the procedures here described.

1. Introduction

This paper investigates a way of incorporating soft-decision information as an integral part of the process of decoding linear block codes [**1**] which have an algebraic structure. This approach stands in contrast to decoding algorithms which employ conventional hard-decision and, as separate items, the digit reliability measures are used in an ad-hoc fashion [**2**] and [**3**]. Some practical savings can therefore be obtained by eliminating the need to combine hard-decisions with digit confidence measures in order to achieve soft-decision decoding when such algorithms are employed. Due to their practical importance only binary codes will be considered in the sequel. However, the concepts introduced can be easily extended to p-ary alphabets, $p \neq 2$.

Soft-decision decoding of (n, k, d) linear binary block codes is studied when the quantised demodulator output levels are represented by elements of a Galois field $GF(2^m)$ [**4**]. The code digits are elements of the ground field GF(2) which

V.C. da Rocha Jr. is a Professor at Departamento de Eletrônica e Sistemas, Universidade Federal de Pernambuco, 50.741 Recife PE, Brasil.
P.G. Farrel is a Professor at Department of Electrical Engineering, University of Manchester, Manchester M13 9PL, England.

at the receiver are interpreted as all-zero and all-one m-tuples, in the absence of noise. This representation actually maps the original codewords into a subset of codewords of a multilevel (n, k, d) code over GF(2^m) which constitutes a subspace. As will be shown below, it is then possible to recalculate parity-checks using the quantised demodulator output levels directly. The concept of a soft-syndrome then emerges naturally. Also, the decomposition of the softly quantised space of n-tuples into cosets is done with a soft standard array where, contrary to the hard-decision case, some coset leaders are allowed to have the same soft syndrome and still be unmistakably correctable. A soft trellis is then introduced which is actually the trellis [**5**] for the multilevel code over GF(2^m), and although it could be used in principle to decode the binary code, it serves perhaps a better purpose in showing the relationship between these two codes. The next obvious step is to investigate the behaviour of soft-decision decoding algorithms which were previously used for the hard-decision decoding of block codes and, as will be shown, are able to process multilevel symbols with only a minor modification. A soft error trapping (ET) decoder [**6**] is described as an application of the theory developed. A slight modification in the basic BCH algebraic decoding algorithm [**7**] is introduced which allows, in some special situations, an efficient handling of error patterns that cannot be corrected by a hard-decision decoder.

2. Channel Output Quantisation

In practice, very often the analogue voltage at the demodulator output of a digital communication system is quantised. Also, it is common to choose the number q of quantisation levels to be a power of 2, i.e., $q = 2^m$ in order to simplify further digital processing [**7**]. This paper is not concerned with problems like optimal quantisation level spacing and choice of metric. In the sequel equally spaced quantiser thresholds and integer metric values from 0 to $2^m - 1$ will be assumed. This choice leads to some impairment in performance which is minor however when eight or more quantisation levels are used [**7**]. The $q = 2^m$ integer metric values have been represented traditionally by binary m-tuples [**8**]. Other representations are possible of course.

Though known not to be an optimal procedure it is acceptable to label the 2^m levels with the integers 0 to $2^m - 1$ because the impairment in performance is only minor [**7**]. Since there is a one to one correspondence between binary m-tuples and the elements of GF(2^m) it has been suggested by the first author [**9**] to represent the demodulator output levels by the associated Galois field elements. Such a representation is not obvious since the idea of order is nonexistent in a Galois field. That is difficult to reconcile with the definition of soft-decision distance [**8**] which states that the soft-decision distance between

two levels is given by the absolute value of their difference. This apparent impasse is removed by observing that for fields of characteristic 2, i.e., GF(2^m), the integer value corresponding to the modulo 2 difference between any two field elements coincides with their soft-decision distance when one of them is either the all-zero or all-one m-tuple. In general, the integer value of the difference between any two field elements may not coincide with their soft-decision distance.

Example 1

Consider q=4 quantisation levels. The elements of the Galois field GF(4) are 0, 1, α, α^2. The demodulator output levels are represented as follows:

GF(4) element	Binary	Integer value
0	00	0
1	01	1
α	10	2
α^2	11	3

For any two levels, it is easily verified that the integer value corresponding to their modulo 2 difference (which is the same as modulo 2 addition) coincides with their soft-decision distance only when one of the levels is either 00 or 11.

In the process of decoding binary codes the components of the softly-quantised received n-tuple are always compared against top confidence levels, i.e., all-zero or all-one m-tuples, which are the components of the valid codewords. Therefore, in this case, the level assignment proposed above is perfectly satisfactory. The above considerations are summarized in the following lemma.

Lemma 1

For fields of characteristic 2, i.e., GF(2^m), the integer of the modulo 2 difference between a pair of elements in the field concides with the value of their soft-decision distance when one of the elements considered is either the all-zero or the all-one m-tuple.

The soft-decision level representation suggested above allows the integration of soft-decision information as part of the shift and add operations of an error-trapping (ET) decoder, as shown later in this paper.

3. Soft Syndromes for Decoding Linear Codes

It is well known in coding theory that the decoding problem can be approached in principle either by using the maximum likelihood criterion, which is codeword oriented, or the syndrome, which is error-pattern oriented. Both approaches have advantages and disadvantages and the eventual choice for one of them depends on the characteristics of the code to be used. In soft-decision decoding, most of the practical approaches to the problem have shown two common points. First, the decoder operates on hard-decision estimates of the demodulador output forming a hard-decision syndrome and, as a separate tool, uses the reliability measures associated with the hard decisions to assist on the correction of errors. Very often the reliability measures are combined with the hard-decision estimates in an ad-hoc manner [2] and [3]. Second, the more sophisticated soft-decision decoding algorithms [5] and [10] are directed to the estimation of bits or codewords instead of error-patterns.

The concept of a soft syndrome becomes plausible from the moment one can operate with the softly quantised symbols of the received n-tuple in order to recalculate parity-checks. The idea is to effectively integrate the demodulator output levels into the decoding process. The following example serves to illustrate this point.

Example 2

Consider the (3, 2, 2) binary single-parity-check code and q=4 quantisation levels. The code parity-check is given by $c = k_1 + k_2$. The demodulator output levels are assumed represented as in Example 1. Suppose the message to be transmittted is 10. Its associated codeword is 101. In the absence of noise it is received at the demodulator output as $(\alpha^2,0,\alpha^2)$. Now suppose that due to noise the received word is $(\alpha,0,\alpha^2)$. The recalculated parity-check is $\alpha+0 = \alpha$. The soft syndrome is found by adding modulo-2 the received and the recalculated parity-checks, i.e., $S = \alpha^2 + \alpha = 1$. This code corrects $t_S = \lfloor((q-1)d - 1)/2\rfloor = 2$ soft errors, where $\lfloor x \rfloor$ is the integer part of x.

4. Soft Standard Array

The standard array [1] is a well known concept in coding theory, commonly presented in conjunction with hard-decision decoding procedures. As a conceptual tool a soft standard array can be useful in throwing some light on the code structure and decoding process. The soft standard array contains

n-tuples which satisfy the code parity-check equations but are not in its top row and therefore do not belong to the (n,k,d) binary code. Such n-tuples are called soft codewords and in general may be seen as belonging to a (n,k,d) code with a higher order alphabet $q = 2^m$ which contains as a proper subset the soft-decision mapped (n,k,d) binary code. As a consequence, contrary to the hard-decision case, many correctable error patterns have the same syndrome. Precisely, the soft standard array has 2^k columns and 2^{mn-k} rows such that sets of $2^{(m-1)k}$ rows have the same soft syndrome.

Example 3

The soft standard array for the (3,2,2) code of Example 2 is

0	0	0		0	α^2	α^2		α^2	0	α^2		α^2	α^2	0
0	1	1		0	α	α		α^2	1	α		α^2	α	1
1	0	1		1	α^2	α		α	0	α		α	α^2	1
1	1	0		1	α	α^2		α	1	α^2		α	α	0
–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
0	0	1		0	α^2	α		α^2	0	α		α^2	α^2	1
0	1	0		0	α	α^2		α^2	1	α^2		α^2	α	0
1	0	0		1	α^2	α^2		α	0	α^2		α	α^2	0
1	1	1		1	α	α		α	1	α		α	α	1
–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
0	0	α		0	α^2	1		α^2	0	1		α^2	α^2	α
0	α	0		0	1	α^2		α^2	α	α^2		α^2	1	0
α	0	0		α	α^2	α^2		1	0	α^2		1	α^2	0
1	1	α		1	α	1		α	1	1		α	α	α
–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
0	0	α^2		0	α^2	0		α^2	0	0		α^2	α^2	α^2
0	1	α		0	α	1		α^2	1	1		α^2	α	α
1	0	α		1	α^2	1		α	0	1		α	α^2	α
1	1	α^2		1	α	0		α	1	0		α	α	α^2

The correctable soft error patterns are the coset leaders of the top eleven rows.

5. Soft-Trellis Decoding of Block Codes

A trellis constructed along the same lines as indicated by Wolf [5] considering all the paths which satisfy the code parity-check equations with symbols from $GF(2^m)$ is called a soft trellis. The soft trellis for the (3,2,2) binary code of

Example 2 is given in **Fig. 1** together with the hard-trellis for comparison. The decoding operations are identical to those of a Viterbi decoder [7].

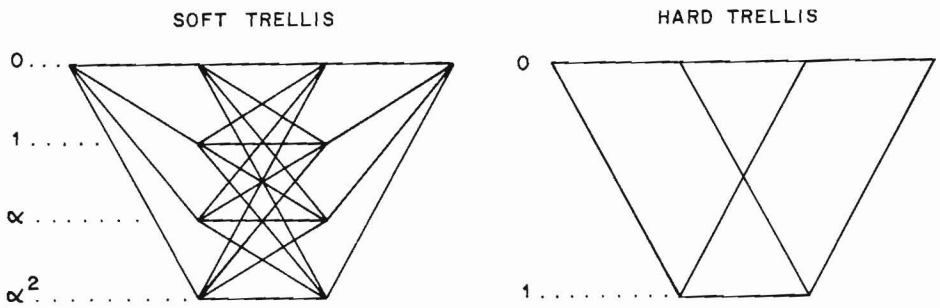

Figure 1. Soft trellis and hard trellis corresponding to the code in Example 2.

6. Soft Cyclic Codes

Consider a (n, k, d) binary cyclic code [1] with generator polynomial g(x) and length $n = 2^m - 1$. A soft cyclic code of characteristic 2 is formed by considering as codewords all n-tuples with symbols from GF(2^m) which satisfy the parity-check equations of the binary (n,k,d) cyclic code. The result is a 2^m-ary (n,k,d) cyclic code.

In a soft-decision receiver, using 2^m quantisation levels, in the absence of noise the received codeword levels would be of top confidence, i.e., either all-zero or all-one m-tuples. Therefore the original binary codewords of the (n,k,d) cyclic code appear mapped as a proper subset of the soft cyclic code. However, the minimum distance between valid codewords is now $d_S = (q-1)d$ rather than d [7]. The concept of a soft cyclic code is very interesting because it allows the tools developed for linear codes to be used in a soft-decision context. For example, the decomposition of the softly quantised space of n-tuples into cosets can be done with a soft standard array, syndromes can be calculated, etc. Some theoretical tools are next introduced in the form of lemmas and theorems. They will be useful in applications presented later.

Lemma 2

An all-zero syndrome corresponds to a soft cyclic codeword.

Proof

By definition all codewords of the soft cyclic code satisfy the binary code parity-check equations and therefore are multiples of the code generator polynomial g(x).

Lemma 3

The m-1 elements, α^i, $0 \leq i \leq m-2$, of $GF(2^m)$ are linearly independent and by linear combinations only generate elements of soft weight less than $(2^m-1)/2$.

Proof

The first part is a well known result since, actually, the m elements, α^i, $0 \leq i \leq m-1$, of $GF(2^m)$ are linearly independent [**4**]. For the second part, considering that the field characteristic is 2, the linear combinations of the α^i, $0 \leq i \leq m-1$, can be thought of as modulo 2 sums S of m-1 bit binary numbers. Thus, the maximum soft weight of S is $W(S) = 2^{m-1} - 1 < (2^m-1)/2$.

At this point it is convenient to describe a decomposition of the soft cyclic code which will be called a soft cyclic code array (SCA). The SCA is a rectangular array with rows and columns. Its top row is filled with the top confidence soft codewords, beginning with the all-zero n-tuple, i.e., as the leader of the first row. The leader of the second row is chosen to be a previously unused soft codeword of lowest soft weight and the remaining row places are each one filled by adding its leader to the top confidence codeword situated in the same column, i.e., immediately above. The third and successive rows are formed in a similar manner, beginning with a previously unused soft codeword of least soft weight. As a result, a total of $2^{(m-1)k}$ rows are thus formed.

Theorem 1

The SCA leaders have soft weight $W \leq t_s$ and therefore represent correctable soft error patterns.

Proof

Suppose a leader L has soft weight $W \geq t_s + 1$. Since the top row of the SCA contains words of soft weight $d_s \geq 2t_s + 1$, this implies the existence of at least one soft codeword of soft weight less than or equal to t_s in the row where L is the leader. Therefore a contradiction to the SCA construction rules.

Theorem 2

Any soft codeword can be written as a sum, over GF(2^m), of a top confidence soft codeword and a soft codeword of soft weight at most t_s.

Proof

This is an immediate consequence of the SCA construction combined with the result of Theorem 1.

Theorem 3

The SCA has $2^{(m-1)k}$ leaders which are composed of elements with soft weight less than $(2^m-1)/2$.

Proof

By definition the soft cyclic code has k information positions which are occupied by elements of GF(2^m). Thus, a total of 2^{mk} soft codewords result. The SCA has 2^k columns and therefore $2^{mk}/2^k = 2^{(m-1)k}$ rows, i.e., $2^{(m-1)k}$ leaders. It is now an easy matter to deduce that the first column of the SCA forms a subspace, i.e., a linear code, of dimension k whose information positions are occupied by the m symbols (0, 1, α, α^2, ..., α^{m-2}) and by Lemma 3 the theorem follows.

Theorem 4

A binary hard-decision version of a received soft codeword gives the right transmitted codeword when the soft error patterns is a correctable one.

Proof

Conceptually, the decoding of a soft codeword υ can be performed as follows. First locate the SCA row where υ is situated and then subtract the row leader r from υ. The result is a top confidence soft codeword c. Since $d_s \leq 2t_s + 1$ and by Theorem 2 and Lemma 3, the row leader r, whose individual components have soft weight less than q/2 and of total soft weight at most t_s, is unique and is thus assumed to be the soft error pattern. Therefore, the nearest binary codeword is a hard-decision version of υ.

7. Soft Error-Trapping Decoder

In this section a soft-decision version of an error-trapping (ET) decoder for cyclic codes is described. The ET decoding technique [1] is very simple and is

usually applied for the hard-decision decoding of cyclic codes. It is most efficient for rate $R<1/t$ codes, where t is the maximum number of errors to be corrected [1]. Modified ET decoders have been proposed which partially avoid this limitation for codes not satisfying $R<1/t$ [11]. Nonbinary ET decoders have been previously proposed [12], however to deal with hard-decision decoding of multilevel cyclic codes.

Assume the channel output quantisation is performed as described above. The softly-quantised received n-tuple is fed into a $GF(2^m)$ division circuit wired for division by the code generator polynomial g(x). As a result the soft syndrome is formed. The syndrome soft-weight (SW) is compared to a threshold t_S, where

$$t_S \leq \left\lfloor \frac{(2^m - 1)\, d - 1}{2} \right\rfloor$$

and $\lfloor x \rfloor$ means the integer part of x. One of the following situations will occur.

a) $SW \leq t_S$

The decoder delivers to the sink a hard-decision version of the received n-tuple if each syndrome component has soft weight less than q/2. Otherwise proceed as in b).

b) $SW > t_S$

The syndrome is shifted inside the division circuit, with feedback on. After each shift the updated syndrome weight SW is compared with t_S. If $SW \leq t_S$ after the i^{th} shift, $1 \leq i \leq n-1$, then a soft error has possibly been trapped. The decoder subtracts the shifted syndrome from the i^{th} cyclic shift of the received n-tuple. If the result is a top confidence codeword, i.e., a codeword whose elements are represented by all-zero or all-one m-tuples, then stop. The error has been trapped and the received word has been corrected. Otherwise, continue the process of shifting the syndrome and comparing SW to t_S. If after n shifts either SW has never been equal to or less than t_S or, if that happenned and the attempted correction did not produce a top confidence codeword, then an error has been detected which cannot be trapped.

The theoretical basis for the above procedure is now described.

Theorem 5

Let a correctable error pattern with SW $\leq t_s$ affect the transmitted codeword. Then one of the following situations will occur.

a) SW = 0

a.1) No errors.
a.2) An error which coincides with a soft codeword whose individual components have soft-weight less than q/2.

b) $0 < SW < t_s$

If each syndrome component has soft weight less than q/2 then a soft error pattern is assumed, where each nonzero position has soft weight less than q/2. Otherwise nothing can be said.

c) $SW = t_s$

All the errors occur in the parity-check section of the received n-tuple.

d) $SW < t_s$

The errors are not all in the parity-check section of the received n-tuple.

Proof

Case a is obvious. Case b can be established with the help of Lemma 3. Case c follows by reasoning that if the assertion made is false, i.e., the errors are not confined to the word parity-check positions, then by subtracting the syndrome from the received n-tuple would cause a total of at most $2t_s$ soft-weight changes in the transmitted codeword and the result would be a valid top confidence codeword. But that is impossible because $d_s \geq 2t_s + 1$ is the minimum number of soft-weight changes needed to produce a valid top confidence codeword. Case d follows trivially from case c.

Example 4

Consider the (7,4,3) binary cyclic Hamming code with generator polynomial $g(x) = x^3 + x + 1$. The demodulator output is quantised into 8 amplitude levels, represented below by the powers of a primitive element α of GF(8), where the element α was chosen to be a root of the primitive polynomial $x^3 + x + 1$.

GF(8) Element	Binary	Integer Value
0	000	0
1	001	1
α	010	2
α^2	100	4
α^3	011	3
α^4	110	6
α^5	111	7
α^6	101	5

The code soft-decision distance is given by $d_S = (8\text{-}1).3 = 21$, therefore $t_S = 10$. Suppose the all-zero codeword is transmitted and the received word in polynomial form is $\alpha^4x^6 + \alpha^2x^5$, i.e., and error of soft weight 6+4 = 10. The received polynomial is divided by g(x) and the remainder, which is the soft syndrome, is found to be $\alpha x^2+\alpha^2x + \alpha$. The evolution of the decoding process is illustrated below, where (c, b, a) represents the coefficients of the polynomial ax^2+bx+c.

SHIFT	Syndrome Register Contents	Soft Weight(SW)
0	$(\alpha, \alpha^2, \alpha)$	8
1	$(\alpha, 0, \alpha^2)$	6
2	$(\alpha^2, \alpha^4, 0)$	10

The soft syndrome has weight 8 which is less than $t_S = 10$ but since its components are not all of soft weight less than q/2=4 the decoder proceeds. After the first shift, SW = 6 < t_S. The received n-tuple is shifted once. Correction is attempted by subtracting the syndrome from the shifted version of the received n-tuple. Since the result is not a top confidence codeword the decoding operation continues. In the second shift SW equals t_S and correction is attempted again. This time it succeeds, i.e., the result of subtracting the

syndrome from the received n-tuple cyclically shifted twice gave as a result a top confidence codeword. The decoding operation is halted. The decoder registers are cleared and wait for the next received word. Notice that such an error pattern would not be corrected by a hard-decision decoder. For this (7,4,3) code it is clear that some double-error patterns cannot be trapped since R > 1/t, i.e., 4/7 >1/2.

8. BCH Decoding

One snag with the algebraic decoding of BCH codes has been its error-correction bounding by the designed distance rather than by the minimum distance. The limitation in error-correction capability of the basic algebraic algorithm possibly results because it makes no essential use of the fact that the binary (n,k,δ) BCH code is a subfield subcode of a Reed-Solomon code with the same δ however over a higher order alphabet. The decoding algorithm being exactly identical for both codes. Some of the ideas developed in this paper may be of relevance here. If the frequency domain decoding approach is used [7] then it follows that for a given δ there are δ-1 known consecutive coefficients of the finite field Fourier transform of the error polynomial and therefore a recursion relation involving an error locator polynomial of degree at most δ-1 could in principle be established. Both the Berlekamp-Massey and Euclidean algorithms [7] only provide error locator polynomials of degree at most $\lfloor(\delta-1)/2\rfloor$ and thus are not applicable in the soft decision case. By using the received digit reliability measures a most likely error locator polynomial could be formed. The recursion relation is tested for consistency. If it works then the correction of the errors proceeds in the normal way. If it fails then it is possible that one or more errors of top confidence have hit the received codeword. In this case some algebra has to be used in order to solve the problem. Unless δ is a small number the complexity of such an approach becomes prohibitive.

9. Comments

The procedures described above are not restricted to codes of lenght $n = 2^m - 1$ with $q = 2^m$ quantisation levels. As m grows it is both impractical and unnecessary to keep the 2^m quantisation levels. Either a smaller field contained in $GF(2^m)$ is employed or, if it is not contained in $GF(2^m)$, each of its elements can be made to represent a cluster of elements of $GF(2^m)$ which are neighbors in the soft-decision sense. The code length in general will be a divisor of $2^m - 1$. It should be remarked that the ET algorithm described is sub-optimum bacause of the channel output quantisation, the use of

soft-decision distance instead of Euclidean distance, and the fact that ET is not always equivalent to minimum distance decoding. Using a slightly modified version of the ET algorithm presented above, which makes use of covering polynomials [11], it is possible to correct most of the error patterns containing two hard-decision errors by means of binary Hamming codes.

ACKNOWLEDGEMENT

This work received partial support from the Brazilian National Council for Scientific and Technological Development (CNPq).

References

[1] S. Lin and D.J. Costello, Jr., "Error Control Coding: Fundamentals and Applications", Prentice-Hall, USA, 1983.

[2] E.J. Weldon, Jr., "Decoding Binary Block Codes on Q-ary Output Channels", IEEE Transactions on Information Theory, vol. IT-17, no. 6, November 1971, pp. 713-718.

[3] D. Chase, "A Class of Algorithms for Decoding Block Codes with Channel Measurement Information", IEEE Transaction on Information Theory, vol. IT-18, no. 1, january 1972, pp. 170-182.

[4] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, 1978.

[5] J.K. Wolf, "Efficient Maximum Likelihood Decoding of Linear Block Codes Using a Trellis", IEEE Transactions on Information Theory, vol. IT-24, no. 1, January 1978, pp. 76-80.

[6] V.C. Rocha, Jr., "Soft Error-Trapping Decoding of Cyclic Codes", IEE Electronics Letters, vol. 25, no. 4, 16th February 1989, pp. 293-294.

[7] G.C. Clark and J.B. Cain, "Error-Correction Coding for Digital Communications", Plenum Press, USA, 1981.

[8] P.G. Farrell, "Soft Decision Detection Techniques", in Algebraic Coding Theory and Applications, CISM Courses and Lectures no. 258, Springer-Verlag, Wien-New York, 1979.

[9] V.C. Rocha, Jr., "A Galois Field Approach to Soft-Decision Decoding", Beijing International Workshop on Information Theory, Beijing, China, 1988.

[10] C.R.P. Hartmann and L.D. Rudolph, "An Optimum Symbol-by-Symbol Decoding Rule for Linear Codes", IEEE Transactions on Information Theory, vol. IT-22, no. 5, September 1976, pp. 514-517.

[11] T. Kasami, "A Decoding Procedure for Multiple-Error-Correcting Cyclic Codes", IEEE Transactions on Information Theory, vol. IT-10, no. 2, April 1964, pp. 134-138.

[12] V.K. Wei, "An Error-Trapping Decoder for Nonbinary Cyclic Codes", IEEE Transactions on Information Theory, vol. IT-30, no. 3, May 1984, pp. 538-541.

VALDEMAR CARDOSO DA ROCHA JUNIOR, for a photograph and biography, see this issue, p. 3.

PATRICK G. FARRELL., photograph and biography not availabre at the time of publication.