Hanaki, A. and Okuyama, T.
Osaka J. Math.
34 (1997), 337–356

GROUPS WITH SOME COMBINATORIAL PROPERTIES

AKIHIDE HANAKI and TETSURO OKUYAMA

(Received July 28, 1995)

1. Introduction

In [1], E. Bannai introduced the concept of fusion algebras at an algebraic level, a purely algebraic concept for fusion algebras in mathematical physics. He showed that there exists a one-to-one correspondence between character algebras (Bose-Mesner algebras at algebraic level) and fusion algebras at an algebraic level. The concept of character algebras is a purely algebraic concept for Bose-Mesner algebras of association schemes.

For any commutative association scheme, a character algebra and the corresponding fusion algebra at algebraic level are constructed. But this fusion algebra at an algebraic level is far from a fusion algebra in mathematical physics. A fusion algebra in mathematical physics is integral, its matrix S is symmetric (and unitary), and it has the modular invariance property. But these are not true for fusion algebras at an algebraic level. So he asked which fusion algebra at an algebraic level have these properties.

In this paper, we construct some p-groups and check the properties of their group association schemes. For our groups, the fusion algebras are integral and S is unitary but not necessary symmetric. Section 4 is a generalization of [2].

2. Fusion algebras at an algebraic level and character algebras

For the definitions of fusion algebras and character algebras, we refer to [1, Definition 1.1 and 2.5].

Theorem 2.1 [1, Theorem 3.1]. *There exists a natural one-to-one correspondence between fusion algebras at an algebraic level and character algebras.*

The correspondence in Theorem 2.1 is the following. Let $\tilde{\mathfrak{A}} = \langle y_0, y_1, \cdots, y_d \rangle$ be a character algebra with basis $y_0, y_1, \cdots, y_d$ and the multiplication

$$y_i y_j = \sum_{k=0}^{d} p_{ij}^k y_k.$$

Define

$$N_{ij}^k = \sqrt{\frac{k_i k_j}{k_k}} p_{ij}^k,$$

where k_i is as in [1, Definition 2.5], and let $\mathfrak{A} = \langle x_0, x_1, \cdots, x_d \rangle$ be the algebra with basis $x_0, x_1, \cdots, x_d$ and the multiplication

$$x_i x_j = \sum_{k=0}^{d} N_{ij}^k x_k.$$

Then $\mathfrak{A} = \langle x_0, x_1, \cdots, x_d \rangle$ becomes a fusion algebra at an algebraic level. When all N_{ij}^k are non-negative integers, we call $\mathfrak{A}$ *integral.*

Now we consider a finite group G. The character algebra (Bose-Mesner algebra) of the group association scheme of G can be identified with the center of the group algebra over the complex number field. The basis of the character algebra is $\{\widehat{C_0}, \widehat{C_1}, \cdots, \widehat{C_d}\}$, where $\mathrm{Cl}(G) = \{C_0, C_1, \cdots, C_d\}$ and $\widehat{C_i} = \sum_{g \in C_i} g$.

Put

$$\widehat{C_i}\widehat{C_j} = \sum_{k=0}^{d} t_{ij}^k \widehat{C_k}.$$

In this case, $k_i = |C_i|$, so the structure constant of the corresponding fusion algebra at an algebraic level is

$$N_{ij}^k = \sqrt{|C_w|/(|C_u||C_v|)}\; t_{ij}^k.$$

Let $\mathrm{Irr}(G) = \{\chi_0, \chi_1, \cdots, \chi_d\}$, and let e_i be the central primitive idempotent corresponding to χ_i. Then $\{e_0, e_1, \cdots, e_d\}$ is also a basis for the character algebra. Thus there exist non-singular matrices $P = (p_{ij})_{0 \le i,j \le d}$, $Q = (q_{ij})_{0 \le i,j \le d}$ such that

$$\begin{aligned}(\widehat{C_0}, \widehat{C_1}, \cdots, \widehat{C_d}) &= (e_0, e_1, \cdots, e_d)P, \\ (|G|e_0, |G|e_1, \cdots, |G|e_d) &= (\widehat{C_0}, \widehat{C_1}, \cdots, \widehat{C_d})Q.\end{aligned}$$

It is easy to see that

$$\begin{aligned} p_{ij} &= \frac{|G|\chi_i(x_j)}{|\mathrm{C}_G(x_j)|\chi_i(1)}, \\ q_{ij} &= \chi_j(1)\overline{\chi_j(x_i)}. \end{aligned}$$

A matrix S is determined from a fusion algebra at an algebraic level [1, Theorem in §4]. In mathematical physics, S is always unitary and symmetric (if S is symmetric, then S is unitary). But this is not true for fusion algebras at an algebraic level.

For group case, it is shown in [1, §5] that S is unitary if and only if the lengths of conjugacy classes and the squares of the degrees of irreducible characters of G coincide with the multiplicity, and S is symmetric if and only if $P = \overline{Q}$. So we discuss these conditions in the following sections. If S is symmetric we call the group *self dual.*

In the rest of this paper, S shall denote the matrix obtained from G in this way.

3. Construction of groups and some properties

Throughout this paper, we use the following notation.

Let q be a prime power, s and l be positive integers, and θ be a generator of the Galois group of $\mathrm{GF}(q^s)$ over $\mathrm{GF}(q)$. We define

$$G = \{u(a_1, a_2, \cdots, a_l) \ ; \ a_i \in \mathrm{GF}(q^s)\}.$$

We write an element $u(a_1, a_2, \cdots, a_l)$ of G by $u(a_i)$ to simplify our description. We define the multiplication in G by $u(a_i)u(b_i) = u(c_i)$, where

$$c_i = a_i + \sum_{j=1}^{i-1} a_{i-j}^{\theta^j} b_j + b_i.$$

Then G is a group. Note that

$$u(a_1, a_2, \cdots, a_l) = \begin{pmatrix} 1 & & & & & \\ a_1 & 1 & & & \mathbf{0} & \\ a_2 & a_1^{\theta} & 1 & & & \\ a_3 & a_2^{\theta} & a_1^{\theta^2} & 1 & & \\ \cdots & \cdots & \cdots & \cdots & \ddots & \\ a_l & a_{l-1}^{\theta} & a_{l-2}^{\theta^2} & \cdots & a_1^{\theta^{l-1}} & 1 \end{pmatrix}$$

with the usual matrix multiplication.

We regard θ as an automorphism of G by $u(a_i)^{\theta} = u(a_i^{\theta})$. We also regard $\lambda \in \mathrm{GF}(q^s)^{\times}$ as an automorphism of G by $u(a_i)^{\lambda} = u(\lambda^{(i)} a_i)$, where $\lambda^{(i)} = \prod_{j=0}^{i-1} \lambda^{\theta^j}$.

We define some subgroups of G as follows:

$$\begin{aligned} G_k &= \{u(a_i) \in G \ ; \ a_i = 0, \quad \text{for } i < k\} \quad \text{for } 1 \le k \le l+1, \\ H &= \{u(e_i) \in G \ ; \ e_i \in \mathrm{GF}(q)\}, \\ H_k &= G_k \cap H. \end{aligned}$$

Then obviously, $G_1 = G$, $G_{l+1} = 1$, $|G_k| = q^{s(l+1-k)}$, and $H = C_G(\theta)$ and abelian.

We assume the following:

HYPOTHESIS. (1) s is odd, and l is less than the least prime divisor of s.
(2) $(s, q) = 1$.
(3) $(s, q-1) = 1$.

Let $\mathrm{Tr} : \mathrm{GF}(q^s) \to \mathrm{GF}(q)$ and $\mathrm{Norm} : \mathrm{GF}(q^s)^\times \to \mathrm{GF}(q)^\times$ be the usual trace map and the norm map, respectively.

Lemma 3.1. (1) Ker Tr *is an* $(s-1)$*-dimensional* $\mathrm{GF}(q)$*-subspace of* $\mathrm{GF}(q^s)$. *For* $a \in \mathrm{GF}(q^s)^\times$, a Ker Tr $=$ Ker Tr *if and only if* $a \in \mathrm{GF}(q)^\times$.
In particular, a Ker Tr $+$ Ker Tr $= \mathrm{GF}(q^s)$ *for any* $a \notin \mathrm{GF}(q)^\times$, $a \neq 0$.
(2) *For* $1 \leq i \leq l$, $a^{\theta^i} = a$ *if and only if* $a \in \mathrm{GF}(q)$.
(3) $\mathrm{GF}(q^s) = \mathrm{GF}(q) \oplus \mathrm{Ker\ Tr}$.
(4) $\mathrm{GF}(q^s)^\times = \mathrm{GF}(q)^\times \times \mathrm{Ker\ Norm}$. *For* $1 \leq i \leq l$ *and* $\lambda \in \mathrm{Ker\ Norm}$, $\lambda^{(i)} = 1$ *if and only if* $\lambda = 1$.

Proof. (1) This holds in general and is easy to prove.
(2) By Hypothesis (1), $\langle \theta^i \rangle = \langle \theta \rangle$.
(3) By Hypothesis (2), $\mathrm{GF}(q^s) = \mathrm{GF}(q) \oplus \mathrm{Ker\ Tr}$.
(4) By Hypothesis (3), $a \notin$ Ker Tr for $a \in \mathrm{GF}(q)^\times - \{1\}$. Thus $\mathrm{GF}(q^s)^\times = \mathrm{GF}(q)^\times \times \mathrm{Ker\ Norm}$. We assume $\lambda \in \mathrm{Ker\ Norm}$ and $\lambda^{(i)} = 1$. By the definition of $\lambda^{(i)}$,

$$(\lambda^{(i)})^\theta (\lambda^{(i)})^{-1} = \lambda^{\theta^i} \lambda^{-1} = 1.$$

So $\lambda^{\theta^i} = \lambda$. Thus $\lambda \in \mathrm{GF}(q)^\times \cap \mathrm{Ker\ Norm} = 1$, by (2). □

For $x = u(a_1, \cdots, a_l) \in G$, we write the i-th entry a_i by x_i.

Lemma 3.2. (1) *Assume* $x \in G_i$, $y \in G_j$, $x_i = a$, $y_j = b$, *and* $i + j = l$. *Then*

$$[x, y]_k = 0, \qquad \textit{for } k < l, \textit{ and}$$
$$[x, y]_l = a^{\theta^j} b - a b^{\theta^i}.$$

(2) *With the assumption of* (1), *suppose* $a \neq 0$. *Then* $a^{\theta^j} b - a b^{\theta^i} = d(cb - (cb)^{\theta^i})$, *and*

$$\{a^{\theta^j} b - a b^{\theta^i} \ ; \ b \in \mathrm{GF}(q^s)\} = d \ \mathrm{Ker\ Tr},$$

where t *is given by Hypothesis* (1) *such that* $1 \leq t \leq s-1$, $\theta^j = \theta^{it}$ *and*

$$d = \prod_{k=0}^{t} a^{\theta^{ik}}, \qquad c = \left(\prod_{k=0}^{t-1} a^{\theta^{ik}} \right)^{-1}.$$

Moreover $a \in \mathrm{GF}(q)$ *if and only if* $d \in \mathrm{GF}(q)$.

Proof. (1) We have

$$\begin{aligned}(xy)_k &= (yx)_k, \qquad \text{for } k < l,\\ (xy)_l &- (yx)_l = a^{\theta^j} b - a b^{\theta^i}.\end{aligned}$$

Thus $xy = yxu$, where $u = u(0, \cdots, 0, a^{\theta^j} b - a b^{\theta^i})$.

(2) The equation in (2) holds as $dc = a^{\theta^{it}} = a^{\theta^j}$ and $dc^{\theta^i} = a^{\theta^0} = a$. So

$$\{a^{\theta^j} b - a b^{\theta^i} \ ; \ b \in \mathrm{GF}(q^s)\} = d \ \mathrm{Ker\ Tr}.$$

Assume $d \in \mathrm{GF}(q)$. Then $d^{\theta^i} = d$ and $a^{\theta^{i(t+1)}} = a$. Thus $a^{\theta^l} = a$. By Hypothesis (1), $a \in \mathrm{GF}(q)$. □

REMARK. G/G_{i+j-1} is isomorphic to a group defined by $(i+j)$ instead of l. Thus if $i + j < l$, Lemma 3.2 holds with l replaced by $i + j$.

Lemma 3.3. (1) $[G_i, G_j] = G_{i+j}$ *if* $i + j \leq l$ *and* $[G_i, G_j] = 1$ *if* $i + j > l$. *In particular,* G_m *is abelian if and only if* $2m \geq l + 1$.

(2) *If* $2m \geq l + 1$,

$$\begin{aligned}G_m &= H_m \times [G_m, \theta],\\ [G_m, \theta] &= \{u(a_i) \in G_m \ ; \ a_i \in \mathrm{Ker\ Tr}\}.\end{aligned}$$

Proof. (1) If $i + j > l$, then obviously $[G_i, G_j] = 1$. If $i + j = l$, then $[G_i, G_j] = G_l$ by Lemma 3.1 (1) and Lemma 3.2. In general, the result follows by induction on $l - (i + j)$ and Lemma 3.2 (and its Remark).

(2) Let $2m \geq l + 1$. Then G_m is abelian. By Hypothesis (2), $G_m = C_G(\theta) \times [G_m, \theta]$. For $u(a_i) \in G_m$, $u(a_i)^{-1} = u(-a_i)$. Thus we get the presentation of $[G_m, \theta]$. □

Lemma 3.4. (1) $C_G(u) = HG_{l+1-i}$ *for* $u \in H_i \setminus H_{i+1}$, $1 \leq i \leq l$.

(2) *Assume* $2m \geq l + 1$, $m \leq l$, $\sigma \in \mathrm{Irr}(H_m)$, *and* $\sigma_{H_l} \neq 1$. *By Lemma* 3.3 (2), *we can see*

$$\sigma \in \mathrm{Irr}(H_m) = \mathrm{Irr}(G_m/[G_m, \theta]) \subset \mathrm{Irr}(G_m).$$

Then $[G_m, \theta]^x [G_m, \theta] \supset G_l$, *for* $x \notin HG_{l+1-m}$.

In particular, $\mathrm{I}_G(\sigma) = HG_{l+1-m}$, *where* $\mathrm{I}_G(\sigma)$ *is the inertia group of* σ *in* G.

Proof. (1) Assume $y \in G_j$, $y \in \mathrm{C}_G(u)$, and $i+j \leq l$. We put $u_i = e \in \mathrm{GF}(q)$ and $y_j = b \in \mathrm{GF}(q^s)$. Then $0 = [u,y]_{i+j} = e(b - b^{\theta^i})$ by Lemma 3.2 (1). Thus $b \in \mathrm{GF}(q)$ and $y \in HG_{j+1}$. As $H \subset \mathrm{C}_G(u)$, we can repeat this argument to get the result.

(2) HG_{l+1-m} normalizes $[G_m, \theta]$. So we may assume that there exists a positive integer i such that $x \in G_i$, $x_i = a \notin \mathrm{GF}(q)$, and $i + m \leq l$. Then $m \leq l - i$, and $[G_{l-i}, \theta] \subset [G_m, \theta]$. So

$$[G_m, \theta]^x [G_m, \theta] \supset [[G_{l-i}, \theta], x][G_l, \theta].$$

By Lemma 3.2 the set of l-th entries of elements of $[[G_{l-i}, \theta], x] \subset G_l$ is $\{ab^{\theta^i} - a^{\theta^j} b\ ;\ b \in \mathrm{Ker\ Tr}\}$, where $j = l - i$. We have

$$\begin{aligned}\{ab^{\theta^i} - a^{\theta^j} b\ ;\ b \in \mathrm{Ker\ Tr}\} + \mathrm{Ker\ Tr} &= \{ab^{\theta^i} - a^{\theta^j} b\ ;\ b \in \mathrm{GF}(q^s)\} + \mathrm{Ker\ Tr} \\ &= d\ \mathrm{Ker\ Tr} + \mathrm{Ker\ Tr} = \mathrm{GF}(q^s),\end{aligned}$$

where d is the element defined in Lemma 3.2 (2). Thus $[[G_{l-i}, \theta], x][G_l, \theta] \supset G_l$ and $[G_m, \theta]^x [G_m, \theta] \supset G_l$.

As $\sigma_{H_l} \neq 1$, $x \notin \mathrm{I}_G(\sigma)$ and thus $\mathrm{I}_G(\sigma) \subset HG_{l+1-m}$. It is easy to see that $\mathrm{I}_G(\sigma) \supset HG_{l+1-m}$ □

Lemma 3.5. (1) *If* $u \in H$ *and* $[u, x] \in_G H$, *then* $[u, x] = 1$.

(2) *If* $u \in H_i \setminus H_{i+1}$ *and* $2k + i \geq l+1$, *then* $[u, G_k] = [G_{k+i}, \theta]$. *In particular, if* $[u, x] \in G_l$, *then* $[u, x] \in [G_l, \theta]$.

Proof. (1) Assume $u \in H_i \setminus H_{i+1}$ and $u_i = e \in \mathrm{GF}(q)^\times$. For $x \notin \mathrm{C}_G(u) = HG_{l+1-i}$, we shall show $[u, x] \notin_G H$. We may assume $x \in G_j$, $i + j \leq l$, and $x_j = a \notin \mathrm{GF}(q)$. Then $[u, x] \in G_{i+j}$ and $[u, x]_{i+j} = e(a - a^{\theta^i})$ by Lemma 3.2. Suppose $[u, x] \in_G H$. Then $[u, x]_{i+j} \in \mathrm{GF}(q)$, and $a - a^{\theta^i} \in \mathrm{GF}(q) \cap \mathrm{Ker\ Tr} = 0$. Thus $a = a^{\theta^i}$ and so $a \in \mathrm{GF}(q)$. This is a contradiction.

(2) In general, we have $[u, xy] = [u, y][u, x][[u, x], y]$.

If x, $y \in G_k$, then $[u, x] \in G_{k+i}$ and $[[u, x], y] \in G_{2k+i} = 1$. G_{k+i} is abelian since $2(k+i) \geq l+1$. Thus

$$[u, G_k] = \{[u, x]\ ;\ x \in G_k\} \subset G_{k+i}.$$

As $u^\theta = u$, $[u, G_k]$ is θ-invariant and $[u, G_k] \cap H = 1$ by (1). Hence $[u, G_k] \subset [G_{k+i}, \theta]$.

If $k + i \geq l + 1$, then $[u, G_k] = [G_{k+i}, \theta] = 1$. Assume $k + i \leq l$. Then

$$\begin{aligned}|[u, G_k]| &= |G_k : \mathrm{C}_{G_k}(u)| \\ &= |G_k : H_k G_{l+1-i}| \\ &= q^{(s-1)(l+1-i-k)}\end{aligned}$$

and

$$|[G_{k+i},\theta]| = q^{(s-1)(l+1-i-k)}.$$

So $[u, G_k] = [G_{k+i}, \theta]$.

When $[u, x] \in G_l$, we apply Lemma 3.4 (1) to G/G_l and we get $x \in HG_{l-i}$. If $i = l$, then $[u, x] = 1$. If $i < l$ then, $[u, x] \in [G_l, \theta]$ by applying the above argument to $k = l - i$. □

In order to calculate the values of the irreducible characters of G we will need some properties of a certain quadratic form over $\mathrm{GF}(q)$. For the rest of this section, let V be an n-dimensional vector space over $\mathrm{GF}(q)$ and let $f : V \to \mathrm{GF}(q)$ be a quadratic form with the symmetric bilinear form $g : V \times V \to \mathrm{GF}(q)$. Namely

$$f(\lambda x + \mu y) = \lambda^2 f(x) + \mu^2 f(y) + \lambda\mu g(x, y)$$

for x, $y \in V$ and λ, $\mu \in \mathrm{GF}(q)$. For the following facts, we shall refer to [4, Chap.6, §2].

Assume f is non-degenerate and n is even. Put $n = 2n_0$. There exists a basis $\{v_1, v_2, \cdots, v_n\}$ for V such that for $x = \sum_{i=1}^{n} \lambda_i v_i$, $\lambda_i \in \mathrm{GF}(q)$, one of the following holds.

(1) $f(x) = \sum_{i=1}^{n_0} \lambda_i \lambda_{i+n_0}$.

(−1) When q is even, $f(x) = \sum_{i=1}^{n_0-1} \lambda_i \lambda_{i+n_0-1} + \lambda_{n-1}^2 + \lambda_{n-1}\lambda_n + \alpha\lambda_n^2$, where $t^2 + t + \alpha \in \mathrm{GF}(q)[t]$ is irreducible.
When q is odd, $f(x) = \sum_{i=1}^{n_0-1} \lambda_i \lambda_{i+n_0-1} + \lambda_{n-1}^2 - \alpha\lambda_n^2$, where $t^2 - \alpha \in \mathrm{GF}(q)[t]$ is irreducible.

Then, for (ε), $\varepsilon = \pm 1$, and $a \in \mathrm{GF}(q)^\times$, we have

$$\begin{aligned} \sharp\{x \in V \ ; \ f(x) = 0\} &= (q^{n_0} - \varepsilon)q^{n_0-1} + \varepsilon q^{n_0}, \\ \sharp\{x \in V \ ; \ f(x) = a\} &= (q^{n_0} - \varepsilon)q^{n_0-1}. \end{aligned}$$

For a θ-invariant $\mathrm{GF}(q)$-subspace U of $\mathrm{GF}(q^s)$, let $[U, \theta] = \{u^\tau - u \ ; \ u \in U, \tau \in \langle\theta\rangle\}$. Then for the trace map $\mathrm{Tr} : \mathrm{GF}(q^s) \to \mathrm{GF}(q)$,

$$\mathrm{Ker}\ \mathrm{Tr} = [\mathrm{GF}(q^s), \theta].$$

Let $l > m > k > 0$ such that $m + k = l$, and put $m - k = i$. We define $f : [\mathrm{GF}(q^s), \theta] \to \mathrm{GF}(q)$ by

$$f(a) = \mathrm{Tr}((a^{\theta^k} - a^{\theta^m})a),$$

and $g : [\mathrm{GF}(q^s), \theta] \times [\mathrm{GF}(q^s), \theta] \to \mathrm{GF}(q)$ by

$$g(a, b) = \mathrm{Tr}((a^{\theta^k} - a^{\theta^m})b + (b^{\theta^k} - b^{\theta^m})a).$$

Then f is a quadratic form and g is the corresponding symmetric bilinear form. We have

$$\begin{aligned} g(a,b) &= \mathrm{Tr}((a-a^{\theta^i})^{\theta^k}b+(b^{\theta^k}a)^{\theta^i}-b^{\theta^m}a) \\ &= \mathrm{Tr}((a-a^{\theta^i})^{\theta^k}b-(a-a^{\theta^i})b^{\theta^m}), \end{aligned}$$

and

$$\{a-a^\theta\ ;\ a\in[\mathrm{GF}(q^s),\theta]\}=[\mathrm{GF}(q^s),\theta].$$

So if $g(a,b)=0$ for all $a\in[\mathrm{GF}(q^s),\theta]$ then $b\in\mathrm{GF}(q)\cap[\mathrm{GF}(q^s),\theta]=0$ by Lemma 3.2 (2). Thus g is non-degenerate and so is f.

Note that $\dim_{\mathrm{GF}(q)}[\mathrm{GF}(q^s),\theta]=s-1$ is even. We want to determine which of the cases (1), (-1) hold for $(f,[\mathrm{GF}(q^s),\theta])$.

Put $s=t^2r_1\cdots r_n$, where r_i's are distinct primes. We define $\varepsilon_i=\pm1$, $i=1,2,\cdots,n$, by $q^{(r_i-1)/2}\equiv\varepsilon_i \pmod{r_i}$, and define $\varepsilon_s=\prod_{i=1}^n\varepsilon_i$. If s is square then we define $\varepsilon_s=1$.

Lemma 3.6. *For $(f,[\mathrm{GF}(q^s),\theta])$, (ε_s) is independent of k and m.*

Proof. Assume that the case (ε) occurs for $(f,[\mathrm{GF}(q^s),\theta])$. Note that f and g are θ-invariant, namely $f(a^\theta)=f(a)$ and $g(a^\theta,b^\theta)=g(a,b)$.

First, we assume that $s=r^c$, where r is a prime. Then r is odd by our assumption. Since θ has no fixed point on $[\mathrm{GF}(q^s),\theta]\setminus\{0\}$, r divides the length of any $\langle\theta\rangle$-orbit on it. Thus for $a\in\mathrm{GF}(q)^\times$,

$$\sharp\{x\in V\ ;\ f(x)=a\}=(q^{(s-1)/2}-\varepsilon)q^{(s-1)/2-1}\equiv 0 \pmod r.$$

Thus $q^{(s-1)/2}\equiv\varepsilon \pmod r$.

Note that $s-1=r^c-1=(r^c-1)/(r-1)\cdot(r-1)$.

If x is even, then $(r^c-1)/(r-1)$ is also even and $(s-1)/2$ is a multiple of $r-1$. So $q^{(s-1)/2}\equiv1 \pmod r$ and $\varepsilon=1$.

If x is odd, then $(r^c-1)/(r-1)$ is also odd and $q^{(s-1)/2}\equiv q^{(r-1)/2} \pmod r$. Thus $\varepsilon\equiv q^{(r-1)/2} \pmod r$. Therefore $\varepsilon=\varepsilon_s$.

Now, in general, we assume $s=r^cu$, where r is a prime and $(r,u)=1$. We put $\theta_1=\theta^{r^c}$, $\theta_2=\theta^u$. By the action of θ_1 on $[\mathrm{GF}(q^s),\theta]$, we have

$$\begin{aligned} [\mathrm{GF}(q^s),\theta] &= ([\mathrm{GF}(q^s),\theta]\cap\mathrm{GF}(q^{r^c}))\oplus[[\mathrm{GF}(q^s),\theta],\theta_1] \\ &= [\mathrm{GF}(q^{r^c}),\theta_2]\oplus[\mathrm{GF}(q^s),\theta_1]. \end{aligned}$$

By the action of θ_2 on $[\mathrm{GF}(q^s),\theta_1]$, we have

$$\begin{aligned} [\mathrm{GF}(q^s),\theta_1] &= ([\mathrm{GF}(q^s),\theta_1]\cap\mathrm{GF}(q^u))\oplus[[\mathrm{GF}(q^s),\theta_1],\theta_2] \\ &= [\mathrm{GF}(q^u),\theta_1]\oplus[[\mathrm{GF}(q^s),\theta_1],\theta_2]. \end{aligned}$$

Thus $[\mathrm{GF}(q^s),\theta] = [\mathrm{GF}(q^{r^c}),\theta_2] \oplus [\mathrm{GF}(q^u),\theta_1] \oplus [[\mathrm{GF}(q^s),\theta_1],\theta_2]$. This is an orthogonal decomposition for g since g is θ-invariant and $(s,q)=1$, and the restriction of f to each component is non-degenerate.

Put $W = [[\mathrm{GF}(q^s),\theta_1],\theta_2]$. Then $\dim W = (r^c-1)(u-1)$. θ_2 acts on W and has no fixed point on $W \setminus \{0\}$. As $|\theta_2| = r^c$, by the same argument as above, if (ε_W) occurs for (f,W) then $\varepsilon_W \equiv q^{(r^c-1)(u-1)/2} \equiv 1 \pmod r$ and $\varepsilon_W = 1$.

This argument can be applied to any non-degenerate θ-invariant f and g. (ε_{r^c}) occurs on the first component and (ε_u) occurs on the second component by induction. Thus $\varepsilon_{r^c}\varepsilon_u\varepsilon_W = \varepsilon_s$ occurs on $[\mathrm{GF}(q^s),\theta]$. The proof is complete. □

4. Conjugacy classes and irreducible characters

In this section we determine the conjugacy classes and the irreducible characters of G.

Theorem 4.1. $\{1\} \cup \{u(e_i)^\lambda \ ; \ u(e_i) \in H \setminus \{1\}, \lambda \in \mathrm{Ker\ Norm}\}$ *is a complete set of representatives of the conjugacy classes of* G.

Proof. Assume $u(e_i)^\lambda =_G u(f_i)^\mu$, where $u(e_i), u(f_i) \in H \setminus \{1\}$ and $\lambda, \mu \in$ Ker Norm. If $u(e_i) \in H_k \setminus H_{k+1}$, then $u(f_i) \in H_k \setminus H_{k+1}$ and $(\lambda\mu^{-1})^{(k)} e_k = f_k \neq 0$. Thus $(\lambda\mu^{-1})^{(k)} \in \mathrm{GF}(q)^\times \cap \mathrm{Ker\ Norm} = 1$. By Lemma 3.1 (4), $\lambda = \mu$. Now $u(e_i) = u(f_i)$ by Lemma 3.5 (1).

The set in the theorem is a subset of the representatives of conjugacy classes. Consider the sum of their lengths,

$$\begin{aligned}
1 + \frac{q^s-1}{q-1} \sum_{u \in H\setminus\{1\}} |G : \mathrm{C}_G(u)| &= 1 + \frac{q^s-1}{q-1} \sum_{i=1}^{l} |G : HG_{l+1-i}||H_i \setminus H_{i+1}| \\
&= 1 + \frac{q^s-1}{q-1} \sum_{i=1}^{l} q^{(s-1)(l-i)}(q^{l+1-i} - q^{l-i}) \\
&= 1 + (q^s-1) \sum_{i=1}^{l} q^{s(l-i)} \\
&= 1 + (q^{sl}-1) = q^{sl} = |G|.
\end{aligned}$$

(We used Lemma 3.4 (1) in the first equation.) The result follows. □

Corollary 4.2. *There exist* $(q^s-1)q^{l-i}$ *conjugacy classes of size* $q^{(s-1)(l-i)}$ *for* $1 \le i \le l-1$ *and* q^s *conjugacy classes of size* 1.

We need some terminology from character theory. Let K be an arbitrary finite group, $Z \lhd K$ and let $\rho \in \mathrm{Irr}(Z)$ be linear and K-invariant. We call $x \in K$ *ρ-special* if $[x,g] \in Z$ implies $[x,g] \in \mathrm{Ker}\,\rho$ for $g \in K$. If $y \in K$ is not ρ-special, then $\chi(y) = 0$ for any $\chi \in \mathrm{Irr}(K|\rho)$ (See [3, Chap.11]).

For $\rho \in \mathrm{Irr}(H_l)$, we can regard $\rho \in \mathrm{Irr}(G_l)$ since $G_l = H_l \times [G_l, \theta]$. We assume $\rho \neq 1$ in the following.

Lemma 4.3. *If $x \in G$ is ρ-special then $x \in_G H$ or $x \in G_l$.*

Proof. Assume $x \notin G_l$. By Theorem 4.1, $x =_G u^\lambda$ for some $u \in H_i \setminus H_{i+1}$, $i \leq l-1$, and $\lambda \in \mathrm{GF}(q^s)^\times$, Norm $\lambda = 1$. Since x is ρ-special, so is u^λ. By Lemma 3.5 (2), $[u^\lambda, G_{l-i}] = [u, G_{l-i}]^\lambda = [G_l, \theta]^\lambda$. Assume $\lambda \neq 1$. Then $\lambda^{(l)} \neq 1$ by Lemma 3.1 (1) and $\lambda^{(l)}\mathrm{Ker}\,\mathrm{Tr} + \mathrm{Ker}\,\mathrm{Tr} = \mathrm{GF}(q^s)$ by Lemma 3.3 (2). Thus $[G_l,\theta]^\lambda [G_l,\theta] = G_l$. This contradicts the fact that $\rho \neq 1$. So $\lambda = 1$ and $x =_G u \in H$. □

Lemma 4.4. *For $\chi \in \mathrm{Irr}(G|\rho)$, $\chi(1) = q^{(s-1)(l-1)/2}$ and $|\chi(u)|^2 = q^{(s-1)i}$ for $u \in H_i \setminus H_{i+1}$, $i \leq l-1$.*

Proof. For $u \in G$ we denote the conjugacy class of G containing u by C_u. If $(u^{-1})^x u^y \in_G HG_l$, then $u^{-1}u^{yx^{-1}} \in_G HG_l$, namely $[u, yx^{-1}] \in_G HG_l$. Then $[u, yx^{-1}] \in G_l$ by Lemma 3.5 (1). By Lemma 3.4 (1), $yx^{-1} \in HG_{l-i}$, and by Lemma 3.5 (2), $[u, yx^{-1}] \in [G_l, \theta]$. Thus

$$\widehat{C_{u^{-1}}}\widehat{C_u} = |G : \mathrm{C}_G(u)|\widehat{[G_l,\theta]} + (\text{non } \rho\text{-special conjugacy class sums}).$$

We consider the value of χ of this equation and we have

$$|G : \mathrm{C}_G(u)|^2 |\chi(u)|^2/\chi(1)^2 = |G : \mathrm{C}_G(u)| q^{s-1}.$$

Thus

$$|G : \mathrm{C}_G(u)||\chi(u)|^2 = q^{s-1}\chi(1)^2.$$

By Lemma 4.3,

$$\begin{aligned} q^{sl} = |G| &= \sum_{x \in G} |\chi(x)|^2 \\ &= \sum_{u \in H \setminus H_l} |G : \mathrm{C}_G(u)||\chi(u)|^2 + \sum_{z \in G_l} |\chi(z)|^2 \\ &= q^{s-1}\chi(1)^2 \sharp(H \setminus H_l) + q^s\chi(1)^2 \\ &= (q^{s-1}(q^l - q) + q^s)\chi(1)^2 \\ &= q^{s-1+l}\chi(1)^2. \end{aligned}$$

Thus $\chi(1)^2 = q^{(s-1)(l-1)}$. $|\chi(u)|^2 = |G : C_G(u)|^{-1}q^{s-1}\chi(1)^2 = q^{(s-1)i}$ for $u \in H_i \setminus H_{i+1}$, $i \leq l-1$. □

By Lemma 4.3, each $\chi \in \mathrm{Irr}(G|\rho)$ is θ-invariant. By Hypothesis (2), we may define the Glauberman correspondence between $\mathrm{Irr}(H)$ and $\mathrm{Irr}_\theta(G)$, the set of θ-invariant irreducible characters of G. Let $\chi = \chi_\alpha \in \mathrm{Irr}(G|\rho)$ correspond to $\alpha \in \mathrm{Irr}(H)$. (See [3, Chap.13].)

Proposition 4.5. *Assume $u \in H_i \setminus H_{i+1}$, $i \leq l-1$, and $l-i$ is odd. Then* $\chi(u) = q^{(s-1)i/2}\alpha(u)$.

Proof. Put $k = (l-i+1)/2$ and $m = (l+i+1)/2$. By Lemma 3.3 (2), G_m is abelian. As $(|G|, s) = 1$ and G_m is θ-invariant, there exists $\sigma \in \mathrm{Irr}_\theta(G_m)$ such that $(\sigma^G, \chi) \neq 0$ [3, Theorem 13.27]. By Lemma 3.3 (2), $G_m = H_m \times [G_m, \theta]$ and so Ker $\sigma \supset [G_m, \theta]$ and $\sigma_{H_l} = \rho \neq 1$. By Lemma 3.4 (2), $\mathrm{I}_G(\sigma) = HG_k$ and there exists $\eta \in \mathrm{Irr}(HG_k)$ such that $\eta^G = \chi$. Then η is θ-invariant and η corresponds to α by [3, Theorem 13.29].

Since $[u, HG_k] = [u, G_k] = [G_m, \theta]$, $u \in \mathrm{Z}(HG_k \bmod [G_m, \theta])$. Thus $\eta(u) = \eta(1)\alpha(u)$.

Assume $u^x \in HG_k$ for $x \in G$. Then $[u^x, G_k] = [u, G_k]^x = [G_m, \theta]^x$. If $x \notin HG_k$, then, by Lemma 3.4 (2), $[G_m, \theta]^x[G_m, \theta] \supset G_l$, and so $u^x \in HG_k$ is not σ-special. Hence $\eta(u^x) = 0$. Now we have $\chi(u) = \eta^G(u) = \eta(u) = \eta(1)\alpha(u)$. The result follows by Lemma 4.4. □

Proposition 4.6. *With the assumptions of Proposition* 4.5, *suppose that $l-i$ is even. Then $\chi(u) = \varepsilon_s q^{(s-1)i/2}\alpha(u)$, where $\varepsilon_s = \pm 1$ is as defined in Section* 3.

Proof. Put $k = (l-i)/2$ and $m = (l+i)/2$. As the proof of Proposition 4.5, there exists $\sigma \in \mathrm{Irr}(H_m) \subset \mathrm{Irr}(G_m)$ such that $\sigma_{H_l} = \alpha$ and $(\sigma^G, \chi) \neq 0$, and there exists $\eta \in \mathrm{Irr}_\theta(HG_{k+1}|\sigma)$ corresponding to α such that $\eta^G = \chi$.

Since $[u, HG_{k+1}] = [G_{m+1}, \theta] \subset [G_m, \theta]$, $u \in \mathrm{Z}(HG_{k+1} \bmod [G_m, \theta])$. Since $[u^x, HG_{k+1}] = [G_{m+1}, \theta]^x$, if $u^x \in HG_{k+1}$ and $x \notin HG_k$, then $\eta(u^x) = 0$ as in the proof of Proposition 4.5. Thus

$$\chi(u) = \eta^G(u) = \sum_{x \in HG_{k+1} \setminus HG_k} \eta(u^x) = \sum_x \eta(u[u,x]) = \eta(u)\sum_x \sigma([u,x]).$$

Put $u_i = e \in \mathrm{GF}(q)$. Then $e \neq 0$. Let $x \in G_k$ and $x_k = a \in \mathrm{GF}(q^s)$. We apply Lemma 3.5 (2) to G/G_l and then $[u,x] \in [G_m, \theta]G_l$. Thus $\mathrm{Tr}([u,x]_j) = 0$ for $j \leq l-1$ by Lemma 3.3 (2). We shall show that $\mathrm{Tr}([u,x]_l) = \mathrm{Tr}((a^{\theta^k} - a^{\theta^m})a)e$. Put $v \in H_i$ such that $v_i = e$, $v_j = 0$ for $j \neq i$, and put $y \in G_k$ such that $y_k = a$, $y_j = 0$ for $j \neq k$. Then $u \in vH_{i+1}$ and $x \in yG_{k+1}$. Now $[u,x] \in [v,y][G_{m+1}, \theta]$ by

Lemma 3.3 (2) and the formula for commutators. Thus $\mathrm{Tr}([u,x]_j) = \mathrm{Tr}([v,y]_j)$ for $1 \le j \le l$. Put $z = [v,y]$. We have $(vy)_l = 0$, $(yv)_k = a$, $(yv)_i = e$, $(yv)_m = a^{\theta^i}e$, and $(yv)_j = 0$ for $j \ne k, i, m$. As $z_m = e(a - a^{\theta^i})$,

$$ez_{l-i} + a^{\theta^m}(a - a^{\theta^i})e + z_l = 0.$$

$\mathrm{Tr}(z_{l-i}) = 0$ by $l - i \le l - 1$, so

$$\begin{aligned}\mathrm{Tr}(z_l) &= \mathrm{Tr}(a^{\theta^m}a^{\theta^i} - a^{\theta^m}a)e \\ &= \mathrm{Tr}(a^{\theta^{m-i}}a - a^{\theta^m}a)e \\ &= \mathrm{Tr}((a^{\theta^k} - a^{\theta^m})a)e.\end{aligned}$$

Thus $[u,x] \equiv x' \bmod [G_m, \theta]$, where $x' \in H_l$, $x'_l = \mathrm{Tr}((a^{\theta^k} - a^{\theta^m})a)e/s$.

When x runs over G_k mod HG_{k+1}, $x_k = a \in \mathrm{GF}(q^s)$ runs over $[\mathrm{GF}(q^s), \theta]$. As $\sigma \in \mathrm{Irr}(H_m) \subset \mathrm{Irr}(G_m)$,

$$\sigma([u,x]) = \sigma(x') = \rho(x').$$

Now by Lemma 3.6,

$$\sum_{x \in HG_{k+1} \setminus HG_k} \sigma([u,x]) = \sum_x \rho(x') = \varepsilon_s q^{(s-1)/2}$$

as $\rho_{H_l} \ne 1$. Thus $\chi(u) = \varepsilon_s q^{(s-1)/2}\eta(1)\alpha(u)$. The result follows by Lemma 4.4.

$\square$

Proposition 4.7. *Let $\chi_\alpha \in \mathrm{Irr}_\theta(G)$ be the character corresponding to $\alpha \in \mathrm{Irr}(H) \setminus \{1_H\}$. If $\alpha \in \mathrm{Irr}(H/H_{k+1}) \setminus \mathrm{Irr}(H/H_k)$, $1 \le k \le l$, then* Ker $\chi_\alpha \supset [G_k, \theta]G_{k+1}$, $\chi_\alpha(1) = q^{(s-1)(k-1)/2}$, $\chi_\alpha(x) = 0$ *for $x \notin_G HG_k$, if $x \in_G HG_k$, then x is conjugate to $u \in H$ modulo* Ker χ_α, *and for $u \in H$,*

$$\chi_\alpha(u) = \begin{cases} q^{(s-1)(k-1)/2}\alpha(u), & \text{for } u \in H_k \setminus H_{k+1}, \\ q^{(s-1)i/2}\alpha(u), & \text{for } u \in H_i \setminus H_{i+1},\ i \le k-1 \text{ and } k-i \text{ is odd}, \\ \varepsilon_s q^{(s-1)i/2}\alpha(u), & \text{for } u \in H_i \setminus H_{i+1},\ i \le k-1 \text{ and } k-i \text{ is even}. \end{cases}$$

Proof. Note that Ker $\chi_\alpha \supset G_{k+1}$. Apply Propositions 4.5 and 4.6 to G/G_{k+1}.

$\square$

Theorem 4.8. $\mathrm{Irr}(G) = \{1_G\} \cup \{\chi_\alpha^\lambda\ ;\ \alpha \in \mathrm{Irr}(H) \setminus \{1_H\}, \lambda \in \mathrm{Ker\ Norm}\}$.

Proof. Assume $\chi_\alpha^\lambda = \chi_\beta^\mu$ for $\alpha, \beta \in \mathrm{Irr}(H) \setminus \{1_H\}$ and $\lambda, \mu \in$ Ker Norm. We have $\chi_\alpha^{\lambda\mu^{-1}} = \chi_\beta$. Then $\alpha \in \mathrm{Irr}(H/H_{k+1}) \setminus \mathrm{Irr}(H/H_k)$ implies $\beta \in \mathrm{Irr}(H/H_{k+1}) \setminus$

$\mathrm{Irr}(H/H_k)$. Thus $[G_k,\theta]^{\lambda\mu^{-1}}[G_k,\theta] \subset \mathrm{Ker}\,\chi_\beta$ and so $(\lambda\mu^{-1})^{(k)} = 1$. Now $\lambda = \mu$ and $\alpha = \beta$. The result follows by comparing the number of conjugacy classes with the size of our set. □

Corollary 4.9. *There exist* $(q^s - 1)q^{l-i}$ *irreducible characters of degree* $q^{(s-1)(l-i)/2}$ *for* $1 \le i \le l-1$ *and* q^s *irreducible characters of degree* 1.

Theorem 4.10. *The matrix* S *obtained by* G *is unitary.*

Proof. It is easy by Corollaries 4.2 and 4.9. □

5. The fusion algebra at an algebraic level of G is integral

Let $\mathrm{Cl}(G) = \{C_i\}_{0\le i\le d}$. For $u \in C_i$, $v \in C_j$, and $w^{-1} \in C_k$, put

$$t_{u,v,w} = \sharp\{(x,y)\ ;\ x =_G u, y =_G v, xy = w^{-1}\}.$$

Then $t_{u,v,w} = t_{ij}^k$, where t_{ij}^k is defined in Section 2. We also put $N_{u,v,w} = N_{ij}^k$. Note that

$$t_{u,v,w} = \frac{|C_u||C_v|}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(u)\chi(v)\chi(w)}{\chi(1)},$$

$$N_{u,v,w} = \frac{\sqrt{|C_u||C_v||C_w|}}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(u)\chi(v)\chi(w)}{\chi(1)}.$$

To show that the fusion algebra at an algebraic level is integral we shall show $N_{u,v,w}$ is a non-negative integer for any u, v, w.

Put

$$T = \{1\} \cup \{u(e_i)^\lambda\ ;\ u(e_i) \in H \setminus \{1\}, \lambda \in \mathrm{Ker\ Norm}\},$$

representatives of the conjugacy classes of G (Theorem 4.1). In this section, we shall assume that u, v, $w \in T$.

Obviously, $N_{u,v,w}$ is symmetric in u, v, w, and if $t_{u,v,w} = 0$ then $N_{u,v,w} = 0$

If $u \in G_i \setminus G_{i+1}$, $w \in G_j \setminus G_{j+1}$, and $i < j$ then $v \in G_i \setminus G_{i+1}$ or $N_{u,v,w} = 0$. So we may assume $u, v \in G_i \setminus G_{i+1}$ and $w \in G_j \setminus G_{j+1}$ for $i \le j$. Then $\sqrt{|C_u||C_v||C_w|}/|G| = q^{(s-1)(l-i)+(s-1)(l-j)/2-sl}$. We may also assume $s \ge 3$ and s is odd.

We put

$$n_{u,v,w}^{(m)} = \sum_{\chi\in\mathrm{Irr}(G/G_{m+1})\setminus\mathrm{Irr}(G/G_m)}\frac{\chi(u)\chi(v)\chi(w)}{\chi(1)},$$

where we regard $\mathrm{Irr}(G/G_m)$ as a subset of $\mathrm{Irr}(G)$ in natural way, and thus

$$N_{u,v,w}^{(m)} = q^{(s-1)(l-i)+(s-1)(l-j)/2-sl} n_{u,v,w}^{(m)}.$$

We have $N_{u,v,w} = \sum_{m=0}^{l} N_{u,v,w}^{(m)}$, where $\mathrm{Irr}(G/G_0)$ is the empty set.

Lemma 5.1. *Let A be a finite abelian group, and let B and C be subgroups of A such that $B \geq C$. Then, for $x, y, z \in A$,*

$$\sum_{\chi \in \mathrm{Irr}(A/C)\setminus \mathrm{Irr}(A/B)} \chi(x)\chi(y)\chi(z) = \begin{cases} |A/C| - |A/B|, & \text{if } xyz \in C, \\ -|A/B|, & \text{if } xyz \in B \setminus C, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. This is easy since $\sum_{\chi \in \mathrm{Irr}(A/B)} \chi(x)\chi(y)\chi(z) = |A/B|$ if $xyz \in B$ and 0 otherwise. □

For x, y, $z \in T$, We define $\delta_m(xyz)$ to be 1 if $xyz \in G_m$ and 0 otherwise. If $x = u$, $y = v$, and $z = w$ we omit uvw, namely $\delta_m = \delta_m(uvw)$.

Lemma 5.2. *If $i = j$, then $\sum_{m=0}^{i} n_{u,v,w}^{(m)} = \delta_{i+1} q^{si}$ and $\sum_{m=0}^{i} N_{u,v,w}^{(m)}$ is an integer.*

Proof. Obviously,

$$\begin{aligned} \sum_{m=0}^{i-1} n_{u,v,w}^{(m)} &= \sum_{\chi \in \mathrm{Irr}(G/G_i)} \frac{\chi(u)\chi(v)\chi(w)}{\chi(1)} \\ &= \sum_{\chi \in \mathrm{Irr}(G/G_i)} \chi(1)^2 \\ &= |G/G_i| = q^{s(i-1)}. \end{aligned}$$

Furthermore, since $u, v, w \in \mathrm{Z}(\chi)$, Theorem 4.8 implies that for $\chi \in \mathrm{Irr}(G/G_{i+1}) \setminus \mathrm{Irr}(G/G_i)$,

$$\begin{aligned} n_{u,v,w}^{(i)} &= \sum_{\chi \in \mathrm{Irr}(G/G_{i+1})\setminus \mathrm{Irr}(G/G_i)} \frac{\chi(u)\chi(v)\chi(w)}{\chi(1)} \\ &= q^{i-1} \sum_{\beta \in \mathrm{Irr}(G_i/G_{i+1})\setminus 1} q^{(s-1)(i-1)} \beta(u)\beta(v)\beta(w) \\ &= q^{s(i-1)}(\delta_{i+1} q^s - 1). \end{aligned}$$

So we have $\sum_{m=0}^{i} n_{u,v,w}^{(m)} = \delta_{i+1} q^{si}$.

By definition of $N^{(m)}_{u,v,w}$,

$$\begin{aligned}\sum_{m=0}^{i} N^{(m)}_{u,v,w} &= q^{3(s-1)(l-i)/2-sl} \sum_{m=0}^{i} n^{(m)}_{u,v,w} \\ &= \delta_{i+1} q^{3(s-1)(l-i)/2-sl+si}.\end{aligned}$$

Now $3(s-1)(l-i)/2 - sl + si = (s-3)(l-i)/2 \geq 0$, and thus $\sum_{m=0}^{i} N^{(m)}_{u,v,w}$ is an integer. $\square$

Lemma 5.3. *Assume $i < j$ and $u \in H$. If $v \notin H$ then $n_{u,v,w} = 0$. When $v \in H$ we define $\tilde{w} \in H$ by $w \in \tilde{w}[G_j, \theta]G_{j+1}$. Then $\sum_{m=0}^{j} n^{(m)}_{u,v,w} = \delta_{j+1}(uv\tilde{w})q^{(s-1)i+j}$ and $\sum_{m=0}^{i} N^{(m)}_{u,v,w}$ is an integer.*

Proof. The first statement obviously holds since $t_{u,v,w} = 0$. Suppose $v \in H$, and define $\tilde{w} \in H$ as in this lemma.

By Theorem 4.7,

$$\begin{aligned}\sum_{m=0}^{j-1} n^{(m)}_{u,v,w} &= \sum_{\chi \in \mathrm{Irr}(G/G_j)} \frac{\chi(u)\chi(v)\chi(w)}{\chi(1)} \\ &= \sum_{\chi \in \mathrm{Irr}(G/G_j)} \chi(u)\chi(v) \\ &= \delta_j |C_{G/G_j}(u)| \\ &= \delta_j q^{(j-1)+(s-1)i},\end{aligned}$$

and

$$\begin{aligned}n^{(j)}_{u,v,w} &= q^{(s-1)i} \sum_{\alpha \in \mathrm{Irr}(H/H_{j+1}) \setminus \mathrm{Irr}(H/H_j)} \alpha(u)\alpha(v)\alpha(\tilde{w}) \\ &= q^{(s-1)i}(\delta_{j+1}(uv\tilde{w})q^j - \delta_j q^{j-1}).\end{aligned}$$

Thus the equation holds.

Furthermore,

$$\begin{aligned}\sum_{m=0}^{j} N^{(m)}_{u,v,w} &= q^{(s-1)(l-i)+(s-1)(l-j)/2-sl} \sum_{m=0}^{j} n^{(m)}_{u,v,w} \\ &= \delta_{j+1} q^{(s-1)(l-i)+(s-1)(l-j)/2-sl+(s-1)i+j}.\end{aligned}$$

Now $(s-1)(l-i) + (s-1)(l-j)/2 - sl + (s-1)i + j = (s-3)(l-j)/2 \geq 0$, and thus $\sum_{m=0}^{j} N^{(m)}_{u,v,w}$ is an integer. $\square$

Lemma 5.4. *If $m > j$, then either*

$$n_{u,v,w}^{(m)} = \varepsilon_s^{(m-j+1)} q^{(s-1)i+(s-1)j/2-(s-1)(m-1)/2+m-1}(\delta_{m+1}q - \delta_m)$$

or $n_{u,v,w}^{(m)} = 0$. *Moreover,* $N_{u,v,w}^{(m)}$ *is an integer.*

Proof. We may assume u, v, $w \in H^\lambda$ for some $\lambda \in$ Ker Norm, otherwise $n_{u,v,w}^{(m)} = 0$. Now we may also assume $\lambda = 1$, namely u, v, $w \in H$.

By Theorem 4.7,

$$\begin{aligned} n_{u,v,w}^{(m)} &= \varepsilon_s^{(m-j+1)} q^{(s-1)i+(s-1)j/2-(s-1)(m-1)/2} \\ &\qquad \sum_{\alpha \in \mathrm{Irr}(H/H_{m+1}) \setminus \mathrm{Irr}(H/H_m)} \alpha(u)\alpha(v)\alpha(w) \\ &= \varepsilon_s^{(m-j+1)} q^{(s-1)i+(s-1)j/2-(s-1)(m-1)/2}(\delta_{m+1}q^m - \delta_m q^{m-1}) \end{aligned}$$

and the equation holds.

Furthermore,

$$\begin{aligned} N_{u,v,w}^{(m)} &= q^{(s-1)(l-i)+(s-1)(l-j)/2-sl+(s-1)i+(s-1)j/2-(s-1)(m-1)/2+m-1}(\delta_{m+1}q - \delta_m) \\ &= q^{3(s-1)l/2-sl-(s-1)(m-1)/2+m-1}(\delta_{m+1}q - \delta_m), \end{aligned}$$

and

$$3(s-1)l/2 - sl - (s-1)(m-1)/2 + m - 1 = (l-m+1)\left(\frac{s-3}{2}\right) \geq 0.$$

Thus $N_{u,v,w}^{(m)}$ is an integer. □

Theorem 5.5. *$N_{u,v,w}$ is a non-negative integer for any $u, v, w \in G$. In particular, the fusion algebra at an algebraic level is integral.*

Proof. Since $t_{u,v,w}$ is non-negative, $N_{u,v,w}$ is non-negative. The result follows immediately by Lemmas 5.2, 5.3, and 5.4. □

6. Self duality of G

In this section, we investigate the self duality of G. Although G is not self dual in general, if l is less than the prime divisor of q and $l = s-1$, then G is self dual.

Recall that if $\mathrm{Cl}(G) = \{C_0, C_1, \cdots, C_d\}$ and $\mathrm{Irr}(G) = \{\chi_0, \chi_1, \cdots, \chi_d\}$, then

$$\begin{aligned} p_{ij} &= \frac{|G|\chi_i(x_j)}{|C_G(x_j)|\chi_i(1)}, \\ q_{ij} &= \chi_j(1)\overline{\chi_j(x_i)}, \end{aligned}$$

where $x_i \in C_i$, and G is self dual if $p_{ij} = \overline{q_{ij}}$ for all $0 \leq i, j \leq d$.

Firstly we shall show that G is not self dual if $l > p$. We need an easy lemma.

Lemma 6.1. *Put $a \in G$, $a_i = e \in \mathrm{GF}(q)$ and $a_j = 0$ for $j \neq i$. then $a^n = u(b_j)$ where $b_{im} = {}_n\mathrm{C}_m e^m$ and ${}_n\mathrm{C}_m$ is a binomial coefficient, and $b_j = 0$ otherwise.*

In particular, for $x \in G_i \setminus G_{i+1}$, x is of order p if and only if $ip > l$.

Proof. By the induction on n, the form of a^n is obtained. By $p \mid {}_p\mathrm{C}_m$ for $1 < m < p$, we have the order of $x \in G_i \setminus G_{i+1}$. □

Proposition 6.2. *Let p be the prime divisor of q. If $l > p$, then G is not self dual.*

Proof. Suppose that G is self dual. It is easy to see that

$$\begin{aligned} p_{0j} &= |G|/|\mathrm{C}_G(x_j)| = |C_j|, \\ q_{0j} &= \chi_j(1)^2. \end{aligned}$$

Thus $|C_i| = \chi_i(1)^2$ for all i.

Let $x_i \in H_1/H_2$. By Lemma 6.1, $x_i G_{p+1} \in G/G_{p+1}$ has order p^2. Thus there exists $\alpha \in \mathrm{Irr}(H/H_{p+1}) \setminus \mathrm{Irr}(H/H_p)$ such that $\alpha(x_i) = \omega$, where ω is a primitive p^2-th root of unity. Let $\chi_j = \chi_\alpha \in \mathrm{Irr}(G/G_{p+1}) \setminus \mathrm{Irr}(G/G_p)$. Then

$$\chi_j(x_i) = \varepsilon_s q^{(s-1)/2}\omega,$$

where $\varepsilon_s = \pm 1$ is as defined above.

Since $|C_i| = q^{(s-1)(l-1)}$, we have $\chi_i(1) = q^{(s-1)(l-1)/2}$ and $\chi_i \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/G_l)$. Similarly, $x_j \in G_{l-p+1} \setminus G_{l-p+2}$. Now $(l-p+1)p - l = (l-p)(p-1) > 0$ and so $(l-p+1)p > l$. Thus x_j has order p and $\chi_i(x_j)$ is a real multiple of a p-th root of unity.

Since p_{ij} and q_{ij} are real multiples of $\chi_i(x_j)$ and $\chi_j(x_i)$, respectively, we have $p_{ij} \neq \overline{q_{ij}}$. □

By Proposition 6.2, if G is self dual, then $l \leq p$. We do not know whether G is self dual or not if $l \leq p$. We have the following result.

Proposition 6.3. *Assume $l < p$ and $l = s - 1$. Then G is self dual.*

Proof. Put $q = p^t$. We denote the usual trace map from $\mathrm{GF}(q)$ to $\mathrm{GF}(p)$ by $\mathrm{Tr}_{q/p}$ to distinguish it from Tr, the trace map from $\mathrm{GF}(q^s)$ to $\mathrm{GF}(q)$. Note that the exponent of G is p by Lemma 6.1, and H is elementary abelian. We fix a primitive p-th root of unity ω.

Put $K = \mathrm{GF}(q) \times \cdots \times \mathrm{GF}(q)$ (l-times) as a direct product of the additive group $\mathrm{GF}(q)$, and put $K_i = \{(a_1, \cdots, a_l) \in K \ ; \ a_j = 0, \ \text{for } j < i\}$ for $1 \leq i \leq l+1$. For $x \in K$, we denote the i-th entry of x by x_i. By Lemma 6.1, H is elementary abelian and so there exists an isomorphism $\varphi : H \to K$ such that $\varphi(H_i) = K_i$ for $1 \leq i \leq l+1$ and $u_i = \varphi(u)_i$ for $u \in H_i$.

For $u \in H$, we define $\alpha_u \in \mathrm{Irr}(H)$ by

$$\alpha_u(v) = \omega^{\mathrm{Tr}_{q/p}\left(\sum_{i+j=l+1} \varphi(u)_i \varphi(v)_j\right)}.$$

Then the map $u \mapsto \alpha_u$ is an isomorphism from H to $\mathrm{Irr}(H)$. Note that $\alpha_u(v) = \alpha_v(u)$ for any $u, v \in H$. Also $u^\lambda \mapsto \chi^\lambda_{\alpha_u}$ induces a one-to-one correspondence between $\mathrm{Cl}(G)$ and $\mathrm{Irr}(G)$. We denote χ_{α_u} by χ_u. We shall show $P = \overline{Q}$ by this correspondence. By Theorems 4.1 and 4.8, we can index the conjugacy classes and irreducible characters of G by $u \in H$ and $\lambda \in \mathrm{Ker\ Norm}$.

Note that if $u \in H_i \setminus H_{i+1}$ then $|C_u| = q^{(s-1)(l-i)}$, $\alpha_u \in \mathrm{Irr}(H/H_{l-i+2} \setminus \mathrm{Irr}(H/H_{l-i+1})$, $\chi_u \in \mathrm{Irr}(G/G_{l-i+2} \setminus \mathrm{Irr}(G/G_{l-i+1})$, and $\chi_u(1) = q^{(s-1)(l-i)/2}$.

We assume $u \in H_i \setminus H_{i+1}$, $v \in H_j \setminus H_{j+1}$, and $\lambda, \mu \in \mathrm{Ker\ Norm}$.

First, we assume $i + j > l + 1$. Then obviously $u^\lambda \in \mathrm{Ker}\ \chi^\mu_v$ and $v^\mu \in \mathrm{Ker}\ \chi^\lambda_u$. Now

$$\begin{aligned} p_{u^\lambda v^\mu} &= \frac{|G|\chi^\lambda_u(v^\mu)}{|\mathrm{C}_G(v^\mu)|\chi^\lambda_u(1)} \\ &= q^{(s-1)(l-j)}, \\ q_{u^\lambda v^\mu} &= \chi^\mu_v(1)\overline{\chi^\mu_v(u^\lambda)} \\ &= q^{(s-1)(l-j)}. \end{aligned}$$

Thus $p_{u^\lambda v^\mu} = \overline{q_{u^\lambda v^\mu}}$.

Second, we assume $i + j < l + 1$. If $\lambda \neq \mu$, then $\chi^\lambda_u(v^\mu) = \chi^\mu_v(u^\lambda) = 0$, and so the result holds. We may assume $\lambda = \mu = 1$. Then

$$\begin{aligned} p_{uv} &= \frac{|G|\chi_u(v)}{|\mathrm{C}_G(v)|\chi_u(1)} \\ &= \varepsilon_s^{(l-i-j)} q^{(s-1)(l-j)} q^{-(s-1)(l-i)/2} q^{(s-1)j/2} \alpha_u(v) \\ &= \varepsilon_s^{(l-i-j)} q^{(s-1)(l+i-j)/2} \alpha_u(v), \\ q_{uv} &= \chi_v(1)\overline{\chi_v(u)} \\ &= \varepsilon_s^{(l-i-j)} q^{(s-1)(l-j)/2} q^{(s-1)i/2} \overline{\alpha_v(u)} \\ &= \varepsilon_s^{(l-i-j)} q^{(s-1)(l+i-j)/2} \overline{\alpha_v(u)}. \end{aligned}$$

Thus $p_{uv} = \overline{q_{uv}}$ by $\alpha_u(v) = \alpha_v(u)$.

Finally, we assume $i+j=l+1$. Put $u_i = a \in \mathrm{GF}(q)$ and $v_j = b \in \mathrm{GF}(q)$. We may assume that $\mu = 1$. We define $\tilde{u} \in H_i$ to be $u^{\lambda} \in \tilde{u}[G_i, \theta]G_{i+1}$ and $\tilde{v} \in H_j$ to be $v^{\lambda^{-1}} \in \tilde{v}[G_j, \theta]G_{j+1}$. Then

$$\begin{aligned}(\tilde{u})_i &= \mathrm{Tr}(a\lambda^{(i)})/s &&= a\ \mathrm{Tr}(\lambda^{(i)})/s,\\ (\tilde{v})_j &= \mathrm{Tr}(b{\lambda^{(j)}}^{-1})/s &&= b\ \mathrm{Tr}({\lambda^{(j)}}^{-1})/s.\end{aligned}$$

Thus

$$\begin{aligned}\chi_u^{\lambda}(v) &= q^{(s-1)(l-i)/2}\alpha_u(\tilde{v}),\\ \chi_v(u^{\lambda}) &= q^{(s-1)(l-j)/2}\alpha_v(\tilde{u}).\end{aligned}$$

We shall show $\alpha_u(\tilde{v}) = \alpha_v(\tilde{u})$. Since

$$\begin{aligned}\alpha_u(\tilde{v}) &= \omega^{\mathrm{Tr}_{q/p}(ab\mathrm{Tr}({\lambda^{(j)}}^{-1}))/s},\\ \alpha_v(\tilde{u}) &= \omega^{\mathrm{Tr}_{q/p}(ab\mathrm{Tr}(\lambda^{(i)}))/s},\end{aligned}$$

it is enough to show that $\mathrm{Tr}(\lambda^{(i)} - {\lambda^{(j)}}^{-1}) = 0$. We have

$$\begin{aligned}\mathrm{Tr}(\lambda^{(i)} - {\lambda^{(j)}}^{-1}) &= \mathrm{Tr}\left(\prod_{k=0}^{i-1}\lambda^{\theta^k} - \prod_{k=0}^{j-1}(\lambda^{\theta^k})^{-1}\right)\\ &= \mathrm{Tr}\left(\prod_{k=0}^{i-1}\lambda^{\theta^k} - \prod_{k=i}^{s-1}(\lambda^{\theta^k})^{-1}\right)\\ &= \mathrm{Tr}\left(\left(\prod_{k=0}^{s-1}\lambda^{\theta^k} - 1\right)\prod_{k=i}^{s-1}(\lambda^{\theta^k})^{-1}\right)\\ &= 0.\end{aligned}$$

Thus $\alpha_u(\tilde{v}) = \alpha_v(\tilde{u})$. Now

$$\begin{aligned}p_{u^{\lambda}v} &= \frac{|G|\chi_u^{\lambda}(v)}{|\mathrm{C}_G(v)|\chi_u^{\lambda}(1)}\\ &= q^{(s-1)(l-j)}q^{-(s-1)(l-i)/2}q^{(s-1)(l-i)/2}\alpha_u(\tilde{v})\\ &= q^{(s-1)(l-j)}\alpha_u(\tilde{v}),\\ q_{u^{\lambda}v} &= \chi_v(1)\overline{\chi_v(u^{\lambda})}\\ &= q^{(s-1)(l-j)/2}q^{(s-1)(l-j)/2}\overline{\alpha_v(\tilde{u})}\\ &= q^{(s-1)(l-j)}\overline{\alpha_v(\tilde{u})}.\end{aligned}$$

Thus $p_{u^{\lambda}v} = \overline{q_{u^{\lambda}v}}$. This completes the proof. □

References

[1] E. Bannai: *Association schemes and fusion algebras* (*an introduction*), J. Alg. Comb. **2** (1993), 327–344.

[2] A. Hanaki: *A condition on lengths of conjugacy classes and character degrees*, Osaka J. Math. **33** (1996), 207–216.

[3] I.M. Isaacs: Character Theory of Finite Groups, Academic Press, New York-San Francisco-London, 1976.

[4] R. Lidl and H. Niederreiter: Finite Fields, Addison-Wesley, Massachusetts, 1983.

A. Hanaki
Faculty of Engineering
Yamanashi University
Takeda 4, Kofu 400, Japan

T. Okuyama
Laboratory of Mathematics
Hokkaido University of Education
Asahikawa Campus
Hokumoncho 9, Asahikawa 070, Japan