International Workshop on Discrete Mathematics and Algorithms

IWDMA'94

国际离散数学与算法研讨会文集

December 18-19, 1994
Jinan University
GuangZhou

Editor Yunlin Su
苏运霖 主编

Jinan University Press
暨南大学出版社

International Workshop on
Discrete Mathematics and
Algorithms

IWDMA '94
国际离散数学与算法研讨会
文 集

December 18—19, 1994

Jinan University

Guangzhou

Editor Yunlin Su
苏运霖 主编

暨南大学出版社
Jinan University Press

粤新登字 13 号

International Workshop on
Discrete Mathematics and
Algorithms
IWDMA' 94
国际离散数学与算法研讨会文集
苏运霖　主编
暨南大学出版社出版发行
暨南大学印刷厂印刷
广东省新华书店经销
开本：787×1092 1/25
印张：10.75
字数：40 万
1994 年 12 月第 1 版　1994 年 12 月第 1 次印刷

印数 1—1000 册
ISBN7—81029—369—9
O·18　定价：20.00 元

Acknowledgement

The Second International Workshop on Discrete Mathematics and Algorithms is to be held on December 18—19, 1994 in Guangzhou. We are pleased to present the Proceedings to all the participants of the workshop and all the readers of it. The organizing committee wants to thank the contributors of the Proceedings and the participants of the workshop. It is they who make the success of the workshop. We also want to thank all the people who work for the workshop. Without their service, it is hard to imagine how can the workshop smoothly proceed.

We also want to point out that though some people didn't show up in the workshop. They have also made contributions to our workshop. Our thanks are to the following individuals or enterprises. They are the sponsors of our workshop. We are most grateful to list their names:

Mr. Antton Haliman

Mr. Zhibin Liang

Mr. Charles Liaw

Mr. Willy Tamblin

Guangzhou Computer Commerce Association

Guangzhou Lansoft

Guangdong Province Computer Company

China Computer System Engineering Company, Nanfang Company

Table of Contents

On Latin Arrays*

Tao Renji
Institute of Software, Academia Sinica
(**Beijing**, 100080)

Abstract

This paper gives a survey on Latin arrays. We first discuss enumeration of Latin arrays, and present some results on numbers of Latin arrays and of isotopy classes. Then we deal with independence of Latin array and give a generation method of Latin arrays by means of permutations with the same independent degrees. Finally, generation of linearly independent permutations is discussed and some algorithms are mentioned.

1 Enumeration of Latin arrays

The problem of designing one-key cryptosystems which can be implemented by finite automata without expansion of the plaintext and with bounded propagation of decoding errors lies on choosing suitable parameters such as the size of alphabets and the length c of ciphertext history and designing three components in the canonical form (Fig. 1) — an autonomous finite automaton *Ma*, a transformation h and a permutation family g_w such that the systems are both efficient and secure[1, 2, 3, 4]. For studying the family of permutations used in this canonical form, the concept of Latin array is introduced and their enumeration and generation problems are investigated[5, 6].

Let $N=\{a_1, \cdots, a_n\}$ be an n element set. Let A be an $n\times nk$ matrix on N. If each element of N occurs exactly once in each column of A and k times in each row of A, then A is said to be an (n, k)-*Latin array.*

Let A be an (n, k)-*Latin array.* If each column of A occurs exactly

* Supported by the National Natural Science Foundation.

r times in columns of A repeatedly, then A is said to be an (n, k, r)-*Latin array*.

Latin arrays in a kind of generalization of Latin squares.

Let A and B be $n \times m$ *matrices* on N. If B can be obtained from A by rearranging rows, rearranging columns and renaming elements, then A and B is said to be *isotopic*.

Clearly, if A is an (n, k)-*Latin array* and *isotopic* with B, then B is an (n, k)-*Latin arrayj* and if A is an (n, k, r)-*Latin array* and *isotopic* with B, then B is *an* (n, k, r)-*Latin array*.

For (n, k)-*Latin arrays* or (n, k, r)-*Latin arrays*, the equivalence class partitioned by isotopy relation is called *isotopy class*.

By $U(n, k)$ denote the number of all (n, k)-*Latin arrays*, $U(n, k, r)$ the number of all (n, k, r)-*Latin arrays*, $I(n, k)$ the number of all isotopy classes of (n, k)-*Latin arrays*, and $I(n, k, r)$ the number of all isotopy classes of (n, k, r)-*Latin arrays*. we have[5, 6]

Proposition 1

(a). $I(n,k,r)=I(n, k/r, 1)$;

(b). $U(n, k, r)=U(n, k/r, 1)(nk/r)! / (nk/r)! (r!)^{nk/r}$.

Proposition 2

Let $1 \leqslant k < (n-1)!$. We then have:

(a). $I(n, k, 1)= I(n, (n-1)! -k, 1)$;

(b). $U(n, (n-1)! -k, 1)= U(n, k, 1)(n! -nk)! / (nk)!$;

(c). $I(n, (n-1)!, 1)= 1$, $U(n, (n-1)!, 1)=(n!)!$.

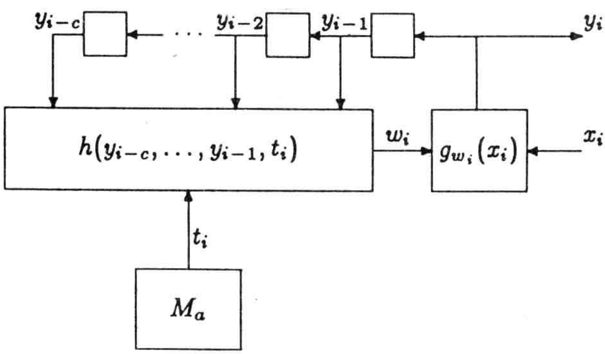

Fig. 1 (*a*). *Encoder M*

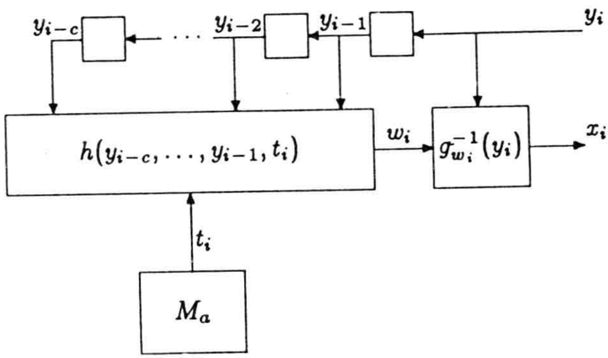

Fig. 1 (*b*). *Decoder M′*

Theorem 1

I(2,k)=1, U(2,k)=(2k)! /(k!)^2, I(2,1,1)=1, U(2,1,1)=2;

I(3,1,1)=1, U(3,1,1)=12,

$I(3,k)=\begin{cases}(k+1)/2 \text{ if k is odd}\\ k/2+1 \text{ otherwise,}\end{cases}$ $U(3,k)=\Sigma_{h=0}^{k}(3k)!\ /(h!\ (k-h)!)^3$,

I(4,1)=2, U(4,1)=(4!)^2, I(4,1,1)=2, U(4,1,1)=(4!)^2,

I(4,2)=11, U(4,2)=12640320 I(4,2,1)=6, U(4,2,1)=10281600,

I(4,3)=46, U(4,3)=805929062400, I(4,3,1)=11, U(4,3,1)=306561024000,

I(4,4)=201, U(4,4)=87285061904040000,

I(4,4,1)=6, U(4,4,1)=10281600×16! /8!.

A program for generating the representatives of (n, k)−Latin array's isotopy classes was run on a JAGER386 computer and the following results was reported. [7]

Theorem 2

I(4,5)=831; *I*(5,2)=864.

An (*n*,*k*)−*Latin array* is said to be an *involutive* (*n*,*k*)−*Latin array* if each column corresponds to an involution.

By *U′*(*n*,*k*) denote the number of all involutive (*n*,*k*)−*Latin arrays.* In [8], *U′*(*N*,*K*) for $2\leqslant n\leqslant 5$ and the following results are given.

Theorem 3

U′(6,1)=457920, *U′*(7,1)=31298400, *U′*(8,1)=427379500800.

2 Linear independent Latin arrays

Let *A* be an (*n*,*k*)−*Latin array.* Denote $r=\lceil log_q\, nk\rceil$. The vector [$u_1$,

$\cdots,u_r]$ over $GF(q)$ is said to be *column label* of column $(u_1q^{r-1}+u_2q^{r-2}+\cdots+u_r)+1$ of A.

Definition Let A be an (n,k)—Latin array. *Let* $x\in\{1,\cdots,n\}$ and $y\in N$. If components of column labels of columns of A in which the elements at row x are y satisfy some *r-ary* polynomial with degree $\leqslant c$ over $GF(q)$, then A is said to be *c-independent with respect to* (x,y), otherwise, A is said to be *c-independent with respect to* (x,y). If A is *c-dependent with respect to* (x,y) for *any* $x\in\{1,\cdots,n\}$ and $y\in N$, then A is said to be *c-dependent*. If A is *c-independent with respect to* (x,y) for any $x\in\{1,\cdots,n\}$ and $y\in N$, then A is said to be *c-independent*. If A is *c-dependent* and not $(c-1)$*-dependent*, then c is said to be *dependent degree of* A, denoted by c_A. If A is c—independent and not $(c-1)$-independent, then c is said to be *independent degree* of A, denoted by I_A.

Linearly independent Latin arrays are useful for simplifying a cryptosystem. [9]

Proposition 3

Let A be an (n,k)—Latin array. Let $r'=\lceil \log_q nk\rceil$, *and* $c_q(n,k)=$

$$\min c\left[1+\binom{r}{1}+\cdots+\binom{r'}{c}>k\right].$$ *Then we have* $c_A\leqslant c_q(n,k)$.

We use R_q^r to denote the vector space of dimension r over $GF(q)$. For any nonnegative integer m, let f_m be a one—one mapping from R_q^m to $\{0,1,\cdots q^m-1\}$ defined by $f_m(x_1,\cdots,x_m)=x_1q^{m-1}+x_2q^{m-2}+\cdots+x_m$. Let φ_1 and φ_2 be two permutations on R_q^r, and φ a transformation on R_q^r. Denote $\Phi=(\varphi_1,\varphi,\varphi_2)$. Construct a $q^r\times q^{2r}$ matrix A_Φ over R_q^r as follows: the element at row $i+1$ and column $j+1$ is $\varphi_1(w_1)\oplus\varphi(\varphi_2(w_2)\oplus f_r^{-1}(i)$, where $(w_1,w_2)=f_{2r}^{-1}(j)$, and w_1 and w_2 have dimension r.

Proposition 4

A_Φ is a (q^r,q^r)—Latin array if and only if φ is a permutation.

Whenever φ is a permutation, A_Φ is said to be (q^r,q^r)—Latin array of Φ.

Definition Let φ be a transformation on R_q^r with component functions $\varphi_1,\cdots,\varphi_r$. For any nonnegative integer c, if there is a 2r—ary polynomial h over GF(q) such that

$$h(x_1,\cdots,x_r,\varphi_1(x_1,\cdots,x_r),\cdots,\varphi_r(x_1,\cdots,x_r))=0, x_1,\cdots,\cdots x_r\in GF(q),$$

then φ is said to be *c-dependent*, and h is said to be *a dependent polynomial of* φ. If φ is not *c-dependent*, then φ is said to be *c-independent*. If φ is *c-*

dependent and $(c-1)$-independent, then c is said to be *dependent degree of* φ, denoted by c_φ, and $c-1$ is said to be *independent degree of* φ, denoted by I_φ.

An affine transformation on R_q^r means $xC \oplus b$, where C is a $r \times r$ matrix over $GF(q)$, b is a row vector of dimension r over $GF(q)$.

Theorem 4

Let φ be a transformation on R_q^r, and p and q be two invertibe offine transformations on R_q^r. Let $\varphi'(x) = p(\varphi(q(x)))$, $x \in R_q^r$. Then we have $c_\varphi = c_\varphi'$ and $I\varphi = I\varphi'$.

Theorem 5

Let φ be a transformation on R_q^r, and φ_1 and φ_2 be two invertible affine transformations on R_q^r. Let $\Phi = (\varphi_1, \varphi, \varphi_2)$, and A_Φ be the (q^r, q^r)-Latin array of Φ. Then we have: (1). $c_{A\Phi} = c_\varphi$, (2). $I_{A\Phi} = I_\varphi$, (3). $C_{A\Phi} = I_{A\Phi} + 1$.

Denote $c_q(r) = c_q(q^r, q^r)$. We have

Proposition 5

For any transformation φ on R_q^r, we have $c_\varphi \leqslant c_q(r)$.

Theorem 6

For $q=2$, $1 \leqslant r \leqslant 6$, there is a permutation φ on R_2^r such that $c_\varphi = c_2(r)$.

3 A kind of linear independent permutations

It is known that all r-*ary* functions on $GF(q)$ is a vector space over $GF(q)$ and has a basis $\{P_{k_1}, \cdots, k_r\}, k_1, \cdots, k_r = 0, 1, \cdots, q-1)$, where $P_{k_1}, \cdots, k_r(x_1, \cdots, x_r) = x_1^{k1} \cdots x_r^{kr}$. Let

$$\Gamma = [P_{00\cdots 00}, P_{00\cdots 01}, \cdots, P_{(q-1)(q-1)\cdots(q-1)(q-2)}, P_{(q-1)(q-1)\cdots(q-1)(q-1)}],$$

then we can formally express

$$f(x_1, \cdots, x_r) = \Gamma_b,$$

where b is a column vector of dimension q^r over $GF(q)$ determined uniquely by f and referred as *polynomial coordinate of* f.[10]

Let φ be a transformation on R_q^r with component functions $\varphi_1, \cdots, \varphi_r$. Let b_i is the polynomial coordinate of φ_i, $i=1, \cdots, r$. The $q^r \times r$ matrix $[b_1, \cdots, b_r]$ is called *polynomial coordinate matrix* of φ and denoted by B_φ. By B_φ^- denote the submatrix of B_φ obtained by deleting its rows $1, 1+q^i$, $i=0, 1, \cdots, r-1$.

Theorem 7

$C_\varphi > 1$ if and only if columns of B_φ^- are linearly independent.

Let $s < r$. φ' be a transformation on R_q^s, and h_i a $(r-i)$-ary function on $GF(q)$, $i=1, \cdots, r-s$. Let $c_1, \cdots, c_{r-s} \in GF(q)$. Define a transformation φ of which component functions are

$$\varphi_1(x_1,\cdots,x_r)=c_1x_1+h_1(x_2,\cdots,x_r),$$
$$\varphi_2(x1,\cdots,x_r)=c_2x_2+h_2(x_3,\cdots,x_r),$$
$$\cdots\cdots$$
$$\varphi_{r-s}(x_1,\cdots,x_r)=c_{r-s}x_{r-s}+h_{r-s}(x_{r-s+1},\cdots,x_r),$$
$$\varphi_r\ r-s+1(x_1,\cdots,x_r)=\phi_1(x_{r-s+1},\cdots,x_r),$$
$$\cdots\cdots$$
$$\varphi_r(x1,\cdots,x_r)=\phi_s(x_{r-s+1,\cdots},x_r),$$
$$x_1,\cdots,x_r\in GF(q),$$

where $\phi_1,\cdots,\varphi_s'$ are the component functions of ϕ. Denote such a φ by $Rec(\phi,h_1,\cdots,h_{r-s},c_1,\cdots,c_{r-s})$.

Lemma 1

If ϕ is a permutation on R_q^s and $c_i\neq 0, i=1,\cdots,r-s$, then $Rec(\phi,h_1,\cdots,h_{r-s}),c_1,\cdots,C_{r-s}$ is a permutation on R_q^r.

Theorem 8

Let $s<r$, ϕ is a permutation on R_q^s and $c_\varphi'>1$. Then elements of

$$\Phi'=\{|\Phi|\ C\varphi>,\ \varphi=Rec(\phi,h_1,\cdots,h_{r-s},C1,\cdots,C_{r-s})$$
$$\text{for some } h_i,\ c_i\neq 0,\ i=1,\cdots,r-s\}$$

are pemutations on R_q^r and number of elements of Φ' is

$$(q-1)^{r-s}q^{(r-s)(r+s+1)/2}\prod_{i=s+1}^{r-1}(q^{q^{i-1}-1}-q^i)$$

Corollary 1

Let $s<r$, ϕ be a permutation on R_q^s and $c_\phi>1$. Let B be a $q^r\times r$ matrix over $GF(q)$ satisfying following conditions: the submatrix consisting of elements in the first q^s rows and the last s columns of B is B_ϕ; elements in the last q^r-q^s rows and the last s columns of B are *zeros*; for any j, $1\leqslant j\leqslant r-s$, in the column j of B, element at row $q^{r-j}+1$ is *nonzero* and elements in the last $q^r-q^{r-j}-1$ rows are *zeros*; for any j, $1\leqslant j\leqslant r-s-1$, in the column j of B, a nonzero element is included in rows $q^{r-j-1}+2$ *to* q^{r-j}; and the first column of the submatrix which consists of elements in the first q^s rows and the last $s+1$ columns of B cannot be linearly expressed by the rest. If B is the polynomial coordinate matrix of φ, then φ is a permutation on R_q^r and $c_\varphi>1$. Furthermore, number of such permutations is

$$(q-1)^{r-s}(q^{q^s}-q^s)\prod_{i=s+1}^{r-1}(q^{q^i}-q^{q^{i-1}+1})$$

4 Generation of linear independent permutations

Let φ be a transformation on R_2^r. Let W_i be a $\binom{r}{i}\times r$ matrix over $GF(2)$ of which rows consist of all difference vectors of dimension r with weight i, $i=0,1,\cdots,r$. Denote the vector with components 1 of dimension $\binom{r}{i}$ by I_t. For any i, $0\leqslant i\leqslant r$, define a $\binom{r}{i}\times r$ matrix U_i over $GF(2)$ of which row j is the value of φ on row j of W_i, $0\leqslant j\leqslant\binom{r}{i}$. Define a $2^r\times(1+r)$ matrix

$$\Phi=\begin{bmatrix} I_0 & W_0 & U_O \\ I_1 & W_1 & U_1 \\ \vdots & \vdots & \vdots \\ I_r & W_r & U_r \end{bmatrix}$$

Denote the submatrix of columns 2 to $r+1$ of Φ by W, and the submatrix of the last r columns of Φ by U_φ.

For convenience sake, we rearrange rows of W_1 so that it is the identity matrix.

Lemma 2

(a). $c_\varphi>1$ if and only if columns of Φ are linearly independent. **(b).** *φ is invertible if and only if rows of U_φ are distinct.*

By E_t denote the $\binom{r}{t}\times\binom{r}{t}$ identity matrix. Let the $2^r\times 2^r$ matrix

$$P=\begin{bmatrix} I_0 & W_0 & & & & & & \\ I_1 & W_1 & & & & & & \\ I_2 & W_2 & E_2 & & & & & \\ 0 & W_3 & 0 & E_3 & & & & \\ I_4 & W_4 & 0 & 0 & E_4 & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & & & \\ I_{r-1}' & W_{r-1} & 0 & 0 & 0 & \cdots & E_{r-1} & \\ I_r' & W_r & 0 & 0 & 0 & \cdots & 0 & E_r \end{bmatrix}$$

where $I_j'=I_j$ if j is even, $I_j'=0I_j$ otherwise. It is easy to verify that P is nonsingular and

$$P^{-1}=\begin{bmatrix} I_0 & W_0 & & & & & \\ I_1 & W_1 & & & & & \\ I_2 & W_2 & E_2 & & & & \\ I_3 & W_3 & 0 & E_3 & & & \\ I_4 & W_4 & 0 & 0 & E_4 & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \\ I_{r-1} & W_{r-1} & 0 & 0 & 0 \cdots E_{r-1} & & \\ I_r & W_r & 0 & 0 & 0 & \cdots & E_r \end{bmatrix}$$

Lemma 3

PΦ is in the form of

$$P\Phi=\begin{bmatrix} I_0 & 0 & V_0 \\ 0 & E_1 & V_1 \\ 0 & 0 & V_2 \\ \vdots & \vdots & \vdots \\ 0 & 0 & V_r \end{bmatrix}$$

where $V_0=U_0$, V_i *is a* $\binom{r}{i}\times$ *matrix*, $i=1,\cdots,r$.

Denote the last r columns of $P\Phi$ by V_φ. Denote the submatrix of V_φ obtained by deleting its first $1+r$ rows by $V_{\varphi-}$.

Lemma 4

$C_\varphi>1$ if and only if columns of $V_{\varphi-}$ are linearly independent.

Lemma 5

For any i, $1\leqslant i\leqslant r$, and any $r\times r$ permutation matrix Q over GF(2), there exists uniquely a $\binom{r}{i}\times\binom{r}{i}$ permutation matrix P_{iQ} such that $P_{iQ}W_i=W_{iQ}$.

Let

$$D_Q=\begin{bmatrix} I_0 & & & & \\ & Q & & & \\ & & P_{2Q} & & \\ & & & \ddots & \\ & & & & P_{rQ} \end{bmatrix}$$

$G_r'=\{D_Q|Q$ is a $r\times r$ permutation matrix over $GF(2)\}$.

It is easy to verify that G_r' is a group and isomorphic to the group consisting of all $r\times r$ permutation matrices over $GF(2)$ under the isomorphism $P_{iQ}\leftrightarrow Q$.

Let $G_r=\{<D_Q,\delta,C>|Q$ is a $r\times r$ permutation matrix over $GF(2)$, δ is a row vector of dimension r over $GF(2)$, C is a $r\times r$ nonsingular matrix over $GF(2)\}$. Let. be an operation on G_r defined by

$$<D_Q, \delta, C>.<D_{Q'}, \delta', C'>=<D_QD_{Q'}, \delta\oplus\delta', C'C>.$$
It is easy to verify that $< G_r, . >$ is a group.

Any $2^r \times r$ matrix V, partition it into blocks

$$V = \begin{bmatrix} V_0 \\ V_1 \\ \vdots \\ V_r \end{bmatrix}$$

where V_i has $\binom{r}{i}$ rows, $0 \leqslant i \leqslant r$. For any $<D_Q, \delta, C>$ in G_r, define

$$< D_Q,\delta,C >= D_Q(V \oplus \begin{bmatrix} \delta \\ 0 \\ \vdots \\ 0 \end{bmatrix})C = D_QVC \oplus \begin{bmatrix} \delta C \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

V and V' are said to be equivalent if there is $< D_Q, \delta, C >$ in G_r such that $V^{<D_Q,\delta,C>} = V'$.

Lemma 6

Assume that $V^{<D_Q,\delta,C>} = V'$. then we have

$$P^{-1}V' = D_Q(P^{-1}V)C \oplus \begin{bmatrix} \delta C \\ \delta C \\ \vdots \\ \delta C \end{bmatrix}$$

Denote the submatrices of V and of V' obtained by deleting their first $1+r$ rows by V_- and V'_-, respectively.

Theorem 9

Assume that V and V' are equivalent. Then we have: (a). Columns of V_- are linearly independent if and only if columns of V'_- are linearly independent; (b). Rows of $P^{-1}V$ are distinct if and only if rows of $P^{-1'}$ are distinst.

By $S(V_0, V_1)$ denote the set of all $2^r \times r$ matrices over $GF(2)$ satisfying the following conditions: the first row of V is V_0, the submatrix of rows *2* to $1+r$ of V is V_1, columns of V_- are linearly independent, and rows of $P^{-1}V$ are distinct.

Corollary 2

Let δ be a row vector of dimension r over $GF(2)$, Q a $r \times r$ permutation matrix over $GF(2)$, and C a $r \times r$ nonsingular matrix over $GF(2)$. Then we have

$$S((V_0 \oplus \delta)C, QV_1C) = \{V^{(Q_Q,\delta,C)} \mid V \in S(V_0, V_1)\},$$

and $|S((V_0 \oplus \delta C, QV_1C)| = |S(V_0, V_1)|$

For any positive integer r, Denote $G_r'' = \{<Q,C>\} \mid Q$ is a $r \times r$ permutation matrix over $GF(2)$, C is a $r \times r$ nonsingular matrix over $GF(2)\}$. Let be an operation on G_r'' defined by $<Q,C>.<Q',.C'>=<QQ', C'C>$. It is easy to verify that $<G_r'',.>$ is a group. For any $r \times r$

matrix V_1 over $GF(2)$ and any $<Q,C>$ in G_r'', denote $V_r^{<Q,C>}=QV_1C$. V_1 and $V_r^{<Q,C>}$ are said to be *equivalent* under G_r''. For $r\times r$ matrices over $GF(2)$, representatives of equivalences under G_r'' are said to be *canonical forms* under G_r''. [11]

Notice that both the property that V_1 has no zero row and the property that rows of V_1 are distinct keeps unchanged under equivalence. Clearly, $S(V_0, V_1)\neq 0$ yields that V_1 has no zero row and that rows of V_1 are distinct. From Corollary 2, it is sufficient to compute $S(0, V_1)$, where V_1 ranges over canonical forms under group G_r'' of which rows are distinct and nonzero. For example, in case of $r=4$, V_1 has only three alternatives:

$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\1&1&0&0\end{bmatrix},\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\1&1&1&0\end{bmatrix},$$

4.1 $\mathbf{S(V_0,V_1)}$

Lemma 7

Let

$$P_R=\begin{bmatrix}I_0&&\\&E_1&\\&&P_R'\end{bmatrix}$$

be a $2^r\times 2^r$ permutation matrix. Assume that

$$R=\begin{bmatrix}I_0&0&0\\0&E_1&0\\0&W^*&P_R'\end{bmatrix}$$

where

$$W^*=W\oplus P_R'W,\ W=\begin{bmatrix}W_2\\W_3\\\vdots\\W_r\end{bmatrix}$$

Then we have $P_RP^{-1}=P^{-1}R$, and R satisfying the above equation is uniquely determined by P_R.

Theorem 10

The following two conditions are equivalent: (1). the first $r+1$ rows of V and of V' are the same, and $P^{-1}V$ and $P^{-1}V'$ are different only in a row permutation;
(2). the first $r+1$ rows of V and of V' are the same and there exists a $(2^r-1-r)\times(2^r-1-r)$ permutation matrix P'_R such that

$$V'_-=(E'\oplus P_R')WV_1\oplus P'_RV_-,$$

where V_- and V'_- are the submatrices of V and of V' obtained by deleting their first $1+$