Permutation representations and rational irreducibility

John D. Dixon
School of Mathematics and Statistics
Carleton University, Ottawa, Canada

March 30, 2005

Abstract

The natural character π of a finite transitive permutation group G has the form $1_G + \theta$ where θ is a character which affords a rational representation of G. We call G a QI-group if this representation is irreducible over $\mathbb{Q}$. Every 2-transitive group is a QI-group, but the latter class of groups is larger. It is shown that every QI-group is 3/2-transitive and primitive, and that it is either almost simple or of affine type. QI-groups of affine type are completely determined relative to the 2-transitive affine groups, and partial information is obtained about the socles of simply transitive almost simple QI-groups. The only known simply transitive almost simple QI-groups are of degree $2^{k-1}(2^k - 1)$ with $2^k - 1$ prime and socle isomorphic to $PSL(2, 2^k)$.

Mathematics Subject Classification (2000): 20C15 20B15

1 Introduction

Let G be a finite transitive permutation group with the natural character π. Then π can be written in the form $1_G + \theta$ where the character θ can be afforded by a representation over the rationals. For the purposes of this paper we shall call G a *QI-group* if this representation is $\mathbb{Q}$-irreducible, and consider the question: which permutation groups are QI-groups? (In what follows all groups considered are finite.)

There is a related question: when is the character θ irreducible over the rationals in the sense that it cannot be written as a sum of two rational valued characters? Lemma 6(c) below shows that the two problems are identical.

There are two well known classes of QI-groups. If G is 2-transitive, then the inner product $[\pi, \pi] = 2$ and so θ is absolutely irreducible. In this case G is certainly a QI-group. On the other hand, if x is a p-cycle for some prime p, then the rational form of the corresponding permutation matrix consists of a block of size 1 and a block of size $p-1$ because the cyclotomic polynomial of order p is irreducible over $\mathbb{Q}$. Every transitive permutation group of degree p contains such an element, and so must be a QI-group. We may consider these two classes of groups as "trivial" examples.

Example 1 *Using GAP [6] and its tables of primitive permutation groups we easily found two nontrivial examples of affine groups which are QI-groups: one of degree* 3^3*, rank* 3 *and of the form* $3^3 : 13$ *and a second of degree* 7^2*, rank* 4 *and of the form* $7^2 : 16$*. Of course all subgroups of the corresponding symmetric groups which contain these groups are also QI-groups.*

Example 2 *Using the ATLAS [3] we found examples of simple groups which* *are QI-groups but not 2-transitive. A transitive permutation representation of $PSL(2,2^3)$ of degree 28 and rank 4, and a transitive permutation representation of $PSL(2,2^5)$ of degree 496 and rank 16 are both QI-groups. Interestingly, $G := PSL(2,2^4)$ has a permutation representation π of degree 120 and rank 8 such that $\pi - 1_G$ is a sum of 7 distinct absolutely irreducible characters of the same degrees, but these characters are not Galois conjugates and so this group does not provide an example of a QI-group.*

Our main results are the following. The first generalizes a classical theorem of Burnside which states that the socle of a 2-transitive group is either a regular elementary abelian p-group or is a simple group (see, for example, [4, Theorem 7.2E]). Recall that a permutation group is $3/2$-transitive if it is transitive and the nontrivial orbits of the point stabilizers all have the same length.

Theorem 3 *Every QI-group is $3/2$-transitive and primitive. It is either almost simple or of affine type.*

In the case of affine type the groups are closely tied to 2-transitive groups.

Theorem 4 *A QI-group G of affine type of degree p^d (p prime) is almost 2-transitive in the sense that it is a subgroup of a 2-transitive group $\bar{G}$ and contains the derived subgroup $\bar{G}'$. Moreover, the index of G in $\bar{G}$ divides $p-1$ and the rank of G is of the form $1+s$ where s divides $p-1$.*

In Section 4 we prove a more precise statement, giving necessary and sufficient conditions for a subgroup of a 2-transitive group of affine type to be a QI-group. A theorem similar to Theorem 4 is false for the class of almost simple QI-groups. Indeed, in the example above, there is a QI-group G of degree 496 isomorphic to $PSL(2,2^5)$, but it is easily shown that the normalizer of G in S_{496} is not 2-transitive (indeed $\pi - 1_G$ is a sum of 15 absolutely irreducible characters, but G has index only 5 in its automorphism group).

2 Basic properties of QI-groups

Let G be a finite transitive permutation group on a set Ω of size n and let $H := G_\alpha$ be a point stabilizer of G for some $\alpha \in \Omega$. Then the permutation character π for G is equal to 1_H^G and (as above) can be written in the form $\pi = 1_G + \theta$. We shall frequently use the following simple observation.

Lemma 5 *The permutation character π of a transitive group G cannot be written in the form $1_G + m\theta'$ for an integer $m > 1$ and character θ'.*

Proof. Since G is transitive, it contains an element x, say, which is fixed point free. The equation $0 = \pi(x) = 1 + m\theta'(x)$ would contradict the fact that $\theta'(x)$ is an algebraic integer. ■

The orbitals of G are the orbits $\Delta_1, \Delta_2, ..., \Delta_r$ of G on the set $\Omega \times \Omega$, where we may assume that Δ_1 denotes the diagonal orbital $\{(\alpha, \alpha) \mid \alpha \in \Omega\}$. The rank r of G is the number of orbitals and, as is well known, $r = [\pi, \pi] := |G|^{-1} \sum_{x \in G} \pi(x)^2$. Using the representation of G in terms of $n \times n$ permutation matrices, the centralizer ring C consists of the rational $n \times n$ matrices which commute with all of these permutation matrices. The ring C is a $\mathbb{Q}$-algebra of dimension r and has a basis $z(\Delta_i)$ $(i = 1, .., r)$ where $z(\Delta_i)$ is a $\{0, 1\}$-matrix whose (α, β)th entry is 1 if and only if $(\alpha, \beta) \in \Delta_i$ (see [12, Chapter V] or [2, Chapters 2 and 3]). We write $Irr(G)$ to denote the set of irreducible characters of G.

Lemma 6 *Using the notation above:*

(a) If G is a QI-group then G is primitive.

(b) A transitive group G is a QI-group if and only there exists $\chi \in Irr(G)$ such that $\theta = \chi_1 + ... + \chi_s$ where $\chi_1, ..., \chi_s$ are the distinct Galois conjugates over $\mathbb{Q}$ of the character χ. In particular in this case, the Schur index $m_{\mathbb{Q}}(\chi)$ of χ is 1 and the rank $r = [\pi, \pi]$ of G is $1 + s$.

(c) A transitive group G is a QI-group if and only if $\theta := \pi - 1_G$ is not the sum of two rational characters of smaller degrees.

(d) G is a QI-group if and only if the centralizer ring C has the form $1 \oplus F$ where F is a field. Indeed, F must be isomorphic to $\mathbb{Q}(\chi)$ (the field generated by the values of χ) where χ is the character referred to in (b).

Remark 7 *For computational purposes we should note that the centralizer ring has a simple representation as a matrix ring of degree r over $\mathbb{Q}$ with respect to the basis $z(\Delta_i)$ $(i = 1, ..., r)$. See, for example, [2, Theorem 3.4].*

Proof. (a) If G is not primitive, then there exists a subgroup M such that $H < M < G$. Now $\pi = (1_H^M)^G$. However, since $M \neq H$, $1_H^M = 1_M + \eta$ where η affords a rational representation, and $\pi = 1_M^G + \eta^G$. Since $M \neq G$, the representation for 1_M^G decomposes into at least two rational representations and η^G provides at least one more rational component. Thus G cannot be a QI-group.

(b) First, the condition is sufficient, since if $\theta = \chi_1 + ... + \chi_s$ where the χ_i are distinct Galois conjugates, then θ cannot be written as a sum of two rational valued characters, and so a rational representation affording θ cannot be written as sum of representations of smaller degree. Thus G is a QI-group.

Conversely, suppose that G is a QI-group. Then θ is the character of a $\mathbb{Q}$-irreducible rational representation, and as such has the form $m(\chi_1 + ... + \chi_s)$

where χ_i is a full set of Galois conjugates of some irreducible character χ, and $m := m_{\mathbb{Q}}(\chi)$ is the Schur index of χ (and hence of all χ_i) (see [11, Corollary (10.2)]). Now Lemma 5 shows that $m = 1$.

(c) Follows at once from (b).

(d) The permutation representation for G is equivalent over $\mathbb{Q}$ to a linear representation τ in block diagonal form

$$\tau(x) = diag(1, \upsilon(x))$$

where υ is a $\mathbb{Q}$-irreducible representation of G affording θ. It follows that the centralizer ring C in the matrix ring $Mat(n, \mathbb{Q})$ has the form $\mathbb{Q} \oplus F$ where F is the centralizer ring of the matrices $\upsilon(x)$ $(x \in G)$ in $Mat(n-1, \mathbb{Q})$ and $\dim_{\mathbb{Q}} C = 1 + s$ by (b) and the remarks at the beginning of this section. We know that F is a division ring by Schur's lemma. Since $m_{\mathbb{Q}}(\chi) = 1$, the character χ can be afforded by an absolutely irreducible representation ρ over $\mathbb{Q}(\chi)$. Thus there exists $c \in GL(n-1, \mathbb{Q}(\chi))$ such that

$$c^{-1}\upsilon(x)c \mapsto diag(\rho_1(x), ..., \rho_s(x))$$

where $\rho_i(x)$ is an absolutely irreducible character affording χ_i obtained by applying a suitable Galois automorphism to the entries of $\rho(x)$. (Note that $\mathbb{Q}(\chi)$ is a subfield of a cyclotomic field and is a Galois extension of $\mathbb{Q}$.) Schur's lemma now shows that the centralizer of the set of matrices $c^{-1}\upsilon(x)c$ $(x \in G)$ in the matrix ring $Mat(n-1, \mathbb{Q}(\chi))$ consists of all block diagonal matrices of the form $diag(\gamma_1 1, \gamma_2 1, ..., \gamma_s 1)$ with $\gamma_i \in \mathbb{Q}(\chi)$ and so has the form $\mathbb{Q}(\chi) \oplus \mathbb{Q}(\chi) \oplus ... \oplus \mathbb{Q}(\chi)$. This ring contains $c^{-1}Fc$, so F is commutative and hence is a field. Projection onto one of the coordinates shows that F can be embedded into $\mathbb{Q}(\chi)$.

Finally $[\mathbb{Q}(\chi) : \mathbb{Q}] = s$ because χ has s Galois conjugates. Thus $[F : \mathbb{Q}] = \dim_{\mathbb{Q}} C - 1 = s = [\mathbb{Q}(\chi) : \mathbb{Q}]$, and so $F \cong \mathbb{Q}(\chi)$. ∎

Let E be the field extension of $\mathbb{Q}$ generated by a primitive eth root of 1 in $\mathbb{C}$ where e is the exponent of G. Then E is a Galois extension of $\mathbb{Q}$ and the values of the characters of every subgroup of G lie in E. Put $A := Gal(E/\mathbb{Q})$. Then for any normal subgroup M of G we have that the group $A \times G$ acts on the set of characters of M via $\phi^{(\nu,x)}(u) := \phi(xux^{-1})^{\nu}$ (for each character ϕ with $(\nu, x) \in A \times G$ and $u \in M$).

Lemma 8 *Let G be a transitive group and let M be a nontrivial normal subgroup. Suppose that the restriction of the natural character π of G to M has the form $\pi_M = 1_M + (\phi_1 + ... + \phi_t)$ with each $\phi_i \in Irr(M)$. Note that (with the notation above) $A \times G$ maps the set $\{\phi_1, ..., \phi_t\}$ onto itself since π is invariant under $A \times G$. Then:*

(a) G is a QI-group if and only if the ϕ_i are distinct and $A \times G$ acts transitively on $\{\phi_1, ..., \phi_t\}$. In particular, in this case all the ϕ_i have the same degree.

(b) If G is a QI-group, then each nontrivial normal subgroup M is $3/2$-transitive. Moreover, if M is regular, then M is abelian.

Proof. (a) Write $\pi = 1_G + (\chi_1 + ... + \chi_s)$ where the $\chi_i \in Irr(G)$, and let $\Gamma_i \subseteq Irr(M)$ be the set of irreducible constituents of $(\chi_i)_M$. Since the χ_i are irreducible, Clifford's theorem shows that each Γ_i is an orbit under G.

If the ϕ_i are distinct and $A \times G$ acts transitively on $\{\phi_1, ..., \phi_t\}$, then the Γ_i are distinct and A acts transitively on $\{\Gamma_1, ..., \Gamma_s\}$. Thus the χ_i are distinct and A is transitive on $\{\chi_1, ..., \chi_s\}$. Hence G is a QI-group by Lemma 6.

Conversely, suppose that G is a QI-group. Then A acts transitively on $\{\chi_1, ..., \chi_s\}$ and hence on $\{\Gamma_1, ..., \Gamma_s\}$. Thus $A \times G$ acts transitively on

$\Gamma_1 \cup ... \cup \Gamma_s = \{\phi_1, ..., \phi_t\}$. In particular, the multiplicity $[\pi_M, \phi_i]$ in π_M of each of the ϕ_i is the same. Since M is a nontrivial normal subgroup of a primitive group, M is transitive, and so Lemma 5 shows that each constituent of π_M has multiplicity 1. This shows that the ϕ_i are distinct.

(b) We have shown in (a) that for every nontrivial normal subgroup M of G the nontrivial irreducible constituents of π_M are all of the same degree, say d. Since M is transitive, a theorem of Frame (see [12, Theorem 30.2]) shows that this condition implies that all nontrivial suborbits of M also have length d. This shows that M is 3/2-transitive. Finally, if M is regular, we have $d = 1$. Then the (faithful) character π_M is a sum of linear characters and so M is abelian. ■

Remark 9 *The nontrivial suborbits of M all have the same length if and only if every 2-point stabilizer $M_{\alpha\beta}$ ($\alpha \neq \beta$) has the same size. Criterion (b) can be applied to eliminate many groups as potential QI-groups by simply checking the sizes of the orbits of a point stabilizer for a single normal subgroup M. Programs such as GAP can compute the orbits of a point stabilizer very efficiently, so the condition is easily verified.*

3 Proof of Theorem 3

We have already shown that every QI-group is primitive (Lemma 6(a)) and 3/2-transitive (Lemma 8(b)).

According to the O'Nan-Scott theorem, primitive groups fall into five classes: (i) groups of affine type (where the socle is a regular elementary abelian group); (ii) groups with regular nonabelian socles; (iii) groups of almost simple type (where the socle is simple nonabelian); (iv) groups of diagonal type; and (v) groups of wreath product type (see, for example, [4, Chap. 4]).

Lemma 8(b) shows that a QI-group cannot be of type (ii), so to complete the proof of Theorem 3 it is enough to show that no primitive group of type (iv) or (v) is a QI-group.

Suppose that a primitive group G is of type (iv) (diagonal type). Then the socle M of G has the form $M = T^m$ where T is a simple nonabelian group with $m > 1$, and the permutation action is equivalent to the following action on Ω. Consider the equivalence relation $\sim$ on the set T^m given by $(a_1, ..., a_m) \sim (a'_1, ..., a'_m)$ provided there exists $t \in T$ such that $a'_i = ta_i$ for each i. Let $[a_1, .., a_m]$ denote the equivalence class containing $(a_1, ..., a_m)$, and let Ω be the set of all equivalence classes (so $|\Omega| = |T|^{m-1}$). Then $M = T^m$ acts on Ω via

$$[a_1, ..., a_m]^{(x_1,...,x_m)} := [a_1^{x_1}, ..., a_m^{x_m}]$$

The stabilizer $M_{[a,1,...,1]}$ of $[a, 1, ..., 1]$ equals $\left\{(a^{-1}xa, x, ..., x) \mid x \in T\right\}$, and the two-point stabilizer $M_{[a,1,...,1]} \cap M_{[1,1,...,1]}$ equals $\{(x, x, ..., x) \mid x \in C_T(a)\}$ and so has size $|C_T(a)|$. Since T is a nonabelian simple group, it contains nontrivial elements a, b such that $|C_T(a)| \neq |C_T(b)|$. Thus the two-point stabilizers of M are not all of the same size and so Lemma 8(b) shows that G is not a QI-group.

Now suppose that we have a primitive group G of type (v) (wreath product type). In this case the socle M of G has the form U^s with $s > 1$. The group U is a direct product of one or more isomorphic nonabelian simple groups and acts transitively but nonregularly on a set Δ, and M acts on Δ^s with the product action. If α and β are distinct points in Δ, then $M_{(\alpha,\alpha,...,\alpha)} = U_\alpha \times U_\alpha \times ... \times U_\alpha$ and $M_{(\beta,\alpha,...,\alpha)} = U_\beta \times U_\alpha \times ... \times U_\alpha$. Thus, since U is not regular, the two-point stabilizers

$$M_{(\alpha,\alpha,\ldots,\alpha)} \cap M_{(\beta,\beta,\ldots,\beta)} = U_{\alpha\beta} \times U_{\alpha\beta} \times \ldots \times U_{\alpha\beta}$$

and

$$M_{(\alpha,\alpha,\ldots,\alpha)} \cap M_{(\beta,\alpha,\ldots,\alpha)} = U_{\alpha\beta} \times U_{\alpha} \times \ldots \times U_{\alpha}$$

have different sizes for suitable α and β. Again Lemma 8 shows that G is not a QI-group. This completes the proof of the theorem.

Remark 10 *More generally, it is shown in [1] that any primitive permutation group with a multiplicity-free permutation character is of type (i), (ii), (iv) or (v) with further restrictions in the last two cases.*

Using GAP [6] and its library of primitive groups of degree < 1000, a direct search was made for QI-groups which have simple socles but are not 2-transitive. GAP's table COHORTS_PRIMITIVE_GROUPS and the function ONanScottType were used to determine the simple socles which occur for each degree. The lengths of the suborbits of these simple permutation groups were then computed and Lemma 8(b) applied taking M as the socle. This criterion eliminated all but four cases of simple socles in this range: A_7 in degree 21 (rank 3), $PSL(2,8)$ in degree 28 (rank 4), $PSL(2,16)$ in degree 120 (rank 8), and $PSL(2,32)$ in degree 496 (rank 16). A more careful examination of these four cases showed that in degrees 21 and 120 there are no QI-groups which are not 2-transitive. In degree 28 there is a unique example of a simply transitive QI-group ($PSL(2,8)$), and in degree 496 there are two examples ($PSL(2,32)$ and $PSL(2,32).5$). These results led us to conjecture the following theorem.

Theorem 11 *(a) Every QI-group with socle isomorphic to A_d ($d \geq 5$) is 2-transitive.*

(b) If a QI-group of degree n has socle isomorphic to $PSL(2,q)$ and is not 2-transitive, then $q=2^k$ for some integer $k>2$ with 2^k-1 prime and $n=2^{k-1}(2^k-1)$. Conversely, in the latter case we always have examples of simply transitive groups which are QI-groups.

Proof. (a) Suppose that $\chi \in Irr(A_d)$ is not rational valued. Since every character of S_d is rational valued, the induced character χ^{S_d} is rational and it is easily verified that $\chi^{S_d}(u) = \chi(u) + \chi(tut^{-1})$ for all $u \in A_d$ where $t \in S_d \setminus A_d$. Hence $\{\chi, \chi^t\}$ is a set of Galois conjugate characters of A_d and χ^{S_d} is irreducible.

Now suppose that G is a QI-group of degree n with socle type A_d and that G is not 2-transitive (so $n>d$). Then $G \cong A_d$ or S_d, and $G \not\cong S_d$ because all irreducible characters of S_d are rational. Hence $G \cong A_d$ and from what we have just shown the permutation character $\pi = 1_G + \chi + \chi^t$ for some $\chi \in Irr(A_d)$ and $t \in S_d \setminus A_d$. Moreover, this is the restriction of a permutation character $\pi' = 1_{S_d} + \chi^{S_d}$ of S_d of degree n with χ^{S_d} irreducible. Hence G is a normal subgroup of a 2-transitive permutation representation of S_d.

However, when $d>7$ it is well known that the only 2-transitive permutation representation of S_d is the natural representation of degree d (see, for example, [4, Exercise 7.7.1]). Thus $d \leq 7$, and a routine examination of the cases $d=5,6,7$ completes the proof.

(b) $M := PSL(2,q)$ is a nonabelian simple group when $q>3$ and has order $q(q^2-1)$ when q is even and order $\frac{1}{2}q(q^2-1)$ when q is odd. The number n_d of irreducible characters of a degree d is given by the following table (see, for example, [5, Section 38]):

Degree	1	q	$q+1$	$q-1$	$\frac{1}{2}(q+1)$	$\frac{1}{2}(q-1)$
q even	1	1	$\frac{1}{2}(q-2)$	$\frac{1}{2}q$	0	0
$q \equiv 1 \pmod 4$	1	1	$\frac{1}{4}(q-5)$	$\frac{1}{4}(q-1)$	2	0
$q \equiv 3 \pmod 4$	1	1	$\frac{1}{4}(q-3)$	$\frac{1}{4}(q-3)$	0	2

Suppose that G is a QI-group of degree n which is not 2-transitive and has M as its socle. Then Lemma 8 shows that $n = 1 + ld$ where d is the degree of an irreducible character and $1 < l \leq n_d$. First consider the case where $d = \frac{1}{2}(q+\varepsilon)$ with $\varepsilon = \pm 1$ (and so q odd). In this case $l = 2$ and $n = q+1+\varepsilon$. Since $n \mid |M|$, we conclude that $n = q$, $\varepsilon = -1$ and $q \equiv 3 \pmod 4$. But n is the index of a point stabilizer in M and it was already known to Galois that $PSL(2,q)$ can only have a subgroup of index q when q is a prime ≤ 11 (see [9, page 214]). It is now easy to check (for example, [3]) that in each of these cases M is 2-transitive.

Now look at the case where $d = q + \varepsilon$ with $\varepsilon = \pm 1$. Since $n \mid |M|$ and $GCD(d,n) = 1$, we can write $n = rs$ where $r = GCD(q,n) = GCD(q, 1 + l(q+\varepsilon)) = GCD(q, l+\varepsilon)$ and $s = GCD(q-\varepsilon, n) = GCD(q-\varepsilon, 2l+\varepsilon)$. Hence $n = 1 + l(q+\varepsilon) = rs \leq (l+\varepsilon)(2l+\varepsilon)$, and so $l \geq \frac{1}{2}q - \varepsilon$. Since $l \leq n_{q+\varepsilon}$, we conclude that q is even, $\varepsilon = 1$ and $l = \frac{1}{2}(q-2)$. This implies that $n = 1+ld = \frac{1}{2}q(q-1)$ and the point stabilizers of M have order $2(q+1)$. The classification of subgroups of $PSL(q)$ (see, for example, [9, page 213]) shows that these point stabilizers are dihedral groups and are maximal in M. Consider any prime $p \mid q+1$. Then $p > 2$ (because q is even) and every dihedral subgroup of M of order $2(q+1)$ has the form $N_M(P)$ where P is a Sylow p-subgroup of M. Thus these dihedral groups form a single class of conjugates in M. In particular, up to equivalence, there is a unique primitive permutation representation of M of degree $\frac{1}{2}q(q-1)$.

We have thus reduced to the case where $M = PSL(2, 2^k) = SL(2, 2^k)$ and $n = 2^{k-1}(2^k - 1)$ and have to determine when there is a QI-group G with $M \leq G \leq Aut(M)$ for this degree. We consider more carefully the characters of degree $q + 1$ for M. Consider the elements

$c := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and $a := \begin{bmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{bmatrix}$ where γ is a primitive root for $GF(2^k)$

in M and let ρ be a primitive $(2^k - 1)$th root of 1 in $\mathbb{C}$. It is shown in [5, Section 38] that characters χ_l $(l = 1, ..., \frac{1}{2}(2^k - 2))$ of degree $2^k + 1$ for M take the values:

$$\chi_l(1) = 2^k + 1,\ \chi_l(c) = 1,\ \chi_l(a^i) = \rho^{il} + \rho^{-il}\ (i = 1, ..., 2^{k-1} - 1)$$

and that χ_l is 0 on the other classes.

Since all elements of order 2 in M are conjugate to c, we can choose an element b in M of order $2^k + 1$ so that some point stabilizer $M_\alpha = \langle b, c \rangle$. This dihedral group has exactly $2^k + 1$ elements of order 2. Since the natural permutation character of M is $\pi = (1_{M_\alpha})^M$, Frobenius reciprocity shows that

$$[\pi, \chi_l] = [1_{M_\alpha}, (\chi_l)_{M_\alpha}] = \frac{1}{2(2^k + 1)} \left\{ 2^k + 1 + (2^k + 1) \cdot 1 \right\} = 1$$

for each l. Counting degrees now gives $\pi = 1_M + (\chi_1 + ... + \chi_{2^{k-1}-1})$.

Finally, the group of outer automorphisms of $PSL(2, 2^k)$ has order k and we can choose representatives of the corresponding cosets of the group of inner automorphisms in $Aut(PL(2, 2^k))$ as the group automorphisms induced by the automorphisms of the field $GF(2^k)$ (see [3, page xvi]). Moreover, each of the latter automorphisms maps $a \mapsto a^{2^j}$ for some j, and so its action on $\{\chi_1, ..., \chi_{2^{k-1}-1}\}$ is equivalent to the action of a Galois automorphism which maps $\rho \mapsto \rho^{2^j}$. Thus any group G of degree $2^{k-1}(2^k - 1)$ with M as its socle acts on the set of characters of M as a group of Galois automorphisms. Hence Lemma 8(a) shows that G is a QI-group if and only if the characters $\chi_1, ..., \chi_{2^{k-1}-1}$ are Galois conjugates. Since the values of these characters all lie in $\mathbb{Q}(\rho + \rho^{-1})$ this is equivalent to the condition that the Galois group $B := Gal(\mathbb{Q}(\rho+\rho^{-1})/\mathbb{Q})$ acts transitively on $\{\chi_1, ..., \chi_{2^{k-1}-1}\}$. If $2^k - 1$ is a prime then, for each l not divisible by $2^k - 1$, there is a Galois automorphism which maps $\rho^i + \rho^{-i} \mapsto \rho^{il} + \rho^{-il}$ for $i = 1, ..., 2^{k-1} - 1$ and so B acts transitively on $\{\chi_1, ..., \chi_{2^{k-1}-1}\}$. Conversely, if $2^k - 1$ is not prime, then $|B| = \frac{1}{2}\phi(2^k - 1) < 2^{k-1} - 1$ and so B cannot be transitive. Hence we conclude that G is a QI-group if and only if $2^k - 1$ is a prime. ■

4 Proof of Theorem 4

Let G be a transitive group of affine type with socle M (so M is a regular, elementary abelian p-group of order p^d for some prime p). Then G is of degree $n := p^d$ and is a semidirect product $M \cdot H$ where H (a point stabilizer) is isomorphic to a subgroup of $Aut(M) \cong GL(d, p)$ acting on the vector space M by conjugation. The group G is primitive if and only if H acts irreducibly on M (see, for example, [4, Sect. 4.7]). The permutation action of H as a point stabilizer of G is equivalent to its action as a group of automorphisms of M (fixing the identity element). The set of scalars in $GL(d, p)$ forms the centre of $GL(d, p)$. This set corresponds (in multiplicative notation) to the subgroup $Z \leq Aut(M)$ consisting of the automorphisms $u \mapsto u^k$ $(u \in M)$ for $k = 1, ..., p - 1$.

Theorem 12 *With the notation above, the transitive group $G = M \cdot H$ is* *a QI-group if and only if $\bar{G} := M \cdot (HZ)$ is 2-transitive.*

Proof. Let $G = M \cdot H$ be a transitive group of affine type and let $\pi := 1_G + (\chi_1 + ... + \chi_s)$ be the permutation character of G where the χ_i are irreducible characters of G. Since M is regular, the restriction π_M of the permutation character to M is the character of the regular representation. Because M is abelian, this implies that $\pi_M = \sum_{\lambda \in Irr(M)} \lambda$. Since M acts trivially on $Irr(M)$, Lemma 8 shows that $A \times H$ acts transitively on $Irr(M) \setminus \{1_M\}$ if and only if G is a QI-group.

Let ω be a primitive pth root of 1. The values of all $\lambda \in Irr(M)$ lie in $\mathbb{Q}(\omega)$ and each ν in A maps ω onto ω^k for some $k \in \{1, 2, ..., p-1\}$. If $\omega^\nu = \omega^k$, then ν acts on $Irr(M)$ via $\lambda^\nu = \lambda^k$ for all $\lambda \in Irr(M)$ where $\lambda^k(u) := \lambda(u^k)$ for all $u \in M$. Similarly, we have an action of A on M defined by $u^\nu := u^k$. Then $A \times H$ acts on both M and $Irr(M)$ such that $\lambda^{(\nu,x)}(u^{(\nu,x)}) = \lambda(u)$ for all $(\nu, x) \in A \times H$, $\lambda \in Irr(M)$ and $u \in M$. Therefore, by a lemma of Brauer (see, for example, [11, (6.32)]), $A \times H$ has the same number of orbits on the two sets. Since $A \times H$ has two orbits on $Irr(M)$ exactly when G is a QI-group, we conclude that this is also true for its action on M. Thus G is a QI-group if and only if $A \times H$ has two orbits on M (which are necessarily $\{1\}$ and $M \setminus \{1\}$).

Finally, the image in $Aut(M)$ of the action of A is equal to Z. Hence G is a QI-group if and only if HZ has two orbits on M or, equivalently, if and only if $\bar{G} := M \cdot (HZ)$ is 2-transitive. ∎

Since $\left|\bar{G} : G\right|$ divides $|Z| = p-1$, Clifford's theorem implies the following.

Corollary 13 *The rank of a QI-group of affine type and degree p^d is of the form $1 + s$ where $s \mid p-1$, so the rank is at most p. In particular a QI-group of affine type and degree 2^d is necessarily 2-transitive.*

A solvable primitive group is necessarily of affine type, and Huppert has given a complete description of all 2-transitive solvable groups. With a small number of exceptions, a 2-transitive solvable group of degree p^d is a subgroup of the extended affine group $A\Gamma L(1, p^d)$ (see [10, Chap. XII Theorem 7.3]). Using this fact, it is not difficult to construct examples of solvable QI-groups. A description of the nonsolvable 2-transitive groups of affine type is more complicated but has been determined by Hering in a series of papers (see [7], [8] and related papers). A summary of Hering's work is given in [10, Chap. XII page 386]

Here are two nontrivial examples of nonsolvable QI-groups of affine type.

Example 14 *There exist sharply* 2*-transitive permutation groups of degrees* 29^2 *and* 59^2*, respectively. In each case the one-point stabilizer has the form* $SL(2,5) \times Z$ *where the centre* Z *is cyclic of order* 7 *and* 29*, respectively (see [10, Chap. XII, Theorem 9.4]). These two permutation groups contain subgroups of the forms* $29^2 : SL(2,5)$ *and* $59^2 : SL(2,5)$*. The theorem above shows that they are QI-groups of ranks* 7 *and* 29*, respectively.*

References

[1] R.W. Baddeley, 'Multiplicity-free and self-paired primitive permutation groups, J. Algebra **162** (1993) 482–530.

[2] P.J. Cameron, *Permutation Groups* (Cambridge University Press, Cambridge, 1999).

[3] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups* (Oxford University Press, Oxford, 1985).

[4] J.D. Dixon and B. Mortimer, *Permutation Groups* (Springer-Verlag, New York, 1996).

[5] L. Dornhoff, *Group Representation Theory (Part A)* (Marcel Dekker, New York, 1971).

[6] The GAP Group, *GAP—Groups, Algorithms, and Programming.* Version 4.4 3 (2004) (http://www.gap-system.org).

[7] C. Hering, 'Transitive linear groups and linear groups which contain irreducible subgroups of prime order', *Geom. Dedicata* **2** (1974) 425–460.

[8] C. Hering, 'Transitive linear groups and linear groups which contain irreducible subgroups of prime order II', *J. Algebra* **93** (1985) 151–164.

[9] B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin, 1967).

[10] B. Huppert and N. Blackburn, *Finite Groups III* (Springer-Verlag, Berlin, 1982).

[11] I.M. Issacs, *Character Theory of Finite Groups* (Academic Press, New York, 1976).

[12] H. Wielandt, *Finite Permutation Groups* (Academic Press, New York, 1964).