3 NYBERG, K.: 'Differentially uniform mappings for cryptography'. Proc. Eurocrypt '93, Lecture notes in Computer Science (Springer Verlag), to appear
4 BIHAM, E., and SHAMIR, A.: 'Differential cryptoanalysis of DES-like cryptosystems', *J. Cryptol.*, 1991, **4**

Cyclic codes for *T*-user adder channel over integer rings

P.Z. Fan, M. Darnell, B. Honary and V.C. da Rocha Jr.

Indexing terms: Codes and coding, Cyclic codes

Coding for the synchronous noiseless T-user real adder channel is considered by employing cyclic codes with symbols from an arbitrary finite integer ring. The code construction is based on the factorisation of $x^n - 1$ over the unit ring of an appropriate extension of a finite integer ring. Any number of users in the system can be independently active and the maximum achievable sum rate is 1 (when all T users are active).

Introduction: In his study of T active users out of N multiple-access communication systems, Mathys introduced a class of codes for the synchronous noiseless discrete-time real adder channel (with gains and offset) without feedback with N real or binary inputs [1]. Mathys codes are uniquely decodable and have a sum rate that approaches 1 if the decoder is informed of which T or less users are active. The sum rate will be reduced to a value of at most 1/2 if the decoder has to identify the subset of active users. In a recent paper, da Rocha proposed the use of cyclic codes over $GF(q)$ for the synchronous noiseless T-user adder channel (T-QAC) [2]. A very low complexity decoding procedure was presented there and it was shown that the maximum achievable sum rate is 1. In this Letter, cyclic codes for the T-QAC with symbols from an arbitrary integer ring Z_M will be discussed.

Factorisation of $x^n - 1$ over integer ring Z_M: In this Section a summary of the theory needed to factor $x^n - 1$ and subsequently to construct cyclic codes over the integer ring Z_M is given, following Shankar [3]. Let M be an arbitrary integer, with prime factorisation $M = \Pi_{i=1}{}^{l} P_i^{k_i}$, where the p_i are distinct primes and the k_i are non-negative integers. Let $Z_{p_i^{k_i}}[y]$ denote the ring of polynomials in the variable y over $Z_{p_i^{k_i}}$ and let $\Phi_i(y)$ be a monic p_i-ary polynomial of degree r, irreducible over GF(p_i), $i = 1, 2, \ldots, l$. Let $R_i = GR(p_i^{k_i}, r) = Z_{p_i^{k_i}}[y]/\Phi_i(y)$ denote the Galois ring, i.e. the set of residue classes of polynomials in y over $Z_{p_i^{k_i}}$, modulo the polynomial $\Phi_i(y)$.

Suppose that $f(x) = \Sigma_{i=1}{}^{n} a_i x^i$ and let $R_M(f(x)) = \Sigma_{i=1}{}^{n} R_M(a_i)x^i$, where $R_M(a_i)$ is the non-negative remainder when the integer a_i is divided by the integer M. For $i = 1, 2, \ldots, l$, let m_i be the smallest integer such that

$$R_{p_i^{k_i}}(m_i) = 1 \text{ and } R_{p_j^{k_j}}(m_i) = 0 \quad \text{for } j \neq i \quad 1 \leq j \leq l$$

Then the polynomial

$$\Phi(y) = R_M(m_1\Phi_1(y) + m_2\Phi_2(y) + \ldots + m_l\Phi_l(y))$$

is monic and irreducible over Z_M and over $GF(p_i)$, $i = 1, 2, \ldots, l$. Let $Q(M,r) = Z_M[y]/\Phi(y)$. Now let $R_i{}^*$ and Q^* denote the group of units of R_i and $Q(M,r)$, respectively, let K_i denote $GF(p_i{}^r)$ and finally let $K_i{}^*$ denote the multiplicative group of $GF(p_i{}^r)$. Let n be a divisor of $GCD((p_1{}^r - 1), (p_2{}^r - 1), \ldots, (p_l{}^r - 1))$ and let $H_{f,n}$ denote the cyclic subgroup of order n of Q^*, generated by f. It follows that $H_{f,n}$ contains all the roots of $x^n - 1$ over Q^*. The polynomial $x^n - 1$ can be factored over Q^* as

$$x^n - 1 = (x - f)(x - f^2)\ldots(x - f^n)$$

if and only if $\bar{\beta} = R_{p_i}(f)$ has order n in $K_i{}^*$, where $(n, p_i) = 1$, $i = 1, 2, \ldots, l$. Summarising, these are the main steps in the factorisation of $x^n - 1$ over Z_M:

(i) Choose $\Phi_i(y)$ to be a monic p_i-ary polynomial of degree r, irreducible over $GF(p_i)$. Find m_i, $i = 1, 2, \ldots, l$ as indicated above; then

$$\Phi(y) = R_M(m_1\Phi_1(y) + m_2\Phi_2(y) + \ldots + m_l\Phi_l(y))$$

is monic and irreducible over Z_M.

(ii) Let β_i be an element of order n in R_i formed as $Z_{p_i^{k_i}}[y]/\Phi_i(y)$, $i = 1, 2, \ldots, l$; then $f = R_M(m_1\beta_1 + m_2\beta_2 + \ldots + m_l\beta_l)$ generates the cyclic subgroup $H_{f,n}$ of the unit group of $Z_M[y]/\Phi(y)$.
(iii) The factors of $x^n - 1$, irreducible over Z_M, are defined by the cyclotomic cosets formed with the roots f^i, $1 \leq i \leq l$, of $x^n - 1$.

If $(n, p_i) \neq 1$ then the factorisation of $x^n - 1$ over Z_M is not guaranteed to be unique; this, however, is not an obstacle to code construction, as shown below.

Cyclic codes over Z_M in T-QAC channel: A blocklength n cyclic code over Z_M is an ideal in the ring of polynomials with coefficients in Z_M, reduced modulo $x^n - 1$, and is generated by a monic polynomial $g(x)$ which is a factor of $x^n - 1$. Let $g_1(x), g_2(x), \ldots g_T(x)$ be a set of T irreducible polynomials which are factors of $x^n - 1$ over Z_M, i.e.

$$x^n - 1 = \prod_{i=1}^{T} g_i^{k_i}(x) \tag{1}$$

where $\Sigma_{i=1}{}^{T} deg[g_i^{k_i}(x)] = n$ and the k_i, $1 \leq i \leq T$ are positive integers. Because $h_i(x) = (x^n - 1)/g_i^{k_i}(x)$ has no factors in common with $g_i^{k_i}(x)$, the Euclidean algorithm can be used to find a polynomial $\beta_i(x)$ such that $\beta_i(x)h_i(x) \equiv 1 \bmod g_i^{k_i}(x)$, $1 \leq i \leq T$. Consider the following sum $r(x)$, where addition is defined over the additive group of Z_M:

$$r(x) = \sum_{i=1}^{t} m_i(x)h_i(x)\beta_i(x) \quad 1 \leq t \leq T \tag{2}$$

Because $\beta_j(x)h_j(x)$ is a multiple of $g_i^{k_i}(x)$ if $j \neq i$, and $\beta_i(x)h_i(x) \equiv 1 \bmod g_i^{k_i}(x)$, it follows that $r(x) \equiv m_i(x) \bmod g_i^{k_i}(x)$ for all i. If $r'(x)$ also satisfies $r'(x) \equiv m_i(x) \bmod g_i^{k_i}(x)$ for all i, then $r'(x) - r(x)$ must be divisible by $g_i^{k_i}(x)$, $1 \leq i \leq t$ and as both $r(x)$ and $r'(x)$ are polynomials of degree less than n, it follows that $r'(x) = r(x) \bmod x^n - 1$. Hence the sum $r(x)$ is uniquely determined by the arbitrary polynomials $m_i(x)$, $1 \leq i \leq t$, if $deg[m_i(x)] < deg[g_i^{k_i}(x)]$ i.e. $m_i(x) = r(x) \bmod g_i^{k_i}(x)$, $1 \leq i \leq t$. Based on the above analysis, a T-QAC system over integer ring Z_M can be constructed. The encoding and decoding algorithms are as follows.

Code construction:

(i) Given an integer ring Z_M, choose a code length n as described in the preceding section and factor $x^n - 1$ into irreducible polynomials over Z_M, $x^n - 1 = \Pi_{i=1}{}^{T} g_i^{k_i}(x)$.

(ii) Assign each user a cyclic code with the generator $h_i(x) = (x^n - 1)/g_i^{k_i}(x)$. Compute the polynominals nomials $\beta_i(x)$ which satisfy, $\beta_i(x)h_i(x) \equiv 1 \bmod g_i^{k_i}(x)$, $1 \leq i \leq T$.

Encoding algorithm: For a given message polynomial $m_i(x) \neq 0$, the transmitted codewords $c_i(x)$ of each user generated by computing $c_i(x) = h_i(x)\beta_i(x)m_i(x) \bmod (x^n - 1)$. Because each codeword $c_i(x)$ in the i th code has $deg[g_i^{k_i}(x)]$ message symbols and $\Sigma_{i=1}{}^{t} deg[g_i^{k_i}(x)] \leq n$ it follows that the maximum achievable sum rate is 1 when all users ($t = T$) are active. To avoid the ambiguity between messages $m_i(x) = 0$ and the case where user i is not active, the message set is restricted to those $m_i(x) \neq 0$ in the encoding algorithm.

Decoding algorithm: The received n-tuples are polynomials, denoted by $r'(x)$, which result from the componentwise real addition of the codewords of the active users. The first step in decoding is to reduce coefficients of $r'(x)$ modulo M. The result of this step is the polynomial $r(x)$. Once the polynominal $r(x) = \Sigma_{i=1}{}^{t} c_i(x)$ is obtained the decoding algorithm is very simple and is given by the equation: $\hat{m}_i(x) = r(x) \bmod g_i^{k_i}(x)$ $1 \leq i \leq T$.

Example: Construct a T-QAC system over Z_4 with code length $n = 7$. Employing the technique described above, the following factorisation results:

$$x^7 - 1 = \sum_{i=1}^{3} g_i(x)$$
$$= (x-1)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3) \quad (3)$$

Let $g_1(x) = x - 1$, $g_2(x) = x^3 + 2x^2 + x + 3$ and $g_3(x) = x^3 + 3x^2 + 2x + 3$. Using the Euclidean algorithm it turns out that $h_1(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $\beta_1(x) = 1$; $h_2(x) = x^4 + x^2 + x + 3$, $\beta_2(x) = 1$; $h_3(x) = x^4 + 3x^3 + 3x^2 + 3$, $\beta_3(x) = x^3 + 2x^2 + 2$. Suppose $m_1(x) = 3$, $m_2(x) = 2x + 3$, $m_3(x) = x$, then the transmitted codewords are

$$c_1(x) = m_1(x)h_1(x)\beta_1(x)$$
$$= 3x^6 + 3x^5 + 3x^4 + 3x^3 + 3x^2 + 3x + 3$$
$$c_2(x) = m_2(x)h_2(x)\beta_2(x)$$
$$= 2x^5 + 3x^4 + 2x^3 + x^2 + x + 1$$
$$c_3(x) = m_3(x)h_3(x)\beta_3(x)$$
$$= x^6 + x^4 + 3x + 1$$

At the receiver, the received sum codeword is $r'(x) = 4x^6 + 5x^5 + 7x^4 + 5x^3 + 4x^2 + 7x + 5$ which, after reduction modulo 4, becomes $r(x) = \Sigma_{i=1}^{3} c_i(x) = x^5 + 3x^4 + x^3 + 3x + 1$. The messages can be easily restored as: $\hat{m}_1(x) = 3 = r(x) \bmod g_1(x)$, $\hat{m}_2(x) = 2x + 3 = r(x) \bmod g_2(x)$ $\hat{m}_3(x) = x = r(x) \bmod g_3(x)$.

Summary: Cyclic codes over the integer ring Z_M for the T-QAC have been discussed in this Letter. It should be noted that the above analysis and encoding/decoding algorithms are valid if $x^n - 1$ has repeated irreducible factors. This means that the present results generalise the code construction given in [2]. Although the maximum number of users will be reduced if there are some repeated irreducible factors in $x^n - 1$, the maximum achievable sum remains the same.

22 November 1993
Electronics Letters Online No: 19940156

P. Z. Fan and M. Darnell (*Department of Electronics Engineering, University of Hull, United Kingdom*)

B. Honary (*Department of Engineering, Lancaster University, United Kingdom*)

V. C. da Rocha Jr. (*Department of Electronics and Systems, Federal University of Pernambuco, 50741-540, Recide, PE, Brazil*)

References

1 MATHYS, P.: 'A class of codes for T active users out of N multiple-access communication system', *IEEE Trans.*, 1990, **IT-36**, (6), pp. 1206–1219

2 DA ROCHA, V.C. JR.: 'On cyclic codes for the T-user Q-ary adder channel'. IEEE Int. Symp. on Inform. Theory, January 1993, (San Antonio, USA), p. 296

3 SHANKAR, P.: 'On BCH codes over arbitrary interger rings', *IEEE Trans.*, 1979, **IT-25**, (4), pp. 480–483

Surface magnetic field measurement technique for nondestructive testing of metals

D. Mirshekar-Syahkal and S.H.H. Sadeghi

Indexing terms: Magnetic field measurement, Nondestructive testing

The Letter explains the principles of a new electromagnetic technique, the surface magnetic field measurement technique (SMFM), for the detection and sizing of surface-breaking cracks in metals. The signals associated with circular-arc cracks are examined and techniques for inverting crack signals to crack dimensions, are outlined.

Introduction: Various methods including ultrasonic, magnetic particle, AC and DC potential drop, magnetic flux leakage and eddy current methods, have been used to detect surface breaking cracks in metals and metal structures. Each method, of course, has its own potentials and weaknesses in a specific application.

Recently, we have developed a new electromagnetic technique, the surface magnetic field measurement technique (SMFM), for the detection and sizing of surface-breaking cracks in metals [1]. Although the technique uses some of the principles of the eddy current method, it has superior features as it does not rely on the impedance measurement and it is free from probe calibration and calibration standards. The SMFM technique is based on the measurement of the tangential component of the AC magnetic field at the metal surface. The field is produced by an inducer located above the metal surface which can consist of several U-shaped wires or can be a rectangular coil, carrying a high frequency AC current. In the measurement of the field, a properly orientated reflection type eddy-current probe is used.

This Letter outlines the principles of the SMFM technique, examines signals associated with circular-arc cracks and discusses the methods which have been developed in order to invert crack signals to crack dimensions.

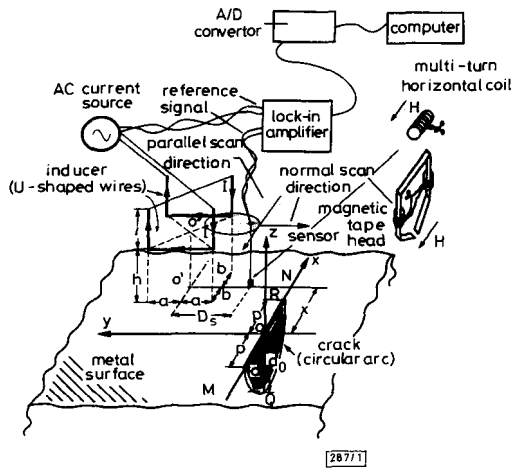

Fig. 1 *SMFM detection system using one of the two sensors shown and an inducer consisting of two U-shaped wires*

The sensor is attached to the inducer at a distance D_s. In a scan, the sensor is close to the metal surface.

Crack detection: In Fig. 1, a schematic diagram of the SMFM system using two U-shaped wires as the inducer is shown. The inducer is excited by a high frequency current source, producing a thin skin eddy current in the work piece. The choice of operating frequency depends on the metal under test and on the minimum crack depth to be resolved. Because we were mostly concerned with the inspection of mild steel structures, an operating frequency of 1.6kHz was found to be sufficient for reliable detection and sizing of cracks of depths greater than 1mm. At this frequency the skin depth is ~0.3mm. However, higher frequencies were also used recently to resolve shallow cracks of the order of 200 μm. The excitation current of 0.5A was found to be adequate for obtaining a very good signal to noise ratio for cracks deeper than 1mm.

A surface crack perturbs the distribution of the eddy current induced in the work piece and the effect is reflected in the magnetic field at the metal surface. Perturbations in the tangential component of the field can be sensed by a magnetic sensor which, as shown in Fig. 1, can be a magnetic tape-head eddy current probe or a multiturn horizontal coil of small dimensions. Although in an inspection task the inducer can be kept in a fixed position and the sensor is moved to interrogate the surface field, this arrangement is not convenient and, in practice, the inducer and the sensor are attached and move together (Fig. 1). The sensor can be attached to the inducer at different positions and can have different orientations. The detector system connected to the sensor is a lock-in amplifier interfaced to a computer.