Journal of Algebra **243,** 142–167 (2001)
doi:10.1006/jabr.2000.8587, available online at http://www.idealibrary.com on IDEAL®

Quasi-permutation Representations of the Group $GL_2(q)$

M. R. Darafsheh

ORE
ed by Elsevier - Publisher Connector

E-mail: darafshe@khayam.ut.ac.ir

M. Ghorbany

Department of Mathematics, Iran University of Science and Technology, Narmak, Tehran, Iran
E-mail: ghorbany@sun.iust.ac.ir

A. Daneshkhah

Department of Mathematics, Faculty of Science, Bu-Ali-Sina University, Hamedan, Iran
E-mail: adanesh@basu.ac.ir

and

H. Behravesh[1]

Department of Mathematics, University of Urmia, Urmia, Iran
E-mail: math@www.dci.co.ir

Communicated by Walter Feit

Received May 3, 2000

A square matrix over the complex field with non-negative integral trace is called a quasi-permutation matrix. For a finite group G the minimal degree of a faithful permutation representation of G is denoted by $p(G)$. The minimal degree of a faithful representation of G by quasi-permutation matrices over the rationals and the complex numbers are denoted by $q(G)$ and $c(G)$ respectively. Finally $r(G)$

[1] Present address: Institute for Studies in Theoretical Physics and Mathematics, P.O. Box 19395-5746, Tehran, Iran.

0021-8693/01 $35.00
Copyright © 2001 by Academic Press
All rights of reproduction in any form reserved.

denotes the minimal degree of a faithful rational valued complex character of G. In this paper $p(G)$, $q(G)$, $c(G)$, and $r(G)$ are calculated for the group $G = GL_2(q)$.
© 2001 Academic Press
Key Words: general linear group; quasi-permutation.

1. INTRODUCTION

In [11] Wong defined a quasi-permutation group of degree n to be a finite group G of automorphisms of an n-dimensional complex vector space such that every element of G has non-negative integral trace. Also Wong studied the extent to which some facts about permutation groups generalize to the quasi-permutation group situation. In [4] the authors investigated further the analogy between permutation groups and quasi-permutation groups. They also worked over the rational field and found some interesting results.

By a quasi-permutation matrix we mean a square matrix over the complex field $\mathbb{C}$ with non-negative integral trace. For a given finite group G, let $p(G)$ denote the minimal degree of a faithful permutation representation of G, let $q(G)$ denote the minimal degree of a faithful representation of G by quasi-permutation matrices over the rational field $\mathbb{Q}$, and let $c(G)$ be the minimal degree of a faithful representation of G by complex quasi-permutation matrices. By a rational valued character we mean a character χ corresponding to a complex representation of G such that $\chi(g) \in \mathbb{Q}$ for all $g \in G$. Let $r(G)$ denote the minimal degree of a faithful rational valued character of G. It is easy to see that for a finite group G the following inequalities hold:

$$r(G) < c(G) \leq q(G) \leq p(G).$$

In [4] the case of equality has been investigated for abelian groups. In [2] above quantities have been found for the groups $SL_2(q)$ and $PSL_2(q)$. In this paper we will calculate $r(G)$, $c(G)$, $q(G)$, and $p(G)$ where G is $GL_2(q)$. All characters concerned are over the complex field $\mathbb{C}$ unless otherwise stated.

Using the definition of $p(G)$ it is proved in [1] that

$$p(G) = \min\left\{ \sum_{i=1}^{n} [G : H_i] : H_i \leq G, \quad \text{for } i = 1, 2, \ldots, n \text{ and } \bigcap_{i=1}^{n} \bigcap_{x \in G} H_i^x = 1 \right\}.$$

Let G be finite group and let χ be an irreducible complex character of G. Let $m_{\mathbb{Q}}(\chi)$ denote the Schur index of χ over $\mathbb{Q}$ and let $\Gamma(\chi)$ be the

Galois group of $\mathbb{Q}(\chi)$ over $\mathbb{Q}$. It is known that

$$\sum_{\alpha \in \Gamma(\chi)} m_{\mathbb{Q}}(\chi) \chi^{\alpha}$$

is a character of an irreducible $\mathbb{Q}(G)$-module [9, Corollary 10.2(b)]. So by knowing the character table of a group and the Schur indices of each of the irreducible characters of G, we can find the irreducible rational characters of G. If $\gamma \in \mathbb{C}$ is an algebraic number over $\mathbb{Q}$, then by $(\mathbb{Q}(\gamma) : \mathbb{Q})$ we mean the Galois group of $\mathbb{Q}(\gamma)$ over $\mathbb{Q}$ and always it is denoted by Γ.

2. BACKGROUND

Assume that E is a splitting field for G and that F is a subfield of E. If $\chi, \psi \in \mathrm{Irr}_E(G)$ we say that χ and ψ are Galois conjugate over F if $F(\chi) = F(\psi)$ and there exists $\sigma \in \mathrm{Gal}(F(\chi)/F)$ such that $\chi^{\sigma} = \psi$, where $F(\chi)$ denotes the field obtained by adding the values $\chi(g)$, for all $g \in G$, to F. It is clear that this defines an equivalence relation on $\mathrm{Irr}_E(G)$.

Let $\mathfrak{n}_i$ for $0 \leq i \leq r$ be Galois conjugacy classes of irreducible complex characters of the G. For $0 \leq i \leq r$ let φ_i be a representative of the class $\mathfrak{n}_i$, with $\varphi_o = 1_G$. Write $\Psi_i = \sum_{\chi_i \in \mathfrak{n}_i} \chi_i$, $m_i = m_{\mathbb{Q}}(\varphi_i)$, and $K_i = \ker \varphi_i$. We know that $K_i = \ker \Psi_i$. For $I \subseteq \{0, 1, 2, \ldots, r\}$ put $K_I = \bigcap_{i \in I} K_i$. By definition of $r(G)$, $c(G)$, and $q(G)$ and using above notations we have

$$r(G) = \min\left\{ \xi(1) : \xi = \sum_{i=1}^{r} n_i \Psi_i,\ n_i \geq 0,\right.$$
$$\left. K_I = 1 \text{ for } I = \{i,\ i \neq 0,\ n_i > 0\} \right\}$$

$$c(G) = \min\left\{ \xi(1) : \xi = \sum_{i=0}^{r} n_i \Psi_i,\ n_i \geq 0,\right.$$
$$\left. K_I = 1 \text{ for } I = \{i,\ i \neq 0,\ n_i > 0\} \right\}$$

$$q(G) = \min\left\{ \xi(1) : \xi = \sum_{i=0}^{r} n_i m_i \Psi_i,\ n_i \geq 0,\ K_I = 1\right.$$
$$\left. \text{for } I = \{i,\ i \neq 0,\ n_i > 0\} \right\},$$

where $n_0 = -\min\{\xi(g) \mid g \in G\}$ in the case of $c(G)$ and $q(G)$.

We know that if G is a finite group and if the Schur index of each non-principal irreducible character of G is equal to m, then $q(G) = mc(G)$ [1, Corollary 3.15].

In [1] we defined $d(\chi)$, $m(\chi)$, and $c(\chi)$ (see Definition 3.4). Here we can redefine it as follows:

Let χ be a complex character of G, such that $\ker \chi = 1$. Then $\chi = \chi_1 + \cdots + \chi_n$ for some $\chi_i \in \mathrm{Irr}(G)$.

DEFINITION 2.1. Let χ be a complex character of G, such that $\ker \chi = 1$. Then define

$$d(\chi) = \sum_{i=1}^{n} |\Gamma_i(\chi_i)|\, \chi_i(1), \tag{1}$$

$$m(\chi) = \begin{cases} 0 & \text{if } \chi = 1_G, \\ \left| \min\left\{ \sum_{i=1}^{n} \sum_{\alpha \in \Gamma_i(\chi_i)} \chi_i^{\alpha}(g) : g \in G \right\} \right| & \text{otherwise}, \end{cases} \tag{2}$$

$$c(\chi) = \sum_{i=1}^{n} \sum_{\alpha \in \Gamma_i(\chi_i)} \chi_i^{\alpha} + m(\chi) 1_G. \tag{3}$$

So

$$r(G) = \min\{ d(\chi) : \ker \chi = 1 \}$$

and

$$c(G) = q(G) = \min\{ c(\chi)(1) : \ker \chi = 1 \}.$$

Now we begin with a summary of facts relevant to the irreducible complex characters of $GL_2(q)$. It is proved in [6] that the Schur index over $\mathbb{Q}$ of each of irreducible characters of the group $G = GL_n(q)$, $n \le 4$, is one. Therefore for these groups, by [1] we obtain $c(G) = q(G)$. It is obvious that if $G = GL_n(q)$, $n \le 4$, and $\chi \in \mathrm{Irr}(G)$, then $\sum_{\alpha \in \Gamma(\chi)} \chi^{\alpha}$ is a character of an irreducible $\mathbb{Q}(G)$-module for every $\chi \in \mathrm{Irr}(G)$. Also by [1], if $\chi \in \mathrm{Irr}(G)$, then $\ker \chi = \ker \sum_{\alpha \in \Gamma(\chi)} \chi^{\alpha}$. Moreover χ is faithful if and only if $\sum_{\alpha \in \Gamma(\chi)} \chi^{\alpha}$ is faithful.

The group $GL_2(q)$ is of order $q(q-1)^2(q+1)$ and representatives of its conjugacy classes are of the four types [10]

$$A_1 = \begin{pmatrix} \varepsilon^a & 0 \\ 0 & \varepsilon^a \end{pmatrix}, \qquad A_2 = \begin{pmatrix} \varepsilon^a & 0 \\ 1 & \varepsilon^a \end{pmatrix}, \qquad A_3 = \begin{pmatrix} \varepsilon^a & 0 \\ 0 & \varepsilon^b \end{pmatrix}_{a \ne b},$$

$$B_1 = \begin{pmatrix} \eta^c & 0 \\ 0 & \eta^{cq} \end{pmatrix},$$

TABLE I
Irreducible Characters of $GL_2(q)$

	$\chi_1^{(n)}$	$\chi_q^{(n)}$	$\chi_{q+1}^{(m,n)}$	$\chi_{q-1}^{(l)}$
A_1	ρ^{2na}	$q\rho^{2na}$	$(q+1)\rho^{(m+n)a}$	$(q-1)\delta^{la(q+1)}$
A_2	ρ^{2na}	0	$\rho^{(m+n)a}$	$\delta^{la(q+1)}$
A_3	$\rho^{n(a+b)}$	$\rho^{n(a+b)}$	$\rho^{ma+nb}+\rho^{na+mb}$	0
B_1	ρ^{nc}	$-\rho^{nc}$	0	$-(\delta^{lc}+\delta^{lcq})$

where ε and η are primitive elements of $GF(q)$ and $GF(q^2)$ respectively and $q+1 \nmid c$. The complex character table of $GL_2(q)$ is given in [10] as Table I, in which $m, n = 1, 2, \ldots, q-1$, $m \neq n$, $(m,n) \equiv (n,m)$, $\rho^{q-1} = 1$, $\delta^{q^2-1} = 1$, $l = 1, 2, \ldots, q^2-2, q+1 \nmid l$, $c = 1, 2, \ldots, q^2-2, q+1 \nmid c$, and $a, b = 0, 1, \ldots, q-2$, $a \neq b$.

The proof of the following facts may be found in [3]. Let ε be a primitive nth root of unity in $\mathbb{C}$. Then $\varepsilon + \varepsilon^{-1}$ is rational if and only if $n = 1, 2, 3, 4, 6$. The values of $\varepsilon + \varepsilon^{-1}$ in these cases are $2, -2, -1, 0, 1$ respectively.

Also $\varepsilon^j + \varepsilon^{-j}$, $1 \leq j \leq n$, is rational if and only if $n = j, 2j, 3j, 4j, 6j, \frac{3}{2}j, \frac{4}{3}j, \frac{6}{5}j$.

In this case if $i \in \mathbb{Z}$ and $d_i = (i, n)$, and $n > 2d_i$, then $[\mathbb{Q}(\varepsilon^i + \varepsilon^{-i}) : \mathbb{Q}] = \frac{1}{2}\varphi(n/d_i)$, and if $n \neq d_i, 2d_i$, then

$$\sum_{\alpha \in \Gamma_i} (\varepsilon^i + \varepsilon^{-i})^{\alpha} = \mu\left(\frac{n}{d_i}\right),$$

where $\Gamma_i = (\mathbb{Q}(\varepsilon^i + \varepsilon^{-i} : \mathbb{Q})$ and μ is the Möbius function.

With the above assumption if we set $\Gamma = (\mathbb{Q}(\varepsilon + \varepsilon^{-1}) : \mathbb{Q})$, then

$$\sum_{\alpha \in \Gamma} (\varepsilon^i + \varepsilon^{-i})^{\alpha} = \frac{\varphi(n)}{\varphi\left(\dfrac{n}{d_i}\right)} \mu\left(\frac{n}{d_i}\right).$$

Let $G = GL_2(q)$, where $q = p^n$ for some prime p, $d = (n, q-1)$, and $\rho_d = \rho^d$. Let $d_i = (\frac{q-1}{d}, i)$, where $1 \leq i \leq \frac{q-1}{d} - 1$. Then we have

$$A(i) = \sum_{\alpha \in \Gamma} (\rho_d^i)^{\alpha} = \frac{\varphi\left(\dfrac{q-1}{d}\right)}{\varphi\left(\dfrac{q-1}{ddi}\right)} \mu(d_i).$$

3. ALGORITHM FOR $p(G)$

We mentioned that

$$p(G) = \min\left\{ \sum_{i=1}^{n} [G : H_i] : H_i \le G, \bigcap_{i=1}^{n} \bigcap_{x \in G} H_i^x = 1 \right\}$$

and therefore in order to obtain $p(G)$ we should study those subgroups of G such that the intersection of their cores is the identity. In this section generally G denotes the group $GL_2(q)$, but there are some results which are true for the group $GL_n(q)$ and therefore they are stated in general form. First we state the following trivial fact whose proof may be found in [5, 8].

Let t be a non-negative integer with $t | q - 1$ and let φ_t: $GL_n(q) \to GF(q)^*$ be given by $\varphi_t(A) = (\det A)^t$ for all $A \in GL_n(q)$. Then φ_t is a homomorphism and its image is isomorphic to a cyclic group of order $\frac{q-1}{t}$. Also let $G(t) = \ker \varphi_t$ and let t_1, t_2 be non-negative divisors of $q - 1$ and $t_1 \mid t_2$. Then $G(t_1) \trianglelefteq G(t_2)$, and $G(t_2)/G(t_1)$ is isomorphic to a cyclic group of order t_2/t_1.

And if $(t_1, t_2) = 1$, then $G(t_1) \cap G(t_2) = SL_n(q) = G(1)$.

LEMMA 3.1. *For any subgroup H of $GL_n(q)$ we have $[H : H \cap SL_n(q)] \le q - 1$.*

Proof. As $HSL_n(q) \le GL_n(q)$, we have $|H||SL_n(q)|/|H \cap SL_n(q)| \le |GL_n(q)|$. Therefore

$$\frac{|H|}{|H \cap SL_n(q)|} \le \frac{|GL_n(q)|}{|SL_n(q)|} = q - 1.$$

∎

LEMMA 3.2. *Let H be a subgroup of $GL_2(q)$ such that* $\mathrm{core}_{SL_2(q)}(H) \cap SL_2(q) = 1$. *Then*

$$[G : H] \ge (q - 1)_2(q + 1),$$

where $(q - 1)_2$ denotes the 2-part of $q - 1$.

Proof. Since $\mathrm{core}_{SL_2(q)}(H \cap SL_2(q)) = \mathrm{core}_{SL_2(q)}(H) \cap SL_2(q) = 1$, hence $H \cap SL_2(q)$ is a core-free subgroup of $SL_2(q)$. By [2, Theorems 3.6 and 3.8]

$$p(SL_2(q)) = (q - 1)_2(q + 1).$$

Thus for any core-free subgroup K of $SL_2(q)$ we have

$$[SL_2(q) : K] \ge (q - 1)_2(q + 1).$$

Therefore

$$\left[SL_2(q) : H \cap SL_2(q)\right] \geq (q-1)_2(q+1).$$

Then as $H \cap SL_2(q) \leq H \leq GL_2(q)$ we get

$$[G:H] = \frac{\left[GL_2(q) : H \cap SL_2(q)\right]}{\left[H : H \cap SL_2(q)\right]} \geq \frac{|GL_2(q)|}{(q-1)|H \cap SL_2(q)|}$$

$$= \left[SL_2(q) : H \cap SL_2(q)\right] \geq (q-1)_2(q+1).$$

▮

LEMMA 3.3. *If $SL_n(q) \leq H \leq GL_n(q)$, then $H = G(t)$ for some $t|q-1$.*

Proof. We have $[Gl_n(q) : SL_n(q)] = [GL_n(q) : H][H : SL_n(q)]$. Let $[H : SL_n(q)] = t$. Then $t|q-1$. Hence $(ASL_n(q))^t = A^t SL_n(q) = SL_n(q)$ for all $A \in H$, and this implies $A^t \in SL_n(q)$. Thus $(\det A)^t = 1$ and therefore $H \subseteq G(t)$. Also since $[GL_n(q) : G(t)] = \frac{q-1}{t}$ and $|H| = t|SL_n(q)|$ and $|G(t)| = t|SL_n(q)|$ we have $H = G(t)$. ▮

Let $G = GL_n(q)$, $q \neq 2, 3$, and $H \leq G$. Since $\operatorname{core}_G(H) \trianglelefteq G$, so $\operatorname{core}_G(H) \supseteq SL_n(q)$ or $\operatorname{core}_G(H) \subseteq Z(G)$. We consider two cases

(a) $\operatorname{core}_G(H) \supseteq SL_n(q)$ if and only if $H \supseteq SL_n(q)$ or $H = G(t)$ for some $t|q-1$. In this case $\operatorname{core}_G G(t) = G(t)$ and $[G : G(t)] = \frac{q-1}{t}$.

(b) If $\operatorname{core}_G(H) \subseteq Z(G)$, then $\operatorname{core}_G(H) = \langle \alpha^i \rangle$, $\alpha^{q-1} = 1$. Also

$$p(G) = \min\left\{ \sum_i [G : H_i] : H_i \leq G,\ \bigcap_{i=1}^{n} \bigcap_{x \in G} H_i^x = 1 \right\}$$

and if $t_1, t_2 | q-1$ and $(t_1, t_2) = 1$ we have $G(t_1) \cap G(t_2) = SL_2(q)$; hence we must study subgroups of $GL_2(q)$, say H, such that $\operatorname{core}_{GL_2(q)}(H) \cap SL_2(q) = 1$. In this case we choose $t_1, t_2, \ldots, t_k$ such $t_1, t_2, \ldots, t_k | q-1$ and $(t_1, \ldots, t_k) = 1$ and $\sum_{i=1}^k (q-1)/t_i$ minimal.

THEOREM 3.4. *If $q \neq 2, 3$, then*

$$p(GL_2(q)) \geq \min_k \left\{ \sum_{i=1}^{k} \frac{q-1}{t_i} \right\} + p(SL_2(q)).$$

Proof. By the above remark, if $H \leq GL_2(q)$ and $\operatorname{core}_{SL_2(q)}(H) \cap SL_2(q) = 1$, then $\operatorname{core}_{GL_2(q)}(H) \cap SL_2(q) = 1$ and by Lemma 3.2

$$[G:H] \geq (q-1)_2(q+1).$$

Therefore

$$p(GL_2(q)) \geq \min_k \left\{ \sum_{i=1}^{k} \frac{q-1}{t_i} \right\} + p(SL_2(q)).$$

▮

LEMMA 3.5. *Let $G = GL_2(q)$, q odd, $q \neq 3$ and $q - 1 = 2^t m$ and m odd. We define*

$$L = \left\{ \alpha \in GF(q)^* : \alpha = \beta^{2^t} \text{ for some } \beta \in GF(q)^* \right\}$$

and

$$Q = \left\{ \begin{bmatrix} \alpha & \beta \\ 0 & \gamma \end{bmatrix} : \alpha \in L,\ \gamma \in GF(q)^*,\ \beta \in GF(q) \right\}.$$

Then $Q \leq GL_2(q)$ and $\operatorname{core}_G Q \cap SL_2(q) = 1$.

Proof. It is clear that $L \leq GF(q)^*$. By consideration of the epimorphism $\varphi: GF(q)^* \to L$ with $\varphi(x) = x^{2^t}$ we have $|L| = (q-1)/\frac{q-1}{m} = m = (q-1)/2^t$. Now it is clear that Q is a subgroup of G and $|Q| = ((q-1)/2^t)(q-1)q$ and therefore $[G : Q] = 2^t(q+1) = (q-1)_2(q+1)$. We know $\operatorname{core}_G(Q) \trianglelefteq G$ and $Q \supseteq \operatorname{core}_G(Q)$ and therefore $\operatorname{core}_G(Q) \supseteq Z(G)$ or $\operatorname{core}_G(Q) \supseteq SL_2(Q)$. If $\operatorname{core}_G(Q) \supseteq SL_2(q)$ then $Q \supseteq SL_2(q)$. But $|Q| = (q(q-1)^2)/2^t$ and $|SL_2(q)| = q(q-1)(q+1)$, implying $((q-1)/2^t)(q-1)q = q(q^2-1)$. Therefore $(q-1)/2^t = q+1$ or $m = q+1$ and this implies that m is even, and this is a contradiction. So $\operatorname{core}_G(Q) \not\supseteq SL_2(q)$ and hence $\operatorname{core}_G(Q) \subseteq Z(G)$. This implies $\operatorname{core}_G(Q)$ is cyclic and $\operatorname{core}_G(Q) \leq \{[\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}] : \alpha \in L\}$. Since $\{[\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}] : \alpha \in L\} \subseteq Q$, we have for all $x \in G$, $\{[\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}] : \alpha \in L\}^x \subseteq Q^x$; therefore $\{[\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}] : \alpha \in L\} \subseteq \bigcap_{x \in G} Q^x = \operatorname{core}_G(Q)$.

Hence $\operatorname{core}_G(Q) = \{[\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}] : \alpha \in L\}$ and $|\operatorname{core}_G(Q)| = m$. Now if $A = [\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}] \in \operatorname{core}_G(Q) \cap SL_2(q)$, then $\lambda \in L$ and $\lambda^2 = 1$; i.e., $\lambda^m = 1$ and $\lambda^2 = 1$. But as $(2, m) = 1$, λ must be 1. Therefore $\operatorname{core}_G(Q) \cap SL_2(q) = 1$. ▮

THEOREM 3.6. *Let $G = GL_2(q)$ and q odd, $q \neq 3, q - 1 = t_1 t_2, \dots, t_k$, $(t_1, \dots, t_k) = 1$; then*

$$p(G) \leq \min_k \left\{ \sum_{i=1}^{k} \frac{q-1}{t_i} \right\} + (q-1)_2(q+1).$$

Proof. By Lemma 3.5 we have $SL_2(q) \cap \mathrm{core}_G(Q) = 1$ and by the above remark and definition of $p(G)$ we have

$$p(G) \leq \min_k \sum_{i=1}^{k} \frac{q-1}{t_i} + [G:Q]$$
$$= \min_k \left\{ \sum_{i=1}^{k} \frac{q-1}{t_i} \right\} + (q-1)_2(q+1).$$

∎

The following concept is defined in [7].

Let G be a finite abelian group; then G is isomorphic to the direct product of its Sylow p-subgroups. Suppose $G = \oplus_{i=1}^{k} \mathbb{Z}_{p_i^{\alpha_i}}$; then we let $T(G) := \sum_{i=1}^{k} p_i^{\alpha_i}$. If $G = 1$, the trivial group, then we let $T(G) = 0$.

THEOREM 3.7. *Let $G = GL_2(q)$ and q odd, $q \neq 3, q - 1 = t_1 t_2, \dots, t_k$, $(t_1, \dots, t_k) = 1$; then $p(G) = T(\mathbb{Z}_{q-1}) + (q-1)_2(q+1)$.*

Proof. See Theorems 3.4 and 3.6. ∎

Note 1. We will determine $p(GL_2(3))$ after finding $q(GL_2(3))$.

THEOREM 3.8. *Let $G = GL_2(q)$ where q is even, $q \neq 2$; then*

$$p(G) = T(\mathbb{Z}_{q-1}) + q + 1 = T(\mathbb{Z}_{q-1}) + p(SL_2(q)).$$

Proof. If $q - 1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, let $t_i = \prod_{j=1, j\neq i}^{k} p_j^{\alpha_j}$, $i = 1, 2, \dots, k$; therefore $(q-1)/t_i = p_i^{\alpha_i}$. In Theorem 3.4 we showed that $p(G) \geq \sum_{i=1}^{k} p_i^{\alpha_i} + (q+1)$. Now we should show that $p(G) \leq \sum_{i=1}^{k} p_i^{\alpha_i} + (q+1)$. When q is even, then $GL_2(q) \cong \mathbb{Z}_{q-1} \times SL_2(q)$, so we choose subgroups H_l of G such that $H_l = K_l \times N_l$, $l = 1, \dots, k, k+1$ and $K_l = \mathbb{Z}_{t_l}$, $N_l = SL_2(q)$ for $l = 1, \dots, k$ and

$$K_{k+1} = \mathbb{Z}_{q-1}, N_{k+1} = \left\{ \begin{bmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{bmatrix} : \alpha \in GF(q)^*, \ \beta \in GF(q) \right\}.$$

As $SL_2(q)$, $q = 2^n$, $n \neq 1$ is simple group; then N_{k+1} is a core-free subgroup of $SL_2(q)$ with $[SL_2(q) : N_{k+1}] = q + 1$. Consequently $\mathrm{core}_G(H_l) = H_l$, $l = 1, \dots, k$ and $\mathrm{core}_G(H_{l+1}) = \mathbb{Z}_{q-1} \times \{1\}$ and $\bigcap_{l=1}^{k+1} \mathrm{core}_G(H_l) = 1$. Thus $p(G) \leq \sum_{i=1}^{k} p_i^{\alpha_i} + q + 1$. By the last notation $p(G) = T(\mathbb{Z}_{q-1}) + q + 1$. ∎

COROLLARY 3.9. *Let $q - 1$ be a prime and let $q \neq 3$. Then $p(G) = 2q$.*

Proof. When $q - 1$ is a prime, then q must be even and therefore $p(SL_2(q)) = q + 1$ and $T(\mathbb{Z}_{q-1}) = q - 1$, and the corollary is proved. ∎

COROLLARY 3.10. *Let $G = GL_2(2)$; then $p(G) = 3$.*

Proof. It follows from the fact that $GL_2(2) \cong S_3$. ∎

Let $G \neq 1$ and $G = K \times H$. Then

$$p(G) = \begin{cases} p(K) & \text{if } H = 1 \\ p(H) & \text{if } K = 1 \\ p(H) + p(K) & \text{otherwise.} \end{cases}$$

Since in the case q is even we have $GL_2(q) \cong GF(q)^* \times SL_2(q)$, so $p(GL_2(q)) = T(GF(q)^*) + p(SL_2(q))$.

4. ALGORITHMS FOR $r(G)$, $c(G)$, AND $q(G)$

Let $G = GL_2(q)$; then G has four type of conjugacy classes, A_1, A_2, A_3, and B_1, and four type of irreducible characters, $\chi_1^{(n)}$, $\chi_q^{(n)}$, $\chi_{q+1}^{(m,n)}$, and $\chi_{q-1}^{(l)}$ (Table I).

LEMMA 4.1. (a) *Let $d = (n, q-1)$; then the kernel of $\chi_1^{(n)}$ consists of precisely the elements*

$$A_1 = \begin{bmatrix} \varepsilon^a & 0 \\ 0 & \varepsilon^a \end{bmatrix}, \qquad A_2 = \begin{bmatrix} \varepsilon^a & 0 \\ 1 & \varepsilon^a \end{bmatrix}, \qquad A_3 = \begin{bmatrix} \varepsilon^{a'} & 0 \\ 0 & \varepsilon^b \end{bmatrix},$$

$$B_1 = \begin{bmatrix} \eta^c & 0 \\ 0 & \eta^{cq} \end{bmatrix},$$

where

$$a = k\left(\frac{q-1}{2d}\right), \qquad a' + b = k'\left(\frac{q-1}{d}\right), \qquad c = k''\left(\frac{q-1}{d}\right),$$

$$1 \le k \le 2d,\ 1 \le k' \le \frac{d(2q-5)}{q-1},$$

$$1 \le k'' \le d(q+1) \qquad \text{and} \qquad q+1 \nmid c.$$

(b) *Let $d = (n, q-1)$; then*

$$\ker \chi_q^{(n)} = \left\langle A_1 = \begin{bmatrix} \varepsilon^a & 0 \\ 0 & \varepsilon^a \end{bmatrix} : a = k\left(\frac{q-1}{2d}\right),\ 1 \le k \le 2d \right\rangle.$$

(c) *Let* $d' = (m+n, q-1)$; *then*

$$\ker \chi_{q+1}^{(m,n)} = \left\langle A_1 = \begin{bmatrix} \varepsilon^a & 0 \\ 0 & \varepsilon^a \end{bmatrix} : a = k\left(\frac{q-1}{d'}\right),\ 1 \le k \le d' \right\rangle.$$

(d) *Let* $d'' = (l, q-1)$; *then*

$$\ker \chi_{q-1}^{(l)} = \left\langle A_1 = \begin{bmatrix} \varepsilon^a & 0 \\ 0 & \varepsilon^a \end{bmatrix} : a = k\left(\frac{q-1}{d''}\right),\ 1 \le k \le d'' \right\rangle.$$

Proof. (a) $A_1 \in \ker \chi_1^{(n)}$ if and only if $\rho^{2na} = 1$ if and only if $q - 1 | 2na$; hence $\frac{q-1}{d} | \frac{2na}{d}$. Since $(\frac{q-1}{d}, \frac{n}{d}) = 1$, $\frac{q-1}{d} | 2a$. Thus $a = k(\frac{q-1}{2d})$, for some k, $1 \le k \le 2d$. Similarly $A_2 \in \ker \chi_1^{(n)}$ if and only if $a = k(\frac{q-1}{2d})$. Also $A_3 \in \ker \chi_1^{(n)}$ if and only if $\rho^{n(a+b)} = 1$ if and only if $q - 1 | n(a+b)$. Since $(\frac{q-1}{d}, \frac{n}{d}) = 1$, therefore $\frac{q-1}{d} | a + b$ and $a + b = k'(\frac{q-1}{d})$ for some k', $1 \le k' \le \frac{d(2q-5)}{q-1}$, and $B_1 \in \ker \chi_1^{(n)}$ if and only if $\rho^{nc} = 1$ if and only if $q - 1 | nc$ and hence $c = k'' \frac{q-1}{d}$, $1 \le k'' \le d(q+1)$, and $q + 1 \nmid c$. (b), (c), and (d) are proved similarly. ∎

LEMMA 4.2. *Let* $d = (n, q-1)$. *Then* $|\Gamma(\chi_1^{(n)})| = \varphi(\frac{q-1}{d})$ *and* $|\Gamma(\chi_q^{(n)})| = \varphi(\frac{q-1}{d})$.

Proof.

$$|\Gamma(\chi_1^{(n)})| = \left[\mathbb{Q}(\chi_1^{(n)}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\rho^{2n}, \rho^{n(a+b)}, \rho^n) : \mathbb{Q}\right]$$
$$= \left[\mathbb{Q}(\rho^n) : \mathbb{Q}\right] = \varphi\left(\frac{q-1}{d}\right),$$

where ρ^n is a primitive $\frac{q-1}{d}$th root of unity in $\mathbb{C}$. The proof of the next statement is similar. ∎

LEMMA 4.3. (a) *Let* $d = (m+n, q-1)$; *then* $[\mathbb{Q}(\rho^{(m+n)a}) : \mathbb{Q}] = \varphi(\frac{q-1}{d})$, $\rho^{q-1} = 1$.

(b) *Let* $d' = (l, q-1)$; *then* $[\mathbb{Q}(\delta^{l(q+1)}) : \mathbb{Q}] = \varphi((q-1)/d')$, $\delta^{q^2-1} = 1$.

Proof. (a) Since $\rho^{q-1} = 1$, therefore $(\rho^{m+n})^{(q-1)/d} = (\rho^{q-1})^{(m+n)/d} = 1$. If s is an integer such that $(\rho^{m+n})^s = 1$, then $q - 1 | (m+n)s$ and therefore $\frac{q-1}{d} | \frac{m+n}{d} s$; thus $\frac{q-1}{d} | s$. It follows that ρ^{m+n} is a primitive $\frac{q-1}{d}$th root of unity. (b) is proved similarly. ∎

LEMMA 4.4. (a) *Let* $d = (m+n, q-1)$; *then* $|\Gamma(\chi_{q+1}^{(m,n)})| = K\varphi(\frac{q-1}{d})$, *where* $K = [\mathbb{Q}(\rho^{(m+n)a}, \rho^{na+mb} + \rho^{ma+nb}) : \mathbb{Q}(\rho^{(m+n)a})]$.

(b) *Let* $d' = (l, q-1)$; *then* $|\Gamma(\chi_{q-1}^{(l)})| = K'\varphi((q-1)/d')$ *where* $K' = [\mathbb{Q}(\delta^{l(q+1)}, \delta^l + \delta^{lq}) : \mathbb{Q}(\delta^{l(q+1)})]$.

Proof.

(a) $|\Gamma(\chi_{q+1}^{(m,n)})|$

$$= \left[\mathbb{Q}\left(\rho^{(m+n)a}, \rho^{ma+nb} + \rho^{na+mb}\right) : \mathbb{Q}\right]$$
$$= \left[\mathbb{Q}\left(\rho^{(m+n)a}, \rho^{ma+nb} + \rho^{na+mb}\right) : \mathbb{Q}\left(\rho^{(m+n)a}\right)\right]\left[\mathbb{Q}\left(\rho^{(m+n)a}\right) : \mathbb{Q}\right]$$
$$= K \cdot \varphi\left(\frac{q-1}{d}\right)$$

[by Lemma 4.3(a)].

(b) Since $0 \le a \le q-2$, $1 \le c \le q^2-1$, an easy computation shows that $[\mathbb{Q}(\delta^{la(q+1)}, \delta^{lc} + \delta^{lcq}) : \mathbb{Q}] = [\mathbb{Q}(\delta^{l(q+1)}, \delta^{l} + \delta^{lq}) : \mathbb{Q}]$ and hence $|\Gamma(\chi_{q-1}^{(l)}| = [\mathbb{Q}(\delta^{la(q+1)}, \delta^{lc} + \delta^{lcq}) : \mathbb{Q}] = [\mathbb{Q}(\delta^{l(q+1)}, \delta^{l} + \delta^{lq}) : \mathbb{Q}]$ $= [\mathbb{Q}(\delta^{l(q+1)}, \delta^{l} + \delta^{lq}) : \mathbb{Q}(\delta^{l(q+1)})][\mathbb{Q}(\delta^{l(q+1)}) : \mathbb{Q}] = K'\varphi((q-1)/d')$ [by Lemma 4.3(b)]. ∎

LEMMA 4.5. *Let $q \equiv 1 \pmod 4$; then there is some $l \in \mathbb{N}, 0 < l < q^2-1$, $q+1 \nmid l$ such that $\delta^l + \delta^{lq}$ is rational and consequently K', mentioned in Lemma 4.4(b), is one and $|\Gamma(\chi_{q-1}^{l})| = \varphi((q-1)/d')$ where $d' = (l, q-1)$.*

Proof. Since $\delta^{q^2-1} = 1$,

$$\delta = \cos\frac{2\pi}{q^2-1} + i\sin\frac{2\pi}{q^2-1}$$

and

$$\delta^l + \delta^{lq}$$
$$= \cos\frac{2\pi l}{q^2-1} + i\sin\frac{2\pi l}{q^2-1} + \cos\frac{2\pi lq}{q^2-1} + i\sin\frac{2\pi lq}{q^2-1}$$
$$= \left(\cos\frac{2\pi l}{q^2-1} + \cos\frac{2\pi lq}{q^2-1}\right) + i\left(\sin\frac{2\pi l}{q^2-1} \sin\frac{2\pi lq}{q^2-1}\right).$$

If

$$\sin\frac{2\pi l}{q^2-1} + \sin\frac{2\pi lq}{q^2-1} = 0,$$

then $\delta^l + \delta^{lq} \in \mathbb{Q}$, and in this case we obtain $l = \frac{(2t+1)(q+1)}{2}$ or $t'(q-1)$, $t' \nmid q+1$.

Now for these l's we have $|\Gamma(\chi_{q-1}^{(l)})| = \varphi((q-1)/d')$.

LEMMA 4.6. *Let q be odd, and let $m = q-1$, $n = \frac{q-1}{2}$, then the character $\chi_{q+1}^{(m,n)}$ is rational. In this case $\chi_{q+1}^{(m,n)}(g) = (-1)^a(q+1)$ for all*

$g \in A_1$, $\chi_{q+1}^{(m,n)}(g) = (-1)^a$ for all $g \in A_2$, $\chi_{q+1}^{(m,n)}(g) = (-1)^a + (-1)^b$ for all $g \in A_3$, and $\chi_{q+1}^{(m,n)}(g) = 0$ for all $g \in B_1$ where $b, a = 0, 1, \ldots, q-2$, and $a \neq b$.

Proof. If $m = q-1$, $n = \frac{q-1}{2}$ then $\rho^{(m+n)a} = (\rho^{(q-1)/2})^{3a} = (-1)^{3a} = (-1)^a$ and $\rho^{ma+nb} + \rho^{na+mb} = \rho^{((q-1)/2)(a+2b)} + \rho^{((q+1)/2)(2a+b)} = (-1)^{a+2b} + (-1)^{2a+b} = (-1)^a + (-1)^b$. Therefore the proof is complete. ∎

LEMMA 4.7. *The character $\chi_{q-1}^{(l)}$ is real if and only if $q-1|l$. In this case $\chi_{q-1}^{(l)}(g) = q-1$ for all $g \in A_1$, $\chi_{q-1}^{(l)}(g) = 1$ for all $g \in A_2$, $\chi_{q-1}^{(l)}(g) = 0$ for all $g \in A_3$, and $\chi_{q-1}^{(l)}(g) = -(\delta^{lj(q-1)} + \delta^{-lj(q-1)})$ for all $g \in B_1$, where $j = 1, 2, \ldots, \frac{q-1}{2}$.*

Proof. If $q-1|l$, then $\delta^{la(q+1)} = \delta^{k(q-1)a(q+1)} = \delta^{(q^2-1)ka} = 1$; therefore $\chi_{q-1}^{(l)}(g) \in \mathbb{R}$ for all $g \in A_1, A_2, A_3$ and $\chi_{q-1}^{(l)}(g) = -(\delta^{k(q-1)c} + \delta^{k(q-1)cq}) = -(\delta^{kc(q-1)} + \delta^{-kc(q-1)}) = 2\,\mathrm{Re}(z)(\delta^{kc(q-1)}) \in \mathbb{R}$ for all $g \in B_1$. Conversely if $\chi_{q-1}^{(l)}$ is real then $\delta^{la(q+1)} \in \mathbb{R}$, $\delta^{lc} + \delta^{lcq} \in \mathbb{R}$, $c = 1, 2, \ldots, q^2-2$, $q+1 \nmid c$; therefore $\sin\frac{2\pi la}{q-1} = 0$. Hence $\frac{2al}{q-1} \in \mathbb{Z}$, in particular for $a = 1$, $\frac{2l}{q-1} \in \mathbb{Z}$. Thus $q-1|2l$. If q is even, then $q-1|l$. But if q is odd, then $l = (\frac{q-1}{2})k$, $k \in \mathbb{Z}$. Also, since $\delta^{lc} + \delta^{lcq}$ should be real, we conclude that k is even; therefore $l = (\frac{q-1}{2})2t$, which implies $q-1|l$, and the proof is complete. ∎

As $r(G)$, $c(G)$, and $q(G)$ for $G = GL_2(q)$ depend on q, we must consider different cases for q, say $q = 2^t$ ($q \equiv 1 \pmod 3$ or $q \equiv 2 \pmod 3$) and q odd ($q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$), which in the last case we have to consider the two cases $q \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$.

LEMMA 4.8. *Let $q = 2^t$.*

(a) *If $(q-1, n) = 1$, then $1 \neq A_1 \notin \ker \chi_1^{(n)}$.*

(b) *If $d = (q-1, n) \neq 1$, then for $a = \frac{k}{2}(\frac{q-1}{d})$, where $0 \leq k < 2d$, $A_1 \in \ker \chi_1^{(n)}$.*

Proof. This follows from Lemma 4.1. ∎

LEMMA 4.9. *Let $q = 2^t$, $d_i = (n_i, q-1) \neq 1$, and $(d_1, d_2, \ldots, d_s) = 1$, for some s, $1 \leq s \leq q-1$; then $A_1 \cap (\bigcap_{i=1}^{s} \ker \chi_1^{(n_i)}) = 1$.*

Proof. We prove the lemma for $s = 2$ and then by induction for any s the result follows. If $d_1, d_2|q-1$ and $(d_1, d_2) = 1$ and $A_1 \in \ker \chi_1^{(n)}$ then $a = (k_1/2)((q-1)/d_1)$ for some $k_1 \in \mathbb{N}$. Also $A_1 \in \ker \chi_1^{(n_2)}$ implies $a = (k_2/2)((q-1)/d_2)$ for some k_2; therefore $k_1/d_1 = k_2/d_2$ and $k_1 d_2 = d_1 k_2$. Thus $d_1|k_1$ and $d_2|k_2$ imply $k_1 = t_1 d_1$, $k_2 = t_2 d_2$; hence $t_1 d_1 d_2 = t_2 d_2 d_1$, so $t_1 = t_2$. By Lemma 4.8(b) we must have $t_1 = t_2 = 1$. Then $a = \frac{q-1}{2}$, and this is a contradiction. Thus $A_1 \cap \ker \chi_1^{(n_1)} \cap \ker \chi_1^{(n_2)} = 1$. ∎

COROLLARY 4.10. *Let* $q = 2^t$ *and let* $d_i = (n_i, q-1) \neq 1, (d_1, \ldots, d_s) = 1$ *for some* s, $1 \leq s \leq q-1$; *then*

(a) $(\bigcap_i \ker \chi_1^{(n_i)}) \cap (\ker \chi_q^{(n')}) = 1$.

(b) $(\bigcap_i \ker \chi_1^{(n_i)}) \cap (\ker \chi_{q+1}^{(m,n)}) = 1$.

(c) $(\bigcap_i \ker \chi_1^{(n_i)}) \cap (\ker \chi_{q-1}^{(l)}) = 1$.

In particular, when $\chi_q^{(n')}$, $\chi_{q+1}^{(m,n)}$, $\chi_{q-1}^{(l)}$ *are rational, the above results hold.*

Proof. It is obvious (by Lemmas 4.1 and 4.9). ∎

Among the characters of type $\chi_q^{(n)}$, there is the rational character $\chi_q^{(q-1)}$ which is called the Steinberg character. Now want to choose those irreducible characters such that they are faithful and rational and are of minimal degree. So we must consider the characters of type $\chi_q^{(n)}$ or $\chi_{q-1}^{(l)}$.

LEMMA 4.11. *Let* $q = 2^t$.

(a) *If* $q \equiv 2 \pmod 3$, *then there is at least a rational character of type* $\chi_{q-1}^{(l)}$.

(b) *If* $q \equiv 1 \pmod 3$, *then* $\chi_{q-1}^{(l)}$ *is not rational.*

Proof. (a) By Lemma 4.7, $\chi_{q-1}^{(l)}$ is rational if and only if $\delta^{j(q-1)} + \delta^{-j(q-1)}$ is rational. Let $\varepsilon = \delta^{q-1}$; by [3, Corollary 3.2] $\varepsilon^j + \varepsilon^{-j} \in \mathbb{Q}$ if and only if $q+1 = 3j, \frac{3}{2}j, \frac{4}{3}j, \frac{6}{5}j$, and $1 \leq j \leq q/2$. Since $q \equiv 2 \pmod 3$, $3 | q+1$ and there is $j = \frac{q+1}{3}$; thus $\chi_{q-1}^{(j(q-1))}$ is rational.

(b) If $q \equiv 1 \pmod 3$, then $q+1 \equiv 2 \pmod 3$ and hence $q+1 \neq 3j, \frac{3}{2}j, \frac{4}{3}j, \frac{6}{5}j$, and this completes the proof. ∎

LEMMA 4.12. *Let* $q = 2^t$ *and* $q - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. *Let* $t_i = \prod_{j=1, j\neq i}^{k} p_j^{\alpha_j}$; *then*

$$\sum_{i=1}^{k} \varphi\left(\frac{q-1}{t_i}\right) \leq \varphi(q-1).$$

Proof. By choosing t_i's, there are $\chi_1^{(n_i)}$'s such that $t_i = (n_i, q-1), (t_1, \ldots, t_k) = 1$. Also $(q-1)/t_i = p_i^{\alpha_i}$; therefore

$$\sum_{i=1}^{k} \varphi\left(\frac{q-1}{t_i}\right) = \sum_{i=1}^{k} \varphi(p_i^{\alpha_i}) = \sum_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$
$$< \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \varphi(q-1).$$

∎

LEMMA 4.13. *Let* $d_i = (n_i, q-1)$. *If* $(d_r, d_s) \neq 1$, *then* $\ker \chi_1^{(n_r)} \cap \ker \chi_1^{(n_s)} \neq 1$.

If $(d_r, d_s) = h \neq 1$, then for $a = \frac{q-1}{h}$, $A_1 \in \ker \chi_1^{(n_r)} \cap \ker \chi_1^{(n_i)}$ because $\rho^{2n_1 a} = \rho^{2n_1((q-1)/h)} = (\rho^{q-1})^{2n_1/h} = 1$ and also $\rho^{2n_2 a} = \rho^{2n_2((q-1)/h)} = (\rho^{q-1})^{2n_2/h} = 1$.

COROLLARY 4.14. *Let $q = 2^t$ and $q - 1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $d_i = (q-1, n_i)$; then*

$$\min\left\{ \sum_{d_i} \varphi\left(\frac{q-1}{d_i}\right) : \bigcap \ker \chi_1^{(n_i)} = 1 \right\} = \sum_{i=1}^{k} \varphi(p_i^{\alpha_i}).$$

Proof. The result follows by Lemma 4.13. ∎

THEOREM 4.15. *Let $q = 2^t$, $q - 1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$; p_i's are prime and $(p_i, p_j) = 1$ for all $i, j, i \neq j$. Then*

$$r(GL_2(q)) = \begin{cases} \sum_{i=1}^{k} \varphi(p_i^{\alpha_i}) + q & \text{if } q \equiv 1 \pmod 3, \\ \sum_{i=1}^{k} \varphi(p_i^{\alpha_i}) + (q-1) & \text{if } q \equiv 2 \pmod 3. \end{cases}$$

Proof. This follows from Corollary 4.10, Lemmas 4.11 and 4.12, Corollary 4.14, and the definition of $r(G)$. ∎

LEMMA 4.16. *Let $q = 2^t$, $q - 1 = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $t_i = \prod_{j=1, j\neq i}^{k} p_j^{\alpha_j}$, $\Gamma_i = (\mathbb{Q}(\rho_{t_i}) : \mathbb{Q})$, where $\rho_{t_i} = \rho^{t_i}$ is a primitive $(q-1)/t_i$th root of unity. Then*

$$\sum_{\alpha \in \Gamma_i} (\rho_{t_i})^{\alpha} = \begin{cases} -1 & \text{if } \alpha_i = 1, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. By [3, Lemma 3.8] we have

$$\sum_{\alpha \in \Gamma_i} (\rho_{t_i})^{\alpha} = \frac{\varphi\left(\frac{q-1}{t_i}\right)}{\varphi\left(\frac{\frac{q-1}{t_i}}{\left(\frac{q-1}{t_i}, t_i\right)}\right)} \mu\left(\frac{\frac{q-1}{t_i}}{\left(\frac{q-1}{t_i}, t_i\right)}\right).$$

But since $((q-1)/t_i, t_i) = 1$, therefore

$$\frac{\varphi\left(\frac{q-1}{t_i}\right)}{\varphi\left(\frac{q-1}{t_i}\right)}\mu\left(\frac{q-1}{t_i}\right) = \mu\left(\frac{q-1}{t_i}\right) = \mu\left(p_i^{\alpha i}\right) = \begin{cases} -1 & \text{if } \alpha_i = 1, \\ 0 & \text{otherwise.} \end{cases}$$

∎

THEOREM 4.17. *Let* $q = 2^t$, $q - 1 = \prod_{i=1}^k p_i^{\alpha_i}$; *then*

$$q(GL_2(q)) = c(GL_2(q)) = \begin{cases} \sum_{i=1}^{k} \varphi(p_i^{\alpha_i}) + q + 1 + \left(-\sum_{j \in J}(-1)\right) \\ \qquad \text{if } q \equiv 1 \pmod 3, \\ \sum_{i=1}^{k} \varphi(p_i^{\alpha_i}) + (q-1) + 2 + \left(-\sum_{j \in J}(-1)\right) \\ \qquad \text{if } q \equiv 2 \pmod 3, \end{cases}$$

where $J \subseteq \{1, 2, \ldots, k\}$, $\alpha_j = 1$.

Proof. Suppose $q \equiv 1 \pmod 3$. Then by Lemmas 4.10(a) and 4.11(b) we may choose the Steinberg character $\chi_q^{(q-1)}$ and $\chi_1^{(n_i)}$'s. The minimum values of these characters appear on classes of type B_1, and are -1 and $(\sum_{j \in J}(-1))$, respectively, where $J \subseteq \{1, 2, \ldots, k\}$, for which $\alpha_j = 1$ (Lemma 4.16).

Therefore

$$m(\chi) = 1 + \left(-\sum_{j \in J}(-1)\right)$$

and this χ is the desired character. So the minimal degree of quasi-permutation characters is

$$\sum_{i=1}^{k} \varphi(p_i^{\alpha_i}) + q + 1 + \left(-\sum_{j \in J}(-1)\right),$$

where $J \subseteq \{1, 2, \ldots, k\}$, $\alpha_j = 1$.

Now assume $q \equiv 2 \pmod 3$. In this case by Corollary 4.10(c) and Lemma 4.11(a) we choose the characters $\chi_1^{(n_i)}$'s and $\chi_{q-1}^{((q+1)/3)}$. Also the minimum values of these characters appear on the classes of type B_1 and are

$\Sigma_{j \in J}(-1)$, $J \subseteq \{1,2,\ldots,k\}$, $\alpha_j = 1$, and -2 respectively and

$$m(\chi) = 2 + \left(-\sum_{j\in J}(-1)\right),$$

where $J \subseteq \{1,2,\ldots,k\}$, $\alpha_j = 1$, and χ is the desired character.

So the minimal degree of a quasi-permutation character is obtained from these characters and the proof is complete. ∎

LEMMA 4.18. *Let* $q \equiv 3 \pmod 4$, $q \neq 3$, *and* $d = (n, q-1)$. *Then*

$$\ker \chi_1^{(n)} \cap \ker \chi_{q+1}^{(q-1, \frac{q-1}{2})} = 1 \qquad \text{if } d = 1 \text{ or } 2$$

$$\ker \chi_1^{(n)} \cap \ker \chi_{q+1}^{(q-1, \frac{q-1}{2})} \neq 1 \qquad \text{if } d \neq 1, 2.$$

Proof. Let $1 \neq A_1 \in \ker \chi_1^{(n)} \cap \ker \chi_{q+1}^{(q-1,(q-1)/2)}$. By Lemma 4.1(c), $a = k((q-1)/(q-1+\frac{q-1}{2}, q-1)) = 2k$, and also by Lemma 4.1(a), $a = k(\frac{q-1}{2d})$. Hence whenever $a = k(\frac{q-1}{2d})$ is even, then $\ker \chi_1^{(n)} \cap \ker \chi_{q+1}^{(q-1,(q-1)/2)} \neq 1$.

Let $d = 1$. Then by Lemma 4.1(a), $1 \leq k \leq 2$. Therefore $k = 1$ or 2; that is, $q = \frac{q-1}{2}$ or $a = q-1$. But $a = \frac{q-1}{2}$ is odd and when $a = q-1$, then $A_1 = 1$. So the result follows when $d = 1$.

Let $d = 2$. Then by Lemma 4.1(a), $1 \leq k \leq 4$. Therefore $k = 1, 2, 3$, or 4; that is, $a = \frac{q-1}{4}, \frac{q-1}{2}, \frac{3(q-1)}{2}$, or $q-1$. The case $a = \frac{q-1}{4}$ cannot happen, as $q \equiv 3 \pmod 4$, and when $a = \frac{q-1}{2}$ or $\frac{3(q-1)}{2}$, then a is odd. So again in this case the result follows.

Now let $d \neq 1, 2$. Then $1 \leq k \leq 2d$, so let $k = 4$. Hence in this case $a = 2(\frac{q-1}{d})$ and a is even. Therefore the result follows.

LEMMA 4.19. *Let* $q \equiv 3 \pmod 4$ *and* $(n, q-1) = 2$; *then* $|\Gamma(\chi_1^{(n)})| = \varphi(q-1)$.

Proof. Since $q \equiv 3 \pmod 4$, $q - 1 = 2(2s+1)$ for some $s \in \mathbb{N}$; thus $\varphi(\frac{q-1}{2}) = \varphi(q-1)$. Therefore, by Lemma 4.2, $|\Gamma(\chi_1^{(n)})| = \varphi(q-1)$. ∎

LEMMA 4.20. *Let* $\chi_{q-1}^{(l)}$ *be rational. Then* $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$.

Proof. By Lemma 4.7, $A_1 \in \ker \chi_{q-1}^{(l)}$, for all A_1. Also some classes of type A_1 belong to $\ker \chi_1^{(n)}$; therefore $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$. ∎

By Lemma 4.1(a),(b) $\ker \chi_q^{(n)} \subseteq \ker \chi_1^{(n)}$ and therefore $\ker \chi_1^{(n)} \cap \ker \chi_q^{(n)} \neq 1$. Also by Lemmas 4.6 and 4.7 if $\chi_{q-1}^{(l)}$ and $\chi_{q+1}^{(m,n)}$ are rational then $\ker \chi_{q+1}^{(m,n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$.

THEOREM 4.21. *Let* $q \equiv 3 \pmod 4$, $q \neq 3$; *then* $r(G) = q + 1 + \varphi(\frac{q-1}{2})$.

Proof. This result follows from the definition of $r(G)$ and Lemmas 4.18, 4.19, and 4.20. ∎

LEMMA 4.22. *Let $q \equiv 3 \pmod 4$, $q \neq 3$. Then $\chi_{q+1}^{(q-1,(q-1)/2)}(g) = -(q+1)$ for $g \in A_1$ if a odd. Conversely if $\chi_{q+1}^{(q-1,(q-1)/2)}(g) = -(q+1)$ for $g \in A_1$ then a is odd.*

Proof. $\chi_{q+1}^{(q-1,(q-1)/2)}(g) = (q+1)\rho^{(3/2)(q-1)a} = (q+1)(\rho^{(q-1)/2})^{3a} = (q+1)(-1)^{3a} = -(q+1)$ for $g \in A_1$ because $3a$ is odd. Conversely if $\chi_{q+1}^{(q-1,(q-1)/2)}(g) = -(q+1)$ for $g \in A_1$ then we should have $(q+1)\rho^{(3/2)(q-1)a} = -(q+1)$. Thus $\rho^{(3/2)(q-1)a} = -1$ and then $(\rho^{(q-1)/2})^{3a} = (-1)^{3a} = -1$, so a must be odd. ∎

LEMMA 4.23. *Let $q \equiv 3 \pmod 4$, $q \neq 3$. Then for $a = 2k+1, a = 0, 1, \ldots, q-2$ and $(n, q-1) = 1$ or 2 we have*

$$\sum_{\alpha \in \Gamma} (\rho^{2na})^{\alpha} = \frac{\varphi(q-1)}{\varphi\left(\dfrac{q-1}{2\left(\dfrac{q-1}{2}, 2a\right)}\right)} \mu\left(\frac{q-1}{2\left(\dfrac{q-1}{2}, 2a\right)}\right).$$

Proof. By [3] and Lemma 4.19 we have

$$\begin{aligned}\sum_{\alpha \in \Gamma} (\rho^{2na})^{\alpha} &= \sum_{\alpha \in \Gamma} ((\rho^{n})^{2a})^{\alpha} \\ &= \frac{\varphi\dfrac{(q-1)}{2}}{\varphi\left(\dfrac{\dfrac{q-1}{2}}{\left(\dfrac{q-1}{2}, 2a\right)}\right)} \mu\left(\frac{\dfrac{q-1}{2}}{\left(\dfrac{q-1}{2}, 2a\right)}\right) \\ &= \frac{\varphi(q-1)}{\varphi\left(\dfrac{q-1}{2\left(\dfrac{q-1}{2}, 2a\right)}\right)} \mu\left(\frac{q-1}{2\left(\dfrac{q-1}{2}, 2a\right)}\right).\end{aligned}$$

∎

LEMMA 4.24. *Let $q \equiv 3 \pmod 4$, $q \neq 3$, $a = 2k+1$, $a = 0, 1, \ldots, q-2$, and $d = (\frac{q-1}{2}, 2a)$. Then there is d such that $\mu(\frac{q-1}{2d}) = -1$.*

Proof. $q \equiv 3 \pmod 4$ implies $q - 1 = 2(2k' + 1)$ for some $k' \in \mathbb{N}$, so $q - 1 = 2.p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$, where all p_i's are odd primes. Let $a = p_2^{\alpha_2 - 1} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$; it is clear that a satisfies the condition of our lemma. Thus $(\frac{q-1}{2}, 2a) = a$; therefore $\mu(\frac{q-1}{2d}) = \mu(p_2) = -1$. ∎

THEOREM 4.25. *Let $q \equiv 3 \pmod 4$, $q \neq 3$; then*

$$q(G) = c(G) = 2(q+1) + \varphi\left(\frac{q-1}{2}\right) + \left| \min_d \frac{\varphi(q-1)}{\varphi\left(\frac{q-1}{2d}\right)} \mu\left(\frac{q-1}{2d}\right) \right|,$$

where $d = (\frac{q-1}{2}, 2a)$, $a = 2k + 1$, $0 \leq a \leq q - 2$.

Proof. It follows from Definition 2.1 and Lemmas 4.22, 4.23, and 4.24.

THEOREM 4.26. *Let $G = GL_2(3)$; then $r(G) = 4$ and $c(G) = q(G) = 8$.*

Proof. By the irreducible character table of G, we have that $\chi_4^{(1,2)}$ and $\Sigma_{\alpha \in \Gamma}(\chi_2^{(l)})^{\alpha}$ are irreducible faithful rational characters of degree 4 and this degree is minimal among the degrees of faithful rational characters, so $r(G) = 4$. Also $\min_{g \in G}\{\chi_4^{(1,2)}(g)\} = -4$ and $\min_{g \in G}\{\Sigma_{\alpha \in \Gamma}(\chi_2^{(l)})^{\alpha}\} = -4$; therefore $q(G) = 4 + (-(-4)) = 8$ and $c(G) = 8$. ∎

THEOREM 4.27. *Let $G = GL_2(3)$; then $p(G) = 8$.*

Proof. It is clear that $Q = \{[\begin{smallmatrix} 1 & \beta \\ 0 & \gamma \end{smallmatrix}] : \beta \in GF(q), \gamma \in GF(q)^*\}$ is a subgroup of $GL_2(3)$ of order 6 and $[G : Q] = 8$. Also Q is a core-free subgroup of $GL_2(3)$, so $p(G) \leq [G : Q] = 8$. But by Theorem 4.26 and inequality $c(G) \leq q(G) \leq p(G)$, we have $8 = c(G) = q(G) \leq p(G) \leq 8$; hence $p(G) = 8$. ∎

LEMMA 4.28. *Let $q = p^n$.*

(a) $(m + n, q - 1) = 1$ *if and only if* $\chi_{q+1}^{(m,n)}$ *is faithful.*

(b) $(l, q - 1) = 1$ *if and only if* $\chi_{q-1}^{(l)}$ *is faithful.*

Proof. (a) By Lemma 4.1(c), $A_1 \in \ker \chi_{q+1}^{(m,n)}$ if and only if $a = k\frac{q-1}{(m+n, q-1)}$ for some k. Since as $1 \leq a \leq q - 1$, $A_1 = 1$ if and only if $(m + n, q - 1) = 1$.

(b) By Lemma 4.1(d), $A_1 \in \ker \chi_{q-1}^{(l)}$ if and only if $a = k\frac{q-1}{(l, q-1)}$ for some k. Since $1 \leq a \leq q - 1$, $\ker \chi_{q-1}^{(l)} = 1$ if and only if $(l, q - 1) = 1$. ∎

LEMMA 4.29. *Let $q \equiv 1 \pmod 4$ and $q - 1 = 2^t$, $t > 1$. Then $\bigcap \ker \chi \neq 1$ where $\chi \in \operatorname{Irr}(G)$ and χ is not faithful.*

Proof. By Lemma 4.1, in this case the element $A_1 = -I$, for $a = \frac{q-1}{2}$, and it is in the kernel of χ, for every irreducible non-faithful character χ of $G = GL_2(q)$. ∎

The minimal degree of rational and rational-valued faithful characters can be found among the irreducible faithful characters.

THEOREM 4.30. *Let $q \equiv 1 \pmod 4$ and $q - 1 = 2^t$, $t > 1$. Then*

(a) $r(G) = (q-1)\varphi(q-1)$

(b) $q(G) = c(G) = 2r(G) = 2(q-1)\varphi(q-1)$

Proof. (a) Since in this case $\chi_1^{(n)}$ and $\chi_q^{(n)}$ are not faithful for all n we consider $\chi_{q-1}^{(l)}$ or $\chi_{q+1}^{(m,n)}$. Also as $q - 1 = \text{degree}(\chi_{q-1}^{(l)}) < \text{degree}(\chi_{q+1}^{(m,n)}) = q + 1$ by Lemmas 4.5 and 4.22(b), we consider the irreducible character $\chi_{q-1}^{(l)}$ such that $|\Gamma(\chi_{q-1}^{(l)})| = \varphi(q-1)$. Thus $r(G) = \varphi(q-1)\chi_{q-1}^{l}(1) = (q-1)\varphi(q-1)$.

(b) As the minimal value of the rational faithful character $\sum_{\alpha\in\Gamma}(\chi_{q-1}^{(l)})^{\alpha}$ is $\varphi(q-1)(-(q-1))$, so $c(G) = q(G) = \varphi(q-1)(q-1) + |\varphi(q-1)(-(q-1))| = 2(q-1)\varphi(q-1) = 2r(G)$. ∎

THEOREM 4.31. *Let $G = GL_2(2)$; then $r(G) = 2$ and $c(G) = q(G) = 3$.*

Proof. As $GL_2(2) \cong S_3$, all of its characters are rational and the minimal degree of its faithful character is 2, so $r(G) = 2$. Also the minimal value of the above character over the classes of S_3 is -1; therefore $c(G) = q(G) = 2 + |(-1)| = 3$. ∎

LEMMA 4.32. *Let $q \equiv 5 \pmod 8$ and $l = (q^2-1)/8$. Then for the character $\chi_{q-1}^{(l)}$ we have $|\Gamma(\chi_{q-1}^{(l)})| = 2$.*

Proof. We recall that $\delta^{q^2-1} = 1$, so for $l = (q^2-1)/8$ we have

$$\begin{aligned}\chi_{q-1}^{(l)}(g) &= (q-1)\delta^{la(q+1)} = (q-1)\delta^{((q^2-1)/8)a(q+1)}\\ &= (q-1)\delta^{((q^2-1)/4)((q+1)/2)a} = (q-1)(i)^{((q+1)/2)a}\\ &= \{\pm(q-1), \pm i(q-1)\}\end{aligned}$$

for all $g \in A_1$, because $q \equiv 5 \pmod 8$, therefore $\frac{q+1}{2} = 2k+1$ for some k; also $0 \le a \le q-2$. And for this reason $\chi_{q-1}^{(l)}(g) = \{\pm 1, \pm i\}$ for all $g \in A_2$, $\chi_{q-1}^{(l)}(g) = 0$ for all $g \in A_3$, and $\chi_{q-1}^{(l)}(g) = -(\delta^{lc} + \delta^{lcq}) = \delta^{((q^2-1)/8)c} + \delta^{((q^2-1)/8)qc} = (\delta^{(q^2-1)/4})^{c/2} + (\delta^{(q^2-1)/4})^{qc/2} = i^{c/2} + i^{qc/2} = i^{c/2}(1 + i^{c(q-1)/2})$ for all $g \in B_1$.

But $\frac{q-1}{2} = 2(2k'+1)$ for some k' and hence we have

$$i^{c(q-1)/2} = i^{2c(2k'+1)} = (i^2)^{c(2k'+1)} = (-1)^{c(2k'+1)}$$
$$= \begin{cases} -1 & \text{if } c \text{ is odd,} \\ 1 & \text{if } c \text{ is even.} \end{cases}$$

Finally, for all $g \in B_1$, we have

$$\chi_{q-1}^{(l)}(g) = \begin{cases} 0 & \text{if } c \text{ is odd} \\ 2i^{c/2} = \{\pm 2, \pm 2i\} & \text{if } c \text{ is even} \end{cases} \qquad \text{for all } g \in B.$$

Now it follows that $|\Gamma(\chi_{q-1}^{(l)})| = [\mathbb{Q}(i):\mathbb{Q}] = 2$. ∎

LEMMA 4.33. *Let $q = p^n$ be odd. Then*

(a) *For $a = \frac{q-1}{2}$, $A_1 \in \ker \chi_1^{(n)}$, for all n, $n = 1, 2, \ldots, q-1$.*

(b) *Let $q \equiv 1 \pmod 4$ and $q \equiv 5 \pmod 8$; then for $a = \frac{q-1}{2}$ and $l = (q^2-1)/8$, $A_1 \notin \ker \chi_{q-1}^{(l)}$.*

Proof. (a) $\chi_1^{(n)}(g) = \rho^{2na} = \rho^{2n(q-1)/2} = (\rho^{q-1})^n = 1 = \chi_1^{(n)}(1)$ for $g \in A_1$; therefore $A_1 \in \bigcap_{n=1}^{q-1} \ker \chi_1^{(n)}$.

(b) $\chi_{q-1}^{(l)}(g) = (q-1)\delta^{la(q+1)} = (q-1)\delta^{((q^2-1)/8)((q-1)/2)(q+1)} = (q-1)(\delta^{(q^2-1)/2})^{(q^2-1)/8} = (q-1)(-1)^{(q^2-1)/8} = -(q-1)$ for $g \in A_1$ because $(q^2-1)/8$ is odd. Therefore $A_1 \notin \ker \chi_{q-1}^{(l)}$. ∎

LEMMA 4.34. *Let $q \equiv 5 \pmod 8$ and $l = (q^2-1)/8$.*

(a) *If $d = (n, q-1)$ is odd, then for $a = \frac{q-1}{d}$, $A_1 \in \ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)}$; consequently* $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{((q^2-1)/8)} \neq 1$

(b) *If $d = (n, q-1) = 2(2k+1)$ for some $k \in \mathbb{N}$, then for $a = \frac{2(q-1)}{d}$, $A_1 \in \ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)}$; consequently* $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$.

(c) *If $d = (n, q-1) = 4(2k+1)$ for some $k \in \mathbb{N}$, then for $a = \frac{4(q-1)}{d}$, $A_1 \in \ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)}$; hence* $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$.

Proof. (a) Let $a = \frac{q-1}{d}$, $\chi_1^{(n)}(g) = \rho^{2na} = \rho^{2n((q-1)/d)} = (\rho^{q-1})^{2n/d} = 1$ for $g \in A_1$. Therefore $A_1 \in \ker \chi_1^{(n)}$ and $\chi_{q-1}^{(l)}(g) = (q-1)\delta^{la(q+1)} = (q-1)\delta^{((q^2-1)/8)((q-1)/d)(q+1)} = (q-1)(\delta^{q^2-1})^{((q-1)/4d)(q+1)/2)} = (q-1)$ for $g \in A_1$; thus $A_1 \in \ker \chi_{q-1}^{(l)}$ and $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$.

(b) Let $a = \frac{2(q-1)}{d}$; then $\chi_1^{(n)}(g) = \rho^{2na} = \rho^{2n(2(q-1)/2)} = (\rho^{q-1})^{4(q-1)/d} = 1$ for $g \in A_1$, so $A_1 \in \ker \chi_1^{(n)}$. And $\chi_{q-1}^{(l)}(g) = (q-1)\delta^{la(q+1)} = (q-1)\delta^{((q^2-1)/8)(2(q-1)/d)(q+1)} = (q-1)(\delta^{q^2-1})^{((q-1)/2d)((q+1)/2)} = (q-1)$ for $g \in A_1$. Thus $A_1 \in \ker \chi_{q-1}^{(l)}$ and $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$.

(c) Let $a = \frac{4(q-1)}{d}$; then $\chi_1^{(n)}(g) = \rho^{2na} = \rho^{2n(4(q-1)/d)} = (\rho^{q-1})^{8n/d} = 1$ for $g \in A_1$, so $A_1 \in \ker \chi_1^{(n)}$ and $\chi_{q-1}^{(l)} = (q-1)\delta^{la(q+1)} = (q-1)\delta^{((q^2-1)/8)(4(q-1)/d)(q+1)} = q-1$, so $A_1 \in \ker \chi_{q-1}^{(l)}$ and therefore $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$. ∎

LEMMA 4.35. *Let* $q \equiv 1 \pmod 8$ *and* $l = (q^2 - 1)/8$. *Then*

(a) *If* $d = (n, q-1) = 2$, *then* $\ker \chi_1^{(n)} = \{A_1 : a = k'\frac{q-1}{4}, k' = 0, 1, 2, 3\}$ *and* $\ker \chi_1^{(n)} \cap \chi_{q-1}^{(l)} = 1$.

(b) *If* $d = (n, q-1) = 4$, *then* $\ker \chi_1^{(n)} = \{A_1 : a = k'\frac{q-1}{8}, k' = 0, 2, 4, 6\}$ *and* $\ker \chi_1^{(n)} \cap \chi_{q-1}^{(l)} = 1$.

Proof. (a) By Lemma 4.1(a), $\chi_1^{(n)}(g) = \rho^{2na}$ for $g \in A_1$; we have $\ker \chi_1^{(n)} = \{A_1 : a = k'\frac{q-1}{4}, k' = 0, 1, 2, 3\}$. Let $k'' = k'(\frac{q-1}{4})(\frac{q+1}{2})$. Then $\frac{q-1}{4}\frac{q+1}{2}$ is odd, because $q \equiv 1 \pmod 4$ and $q \equiv 5 \pmod 8$. Let $k' \neq 0$. Then $\chi_{q-1}^{(l)}(g) = (q-1)\delta^{((q^2-1)/8)k'((q-1)/4)(q+1)} = (q-1)(\delta^{(q^2-1)/4})^{k'((q-1)/4)((q+1)/2)} = (q-1)(i)^{k''} = \{-(q-1), \pm i(q-1)\}$ for $g \in A_1$. Hence $A_1 \notin \ker \chi_{q-1}^{(l)}$ and therefore $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} = 1$.

(b) It is clear that $\ker \chi_1^{(n)} = \{A_1 : a = k'\frac{q-1}{8}, k' = 0, 2, 4\}$. But

$$\begin{aligned}\chi_{q-1}^{(l)}(g) &= (q-1)\,\delta^{((q^2-1)/8)(k'(q-1)/8)(q+1)} \\ &= (q-1)\left(\delta^{(q^2-1)/4}\right)^{k'(q-1)/8-(q+1)/2} \\ &= \{-(q-1), \pm i(q-1)\}\end{aligned}$$

for $g \in A_1$, because $k'(\frac{q-1}{8})\frac{q+1}{2}$ is odd or $k'/2 = 2$ if $k' = 4$. Therefore $A_1 \notin \ker \chi_{q-1}^{(l)}$ and $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} = 1$ will be the identity. ∎

We see that if $q \equiv 5 \pmod 8$ and if $d = (n, q-1)$ is $2k+1$ or $2(2k+1)$ or $4(2k+1)$, for some $k \in \mathbb{N}$, then $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$ for $l = (q^2-1)/8$ so for finding $r(G)$, we do not consider those $\chi_1^{(n)}$.

Also, if $d = (n, q-1) = 2$ or 4, then $\varphi(\frac{q-1}{2}) = \varphi(\frac{q-1}{4})$ because $q \equiv 5 \pmod 8$ implies $q - 1 = 4(2k+1)$ for some $k \in \mathbb{N}$ and then $\varphi(\frac{q-1}{4}) = \varphi(2)\varphi(\frac{q-1}{4}) = \varphi(2\frac{q-1}{4}) = \varphi(\frac{q-1}{2})$ and it is clear that $\varphi(\frac{q-1}{2}) < \varphi(q-1)$.

THEOREM 4.36. *Let* $q \equiv 5 \pmod 8$. *Then*

$$r(G) = 2(q-1) + \varphi\left(\frac{q-1}{4}\right).$$

Proof. By Lemmas 4.32, 4.33, 4.34, and 4.35 and the fact that if l or $m+n$ is even or $\chi_{q-1}^{(l)}$ and $\chi_{q+1}^{(m,n)}$ are rational, $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} \neq 1$ and $\ker \chi_1^{(n)} \cap \ker \chi_{q+1}^{(m,n)} \neq 1$; we must consider the irrational characters of types $\chi_{q-1}^{(l)}$ or $\chi_{q+1}^{(m,n)}$. But by Lemma 4.32 there is l such that $|\Gamma(\chi_{q-1}^{(l)})| = 2$ and by Lemma 4.35 there are n, such that $\ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(l)} = 1$ (for the above l). So by definition of $r(G)$ we consider such $\chi_1^{(n)}, \chi_{q-1}^{(l)}$ and therefore

$$r(G) = \sum_{\alpha \in \Gamma'} \left(\chi_1^{(n)}(1)\right)^{\alpha} + \sum_{\alpha \in \Gamma} \left(\chi_{q-1}^{(l)}\right)^{\alpha} = \varphi\left(\frac{q-1}{4}\right) + 2(q-1),$$

where Γ' is the Galois group of $\chi_1^{(n)}$ over $\mathbb{Q}$. ∎

LEMMA 4.37. *Let* $q \equiv 5 \pmod 8$ *and* $l = (q^2 - 1)/8$. *Then* $\chi_{q-1}^{(l)}(g) = -(q-1)$ *for* $g \in A_1$, *if and only if* $a = 2(2k+1)$ *and* $k = 0, 1, 2, \dots, \frac{q-5}{4}$ *and conversely.*

Proof. $\chi_{q-1}^{((q^2-1)/8)}(g) = (q-1)\delta^{((q^2-1)/8)2(2k+1)(q+1)} = (q-1)(\delta^{(q^2-1)/4})^{2(2k+1)((q+1)/2)} = (q-1)(i^2)^{(2k+1)((q+1)/2)} = -(q-1)$ for $g \in A_1$, because $(2k+1)\frac{q+1}{2}$ is odd. Conversely if $\chi_{q-1}^{(q^2-1)/8}(g) = -(q-1)$, for $g \in A_1$, then $\delta^{((q^2-1)/8)(a(q+1))} = -1$; therefore $\delta^{((q^2-1)/2)(a/2)((q+1)/2)} = ((-1)^{(q+1)/2})^{a/2} = (-1)^{a/2} = -1$. Hence $\frac{a}{2}$ must be odd, so $a = 2(2k+1)$. ∎

LEMMA 4.38. *Let* $q \equiv 5 \pmod 8$. *Then for* $a = 2(2k+1)$, $k = 0, 1, 2, \dots, \frac{q-5}{4}$ *and* $d = (n, q-1) = 2$ *or* 4 *we have*

$$\sum_{\alpha \in \Gamma} \left(\rho^{2na}\right)^{\alpha} = \sum_{\alpha \in \Gamma} \left(\left(\rho^{2n}\right)^{a}\right)^{\alpha} = \frac{\varphi\left(\frac{q-1}{4}\right)}{\varphi\left(\frac{\frac{q-1}{4}}{\left(\frac{q-1}{4}, 2(2k+1)\right)}\right)} \mu\left(\frac{\frac{q-1}{4}}{\left(\frac{q-1}{4}\right), 2(2k+1)}\right).$$

Proof. This follows from Lemma 4.37. ∎

LEMMA 4.39. *With the above assumptions let* $d' = (\frac{q-1}{4}, a)$. *Then* $\mu((q-1)/4q') = -1$ *for some* d'.

Proof. By assumption $q - 1 = 2^2.p_2^{\alpha_2} \cdots p_{k'}^{\alpha_{k'}}$. We let $a = 2p_2^{\alpha_2 - 1} \cdots p_{k'}^{\alpha_{k'}}$ so $d' = (\frac{q-1}{4}, a) = (2k+1) = p_2^{\alpha_2-1}p_3^{\alpha_3} \cdots p_{k'}^{\alpha_{k'}}$; therefore $\mu((q-1)/4d') = \mu(p_2) = -1$. ∎

THEOREM 4.40. *Let* $q \equiv 5 \pmod 8$. *Then*

$$c(G) = q(G) = 4(q-1) + \varphi\left(\frac{q-1}{4}\right) + \left|\min_{d} \frac{\varphi\left(\frac{q-1}{4}\right)}{\varphi\left(\frac{q-1}{4d}\right)} \mu\left(\frac{q-1}{4d}\right)\right|,$$

where $d = (\frac{q-1}{4}, a)$, $a = 2(2k+1)$, $k = 0, 1, \dots, \frac{q-5}{4}$.

Proof. This follow from Definition 2.1 and Lemmas 4.37, 4.38, and 4.39. ∎

LEMMA 4.41. *Let* $q \equiv 1 \pmod 8$. *If* $d = (m+n, q-1) = 2k$ *for some* $k \in \mathbb{N}$ *and* $d' = (l, q-1) = 2k' \in \mathbb{N}$ *for some* k', *then* $\ker \chi_{q-1}^{(l)} \cap \ker \chi_1^{(n)} \neq 1$ *and* $\ker \chi_{q+1}^{(m,n)} \cap \ker \chi_1^{(n)} \neq 1$.

Proof. By assumption l and $m+n$ must be even, so for $a = \frac{q-1}{2}$, $\chi_{q-1}^{(l)}(g) = (q-1)\delta^{l((q-1)/2)(q+1)} = (q-1)(\delta^{(q^2-1)/2})^l = (q-1)(-1)^l = q-1 = \chi_{q-1}^{(l)}(1)$, for $g \in A_1$ and $\chi_{q+1}^{(m,n)}(g) = (q+1)\rho^{(m+n)a} = (q+1)(\rho^{(q-1)/2})^{m+n} = (q+1)(-1)^{m+n} = q+1 = \chi_{q+1}^{(m,n)}(1)$, for $g \in A_1$. So the result follows. ∎

LEMMA 4.42. *Let* $q \equiv 1 \pmod 8$. *Let* $d = (l, q-1)$ *and* $d' = (n, q-1)$, $(d, d') = 1$; *then* $\ker \chi_{q-1}^{(l)} \cap \ker \chi_1^{(n)} = 1$.

Proof. Suppose $\ker \chi_{q-1}^{(l)} \cap \ker \chi_1^{(n)} \neq 1$; therefore by Lemma 4.1 there is $A_1 \in \ker \chi_1^{(n)} \cap \ker \chi_{q-1}^{(n)}$. Hence $a = k'((q-1)/2d')$, $a = k((q-1)/d)$, $k'((q-1)/2d') = k(q-1)/d$, so $k'd = 2d'k$. Since d is odd and $(d, d') = 1$ it should follow that $k = dt$, $k'd = 2d'dt$ and therefore $k' = 2d't$, but this is a contradiction, because $0 \le k' < 2d'$ [Lemma 4.1(a)]. ∎

THEOREM 4.43. *Let* $q \equiv 1 \pmod 8$ *and* $d = (l, q-1) = 2k+1$, $d' = (n, q-1)$, $(d, d') = 1$; *then*

$$r(G) = \min_{d, d'} \left\{ \varphi\left(\frac{q-1}{d}\right)(q-1) + \varphi\left(\frac{q-1}{d'}\right) \right\}.$$

Proof. This result follows from definition of $r(G)$, Lemmas 4.2(a), 4.3(a), 4.5, and 4.41, the fact that if $l = (\frac{q+1}{2})^2$ then $\delta^l + \delta^{lq} \in \mathbb{Q}$ and therefore

$$\left|\Gamma\left(\chi_{q-1}^{(l)}\right)\right| = \left|\Gamma\left(\chi_{q-1}^{((q+1)/2)^2}\right)\right| = \begin{cases} \varphi(q-1) & \text{if } (l, q-1) = 1, \\ \varphi\left(\dfrac{q-1}{d}\right) & \text{if } (l, q-1) = d. \end{cases}$$

∎

LEMMA 4.44. *Let* $q \equiv 1 \pmod 8$, $d = (l, q-1) = 2k+1$ *for some* $k \in \mathbb{N}$; *then* $\chi_{q-1}^{(l)}(g) = -(q-1)$ *for* $g \in A_1$ *if and only if* $a = \frac{(2s+1)(q-1)}{2d}$ *where* $s < \frac{d-1}{2}$.

Proof. Let $a = \frac{(2s+1)(q-1)}{2d}$; therefore $\chi_{q-1}^{(l)}(g) = (q-1)\delta^{l((2s+1)(q-1)/2d)(q+1)} = (q-1)(\delta^{(q^2-1)/2})^{l((2s+1)/d)} = (q-1) \times (-1)^{l((2s+1)/d)} = -(q-1)$ for $g \in A_1$, because both l and d are odd. Conversely if $\chi_{q-1}^{(l)}(g) = -(q-1)$, for $g \in A_1$, then $\delta^{la(q+1)} = -1$; therefore $(q^2-1)/2 | la(q+1)$ and $la(q+1)$ is odd. Therefore $\frac{q-1}{2} | la$ and then $\frac{q-1}{2d} | \frac{l}{d}a$. Since $(\frac{q-1}{2d}, \frac{l}{d}) = 1$, $\frac{q-1}{2d}$ should divide a and thus $a = (2s+1)(\frac{q-1}{2d})$. ∎

LEMMA 4.45. *Let* $q \equiv 1 \pmod 8$, $d = (l, q-1)$, $d' = (n, q-1)$, *and* $(d, d') = 1$; *then*

$$\sum_{a\in\Gamma}\left(\rho^{2na}\right)^{\alpha} = \sum_{\alpha\in\Gamma}\left((\rho^{n})^{2a}\right)^{\alpha} = \frac{\varphi\left(\dfrac{q-1}{d'}\right)}{\varphi\left(\dfrac{\dfrac{q-1}{d'}}{\left(\dfrac{q-1}{d'}, \dfrac{(2s+1)(q-1)}{d}\right)}\right)} \times \mu\left(\frac{\dfrac{q-1}{d'}}{\left(\dfrac{q-1}{d'}, \dfrac{(2s+1)(q-1)}{d}\right)}\right),$$

where $a = \frac{(2s+1)(q-1)}{2d}$, $s < \frac{d-1}{2}$.

Proof. This follows from [3, Lemma 3.4], and properties of a, d, d'. ∎

With the above assumptions, let

$$A(s) = \frac{\varphi\left(\dfrac{q-1}{d'}\right)}{\varphi\left(\dfrac{\dfrac{q-1}{d'}}{\left(\dfrac{q-1}{d'}, \frac{(2s+1)(q-1)}{d}\right)}\right)} \mu\left(\frac{\dfrac{q-1}{d'}}{\left(\dfrac{q-1}{d'}, \dfrac{(2s+1)(q-1)}{d}\right)}\right).$$

THEOREM 4.46. *Let* $q \equiv 1 \pmod 8$. *Then*

$$c(G) = q(G) = \min_{d,d'}\left\{\varphi\left(\frac{q-1}{d}\right)(q-1) + \varphi\left(\frac{q-1}{d'}\right)\right\} + m(x)$$

where

$$m(x) = \begin{cases} \displaystyle\min_{d,d'}\left\{\varphi\left(\frac{q-1}{d}\right)(q-1) + \varphi\left(\frac{q-1}{d'}\right)\right\} + \left|\min_{s} A(s)\right| \\ \qquad \text{if } A(s) < 0, \text{ for some } s, \\ \displaystyle\left|\min_{d,d'}\left\{\varphi\left(\frac{q-1}{d}\right)(q-1) + \varphi\left(\frac{q-1}{d'}\right)\right\} - \min_{s} A(s)\right| \\ \qquad \text{otherwise}. \end{cases}$$

Proof. This result follows from Definition 2.1 and Lemmas 4.44 and 4.45. ∎

REFERENCES

1. H. Behravesh, Quasi-permutation representations of p-groups of class 2, *J. London Math. Soc. (2)* **55** (1997), 251–256.
2. H. Behravesh, Quasi-permutation representations of $SL(2, q)$ and PSL$(2, q)$, *Glasgow Math. J.* **41** (1999), 393–408.
3. H. Behravesh, The rational character table of special linear groups, *J. Sci. I.R.I.* **9,** No. 2 (1998), 173–180.
4. J. M. Burns, B. Goldsmith, B. Hartley, and R. Sandling, On quasi-permutation representations of finite groups, *Glasgow Math. J.* **36** (1994), 301–308.
5. L. E. Dickson, "Linear Groups in Galois Fields," Leipzig, 1901.
6. R. Gow, Schur indices of some groups of Lie type, *J. Algebra* **42** (1976), 102–120.
7. M. Hoffman, An invariant of finite abelian groups, *Amer. Math. Monthly* **94** (1987), 664–666.
8. B. Huppert, "Endliche Gruppen I," Springer-Verlag, Berlin, 1967.
9. I. M. Isaacs, "Character Theory of Finite Groups," Academic Press, New York, 1976.
10. R. Steinberg, The representations of $GL(3, q)$, $GL(4, q)$, $PGL(3, q)$, and $PGL(4, q)$, *Canad. J. Math.* **3** (1951), 225–235.
11. W. J. Wong, Linear groups analogous to permutation groups, *J. Austral. Math. Soc. Ser. A* **3** (1963), 180–184.