Constructions of Finite Groups

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

Haiyue Zhang, Daoyun Xu
Department of Computer Science
Guizhou University (*550025*)
Guiyang, China

***Abstract*—Y-group (as a matrix) in [1] presents a new representation of finite algebra systems. A complete Y-group decides a finite group, and the computation table of a finite group is a complete Y-group. Ones can comprehend deeply constructions of finite groups based on geometric properties of matrixes. In this paper, we analyse inherent connections between the three (ordinary finite group, permutation group, and matrix group for ordinary multiplication), and investigate some methods for constructing finite groups based on geometry (or structure) properties of matrixes. It is helpful for classifying and decomposing finite groups.**

Keywords—Finite group; CY-matrix; permutation; geometry method; construction; classification

I. INTRODUCTION

Let $G = \{g_1, \cdots, g_n\}$ be a finite group and let $g_1 = e$ be the unit element of G, then for any $g_i \in G$, $g_iG = \{g_ig_1, \cdots, g_ig_n\} = G$. The operation table on G can be represented as a $n \times n$ matrix $M_G = (g_{i,j})$, where $g_{i,j} = g_ig_j$ 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 other three. i.e., M_G associates with a function $F: G^3 \to G$ satisfying the constraints: $F(b,a,c) = d \Leftrightarrow F(d,b,a) = c \Leftrightarrow F(a,c,d) = b \Leftrightarrow F(c,d,b) = a$.

This characterization is called as "Four Endpoint Rule" (FER) in [1].

(3) 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 $i = 1, 2, \cdots, n$, i.e., the unit element e is located at main diagonal line of $M_{G(e)}$, such matrix is called normal matrix. Thus, the operation $a * b = c$ in G can be represented by a block $\begin{pmatrix} e & b \\ a & c \end{pmatrix}$ in $M_{G(e)}$.

Clearly, for any fixed $e' \in G$, we get a new matrix $M_{G(e')}$ from M_G by the same method, and $M_{G(e')}$ 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 $\begin{pmatrix} e' & b \\ a & d \end{pmatrix}$ in $M_{G(e')}$. Clearly, G' is isomorphic to G.

It defines a new group G' with the unit element a, and G' is isomorphic to G.

The matrix M_G can be represented by a coordinate function $\eta_G : [n] \times [n] \to G$, where $[n] = \{1, 2, \cdots, n\}$. $\eta_G(i,j) = a$ means assigning the coordinate (i,j) to a. It is seen that if G is a group, then there are exactly n coordinates assigned to a, and these coordinates have not same row-coordinates or column-coordinates. The characterization function of set of these coordinates is presented as a $n \times n$ (0/1)-matrix $\chi_a^{M_G}$.

For any normal matrix $M_{G(e')}$, associating a coordinate function $\eta_{e'}$, $\chi_a^{M_{G(e')}}(i,j) = 1 \Leftrightarrow \eta_{e'}(i,j) = a$. It is easy to show that $\chi_a^{M_{G(e')}} * \chi_b^{M_{G(e')}} = \chi_d^{M_{G(e')}}$ (multiplication of matrixes) if and only if there is the block $\begin{pmatrix} e' & b \\ a & d \end{pmatrix}$ in $M_{G(e')}$.

Note that the characterization matrix $\chi_a^{M_{G(e')}}$ is a permutation matrix P_{π_a} ,on [n], where $\pi_\alpha(i) = j \Leftrightarrow \chi_a^{M_{G(e')}}(i,j) = 1 \Leftrightarrow \eta_e(i,j) = a$. Thus, we have the following table of relations:

groups	***ordinary group***	***group for permutations***	***group for matrixes***
elements	α	π_a	$\chi_a^{M_{G(e)}}$
operations	αb	$\pi_a \circ \pi_b$	$\chi_a^{M_{G(e)}} * \chi_b^{M_{G(e)}}$
results	$\alpha b = c$	$\pi_a \circ \pi_b = \pi_c$	$\chi_a^{M_{G(e)}} * \chi_b^{M_{G(e)}} = \chi_c^{M_{G(e)}}$

We think for a finite group $G = (\Omega, *)$, the matrix M_G is a geometric representation of basic set Ω in G, and FER in $M_{G(e)}$ describe some constraints of geometry structures on Ω, and the constraints come from the operation "*".

A reverse idea is whether or not we can define originally finite algebra systems from geometry structures satisfying constraints (FER) on Ω. This idea comes from the author of reference [1].

In [1], the author introduces two basic concepts, Y-group and CY-group (complete Y-group). Simply, a Y-group on Ω is a $p \times q$ matrix M, shortly for Y-matrix, if M satisfies FER. M is presented as a function $\eta : [p] \times [q] \to \Omega$. In a Y-matrix M, each element α in Ω occurs at most once in each row

(column) of M. The size of M is defined by $k/min\{p,q\}$, where k is the number of elements occurring in M of Ω. If k=1, then M is called as complete, shortly for CY-matrix. If a Y-matrix M is complete, then $p = q = k$, and each element a in Ω occurs exactly once in each row (column) of M. The important property is that Y-matrix satisfies FER.

Thus, in this paper, we discuss mainly matrixes with the property FER in languages of matrixes. We will find that between CY-matrixes and finite groups are one-to-one. Between the three, ordinary finite group, permutation group, and matrix group for ordinary multiplication, have natural inherent connections.

The geometry properties of matrixes will be useful for constructing finite groups, classifying and decomposing of finite groups. In this paper, a lot of ideas are original or citing from [1], and constructing, classifying and decomposing for finite groups are classical and ancient problems, we cite a few of references except necessary. The relevant references can be seen in [2, 3, 4, 5, 6, 7, 8].

In paper, we present some methods for constructing finite groups based on geometry (or structure) properties of matrixes. It is helpful for classifying and decomposing finite groups.

II. FINITE EUCLIDEAN SPACES

For given sets $N_{n_i} = 1, 2, \cdots, n_i$ $(i = 1, 2, \cdots k)$, the Descartes product $N_{n_1} \times \cdots \times N_{n_k}$ is called the k-dimension finite Euclidean space (see [9]). Specially, 2-dimension finite Euclidean space is called as finite Euclidean plane. The finite Euclidean plane $N_p \times N_q$ can be represented by a $p \times q$ matrix $S = ((i,j))_{p\times q}$, where the original point is defined to (1,1), and the eatery (i,j) is a coordinate point.

For a finite set $\Omega = \{a_1, \cdots a_n\}$ (in short, $\Omega = \{1, \cdots, n\}$), the partial function $\eta :\subseteq N_p \times N_q \to \Omega$ is taken as assigning coordinates to elements in Ω, called a representation of Ω. Normally, we define the function η as a total function, and take $p = q$.

A function $\eta :\subseteq N_p \times N_q \to \Omega$ can be represented as a matrix $= (\eta(i,j))_{p\times q}$, denote as $[\![\eta]\!]$.

In the coordinate matrix $S = ((i,j))_{p\times q}$, any a 2×2 submatrix (called a block) consists of four points $\{(i,j),(i,j'),(i',j),(i',j')\}$, i.e. a block depends on at most four parameters i,j,i',j', or at most three points $\{(i,j),(i,j'),(i',j)\}$. By the function η, a block in S is projected to a block in $[\![\eta]\!]$.

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

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: 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, then the value of fourth point is same.

The constraint relation is called shortly as "Four Endpoints Rule (FER)".

If the function $\eta : N_p \times N_q \to \Omega$ satisfies FER, we can introduce a function F : $\Omega^3 \to \Omega$ defined by $F(b,a,c) = d$, where the 2×2 matrix $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ is a block in the matrix $[\![\eta]\!]$. The general definition is from [1].

Definition 1 A 5-tuple $[\Omega, N_p, \eta, F, k]$ is called k-dimension Y-group, where

(1) $\Omega = \{1, 2, \cdots, n\}$ is a finite set, $N_p = \{1, 2, \cdots, p\}$ is a finite set of index.

(2) $\eta : N_p^k \to \Omega$ is a representation function, $(i_1, \cdots, i_k) \longmapsto \eta(i_1, \cdots, i_k)$.

(3) The function $F : \Omega^{k+1} \to \Omega$ satisfies the condition on replacing coordinates: for any $i_1, \cdots, i_k, j_1, \cdots, j_k \in N_p$, $F(\eta(i_1, \cdots, i_k), \eta(j_1, i_2 \cdots, i_k), \cdots, \eta(i_1, j_2, \cdots, i_k), \cdots, \eta(i_1, i_2, \cdots, i_{k-1}, j_k) = \eta(j_1, j_2, \cdots, j_k)$.

If the function η is a full projection and for any $1 \le s \le k$ and any $t, t' \in N_p$, $t \ne t'$ implies $\eta(i_1, \cdots, i_{s-1}, t, i_{s+1}, \cdots, i_k) \ne \eta(i_1, \cdots, i_{s-1}, t', i_{s+1}, \cdots, i_k)$, then call the system $[\Omega, N_p, \eta, F, k]$ complete Y-group, in short CY-group.

In this paper, we focus on the case k=2, the complete Y-group$[\Omega, N_p, \eta, F, 2]$ is simplified into 4-tuple$[\Omega, N_p, \eta, F]$, and the condition (3) in the definition is written as $F(\eta(i',j), \eta(i,j), \eta(i,j') = \eta(i',j')$for any $i,j,i',j' \in N_p$. It corresponds to a block in the matrix $[\![\eta]\!]$:

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

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

In the finite Euclidean space, $S = ((i,j))_{p\times q}$, we introduce similarly the notation on lines. The set of points $(1,b)$, $(2, ab\ (mod\ q)), \cdots, (p, (p-1)ab\ (mod\ q))$ is called as a line in S, if $b, ab\ (mod\ q), \cdots, (p-1)ab\ (mod\ q)$ are distinct.

III. Basic properties of complete Y-group$[\Omega, \boldsymbol{N_p}, \boldsymbol{\eta}, \boldsymbol{F}]$

In the section, we consider some basic and important properties of the complete Y-group $[\Omega_p, N_p, \eta, F]$, where $|\Omega| = p$.

By the completeness and FER, it is easy to prove the following properties.

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

(1.1) $F(F(a,c,f), f, d) = F(a,c,d)$, corresponding the submatrix in $[\![\eta]\!]$

$$\begin{pmatrix} a & e & b \\ c & f & d \end{pmatrix}$$

(1.2) $F(a, e, F(e,c,d)) = F(a,c,d)$, corresponding the submatrix in $[\![\eta]\!]$

$$\begin{pmatrix} a & b \\ e & f \\ c & d \end{pmatrix}$$

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

Property 2 In a complete Y-group $[\Omega_p, N_p, \eta, F\ ]$, each element a in Ω occurs exactly once in each row (column) in matrix$[\![\eta]\!]$.

Property 3 For a given complete Y-group $[\Omega_p, N_p, \eta, F\ ]$, the system $[\Omega_p, N_p, \eta', F'\ ]$ is a new system defined by arranging the order of rows (or columns) of $[\![\eta]\!]$, then $F = F\ '$, i.e., the function F is an invariant under arranging the order of rows (or columns).

In fact, the diagonal relationship between elements in $[\![\eta]\!]$ is fixed under rearranging the order of rows (or columns) of $[\![\eta]\!]$.

Based on Property 3, we can introduce the formal form of the matrix $[\![\eta]\!]$. 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 $\{1, 2, \cdots, n\}$, a permutation $\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$ 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 $[A(1, :), \cdots, A(n, :)]^T$ in arrays of rows, or $[A(:, 1), \cdots, A(:, n)]$ in arrays of columns. Then, we have the following relations:

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

(2) $\mathrm{Col}_\pi^{-1} \cdot \mathrm{A} = \mathrm{Row}_\pi \cdot [\mathrm{A}(1, :), \cdots, \mathrm{A}(\mathrm{n}, :)]^{\mathrm{T}} = [\mathrm{A}(\pi(1), :), \cdots, \mathrm{A}(\pi(\mathrm{n}), :)]^{\mathrm{T}}$.

Therefore, we have that

Property 4 For a given complete Y-group $[\Omega, N_p, \eta, F\ ]$, the representation matrix is $[\![\eta]\!]$, then for any fixed element $a \in \Omega$, there is a permutation π on $[p]$, such that the system $[\Omega_p, N_p, \eta_a, F\ ]$ is a complete Y-group, where the element a is located at the main diagonal line of $[\![\eta_a]\!]$, and $[\![\eta_a]\!]$=$Row_\pi \cdot [\![\eta]\!]$.

Please note that the function F is an invariant up to permutations. In [1], the author presents a directly definition of complete Y-group, if the function F: $\Omega^3 \to \Omega$ on Ω holds the following properties, then F decides a complete Y-group.

(1) FER condition: for any a, b, c, d $\in \Omega$, presenting as block $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$

$F\ (b, a, c) = d \Leftrightarrow F\ (a, c, d) = b \Leftrightarrow F\ (c, d, b) = a \Leftrightarrow F\ (d, c, a) = b$.

(2) Composite condition: for any $a, b, c, d, e, f\ \in \Omega$

$F\ (F\ (a, c, f\ ), f, d) = F\ (a, c, d), and\ F\ (a, e, F\ (e, c, d)) = F\ (a, c, d)$.

In fact, FER implies the composite condition.

IV. Complete Y-groups and finite groups

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

(1) A finite group defines a complete Y-group $[\Omega, N_p, \eta, F\ ]$.

(2) complete Y-group $[\Omega, N_p, \eta, F\ ]$ can decide a usual finite group. For any fixed element $\theta \in \Omega$, define an operation $*, a * b = F\ (a, \theta, b)$, it corresponds to a block $\begin{pmatrix} \theta & b \\ a & F(a, \theta, b) \end{pmatrix}$.

We now introduce another method defining a finite group from a complete Y-group. Basic idea comes from [1].

For a given complete Y-group $[\Omega, N_p, \eta, F\ ]$, we have a representation square matrix $[\![\eta]\!]$ of p-order. For an element $a \in \Omega$, define a 0/1 square matrix $\chi_a^{[\![\eta]\!]}$ of p-order as follows: $\chi_a^{[\![\eta]\!]}(i, j) = \begin{cases} 1 & \eta(i, j) = a \\ 0 & o.w. \end{cases}$.

The matrix $\chi_a^{[\![\eta]\!]}$ is called the characterization matrix of a.

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

Proof: Let $[\Omega, N_p, \eta, F\ ]$ be a complete Y-group, then $|\Omega| = p$ and the function $\eta: \Omega \to N_p$ can be represented as a p × p matrix $[\![\eta]\!]$, where the matrix $[\![\eta]\!]$ satisfies FER. For a given element θ in Ω, the formal matrix is denoted as $[\![\eta]\!]_\theta$,corresponding to a function $\eta_\theta: \Omega \longrightarrow N_p$, and $[\![\eta]\!]_\theta$satisfies FER.($[\![\eta]\!]_\theta = [\![\eta_\theta]\!]$).

Let $\Omega = \{\theta, a_2, \cdots, a_p\}(a_1 = \theta)$, and $\eta_\theta(1, 1) = \theta$, $\eta_\theta(1, 2) = a_2, \cdots, \eta_\theta(1, p) = a_p$. Based on Property 2 in Section 3, for any $a \in \Omega$, the matrix $\chi_a^{[\![\eta]\!]_\theta}$ is a permutation matrix, corresponding to a permutation π_a, i.e., $\chi_a^{[\![\eta]\!]_\theta} = Col_{\pi_a}$.

For any $a \in \Omega$ and each $1 \le k \le p$, we have two coordinate arguments, a row argument $r_a^{[k]}$ and a column argument $c_a^{[k]}$, corresponding to $\chi_a^{[\![\eta]\!]_\theta}\left(k, c_a^{[k]}\right) = 1$ and $\chi_a^{[\![\eta]\!]_\theta}\left(r_a^{[k]}, k\right) = 1$.

For any block $\begin{pmatrix} \theta & b \\ a & c \end{pmatrix}$ in $[\![\eta]\!]_\theta$ and each $1 \le k \le p$, we have the following relations: $\eta_\theta(k, k) = \theta, \eta_\theta\left(k, c_b^{[k]}\right) = b, \eta_\theta\left(r_a^{[k]}, k\right) = a, \eta_\theta\left(r_a^{[k]}, c_b^{[k]}\right) = c$.

For any $a \in \Omega$, the characterization matrix $\chi_a^{[\![\eta]\!]_\theta}$ has the property that for each $1 \le k \le p$, $\chi_a^{[\![\eta]\!]_\theta}(i, k) = 1 \Leftrightarrow i = r_a^{[k]}\ and\ \chi_b^{[\![\eta]\!]_\theta}(k, j) = 1 \Leftrightarrow j = c_b^{[k]}$.

Let $\chi_a^{[\![\eta]\!]_\theta} = (a_{i,j})_{p\times p}$, $\chi_b^{[\![\eta]\!]_\theta} = (b_{i,j})_{p\times p}$ and $\chi_c^{[\![\eta]\!]_\theta} = (c_{i,j})_{p\times p}$,and denote $(a_{i,j})_{p\times p} * \left(b_{i,j}\right)_{p\times p} = (d_{i,j})_{p\times p}$, then $d_{i,j} = \sum_{k=1}^{p} a_{i,k} b_{k,j}$ in the usual multiplication of matrix for each pair $1 \le i, j \le p$.

We have that $0 \le d_{i,j} \le 1$, otherwise, there exist $k, k'(1 \le k \ne k' \le p)$ such that $a_{i,k} b_{k,j} = a_{i,k'} b_{k',j} = 1$. It implies that $a_{i,k} = a_{i,k'} = 1$. It contradicts with Property 2.

Further, we have that $d_{i,j} = 1$ if and only if there is the unique k_* such that $(a_{i,k_*} = 1) \wedge (b_{k_*,j} = 1)$ Please note that $(a_{i,k_*} = 1) \wedge (b_{k_*} = 1) \Leftrightarrow [(i = r_a^{[k_*]}) \wedge (j = c_b^{[k_*]})]$, it corresponds to a block in $[\![\eta]\!]_\theta$.

$$\begin{pmatrix} (k_*, k_*) & (k_*, c_b^{[k_*]}) \\ (r_a^{[k_*]}, k_*) & (r_a^{[k_*]}, c_b^{[k_*]}) \end{pmatrix} \underset{\eta\theta}{\rightarrow} \begin{pmatrix} \theta & b \\ a & c \end{pmatrix}.$$

It means that $(d_{i,j} = 1) \Leftrightarrow (d_{i,j} = \sum_{k=1}^{p} a_{i,k} b_{k,j} = a_{i,k_*} b_{k_*,j} = 1) \Leftrightarrow (a_{r_a^{[k_*]},k_*} b_{k_*,c_b^{[k_*]}} = 1)$. Therefore, $(d_{i,j} = 1) \Leftrightarrow (c_{i,j} = 1)$, i.e., $d_{i,j} = c_{i,j}$.

Therefore, we have that

Theorem 1 For a given complete system $[\Omega, N_p, \eta, F]$ and a fixed element θ in Ω, let $M = \{\chi_a^{[\![\eta]\!]_\theta} : a \in \Omega\}$ 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 $\chi_\theta^{[\![\eta]\!]_\theta}$ is the unit element in the group.

Generally, let $[\Omega, N_p, \eta, F]$ be a complete Y-group, we can decide the function $F : \Omega^3 \rightarrow \Omega$ from the matrix representation $[\![\eta]\!]$ of η, and F is an invariant, i.e., it is independent on the order of rows (columns) in $[\![\eta]\!]$. For any fixed element θ in Ω, we can get a normal function $\eta_\theta : N \times N_p \rightarrow \Omega$ and a normal matrix $[\![\eta]\!]_\theta = [\![\eta_\theta]\!]$.

Based on $[\![\eta_\theta]\!]$, we rewrite $F(a, \theta, b)$ as $F_\theta(a, b)$ .The function $F_\theta : \Omega^2 \rightarrow \Omega$ defines a binary operation on Ω by a block $\begin{pmatrix} \theta & b \\ a & c \end{pmatrix}$ in $[\![\eta_\theta]\!]$:$(a *_\theta b) = (a * b)_\theta = F_\theta(a, b) = c$.

If there are two blocks $\begin{pmatrix} \theta & b \\ a & c \end{pmatrix}$ and $\begin{pmatrix} \theta & a \\ b & c' \end{pmatrix}$ in $[\![\eta_\theta]\!]$ such that $c \ne c'$, then call that the operation is not exchangeable. Otherwise, the operation is exchangeable.

There are unexchangeable complete Y-groups.

Let $\chi_a^{[\![\eta]\!]}$ (resp. $\chi_a^{[\![\eta_\theta]\!]}$) be the characterization matrix of the element a from $[\![\eta]\!]$ (resp. $[\![\eta_\theta]\!]$) for any $a \in \Omega$. We get a permutation π_α on N_p from $\chi_a^{[\![\eta]\!]}$, where $Col_{\pi_a} = \chi_a^{[\![\eta]\!]}$.

We have the following relations:

(1) $[\![\eta_\theta]\!] = Row_{\pi_\theta} * [\![\eta]\!]$.

(2) $\chi_a^{[\![\eta_\theta]\!]} = Row_{\pi_\theta} * \chi_a^{[\![\eta]\!]}$ for any $a \in \Omega$.

(3) $\chi_a^{[\![\eta_\theta]\!]} * \chi_b^{[\![\eta_\theta]\!]} = \chi_c^{[\![\eta_\theta]\!]} \Leftrightarrow \chi_a^{[\![\eta]\!]} * Row_{\pi_\theta} * \chi_b^{[\![\eta]\!]} = \chi_c^{[\![\eta]\!]} \Leftrightarrow \pi_a \circ \pi_\theta^{-1} \circ \pi_b = \pi_c$.

(4) $[\![\eta]\!] = \sum_{a\in\Omega} a \cdot \chi_a^{[\![\eta]\!]}$.

V. 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 $[n] = \bigcup_{i=1}^{k} S_{\pi_i}$ 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 $B^\pi(1, :)$.

VI. Basic complete Y-groups

Let p be a natural number, e.g. p is a prime number, and denote C_p as a complete Y-group defined by a cyclic permutation on $[p] = \{1, 2, \cdots, p\}$. C_p is described in matrix of p-order. Such matrixes of form C_p are basic (or atomic) components constructing more complex complete Y-groups. In this section, we consider the classifying and operations about C_p.

Let $(a) = (a_1, a_2, \cdots, a_p)$ be a cyclic sequence of symbols associating a function $next_a$, $next_a(a_i) = a_{(i+1)(mod\ p)}$, and a set $Sym(a) = \{a_1, \cdots, a_p\}$, where p is the length of (a). For $1 \le r \le p-1$, we call that 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 $\{1, [r\ (mod\ p)] + 1, [(2r)\ (mod\ p)] + 1, \cdots, [(p-1)r\ (mod\ p)] + 1\} = \{1, 2, \cdots, p\}$. Such r is called as Euler number of p. Define a set $Euler(p) = \{r : r\ is\ a\ Euler\ number\ of\ p\}$. Clearly,

Euler(p) contains 1 for any $p \geq 2$, and if p is a prime number, then $Euler(p) = \{1, 2, \cdots, p-1\}$.

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

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

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

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

Clearly, if $(r, p) = 1$, then $\{C_{p,r}(1,1), C_{p,r}(2,1), \cdots, C_{p,r}(p,1)\} = \{1,2, \cdots, p\} = [p]$, therefore, $C_{p,r}$ is a complete Y-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 $\Omega = \{a_1, a_2, \cdots, a_p\}$ and a cyclic sequence $(a) =< a_1, a_2, \cdots, a_p >$ 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 $1 \leq i \leq p, 2 \leq j \leq p$.

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 $j = 1, 2, \cdots, p-1$, 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 $Sym(a) \cap Sym(b) = \emptyset$,$Sym(a) \cap Sym(c) = \emptyset$, 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 $(a_1), \cdots, (a_q)$ 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 a cyclic 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 $R(i, j) = r_{i,j}$.

VII. Construction of Finite Groups

For $p, q \geq 2$ and the cyclic sequence $(p) = (1,2, \cdots, p)$, we define a cyclic sequence $(p)_b = ((b-1)p + 1, (b-1)p + 2, \cdots, bp)$ for $1 \leq b \leq q$. Let R be a $q \times q$ matrix on the set *Euler(p)* of Euler number with respect to p, such that for any 2×2 block $\begin{pmatrix} r & s \\ u & v \end{pmatrix}$ in R, $rv \equiv su(mod\ p)$, it is called the diagonal congruence w.r.t. p.

We now define two products of cyclic matrixes, $C_{p,r'} \otimes C_{q,r}$ and $C_{p,1} \otimes_R C_{q,r}$, where $r' \in Euler(p)$, $r \in Euler(q)$ as follows:

(1) $C_{p,r'} \otimes C_{q,r} \coloneqq C_{p,r'} \otimes (b_{i,j})_{q\times q} = (B_{i,j})_{q\times q}$ a matrix of matrixes , which is a square matrix of pq-order, where$C_{q,r} = (b_{i,j})_{q\times q}$, $(B_{i,j})_{q\times q} = C_{p,r'}((p)_{b_{i,j}})$.

(2) $C_{p,1} \otimes_R C_{q,r} \coloneqq C_{p,1} \otimes_{(r_{i,j})_{q\times q}} (b_{i,j})_{q\times q} = (D_{i,j})_{q\times q}$, a matrix of matrixes, which is a square matrix of pq-order, where $C_{q,r} = (b_{i,j})_{q\times q}$, $(D_{i,j})_{q\times q} = C_{p,r_{i,j}}((p)_{b_{i,j}})$.

We can write the combination of $R = (r_{i,j})_{q\times q}$ and $C_{q,r} = (b_{i,j})_{q\times q}$ as a new matrix $C^R_{q,r} = (b_{i,j}|r_{i,j})_{q\times q}$.It is easy to prove that

(1) $C_{p,1} \cong C_{p,r'}$, for any $' \in Euler(p)$.

(2) $C_{p,r'} \otimes C_{q,r} \cong C_{q,r'} \otimes C_{p,r'}$ for any $r' \in Euler(p), r \in Euler(q)$.

(3) $C_{p,1} \otimes_R C_{q,r} \cong C_{p,1} \otimes_R C_{q,1}$ for any fixed R.

Thus, we conclude that for $p, q \geq 2$, classifying $C_{p,1} \otimes_R C_{q,r}$ depends only on the classification of R.

Definition 2 For $p, q \geq 2$, the matrixes R and R' are square matrixes of q-order on *Euler(p)*, satisfying the diagonal congruence w.r.t. p., we call that R, R' have the same type, denote as $R \bowtie R'$, if $C_{p,1} \otimes_R C_{q,1} \cong C_{p,1} \otimes_{R'} C_{q,1}$.

VIII. Basic Structures of Finite Groups

It is known that between complete Y-matrixes and finite groups are one-to-one. We can investigate structures of finite groups by complete Y-matrixes.

Lemma 4 (1) For any natural number $p \geq 2$, a cyclic group of p-order is isomorphic to a group defined by the complete Y-matrix $C_{p,1}$.

(2) Let G be a group of n-order ($n \geq 2$), where $n = pq$ $(p, q \geq 2)$, and both p and q are prime numbers. Then there is a matrix $R = (r_{i,j})_{q\times q}$ of row-rotations parameters, where $r_{i,j} \in Euler(p)$, such that $T_G \cong C_{p,1} \otimes_R C_{q,1}$, where T_G is the computation table of group G, and the unit element is located at the main diagonal of T_G.

Proof: (1) Let G be a cyclic group of p-order ($p \geq 2$), and let a generator of G¿ Then, $(e, a, a^2, \cdots, a^{p-1})(e = a^p)$ is a cyclic sequence of symbols, where e is the unit element of G. Clearly, the computation table of group G is isomorphic to $C_{p,1}$, and then G is isomorphic to a group defined by the complete Y-matrix $C_{p,1}$.

(2) Let G be a group of n-order ($n \geq 2$), and let p be a prime factor of n, $n = pq$ $(p, q \geq 2)$.

Then, there is an element a of p-order. We take a as a generator, and construct a cyclic group $H_1$of p-order. Without loss of generality (w.l.o.g.), we write $H_1 = \{e, a_1, \cdots, a_{p-1}\}$, where e is the unit element of G, and a_1 is the generator of H, $a_i = a_1^i (i = 1, 2, \cdots, p-1)$ and $a_1^p = e$.

Further, there are $(q-1)$ elements, $b_2, b_3, \cdots, b_q$ in G, such that

(1) $H = \{b_1 = e, b_2, \cdots, b_q\}$ is a subgroup of G.

(2) $\{H_1, \cdots, H_q\}$ is a partition of G , where $H_k = b_k H_1 = \{b_k a: a \epsilon H_1\} (k = 2, \cdots, q)$, $G = \bigcup_{k=1}^{q} H_k$ and $H_i \cap H_j = \emptyset$ for any $1 \le i \ne j \le q$ .Based on $H_1, \cdots, H_q$,we get q cyclic sequence of symbols: $(A_1) = \left(e, a_1, a_1^2, \cdots, a_1^{p-1}\right) = (a_{1,1}, a_{1,2}, \cdots, a_{1,p})$ and $(A_k) = \left(b_k,\ b_k a_1, \cdots, b_k a_1^{p-1}\right) = \left(a_{1,(k-1)p+1},\ a_{1,(k-1)p+2}, \cdots, a_{1,kp}\right) k = 2,3, \cdots, q$.

We can define a complete Y-matrix $C_{p,1}$, and normalize $C_{p,1}$ into $C_{p,p-1}$, where the unit e is located at main diagonal of $C_{p,p-1}$. Please note for each $2 \le k \le q$ that H_k has such closure property: $b_k a$, $b_k b \in H_k$ for any $a, b \in H_1$. Thus, we can get a complete Y-matrix B_k and $B_k \cong C_{p,1}$.

On the other hand, the subgroup $H = \{e, b_2, \cdots, b_q\}$ decides a CY-matrix. Since q is a prime number, the group H is a cyclic group. So, it is isomorphic to $C_{q,1}$. Take $B_1, B_2, \cdots, B_q$ as elements, one can construct a group C_q^* to be isomorphic to $C_{q,1}$, and the expansion of C_q^* is isomorphic to G. Therefore, there is a matrix $R = \left(r_{i,j}\right)_{q \times q}$ of row-rotations parameters, where $r_{i,j} \in Euler(p)$, such that $T_G \cong C_{p,1} \otimes_R C_{q,1}$, where T_G is the computation table of group G, and the unit element is located at the main diagonal of T_G.

IX. 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 "Four Endpoints Rule (FER)" is main geometric characterization of complete Y-matrixes. In this paper, we have discussed relations between the three (ordinary finite group, permutation group, and matrix group), and presented some basic structures and construction methods of finite groups. It is helpful for classifying and decomposing finite groups. The methods deal only with rotation of rows in matrixes. Further, we can consider the following method to construct finite groups.

(1) Combining rotations of rows and columns in matrixes.

(2) Combining cross rotations of rows and columns in matrixes.

Based on combination of factorization factors of natural number n and rotations, ones can construct finite groups with different structures.

Acknowledgements

The research work was supported by National Natural Science Foundation of China unNBder Grant No. 61262006, Major Applied Basic Research Program of Guizhou Province under Grant No.JZ20142001 and Science 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] J. B. Fraleigh, A First Course in Abstract Algebra, 5th Edition, Addison-Wesley (1994).

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

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

[7] S. Sternberg, Group theory and physics, Cambridge University Press (1994).

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

[9] Batten, Lynn Margaret, Combinatorics of Finite Geometries, Cambridge University Press (1997).