A Method Constructing Orthogonal Latin Squares Based on Complete Y-Matrixes

Yongbin Qin
Department of Computer Science
Guizhou University (*550025*)
Guiyang, China
ybqin@foxmail.com, 18085008039

Jie Li, Daoyun Xu
Department of Computer Science
Guizhou University (*550025*)
Guiyang, China

***Abstract*—The complete classes of orthogonal Latin squares can be constructed from Galois fields. The complete Y-matrix in [1] presents a new representation of finite group. A complete Y-matrix decides a finite group, and a finite group induces a complete-matrix. Based on this idea, we can construct Galois fields by constructing a pair of complete Y-matrixes, one is associated to additive group, and another is associated to multiplication group of the Galois field. The complete Y-matrix corresponding to multiplication group is constructed by some proper cyclic permutations since a cyclic group can be constructed a cyclic permutation. In this paper, we present a method to generate orthogonal Latin squares based on the construction of fields by complete-matrixes.**

Keywords—finite group; complete Y-matrix; Galois field; orthogonal Latin square; method

I. INTRODUCTION

For a finite set $\Omega = \{a_1, \ldots, a_n\}$ (in short, $\Omega = \{1, \cdots, n\}$), the function $\eta : N_p \times N_q \to \Omega$ is taken as assigning coordinates to elements in Ω, it is represented as $M = (\eta(i,j))_{p\times q}$, denote as $[\![\eta]\!]$, called the representation matrix of Ω with respect to (w.r.t.) η.

By the function η, we have the following relation:

$$\begin{pmatrix} (i,j) & (i,j') \\ (i',j) & (i',j') \end{pmatrix} \xrightarrow{\eta} \begin{pmatrix} \eta(i,j) & \eta(i,j') \\ \eta(i',j) & \eta(i',j') \end{pmatrix}$$

The point (i',j') can be viewed as the result by replacing the coordinates from the point (i,j) step by step.

In the above matrix $[\![\eta]\!]$, we can observe an interesting result: for any two blocks $\begin{pmatrix} \eta(i,j) & \eta(i,j') \\ \eta(i',j) & \eta(i',j') \end{pmatrix}$ and $\begin{pmatrix} \eta(s,t) & \eta(s,t') \\ \eta(s',t) & \eta(s',t') \end{pmatrix}$, if any values of three points are same at corresponding positions respectively, then the value of fourth point is same, e.g. $\eta(i,j) = \eta(s,t)$, $\eta(i',j) = \eta(s',t)$, $\eta(i,j') = \eta(s,t')$ imply $\eta(i',j') = \eta(s',t')$.

The constraint relation is called shortly as "Four Endpoints Rule (FER)". The general definition is seen in [1]. Such matrix is called complete Y-matrix, in short CY-matrix.

The computation table of a finite group is a CY-matrix. Let $G = \{g_1, \ldots, g_n\}$ be a finite group and let $g_1 = e$ be the unit element of G, then for any $g_i \in G$, $g_i G = \{g_i g_1, \ldots, g_i g_n\} = G$, The operation table on G can be represented as a $n \times n$ matrix $M_G = (g_{i,j})$, where $g_{i,j} = g_i g_j$ for $1 \le i,j \le n$. The matrix M_G has the following basic properties.

(1) Each element a in G occurs exactly once in each row (column) of M_G. Then, each element a in G defines a permutation matrix on G.

(2) For any a 2×2 submatrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in M_G, shortly for a block, anyone can be decided only by other three. i.e., M_G associates with a function $F: G^3 \to G$ satisfying the constraints: $F(b,a,c) = d \Leftrightarrow F(d,b,a) = c \Leftrightarrow F(a,c,d) = b \Leftrightarrow F(c,d,b) = a$.

(3) Such function F is an invariant up to permutations on rows or columns of the matrix M_G. By changing properly order of rows (or columns) of M_G, we can get a new matrix $M_{G(e)} = (g'_{i,j})$ such that $g'_{i,j} = e$ for $i = 1, 2, \ldots, n$, i.e., the unit element e is locatedat main diagonal line of $M_{G(e)}$, such matrix is called normal matrix. Thus, the operation $a \times b = c$ in G can be represented by a block $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $M_{G(e)}$. Clearly, for any fixed $g' \in G$, we get a new matrix $M_{G(e')}$ from M_G, by the same methodand $M_{G(e')}$ decides a new group G' with the unit element e', the operation $a \Delta b = d$, denoted by $(a * b)_{e'}$ in G', is decided by the block $\begin{pmatrix} a' & b \\ c & d \end{pmatrix}$ in $M_{G(e')}$. Clearly, G' is isomorphic to G.

The essence characterization of CY-matrixes is the property FER. A CY-matrix can decide a finite group. The geometry properties of matrixes will be useful for constructing finite groups, classifying and decomposing of finite groups. The relevant references can be seen in[2, 3, 4, 5, 6, 7, 8].

A finite field $(G, +, *)$ is decided by two finite groups, $(G, +)$ (additive group) and $(G', *)$ (multiplication group), where $|G'| = |G| - 1$, $(G', *)$ is a cyclic group and there lation of two operations is limited by the distribution law.

In paper, we present some methods for constructing CY-matrixes and Galois fields, and then a method to generate complete classes of orthogonal Latin squares.

II. COMPLETE Y-MATRIXES AND FINITE GROUPS

Let $M = (a_{i,j})_{p\times p}$ be a matrix on Ω, if M satisfies the condition Four Endpoints Rule(FER), i.e., for any two blocks $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ and $\begin{pmatrix} a & c \\ b & d' \end{pmatrix}$ in M, it must be $d = d'$, then call it a complete Y-matrix, in short CY-matrix. If M is a CY-matrix, then for any fixed element a in Ω, we can get a binary function $F_a : \Omega \times \Omega \to \Omega$ defined by $\begin{pmatrix} a & y \\ x & F_a(x,y) \end{pmatrix}$. So, one can define a binary operation $*$ on Ω:

$$(x \times y)_a \Leftrightarrow \begin{pmatrix} a & y \\ x & z \end{pmatrix} \Leftrightarrow F_a(x,y) = z.$$

The CY-matrixes have some basic and important properties.

(1)The function F holds the composite rule, i.e., for any $a,b,c,d,e,f \in \Omega\, F(F(a,c,f),f,d) = F(a,c,d)$, and $F(a,e,F(e,c,d)) = F(a,c,d)$.

(2)For any $a,b \in \Omega, F(a,a,b) = b, F(a,b,b) = a$.

(3)Each element a in Ω occurs exactly once in each row (column) in matrix M.

(4)The function F is an invariant under arranging the order of rows (or columns), since permutations of rows or columns in matrixes preserve the diagonal relations between elements.

Based on (3), we can introduce the formal form of the matrix M.For any fixed element a in Ω, we can adjust a to the main diagonal of a matrix.

The normal form is similar to the table of computation for a finite group, where the element a on the main diagonal of the matrix is equivalent to the unit element in group.

Let $[n]$ denote the set $\{1,2,\dots,n\}$, a permutation $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$ on $[n]$ can be shown a (0/1)-matrix Col_π, where, $Col_\pi(i,j) = 1$ if $i = \pi(j)$, otherwise $Col_\pi(i,j) = 0$. Clearly, $Col_{\pi^{-1}} = Col_\pi^{-1} = (Col_\pi)^T$ for any permutation π, denote $Row_\pi = Col_{\pi^{-1}}$, i.e., $Row_\pi = Col_{\pi^{-1}}$ where π^{-1} is the inverse transformation of π, and the matrix A^T is the transpose of matrix A.

For a matrix $A = (a_{i,j})$, we write A as $[A(1,:),\dots,A(n,:)]^T$ in arrays of rows, or $[A(:,1),\dots,A(:,n)]$ in arrays of columns. Then, we have the following relations:

(1) $A \cdot Col\pi = [A(:,1),\dots,A(:,n)] \cdot Col_\pi = [A(:,\pi(1)),\dots,A(:,\pi(n)]$.

(2) $Col_\pi^{-1} \cdot A = Row_\pi \cdot [A(1,:),\dots,A(n,:)]^T = [A(\pi(1),:),\dots,A(\pi(n),:)]^T$.

In [1], the author presents the following results:

(1) A finite group defines a CY-matrix.

(2) A CY-matrix can decide a finite group.

For a given CY-matrix M and any element $a \in \Omega$, we can define a 0/1 square matrix χ_a^M of p-order, called the characterization matrix of a, where

$$\chi_a^M(i,j) = \begin{cases} 1 & M(i,j) = a \\ 0 & o.w. \end{cases}.$$

In [9, 10], we have shown the following results.

Lemma 1 For a given CY-matrix M and a fixed element θ in Ω, M_θ is a formal matrix on θ from M, i.e., the element θ is located at main diagonal of the matrix by rearranging order of rows in M, then for any block $\begin{pmatrix} \theta & b \\ a & c \end{pmatrix}$ in M_θ, we have that $\chi_a^{M_\theta} * \chi_b^{M_\theta} = \chi_c^{M_\theta}$, where the operation "$*$" is the usual multiplication of matrix.

Therefore, we have that

Theorem 1 For a given CY-matrix M and a fixed element θ in Ω, let $M = \{\chi_a^{M_\theta} : a \in \Omega\}$ be a set of (0/1)-matrixes of p-order, then $(M,*)$ is a group, where the binary operation "$*$" is the usual multiplication of matrix, and $\chi_\theta^{M_\theta}$ is the unit element in the group.

III. BASIC CY-MATRIXES

Let p be a natural number. A number $r(1 \leq\leq p-1)$ is called a Euler number of p, or between r and p are coprime, denoted by $(r,p) = 1$, if for any $i,j(1 \le i \ne j \le p)$, $(i \cdot r)(mod\ p) \ne (j \cdot r)(mod\ p)$, or $\{1,[r(mod\ p)]+1, [(2r)(mod\ p)]+1,\dots,[(p-1)r(mod\ p)]+1\} = \{1,2,\dots,p\}$. Define a set $Euler(p) = \{r : r\ is\ a\ Euler\ number\ of\ p\}$. Clearly, $Euler(p)$ contains 1 for any $p \ge 2$, and if p is a prime number, then $Euler(p) = \{1,2,\dots,p-1\}$.

Let $(a) = (a_1,a_2,\dots,a_p)$ be acyclic sequence of symbols associating a function $next_a$, $next_a(a_i) = a_{(i+1)(mod\ p)}$, and a set $Sym(a) = \{a_1,\dots,a_p\}$, where p is the length of (a).

If $(r,p) = 1$, we define recursively a cyclic matrix as follows:

(1) $C_{p,r}(1,j) = j\ for\ j = 1,2,\dots,p$.

(2) $C_{p,r}(i+1,1) = (ir)(mod\ p)+1\ for\ i = 1,2,\dots,p-1$.

(3) $C_{p,r}(i,j+1) = \left[C_{p,r}(i,j)(mod\ p)\right]+1\ for\ j = 1,2,\dots,p-1$.

Clearly, if $(r,p) = 1$, then $C_{p,r}(1,1), C_{p,r}(2,1),\dots,C_{p,r}(p,1)\} = \{1,2,\dots,p\} = [p]$, therefore, $C_{p,r}$ is a CY-matrix.

The matrix $C_{p,r} = (c_{i,j})_{p\times p}$ will be viewed as a basic model (or matrix of index) of complete Y-group. For a set $\Omega = \{a_1,a_2,\dots,a_p\}$ and a cyclic sequence $(a) =< a_1,a_2,\dots,a_p >$ of symbols. $C_{p,r}(a)$ defines a complete Y-group on Ω associating with a function $\eta : N_p \times N_p \to \Omega$, where $\eta(1,j) = a_j$, $\eta(i,1) = a_{[r(i-1)](mod\ p)+1}$ and $\eta(i,j) = next_a(\eta(i,j-1))$ for $1 \le i \le p, 2 \le j \le p$.

Lemma 2 Assume that $p \geq 2$ and $(r,p)=1$, then $C_{p,r} = Row_{\pi_{p,r}} * C_{p,1}$, where $\pi_{p,r}(1) = r+1$, $\pi_{p,r}(j+1) = (\pi_{p,r}(j)+r)(mod\ p)+1$ for $j = 1,2,\dots,p-1$, the number r is called as rotation parameter of rows in $C_{p,1}$.

Lemma 3 [1]Let *(a), (b), (c)* and *(d)* be four cyclic sequences of symbols of length *p*, where $Sym(a)\ Sym(b) = \emptyset$, $Sym(a) \cap Sym(c) = \emptyset$, and $Sym(b) \cap Sym(d) = \emptyset$. Then, the matrix $M = \begin{pmatrix} C_{p,r}(a) & C_{p,s}(b) \\ C_{p,u}(c) & C_{p,v}(d) \end{pmatrix}$ is a Y-matrix, if and only if $rv \equiv su\ (mod\ p)$, where $(r,p)=(s,p)=(u,p)=(v,p)=1$.

If $Sym(a) = Sym(d)$ and $Sym(b) = Sym(c)$, then *M* is a CY-matrix when *M* is a Y-matrix.

For natural numbers $p \geq 2, q \geq 2$, let $(a_1),\dots,(a_q)$ be q distinct cyclic sequences of symbols of length *p*, i.e., $Sym(a_i) \cap Sym(a_j) = \emptyset$ for $i \neq j$. Define a $q \times q$ matrix $R = (r_{i,j})$ of rotation parameters of rows in $C_{p,1}$, where $(r_{i,j}, p) = 1$ for any $1 \leq i,j \leq q$, such that for any 2×2 block $\begin{pmatrix} r & s \\ u & v \end{pmatrix}$ in *R*, $rv \equiv su\ (mod\ p)$.

We view (a_i) as a symbol, and fix a cyclic sequence $(\vec{a}) = ((a_1),\cdots,(a_q))$, take acyclic matrix $C_{q,r^*}((r^*,q)=1)$ as a model getting matrix $C_{q,r^*}(\vec{a})$. Combining R with $C_{q,r^*}(\vec{a})$, we can construct a complete Y-matrix $M = (M_{i,j})$, where $M_{i,j}$ is the form of $C_{p,r_{i,j}}(a_t)$, $C_{q,r^*}(i,j) = (a_t)$ and $R(i,j) = r_{i,j}$.

In the construction of M, we view $C_{p,1}$ as factors, R as models of row-rotations, $C_{q,r*}$ as bases, then write $M = C_{p,1} \otimes_R C_{q,r*}$.

In fact, FER implies the composite condition.

IV. Construction of Cyclic Groups Based on Permutations

Let [n] denote the set $\{1,2,\dots,n\}$, and let $\pi = \begin{pmatrix} 1 & 2 & \dots & \dots & n \\ \pi(1) & \pi(2) & \dots & \dots & \pi(n) \end{pmatrix}$ be a permutation on [n]. The permutation π can be decomposed a set of cyclic permutation, $\pi_1,\dots,\pi_k$, where π_i is a cyclic permutation on some subsets S_{π_i} of *[n]*, such that $[n] = i = \bigcup_{i=1}^{k} S_{\pi_i}$ and $S_{\pi_i} \cap S_{\pi_j} = \emptyset$ for any $i,j (1 \leq i \neq j \leq k)$. The size of S_{π_i}, $|S_{\pi_i}|$, is called the length of cyclic permutation π_i. In this paper, we assume that $|S_{\pi_i}| \geqslant 2$ for each *i*, since the element *a* can be deleted from *[n]* if $S_{\pi_i} = \{a\}$ for some cyclic π_i. Such π is called nontrivial permutation. If $k = 1$, then π is a cyclic permutation of length *n*, and it can be written as $(j_1\ j_2\ \dots\ j_n)$, which defines an order $(j_1 \prec j_2 \prec \cdots \prec j_n)$ on *[n]*, where $j_i = \pi(1)$.

Let π be a cyclic permutation of length *n* on *[n]*. Define $\pi^0 = Id_{[n]}$ (identical transformation), $\pi^{k+1} = \pi \circ \pi^k\ (k = 0,1,2,\dots,n-1)$ and $\pi^k([n]) = (\pi^k(1),\ \dots, \pi^k(n))$, then the matrix $A^\pi = (\pi^0([n]), \pi^1([n]),\dots,\pi^{n-1}([n]))^T$ decides a complete Y-group.

For the permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = (1\ \ 3\ \ 5\ \ 2\ \ 4)$,

$$A^\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} \pi^0([n]) \\ \pi^1([n]) \\ \pi^2([n]) \\ \pi^3([n]) \\ \pi^4([n]) \end{pmatrix}.$$

Clearly, the matrix A^π satisfies FER, so, it decides a complete Y-group.

We now introduce another method to define a matrix $B^\pi = (b_{i,j})$ based directly on FER, such that $b_{1,k} = b_{k,1} = k\ (k = 1,2,\dots,n)$.

Let $\pi = (j_1\ j_2\ \dots\ j_n)$ be a cyclic permutation of length n on [n].

(1) Set $(b_{1,1}, b_{1,2},\dots,b_{1,n}) = (1,2,\dots,n)$ first row of B^π,

$(b_{j_1,1}, b_{j_1,2},\dots,b_{j_1,n}) = (\pi(1),\pi(2),\dots,\pi(n))$ j_1-*th* row of B^π, and

$(b_{1,j_1}, b_{2,j_1},\dots,b_{n,j_1}) = (\pi(1),\pi(2),\dots,\pi(n))$ j_1-*th* column of B^π.

(2) For $k = 1,2,\dots,n-1$, suppose that j_k-*th* column $B^\pi(:,j_k)$ of B^π has been computed, computing j_{k+1}-*th* column $B^\pi(:,j_{k+1})$ of B^π based on $B^\pi(:,j_k)$ by FER:

For $i \in [n] - \{1,j_1\}$, let $a = b_{i,j_k}$, finding column index c_a of a in $B^\pi(1,:)$, i.e., $a = b_{1,c_a}$, set $b_{i,j_{k+1}} = b_{j_1,c_a}$.

The following graph shows the computing process:

	$\cdots$	j_k	$\cdots$	j_{k+1}	$\cdots$	c_a
1	$\cdots$	j_k	$\cdots$	j_{k+1}	$\cdots$	a
$\vdots$		$\vdots$		$\vdots$		$\vdots$
j_1	$\cdots$	j_{k+1}	$\cdots$	j_{k+2}	$\cdots$	b
$\vdots$		$\vdots$		$\vdots$		$\vdots$
i	$\cdots$	a	$\cdots$	?		

$\longrightarrow$

	$\cdots$	j_k	$\cdots$	j_{k+1}	$\cdots$	c_a
1	$\cdots$	j_k	$\cdots$	j_{k+1}	$\cdots$	a
$\vdots$		$\vdots$		$\vdots$		$\vdots$
j_1	$\cdots$	j_{k+1}	$\cdots$	j_{k+2}	$\cdots$	b
$\vdots$		$\vdots$		$\vdots$		$\vdots$
i	$\cdots$	a	$\cdots$	$\boldsymbol{b}$		

The FER shows as follows, where $b = b_{j_1,c_a} = \pi(c_a)$.

$\begin{pmatrix} j_k & j_{k+1} & a \\ j_{k+1} & j_{k+2} & b \\ a & b & \end{pmatrix}, \begin{pmatrix} j_k & j_{k+1} \\ a & b \end{pmatrix}, \begin{pmatrix} j_k & a \\ j_{k+1} & b \end{pmatrix}$. Constructing complete Y-groups from permutations.

Let [n] denote the set $\{1,2,\cdots,n\}$, and let $\pi = \begin{pmatrix} 1 & 2 & \cdots & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \cdots & \pi(n) \end{pmatrix}$ be a permutation on $[n]$. The permutation π can be decomposed a set of cyclic permutation , $\pi_1,\cdots,\pi_k$, where π_i is a cyclic permutation on

some subsets S_{π_i} of $[n]$, such that $[n] = \cup_{i=1}^{k} S_{\pi_i}$ and $S_{\pi_i} \cap S_{\pi_j} = \emptyset$ for any i, j $(1 \le i \ne j \le k)$. The size of S_{π_i}, $|S_{\pi_i}|$, is called the length of cyclic permutation π_i. In this paper, we assume that $|S_{\pi_i}| \ge 2$ for each i, since the element a can be deleted from $[n]$ if $|S_{\pi_i}| = \{a\}$ for some cyclic π_i. Such π is called nontrivial permutation. If $k = 1$, then π is a cyclic permutation of length n, and it can be written as $(j_1 j_2 \cdots j_n)$, which defines an order $(j_1 \prec j_2 \prec \cdots \prec j_n)$ on [n], where $j_1 = \pi(1)$.

Let π be a cyclic permutation of length n on [n]. Define $\pi^0 = Id_{[n]}$ (identical transformation), $\pi^{k+1} = \pi \circ \pi^k$ $(k = 0, 1, 2, \cdots, n-1)$ and $\pi^k([n]) = (\pi^1([n]), \cdots\cdots, \pi^k([n]))$, then the matrix $A^\pi = (\pi^0([n]), \pi^1([n]), \cdots, \pi^{n-1}([n]))^T$ decides a complete Y-group.

We now introduce another method to define a matrix $B^\pi = (b_{i,j})$ based directly on FER, such that $b_{1,k} = b_{k,1} = k$ $(k = 1, 2, \cdots, n)$.

Let $\pi = (j_1 j_2 \cdots \cdots j_n)$ be a cyclic permutation of length n on $[n]$.

(1) Set $(b_{1,1}, b_{1,2}, \cdots, b_{1,n}) = (1,2, \cdots, n)$ first row of B^π, $(b_{j_1,1}, b_{j_1,2}, \cdots, b_{j_1,n}) = (\pi(1), \pi(2), \cdots, \pi(n))$ j1-th row of B^π and $(b_{1,j_1}, b_{2,j_1}, \cdots, b_{n,j_1}) = (\pi(1), \pi(2), \cdots, \pi(n))$ j1-th column of B^π.

(2) For $k = 1,2, \cdots, n-1$ suppose that jk-th column $B^\pi(:, j_k)$ of B^π has been computed ,computing jk+1-th column $B^\pi(:, j_{k+1})$ of B^π based on $B^\pi(:, j_k)$ by FER:

For $\in [n] - \{1, j_1\}$, let $a = b_{i,j_k}$,finding column index c_a of a in $B^\pi(1, :)$.

V. Construction of orthogonal Latin squares

The main ideas constructing orthogonal Latin squares come from the method of Galois fields.

Let $\Omega = \{1, 2, \ldots, n\}$ be a finite set, a square (matrix) $A = (a_{i,j})_{n \times n}$ on Ω is called Latin square, if each element a in Ω occurs exactly once in each row (and column) of *A*. Two Latin squares $A = (a_{i,j})_{n \times n}$ and $B = (b_{i,j})_{n \times n}$ on Ω are orthogonal if each pair $(a_{i,j}, b_{i,j})$ for $1 \le i, j \le n$ occurs exactly once in the matrix $((a_{i,j}, b_{i,j}))_{n \times n}$.

A set $\{A_1, \ldots, A_m\}$ of mutually orthogonal Latin squares is complete, if for any Latin square A, there is at least one A_i $(1 \le i \le m)$ such that A and A_i is not orthogonal. It is known that if a set $\{A_1, \ldots, A_m\}$ is mutually orthogonal n-order Latin squares, then $m \le n - 1$[11]. A classical result is that if $n = p^m \ge 3$, where p is a prime and m is a positive, then there are $n - 1$ mutually orthogonal Latin squares. The construction method is based on a Galois fields $GF[p^m]$. The detail method is seen in [11].

Let $t_0, t_1, \ldots, t_{n-1}$ be elements in $GF[p^m]$, we can construct $n - 1$ matrix $A_1, \ldots, A_{n-1}$,where $A_k = (a_{i,j}^{[k]})_{n \times n}, a_{i,j}^{[k]} = t_k * t_i + t_j$, $0 \le i, j \le n-1, k = 1, 2, \ldots, n-1$.

Thus, the key technology is how to construct Galois fields $GF[p^m]$. According to additive and multiplication operations in $GF[p^m]$, it is easy to construct complete set $\{A_1, \ldots, A_{n-1}\}$ or orthogonal Latin squares.

In this paper, we focus on constructing Galois fields $GF[2^m]$. The method is different from classical method finding irreducible polynomials.

Our method is to construct directly two finite groups, one as additive group and another as multiplication group, by constructing two CY-matrixes, such that the distribution law holds for two operations.

The method is described as follows:

(1) Take the base-matrix $C_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and compute the CY-matrix $M = C_2 \otimes \ldots \otimes C_2 C_2^{\otimes m}$ (m times).

(2) Define an additive group G_A on $\{0, 1, 2, \ldots, 2^m - 1\}$ with unit element 0.

(3) Find a cyclic permutation π on $\{0, 1, 2, \ldots, 2^m - 1\}$, and generate a CY-matrix B^π.

(4) Define a multiplication group G_M on $\{1, 2, \ldots, 2^m - 1\}$ with unit element 1. Note that the choice of π in (3) satisfies the condition that the distribution law of multiplication for additive holds.

(5) The combination of G_A and G_M forms a field.

For example, we consider the construction of fields being isomorphic to $GF[2^3]$.

(1) Compute the matrix for additive group.

$$G_A = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\ 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\ 4 & 5 & 5 & 7 & 0 & 1 & 2 & 3 \\ 5 & 4 & 7 & 6 & 1 & 0 & 3 & 2 \\ 6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{pmatrix} = C_2^{\otimes 3}.$$

(2) Take a cyclic permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 3 & 6 & 7 & 2 \end{pmatrix}.$$

(3) Compute the CY-matrix Bπ and get the matrix G_M for multiplication.

$$G_M = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 5 & 7 & 6 & 4 & 3 & 1 \\ 0 & 3 & 7 & 4 & 2 & 1 & 5 & 6 \\ 0 & 4 & 6 & 2 & 7 & 3 & 1 & 5 \\ 0 & 5 & 4 & 1 & 3 & 6 & 7 & 2 \\ 0 & 6 & 3 & 5 & 1 & 7 & 2 & 4 \\ 0 & 7 & 1 & 6 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

It is easy to check that the distribution law of multiplication for additive holds the condition.

According to the formulation $A_k = (a_{i,j}^{[k]})_{n\times n}$, $a_{i,j}^{[k]} = t_k * t_i + t_j$, we can compute $A_1, \ldots, A_{n-1}$.

VI. Conclusions and Future Works

The matrix representation of a finite group is a complete Y-matrix, and a complete Y-matrix decides a finite group. The complete class of orthogonal Latin squares can be constructed by Galois fields. We have given a method to construct some fields by complete Y-matrixes, and can construct some complete classes of Latin squares. The methods and some ideas in this paper are helpful to investigate structures of fields. The future works are to investigate relations between operations defined by different complete Y-matrixes, and then observe some geometric properties of finite fields.

Acknowledgements

The research work was supported by National Natural Science Foundation of China under Grant No. 61262006, Major Applied Basic Research Program of Guizhou Province under Grant No.JZ20142001andScience and Technology Foundation of Guizhou Province under Grant No.20122125.

References

[1] Y. Cao, Introduction to Y Group. Science Press, Beijing,2012.

[2] A. Baker, Representations of Finite Groups, http: //www.maths.gla.ac.uk/ajb

[3] J. L. Alperin & R. B. Bell, Groups and Representations, Springer-Verlag, 1995.

[4] G. James & M. Liebeck, Representations and Characters of Groups, Cambridge University Press, 1993.

[5] J.P. Serre, Linear Representations of Finite Groups, Springer-Verlag,1977.

[6] S.Sternberg, Group theory and physics, Cambridge University Press, 1994.

[7] J. B. Fraleigh, A First Course in Abstract Algebra. University of Rhode Island: 5th Edition, Addison-Wesley, 1994.

[8] R. Solomon, On Finite Simple Groups and Their Classification, Notices American Mathematical Society. 42, 231-239, 1995.

[9] D.Y. Xu and Y.B. Qin, Constructions of Finite Groups, (subbmitted to ICAPM2013).

[10] L. Zhang, J.Y. Wei and D.Y. Xu, Algorithms of Generating Finite Groups (subbmit-ted to ICCAE2013)

[11] Z.S. Yang, Combination mathematics and its algorithms, Press of Science and Technology in China, Hefei, 2006.