

**Representation theory for finite groups
in computer system "CAYLEY"**

千葉大学 自然科学研究科 脇 克志 (Katsushi WAKI)

Recently, computational methods are useful for the representation theory, and have been executed by the CAYLEY system by Cannon[1]. In this paper, we will show a usage and some applications of the CAYLEY in the representation theory.

1. Representation in CAYLEY

Let G be a finite group with a set of generators $\{g_1, \dots, g_l\}$ and F a splitting field for G such that the characteristic of F divides the group order $|G|$.

In this paper we treat the action of an element g of G on the F -vector space V as the product of a vector by a matrix $V(g)$ on the right. So we can consider the vector space V as a right FG -module for the group algebra FG . In the CAYLEY system, we treat a set $\{M(g_1), \dots, M(g_l)\}$ as a representation of FG -module V . A series of submodules of V

$$0 = V_0 < V_1 < \dots < V_n = V \quad \text{where } V_i/V_{i-1} \text{ is simple}$$

is called a composition series for an FG -module V .

2. The socle

Let $\text{Soc}(V)$ denote the socle of V , namely the sum of all simple FG -submodules of V .

LEMMA 1. *Let V be an FG -module and U an FG -submodule of V such that V/U is isomorphic to a simple FG -module W . Then the following statements are equivalent.*

- (i) *There is an FG -submodule T which is isomorphic to W and $\text{Soc}(V) = \text{Soc}(U) \oplus T$.*
- (ii) *V is isomorphic to $U \oplus W$.*

PROOF: (i) $\Rightarrow$ (ii). Since $U \cap T = \text{Soc}(U) \cap T = 0$, $U \oplus T$ is an FG -submodule of V . But the dimension of V is equal to this submodule. So $V = U \oplus T$.

(ii) $\Rightarrow$ (i). Immediate from the definition of the socle.

There is the standard function *composition factor* which is written by Schneider[3] in the CAYLEY system. From Lemma 1, we can get the socle of the FG -module V by the following algorithm.

ALGORITHM SOC:

- (1) Let get a composition series $\{V_i\}_{(i=1,\dots,n)}$ of V and *socsq* be empty.
- (2) For each i , see whether V_i is isomorphic to $V_{i-1} \oplus V_i/V_{i-1}$ or not. If V_i can split then append V_i/V_{i-1} to *socsq*.
- (3) Print *socsq* as the socle of the FG -module V .

The main part of this algorithm is investigating that V_i can split or not. Let V be an FG -module and U an FG -submodule of V such that V/U is isomorphic to a simple FG -module W . The dimension of the module U and the module W are u and w , respectively. In a good basis of V , $V(g)$ is a following matrix

$$\begin{pmatrix} U(g) & 0 \\ D(g) & W(g) \end{pmatrix} \quad \text{for each element } g \text{ of } G$$

where $D(g)$ is a $w \times u$ -matrix. Since V is an FG -module, D satisfies a following equation.

$$(*) \quad D(gg') = D(g)U(g') + W(g)D(g') \quad \text{for any } g, g' \text{ in } G$$

The module V is isomorphic to $U \oplus W$ if and only if there are some regular matrices P and

$$(1) \quad PV(g)P^{-1} = \begin{pmatrix} U(g) & 0 \\ 0 & W(g) \end{pmatrix}$$

for all elements g of G . What made it difficult is the number of unknowns which have to be processed to find the matrix P . Thus we prove the next lemma to reduce the number of unknowns.

LEMMA 2. Using the above conditions, the following statements are equivalent.

- (i) There is such a matrix P .
- (ii) There is a $w \times u$ matrix Q such that $D(g) = W(g)Q - QU(g)$ for any g in G .

By Lemma 2, it suffices to find the matrix Q instead of the matrix P . So we can reduce the number of unknowns from $(m+n)^2$ to nm and see it as the problem of basic linear algebra.

PROOF: (i) $\Rightarrow$ (ii)

$$\text{Let } P = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \quad \text{where } \begin{cases} p_1 : u \times u \text{ matrix} & p_2 : u \times w \text{ matrix} \\ p_3 : w \times u \text{ matrix} & p_4 : w \times w \text{ matrix} \end{cases}$$

Then from (1), we get the following equations for all elements g of G .

$$(2) \quad p_1 U(g) + p_2 D(g) = U(g)p_1$$

$$(3) \quad p_2 W(g) = U(g)p_2$$

$$(4) \quad p_3 U(g) + p_4 D(g) = W(g)p_3$$

$$(5) \quad p_4 W(g) = W(g)p_4$$

If matrix p_4 is regular then let Q be $p_4^{-1}p_3$. The matrix Q satisfies the condition (ii) from (4) and (5).

Since W is the simple module and we can see that p_4 is an endomorphism of FG -module W from (5).

So if the matrix p_4 is not regular then p_4 must be a zero-matrix by Schur's lemma. From the equations (3) and (4), $p_3 p_2 W(g) = W(g)p_3 p_2$. If $p_3 p_2$ is not a zero-matrix then $p_3 p_2$ is αI by Schur's lemma where α is a non-zero element of F and I is the unit matrix. The product of (2) and $\alpha^{-1}p_3$ on the left gives

$$\alpha^{-1}p_3 p_1 U(g) + D(g) = W(g)\alpha^{-1}p_3 p_1$$

by the equation (4). So Q is $\alpha^{-1}p_3 p_1$.

If $p_3 p_2$ is a zero-matrix then there is a positive integer k such that $p_3 p_1^n p_2 = 0$ ($0 \leq n \leq k$) and $p_3 p_1^{k+1} p_2 \neq 0$ and

$$(2') \quad p_1^{n+1} U(g) = U(g)p_1^{n+1} - \sum_{i=0}^n p_1^i p_2 D(g) p_1^{n-i} \quad \text{for the natural number } n$$

by the easy calculation. When $n = k$, the product of (2') and p_3 on the left gives $p_3 p_1^{k+1} U(g) = W(g) p_3 p_1^{k+1}$ by the equation (4) and $p_3 p_1^{k+1} p_2 W(g) = W(g) p_3 p_1^{k+1} p_2$ by the equation (3). We can see that $p_3 p_1^{k+1} p_2$ is αI by Schur's lemma where α is a non-zero element of F and I is the unit matrix. When $n = k + 1$, the product of (2') and $\alpha^{-1} p_3$ on the left gives

$$\alpha^{-1} p_3 p_1^{k+2} U(g) = W(g) \alpha^{-1} p_3 p_1^{k+2} - D(g)$$

by the equation (4). So Q is $\alpha^{-1} p_3 p_1^{k+2}$.

(ii) $\Rightarrow$ (i)

Let $P = \begin{pmatrix} I_m & 0 \\ Q & I_n \end{pmatrix}$ where I_m and I_n are the m and n -dimensional unit matrix.

Then the matrix P satisfies the equation (1).

By the way, let think about a $w \times u$ -matrix $D(g)$. Let $F^{w \times u}$ be a set of $w \times u$ -matrices over F , $E(W, U)$ a set of map D from G to $F^{w \times u}$ which is satisfies (*) and $e(W, U)$ a set of map D_Q such that $D_Q(g) = W(g)Q - QU(g)$ where Q is a $w \times u$ -matrix. Then $E(W, U)$ is an F -space and $e(W, U)$ an F -subspace of $E(W, U)$. And $E(W, U)/e(W, U)$ is isomorphic to $\text{Ext}_{FG}^1(W, U)$ as F -space. So we can compute the dimension of $\text{Ext}_{FG}^1(W, U)$ from this equation. In particular, $E(W, U)$ and $e(W, U)$ are $Z^1(G, U)$ and $B^1(G, U)$ respectively if W is the trivial module.

3. $\Omega^{-1}(M)$

Suppose G is p -group. Using $E(W, U)$, we can construct the Heller module $\Omega^{-1}(M)$ of an FG -module M . Let $\bar{E}(M)$ denote $E(\mathbf{F}, M)/e(\mathbf{F}, M)$ where $\mathbf{F}$ is the trivial FG -module and $\{\bar{d}_i^1\}$ ($1 \leq i \leq m_1$) an F -basis of $\bar{E}(M)$. Then we can make a following representation

$$M_1(g) = \begin{pmatrix} M(g) & & 0 \\ d_1^1(g) & 1 & \\ \vdots & & \ddots \\ d_{m_1}^1(g) & & & 1 \end{pmatrix}$$

where the FG -module M_1 has M as a submodule of M_1 and M_1/M is isomorphic to m_1 copies of the trivial module $\mathbf{F}$. Moreover $\text{Soc}(M) \simeq \text{Soc}(M_1)$. By the same process, we can make FG -module M_2 such that M_2 has M_1 as a submodule and M_2/M_1 is isomorphic

to $m_2(= \dim_F \bar{E}(M_1))$ copies of the trivial module $\mathbf{F}$ and $\text{soc}(M_1) \simeq \text{Soc}(M_2)$. So if we continue this process, then we get

$$M_k(g) = \begin{pmatrix} M(g) & & & & \\ d_1^1(g) & 1 & & 0 & \\ \vdots & & \ddots & & \\ d_{m_1}^1(g) & 0 & & 1 & \\ & d_1^2(g) & & & 1 \\ & \vdots & & \ddots & \\ & d_{m_k}^k(g) & & & 1 \end{pmatrix}$$

as the injective hull of M . And it's easy to calculate $\Omega^{-1}(M) = M_k/M$.

4. Example

Let $G = \langle x, y, z | x^3 = y^3 = z^3 = (x, z) = (y, z) = 1, (x, y) = z \rangle$ and $F = GF(3)$ then G is the extra-special 3-group, $|G| = 27$ and

M	the dimension of M	the dimension of the socle series of M
FG	27	(1, 2, 4, 4, 5, 4, 4, 2, 1)
$\Omega^{-1}(\mathbf{F})$	26	(2, 3, 3, 5, 4, 4, 2, 1)
$\Omega^{-2}(\mathbf{F})$	28	(4, 4, 6, 3, 6, 3, 2)
$\Omega^{-3}(\mathbf{F})$	80	(6, 9, 14, 13, 14, 12, 8, 4)
$\Omega^{-4}(\mathbf{F})$	82	(7, 10, 16, 12, 15, ...)

REFERENCES

1. Cannon, J.J. (1984), *An introduction to the group theory language CAYLEY*, In: (Atkinson, M., ed) Computational Group Theory. London: Academic Press, 145–183.
2. Landrock, P. (1983), *Finite group algebras and their modules*, London Mathematical Society Lecture Notes 84. Cambridge: Cambridge University Press.
3. Schneider, G.J.A. (1987), *Representation theory in Cayley*, The CAYLEY Bulletin 3.