数理解析研究所講究録
第 551 巻 1985 年 44-61

A Computer-Algebraic Problem on Two-dimensional Linear Recurring Arrays - Cycle Representatives of Two-dimensional Cyclic Codes

阪田省二郎 Shojiro SAKATA
(豊橋技科大) Toyohashi Univ. of Tech.

ABSTRACT

Most problems on two-dimensional(2-D) linear recurring arrays are also important from the standpoint of computer algebra, one of which is treated in this paper. In particular this problem has a close connection with Buchberger's algorithm. A method of finding cycle representatives of 2-D cyclic codes defined by primary ideals in the bivariate polynomial ring is presented. This is based also on a two-dimensional generalization of Kurudjukov's result on cyclic codes defined by non-squarefree parity check polynomials. Our result is useful for determining the weight distribution of any 2-D cyclic code and exhibits an example suitable for applying a formula manipulating system.

I. INTRODUCTION

The two-dimensional (2-D) cyclic codes are a generalization of the important class of one-dimensional (1-D) cyclic codes [1-5]. A 'cycle' of a 2-D cyclic code is the collection of codewords which are cyclic shifts of a codeword, as in the case of a 1-D cyclic code. If we can find the cycle representatives, we can immediately determine the weight distribution of the code. The problem of finding the cycle representatives of 2-D cyclic codes remains open except in the case of irreducible (IR) 2-D cyclic codes; an IR 2-D cyclic code is equivalent to (a repetition of) an IR 1-D cyclic code [4,5]. For 1-D cyclic codes, this problem has been solved [6-10].

In the present paper, we present a method of finding the cycle representatives of any quasi-irreducible (QIR) 2-D cyclic code by extending Kurdjukov's result [10] on quasi-irreducible (i.e., non-squarefree) 1-D cyclic codes. This also implies that we can find the cycle representatives of any 2-D cyclic code by combining its QIR components with the aid of Seguin's method [8]. In the following discussions, with no loss of generality we confine ourselves to the binary case where the symbol field is the binary Galois field GF(2).

II. PRELIMINARIES ON 2-D CYCLIC CODES AND GROBNER BASIS

Let $R \overset{\Delta}{=} F[x,y]$ be the ring of bivariate polynomials over the field $F \overset{\Delta}{=}$ GF(2) and $I_{m,n} \overset{\Delta}{=} (x^m+1, y^n+1)$ be the ideal generated by x^m+1 and y^n+1. A binary 2-D cyclic code C of area $m\times n$ is an ideal $\tilde{I} = I/I_{m,n}$ in the factor ring $\tilde{R}_{m,n} \overset{\Delta}{=} R/I_{m,n}$ [3,5], where I is an ideal in R such that $I \supset I_{m,n}$. On the other hand, we may define a 2-D cyclic code $C = \tilde{I}$ by the parity check ideal $\tilde{J} = J/I_{m,n}$ $(J \supset I_{m,n})$ in $\tilde{R}_{m,n}$ (or J in R) such that $\tilde{I}\cdot\tilde{J} = \tilde{0}$ (the zero idel in $\tilde{R}_{m,n}$) and denote it by $C_{\tilde{J}}$ (or C_J).

The elements (codewords) u of C are either referred to as bivariate polynomials $u(x,y) = \Sigma_{(i,j)\varepsilon Z^2_{m,n}} u_{ij}x^iy^j$ (modulo $I_{m,n}$) or as 2-D $m\times n$ arrays (u_{ij}), $(i,j)\varepsilon Z^2_{m,n}$, where $Z^2_{m,n}$ is the set of pairs (i,j) of integers i modulo m and j modulo n, i.e. the subscripts i and j are to be interpreted respectively modulo m and n. The multiplication by a polynomial $f(x,y) = \Sigma_{(k,l)\varepsilon Z^2_{m,n}} f_{kl}x^ky^l$ amounts to send $u = (u_{ij})$ to $f(x,y)u = (\Sigma_{(k,l)\varepsilon Z^2_{m,n}} f_{kl}u_{i-k,j-l})$.

In particular, cyclic shifts $x\cdot u$ and $y\cdot u$ of a codeword u of C are also codewords of C. From now on we regard each codeword as a doubly periodic (DP) array by considering cyclic shifts.

A DP array u is characterized by a fundamental period (FP) parallelogram $\underline{l}_1\times\underline{l}_2 = \{(\omega_1 l_{11}+\omega_2 l_{21}, \omega_1 l_{12}+\omega_2 l_{22}) \varepsilon Z^2_{m,n} \mid 0\leq\omega_1,\omega_2<1\}$ with side vectors $\underline{l}_1=(l_{11},l_{12})$ and $\underline{l}_2 =(l_{21},l_{22})$ such that any period vector $\underline{l}$ of u can be represented as an integral linear combination $\underline{l} = k_1\underline{l}_1 +k_2\underline{l}_2$ of $\underline{l}_1$ and $\underline{l}_2$, $k_1,k_2 \varepsilon Z$ [4]. The 'period' of u is the area $|\underline{l}_1\times\underline{l}_2| = |\det(\begin{bmatrix} l_{11} & l_{12} \\ l_{21} & l_{22}\end{bmatrix})|$ of a FP parallelogram $\underline{l}_1\times\underline{l}_2$. In general $Z^2_{m,n}$ is covered with a network of congruent parallelograms obtained by shifting cyclically a FP parallelogram through $k_1\underline{l}_1+k_2\underline{l}_2$, $k_1,k_2 \varepsilon Z$.

Let $d \overset{\Delta}{=} \dim C_J$ be the dimension of the code C_J (as a linear subspace). Then, there exists a set of integer pairs $\{(\kappa_1,\lambda_1),\ldots,(\kappa_M,\lambda_M)\}$ associated with an 'independend point (IP) set' of J

$$\Delta(J) = \bigcup_{s=1}^{M-1}\{(i,j) \mid 0\leqq i<\kappa_{s+1}, 0\leqq j<\lambda_s\} \subset Z^2_{m,n}$$

which satisfies the following conditions [5]:

(1) $\kappa_1=0<\kappa_2<\cdots<\kappa_M\leqq m$, $n\geqq\lambda_1>\lambda_2>\cdots>\lambda_M=0$;

(2) J has a normal basis $\{f^{(1)}(x,y),\cdots,f^{(M)}(x,y)\}$ composed of the generator polynomials $f^{(s)}(x,y)$ with the 'quasi-degree' $\mathrm{Deg}\, f^{(s)} = (\kappa_s,\lambda_s)$, $1\leqq s\leqq M$;

(3) $\Delta(J)$ has the cardinality $|\Delta(J)| = d$;

(4) any non-zero polynomial of the form

$$f(x,y) = \Sigma_{(i,j)\varepsilon\Delta(J)} f_{ij}x^i y^j$$

is not an element of J.

The above normal basis is nothing but the Gröbner basis [11] of J, which can be obtained from any basis of J by a constructive method [5]. Although the algorithm is found to be equivalent to Buchberger's algorithm [11], the former which originated in a problem of encoding any 2-D cyclic code was devised independently and applied to construct some new 2-D cyclic codes [5]. The idea behind the algorithm is as follows. Suppose that, for each $(i,j) \varepsilon \Delta(J)$, an arbitrary value is assigned to the component u_{ij} of a codeword in C_J. From these values u_{ij}, $(i,j) \varepsilon \Delta(J)$, we can determine the other components u_{kl}, $(k,l) \not\varepsilon \Delta(J)$ by applying succesively a series of polynomials in $\{f^{(1)}, \ldots, f^{(M)}\}$. The set $\{f^{(1)}, \ldots, f^{(M)}\}$ is a Gröbner basis of J if and only if u_{kl}, $(k,l) \not\varepsilon \Delta(J)$, is determined uniquely, i.e. independently of any combination and any order of the polynomials used in determining u_{kl}.

III. QIR 2-D CYCLIC CODES C_Q

A quasi-irreducible (QIR) 2-D cyclic code C_Q is defined by a primary ideal Q. The code (ideal in $R_{m,n}$) C_Q has a minimal subideal C_P, i.e. an irreducible (IR) 2-D cyclic code. The IR code C_P is defined by the (maximal) prime ideal P associated with the primary ideal Q such that $P \supset Q \supset P^{\sigma}$ for a certain integer σ. There exists a pair of irreducible (over F) polynomials $f = f(x)$ and $h = h(x,y)$ which generate P, i.e. $P = (f, h)$. Let $d_1 \triangleq \deg_x f$ and $d_2 \triangleq \deg_y h$, where $\deg_x g$ ($\deg_y g$) is the degree of a polynomial $g = g(x,y)$ with respect to x (y). The IR code C_P has an IP set $\Delta(P) = \{(i,j) \mid 0 \leqq i < d_1,\ 0 \leqq j < d_2\}$. Thus, the dimension of C_P is equal to $d \triangleq |\Delta(P)| = d_1 d_2$ [4]. Let τ be the least integer satisfying $2^{\tau} \geqq \sigma$. Then, from the inclusion

$$Q \supset P^{2^{\tau}} \supset (f^{2^{\tau}},\ h^{2^{\tau}}),$$

it follows that the QIR code $C = C_Q$ is a subcode of the QIR code C_{Q_τ} defined by the primary ideal $Q_\tau \triangleq (f^{2^{\tau}},\ h^{2^{\tau}})$. The latter code C_{Q_τ} can be constructed by interleaving the codewords of the IR code C_P.

For an array (codeword) u of a 2-D cyclic code C_J, we define the characteristic ideal of u by $I(u) = \{f \in R \mid f \cdot u = (0)\}$. In like manner we have the characteristic ideal of a collection of arrays $u_1, \ldots, u_K$ such that

$$\begin{aligned} I(u_1, \ldots, u_K) &\triangleq \{f \in R \mid f \cdot u_1 = (0),\ \ldots,\ f \cdot u_K = (0)\} \\ &= \textstyle\bigcap_{s=1}^{K} I(u_s). \end{aligned}$$

Dualistically, for an ideal J (2-D cyclic code C_J) there exists a finite set $\{u_1, \ldots, u_L\}$ of 'representative arrays (codewords)' such that $J = I(u_1, \ldots, u_L)$, i.e. $C_J = \Sigma_{s=1}^{L} R \cdot u_s$ [5].

Let $H(Q)$ be the multiplicative group of invertible elements in the factor ring R/Q and $\{x^i y^j\}$ be the subgroup of $H(Q)$ consisting of all powers $x^i y^j$ of x and y. A major point of the present problem is to find the representatives of cosets in the factor group $H(Q)/\{x^i y^j\}$. In particular, if the parity check ideal J (2-D cyclic code C_J) has a single representative array (codeword) u, then for a complete set $\{g_1, \ldots, g_M\}$ of coset representatives of $H(J)/\{x^i y^j\}$ $\{g_1 \cdot u, \ldots, g_M \cdot u\}$ is a complete set of cycle representatives which are contained in C_J, but not in any proper subcode of C_J.

IV. CYCLE REPRESENTATIVES OF C_{Q_τ}

In this section we consider the QIR 2-D cyclic code C_{Q_τ} defined by the parity check ideal $Q_\tau = (f^{2^\tau}, h^{2^\tau})$. The QIR code C_{Q_τ} has a single representative array u. For example, we can determine such an array $u \epsilon C_{Q_\tau}$ by

$$u_{ij} = \begin{cases} 1, & (i,j) = (\kappa-1, \lambda-1); \\ 0, & (i,j) \epsilon \Delta(Q_\tau) - \{(\kappa-1, \lambda-1)\}, \end{cases} \qquad (1)$$

where $\kappa = d_1 2^\tau$, $\lambda = d_2 2^\tau$ and $\Delta(Q_\tau) = \{(i,j) \mid 0 \leq i < \kappa, 0 \leq j < \lambda\}$ [5].

The primary ideal Q_τ has a unique minimal primary superideal $Q_\tau' \triangleq (f^{2^\tau}, f^{2^\tau - 1} h^{2^\tau - 1}, h^{2^\tau})$ which belongs to the same prime ideal $P = (f, h)$. Correspondingly, C_{Q_τ}' is the maximal subcode of C_{Q_τ}, where the difference between the dimensions of these codes is

$$\dim C_{Q_\tau} - \dim C_{Q_\tau}' = d \ (= \dim C_P).$$

Hence the cardinality of the difference set $C_{Q_\tau} - C_{Q_\tau}'$ is equal to

$$2^{d2^{2\tau}} - 2^{d(2^{2\tau}-1)} = 2^{d(2^{2\tau}-1)}(2^d-1). \qquad (2)$$

The period of any element in $C_{Q_\tau} - C_{Q_\tau}'$ is equal to $p2^{2\tau}$, where p is the period of a non-zero element in C_P. Thus, the number of cycles in $C_{Q_\tau} - C_{Q_\tau}'$ is

$$2^{d(2^{2\tau}-1)}(2^d-1)/(p2^{2\tau}) = s2^{d(2^{2\tau}-1)-2\tau}, \qquad (3)$$

where $s \overset{\Delta}{=} |T(P)| = (2^d-1)/p$ is the cardinality of the set $T(P)$ of coset representatives in $H(P)/\{x^i y^j\}$. Let a polynomial $\alpha = \alpha(x,y)$ denote a primitive element of the extension field $GF(2^d)$, which is isomorphic to R/P, then $T(P) = \{\alpha^0, \alpha^1, \ldots, \alpha^{s-1}\}$.

For a non-zero array u in C_P, let $\underline{i}_1 \times \underline{i}_2$ be a FP parallelogram of u with $\underline{i}_1 = (i_1, j_1)$ and $\underline{i}_2 = (i_2, j_2)$, where $p = \left|\det\begin{pmatrix} i_1 & j_1 \\ i_2 & j_2 \end{pmatrix}\right|$. Then, there exist unique polynomials a_1, b_1, c_1, a_2, b_2, and c_2 such that

$$\begin{aligned} x^{i_1}y^{j_1} + 1 &= a_1 f + b_1 h + c_1 fh, \\ x^{i_2}y^{j_2} + 1 &= a_2 f + b_2 h + c_2 fh \end{aligned} \qquad (4)$$

$(\deg_y a_1,\ \deg_y a_2 < d_2;\ \deg_x b_1,\ \deg_x b_2 < d_1)$.

In fact, we can take $j_1=0$, $i_1>i_2\geq 0$ [5]. Thus, $b_1=c_1=0$, $a_1\neq 0$, $b_2\neq 0$. For any integer σ, we define S_σ to be the set of polynomials g with $\deg_x g < 2^{\sigma-1}d_1$ and $\deg_y g < 2^{\sigma-1}d_2$. Let

$$\tilde{a}_1 \overset{\Delta}{\equiv} a_1^{2^{\sigma-1}},\ \tilde{a}_2 \overset{\Delta}{\equiv} a_2^{2^{\sigma-1}},\ \tilde{b}_1 \overset{\Delta}{\equiv} b_1^{2^{\sigma-1}} (=0),\ \tilde{b}_2 \overset{\Delta}{\equiv} b_2^{2^{\sigma-1}}$$
$$\text{modulo } (f^{2^\sigma},\ h^{2^\sigma}), \qquad (5)$$

and $S_{\sigma 1}$ $(S_{\sigma 2})$ be the set of polynomials in S_σ which do not contain $x^{r_1}y^{s_1}$ $(x^{r_2}y^{s_2})$, where $x^{r_1}y^{s_1}$ $(x^{r_2}y^{s_2})$ is a nonzero term of the polynomial $\tilde{a}_1$ $(\tilde{b}_2)$. Then we have the following theorem, which is proved in the Appendix.

Theorem 1: A complete set of coset representatives in $H(Q_\tau)/\{x^i y^j\}$ is given by

$$t(1+fk_1+hl_1+fhm_1)(1+f^2k_2+h^2l_2+f^2h^2m_2)\cdots$$
$$(1+f^{2^{\tau-1}}k_\tau+h^{2^{\tau-1}}l_\tau+f^{2^{\tau-1}}h^{2^{\tau-1}}m_\tau), \qquad (6)$$

where $t\in T(P)$, $(k_\sigma,l_\sigma,m_\sigma)\in L_\sigma \overset{\Delta}{=} S_{\sigma 1}\times S_{\sigma 2}\times S_\sigma$ $(\sigma=1,\ldots,\tau)$; a complete set of cycle representatives in $C_{Q_\tau} - C_{Q_\tau}'$, is obtained by multiplying the representative array u (1) of C_{Q_τ} by polynomials (6).

V. CYCLE REPRESENTATIVES OF ANY QIR CODE

Now we will show that Theorem 1 is also useful for obtaining the coset representatives of $H(Q)/\{x^i y^j\}$, where Q is any primary ideal belonging to the same prime ideal $P = (f(x), h(x,y))$ such that $P \supset Q \supset Q_\tau = (f^{2^\tau}, h^{2^\tau})$.

Let I be an ideal in R and $\Delta(I)$ be an independent point set of I. We represent each element (coset) of the factor ring R/I by a polynomial of the form

$$g(x,y) = \Sigma_{(i,j)\varepsilon\Delta(I)} g_{ij} x^i y^j .$$

Let I' be a subideal of I. By virtue of the isomorphism $R/I \cong (R/I')/(I/I')$, we can select the coset representatives of R/I out of those of R/I'. To be precise, we have only to pick up the elements g with the quasi-degree Deg g $\varepsilon\Delta(I)$, since $\Delta(I) \subset \Delta(I')$. Thus, in view of $\dim_F(R/I) = |\Delta(I)|$, the set of elements of R/I is identical with the set of elements of R/I' satisfying Deg g ε $\Delta(I)$.

Furthermore, let g be an invertible element of R/I' satisfying Deg g $\varepsilon\Delta(I)$. Then there exists a polynomial g^{-1} such that $g \cdot g^{-1} \equiv 1 \bmod I'$ and Deg g^{-1} ε $\Delta(I')$. Since $I' \subset I$, $g \cdot \tilde{g}^{-1} \equiv 1 \bmod I$, where $\tilde{g}^{-1} \equiv g^{-1} \bmod I$ and Deg $\tilde{g}^{-1}$ ε $\Delta(I)$. Therefore g is invertible as an element of R/I. Consequently, we have the following lemma.

Lemma 2: Let I and I' be ideals in R and $I \supset I'$.

The invertible elements of R/I are given by the invertible elements g of R/I' satisfying Deg $g \in \Delta(I)$, i.e. $H(I) = \{g \in H(I') \mid \text{Deg } g \in \Delta(I)\}$.

The following theorem is an immediate consequence of Theorem 1 and Lemma 2.

Theorem 3: Let Q be a primary ideal belonging to a prime ideal $P = (f, h)$ and $P \supset Q \supset Q_\tau = (f^{2^\tau}, h^{2^\tau})$. The coset representatives of $H(Q)/\{x^i y^j\}$ can be selected among the elements (6) whose quasi-degrees are contained in $\Delta(Q)$.

To find the cycle representatives of C_Q, we need a collection of representative arrays $\{u_1, \ldots, u_N\}$ of Q which satisfies the following conditions:

(1) $C_Q = \bigcup_{s=1}^{N} C_{I(u_s)}$, in particular $Q = \bigcap_{s=1}^{N} I(u_s)$;

(2) there does not exist any array v such that $I(u_s) \supsetneqq I(v) \supsetneqq Q$.

To obtain such a collection of arrays $\{u_1, \ldots, u_N\}$ for C_Q, we may begin with the set of representative arrays $\{u^{(1)}, \ldots, u^{(M-1)}\}$ defined by

$$u_{ij}^{(s)} = \begin{cases} 1, & (i,j) = (\kappa_{s+1}-1, \lambda_s-1), \\ 0, & (i,j) \in \Lambda(Q) - \{(\kappa_{s+1}-1, \lambda_s-1)\}, \end{cases} \quad (1 \leqq s \leqq M-1) \quad (7)$$

where $\Delta(Q) = \bigcup_{s=1}^{M-1}\{(i,j) \mid 0 \leqq i < \kappa_{s+1},\ 0 < j < \lambda_s\}$ is an independend point set of Q [5]. Then, we continue to select linear

combinations $u = g^{(1)}u^{(1)}+\cdots+g^{(M-1)}u^{(M-1)}$ satisfying the condition (2) until the condition (1) is fulfilled.
Each array u_s has a largest FP parallelogram among the arrays in $C_{I(u_s)}$ and $I_s = I(u_s)$ has a unique minimal superideal I_s' which is a primary ideal belonging to P. Thus we obtain the cycle representatives in $C_Q - \bigcup_{s=1}^{N} C_{I_s'} = \bigcup_{s=1}^{N}(C_{I_s} - C_{I_s'})$ by multiplying the arrays u_s by the polynomials mentioned in Theorem 3.

Example 1: Let $P = (f, h)$, where $f = x+1$, $h = y^2+y+1$. Then $d_1 = 1$, $d_2 = 2$, $d = 1\cdot 2 = 2$. $(i_1,j_1)\times(i_2,j_2) = (1,0)\times(0,3)$ is a FP parallelogram and the period of C_P is $p = 3$. Thus $s = (2^d-1)/p = 3/3=1$ and $T(P) = \{1\}$, $\alpha = x$.
From

$$x+1 = 1\cdot f,$$
$$y^3+1 = (y+1)\cdot h,$$

it follows that $a_1 = 1$, $a_2 = 0$, $b_1 =0$, $b_2 = y+1$, $c_1 = c_2 = 0$. For $Q = (f^2, h^2)$, $Q' = (f^2, fh, h^2)$, the period of every element of $C_Q - C_{Q'}$ is equal to $3\cdot 2^2 = 12$. Let $S_1 = \{g \mid \deg_x g = 0, \deg_y g \leqq 1\} = \{0, 1, y, y+1\}$, $S_{11} = S_{12} = \{0, y\}$ and $L_1 = S_{11}\times S_{12}\times S_1$. The total number of cycles is equal to $|T(P)|\cdot 2^{3d-2} = 16$ $(= |L_1|)$. The cycle representatives are shown in Fig. 1. On the other hand, the primary ideal Q' has five minimal superideals $I_1 = (f^2, h)$, $I_2 = (f^2, h+f) = (x^2+1, y^2+y+x)$, $I_3 = (f, h^2)$, $I_4 = (f^2, h+yf) = (x^2+1, y^2+xy+1)$, $I_5 = (f^2, h+(y+1)f) = (x^2+1, y^2+xy+x)$, i.e.

$C_{Q'} = \cup_{i=1}^{5} C_{I_i}$. The cycle representatives in C_{I_i} - [illegible] $(1 \leq i \leq 5)$ and their FP parallelograms are shown in Fig. 2. In particular, the 2×6 code C_{I_2} has the code parameters (n, k, d) = (12,4,6) and the weight enumerator $A(z) = 1+12z^6+3z^8$, where n = code length, k = dimension, d = minimum distance and the coefficient A_i of $A(z) = \Sigma_{i=0}^{n} A_i z^i$ is the number of codewords having weight i. This code has the largest minimum distance d=6 among the linear codes with the parameters (n, k) = (12,4) [5].

Example 2: Let $P = (f, h)$ and $Q = (f^2, h)$, where $f = x^2+x+1$, $h = y+x+1$. The cycle representatives of the 6×6 code C_Q and their FP parallelograms are shown in Fig. 3. The left array is in $C_Q - C_P$ and the right array in C_P. Thus this code C_Q is an optimal linear code with the parameters (36,4,18) and the weight enumerator $A(z) = 1+12z^{18}+3z^{24}$ [5].

VI. CONCLUSION

We have presented a method of finding the cycle representatives of any quasi-irreducible two-dimensional cyclic code by extending Kurdjukov's result on one-dimensional (ordinary) cyclic codes. This result is useful for determining the weight enumerator of any two-dimensional cyclic code.

REFERENCES

[1] F. J. MacWilliams, "Binary codes which are ideals in the group algebra of an Abelian group," Bell Syst. Tech. J., vol. 49, pp.987-1011, 1970.

[2] T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "A theory of two-dimensional linear recurring arrays," IEEE Trans. Inform. Theory, vol. IT-18, pp.775-785, 1972.

[3] T. Ikai, H. Kosako, and Y. Kojima, "Basic theory of two-dimensional cyclic codes - Generator polynomials and the positions of check symbols," IECE Trans., vol. 59-A, no. 4, pp.311-318, 1976.

[4] S. Sakata, "General theory of doubly periodic arrays over an arbitrary finite field and its applications," IEEE Trans. Inform. Theory, vol. IT-24, pp.719-730, 1978.

[5] S. Sakata, "On determining the independent point set for doubly periodic arrays and encoding two-dimensional cyclic codes and their duals," IEEE Trans. Inform. Theory, vol. IT-27, pp. 556-565, 1981.

[6] S. E. Tavares, P. E. Allard, and S. S. Shiva, "On the decomposition of cyclic codes into cyclic classes," Inform. Contr., vol. 18,, pp. 342-354, 1971.

[7] - , "A note on the decomposition of cyclic codes into cyclic classes," Inform. Contr., vol.22, pp. 100-106, 1973.

[8] G. Seguin, "On obtaining orbit representatives for a class of groups with operators," SIAM J. Appl. Math., vol. 26, pp. 772-775, 1974.

[9] M. Willett, "Cycle representatives for minimal cyclic codes," IEEE Trans. Inform. Theory, vol. IT-21, pp. 716-718, 1975.

[10] A. P. Kurdjukov, "Determination of cyclic representatives of cyclic codes," Problemy Peredachi Informatsii, vol. 12, no. 4, pp.107-108, 1976.

[11] B. Buchberger, "A theoretical basis for the reduction of polynomials to canonical forms," ACM SIGSAM Bulletin 39, pp.19-29, 1976.

APPENDIX

Simplified proof of Theorem 1: The total number of elements written by (6) is

$$\begin{aligned}|T(P)|\prod_{i=1}^{\tau}|L_i| &= |T(P)|\prod_{i=1}^{\tau}2^{3\cdot 2^{2(i-1)}d-2}\\ &= |T(P)|2^{d(2^{2\tau}-1)-2\tau},\end{aligned}$$

which is equal to the number of cycles (3). For the remaining part of the proof, we can show inductively by an argument close to Kurdjukov's that distinct elements of (6) belong to different cosets. In the course, we remark that the representative array u has a FP parallelogram $2^{\tau}\underline{i}_1\times 2^{\tau}\underline{i}_2$. Furthermore we need the following lemma.

Lemma: A maximal subset S of the Cartesian product $S_\sigma\times S_\sigma$ which satisfies the following condition is identical with $S_{\sigma 1}\times S_{\sigma 2}$:

$(k+k'\equiv\tilde{a}_1$ or $l+l'\equiv 0)$ and $(k+k'\equiv\tilde{a}_2$ or $l+l'\equiv\tilde{b}_2)$ and
$(k+k'\equiv\tilde{a}_1+\tilde{a}_2$ or $l+l'\equiv\tilde{b}_2)$ all modulo $(f^{2^\sigma}, h^{2^\sigma})$

for each pair (k,l), (k',l') ϵ S such that $(k,l)\neq(k',l')$.

$$\begin{array}{cccc}
\boxed{\begin{matrix}1&0&0&0&1&0\\0&0&1&0&1&0\end{matrix}} & \begin{matrix}1&0&0&0&1&0\\0&0&0&1&0&1\end{matrix} & \begin{matrix}1&0&0&0&1&0\\0&0&0&0&0&0\end{matrix} & \begin{matrix}0&1&0&0&0&1\\0&0&1&1&1&1\end{matrix} \\[1em]
\begin{matrix}0&0&1&0&1&0\\0&0&1&1&1&1\end{matrix} & \begin{matrix}0&0&0&0&0&0\\1&1&1&0&0&1\end{matrix} & \begin{matrix}1&0&0&0&1&0\\1&1&0&1&1&0\end{matrix} & \begin{matrix}1&0&0&0&1&0\\1&1&1&1&0&0\end{matrix} \\[1em]
\begin{matrix}1&1&0&0&1&1\\1&1&1&0&0&1\end{matrix} & \begin{matrix}1&1&0&0&1&1\\1&1&0&1&1&0\end{matrix} & \begin{matrix}1&1&0&0&1&1\\1&1&1&1&0&0\end{matrix} & \begin{matrix}1&1&0&1&1&0\\1&1&1&0&0&1\end{matrix} \\[1em]
\begin{matrix}1&1&0&1&1&0\\1&1&1&1&0&0\end{matrix} & \begin{matrix}1&0&1&1&0&1\\0&1&0&0&0&1\end{matrix} & \begin{matrix}1&0&0&0&1&0\\0&1&0&0&0&1\end{matrix} & \begin{matrix}1&0&0&1&1&1\\1&0&0&0&1&0\end{matrix}
\end{array}$$

Fig. 1 Example of cycle representatives of a QIR 2-D cyclic code

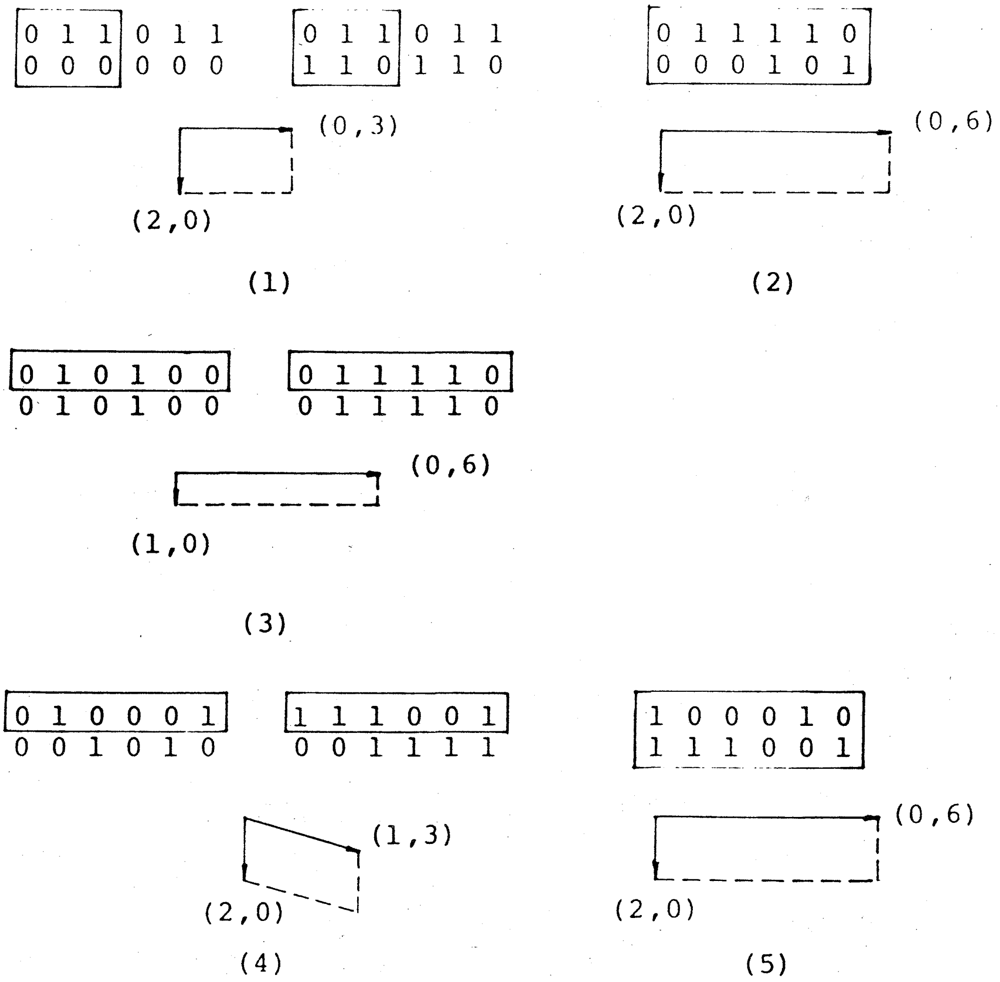

Fig. 2 Example of cycle representatives with their FP parallelograms

$$\begin{array}{|cc|cccc}
\hline
0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 \\
\hline
\end{array}
\qquad\qquad
\begin{array}{|c|ccccc}
\cline{1-1}
0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 \\
\cline{1-1}
\multicolumn{1}{c}{0} & 1 & 1 & 0 & 1 & 1 \\
\multicolumn{1}{c}{1} & 0 & 1 & 1 & 0 & 1 \\
\multicolumn{1}{c}{1} & 1 & 0 & 1 & 1 & 0 \\
\end{array}$$

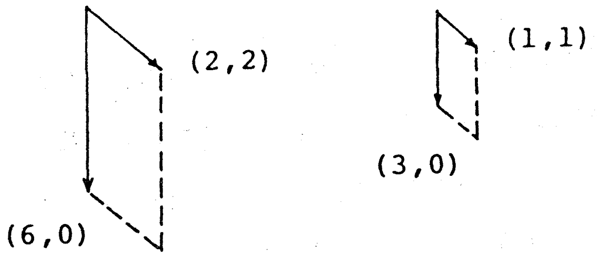

Fig. 3 Example of cycle representatives with their FP parallelograms