

Characterising a family of elusive permutation groups*

Michael Giudici and Shane Kelly[†]

School of Mathematics and Statistics
The University of Western Australia
35 Stirling Highway
Crawley WA 6009
Australia
email: giudici@maths.uwa.edu.au
shanekelly64@hotmail.com

Abstract

A finite transitive permutation group is said to be *elusive* if it has no fixed point free elements of prime order. In this paper we show that all elusive groups $G = N \rtimes G_1$ with N an elementary abelian minimal normal subgroup and G_1 cyclic, can be constructed from transitive subgroups of $\text{AGL}(1, p^2)$, for p a Mersenne prime, acting on the set of $p(p+1)$ lines of the affine plane $\text{AG}(2, p)$.

1 Introduction

According to the Orbit-Counting Lemma (see for example [1, Theorem 2.2]), the average number of fixed points of a finite permutation group acting on

*This paper forms part of an Australian Research Council Discovery project which supported the second author while the work for this paper was conducted. The first author was supported by an Australian Postdoctoral Fellowship.

[†]Current address: Via Libia, 29, Padova 35141 PD, Italy

a finite set is the number of orbits. Since the identity fixes all the points, it follows that a finite transitive permutation group of degree at least two must have a fixed point free element. Using the Classification of Finite Simple Groups, Fein, Kantor and Schacher [6] proved that there is actually a fixed point free element of prime power order. However, there is not necessarily one of prime order as they demonstrated with the groups $\text{AGL}(1, p^2)$ for p a Mersenne prime acting on the set of $p(p + 1)$ lines of the affine plane $\text{AG}(2, p)$. We call a finite transitive permutation group with no fixed point free elements of prime order *elusive*.

Any transitive subgroup of an elusive group is elusive and so we call any transitive subgroup of the elusive group $\text{AGL}(1, p^2)$ an *FKS-group*. Another example of an elusive permutation group is the Mathieu group M_{11} in its action on 12 points. This contains $\text{AGL}(1, 9)$ and $M_{10} \cong A_6 \cdot 2$ as transitive subgroups. In fact, M_{11} and M_{10} in their actions on 12 points are the only elusive permutation groups which are almost simple [8, Theorem 1.4]. It was also shown in [8] that the only elusive groups with a transitive minimal normal subgroup are the groups $M_{11} \text{ wr } K$ acting on 12^k points with K a transitive subgroup of S_k . More examples and constructions of elusive groups were given in [2, 7].

The FKS-groups have abstract structure $G = N \rtimes G_1$, where N is a minimal normal elementary abelian p -group G and G_1 is cyclic. Note that N has $p + 1$ orbits of length p . The elusive groups provided by the doubling construction in [2, Theorem 3.3] using an FKS-group as input also have this abstract structure. The doubling construction was generalised in [7] (see Construction 2.3) to a priming construction which multiplies the order of G_1 by a prime dividing $p - 1$. Again all the groups constructed have abstract structure $G = N \rtimes G_1$ with N an elementary abelian p -group and G_1 cyclic. In this paper we prove that the groups yielded by the priming construction are the only elusive groups with this abstract structure.

Theorem 1.1. *Let G be an elusive permutation group such that $G = N \rtimes G_1$ for N an elementary abelian minimal normal subgroup and G_1 cyclic. Then G can be obtained by repeatedly applying Construction 2.3 to an FKS-group.*

Corollary 1.2. *Let G be an elusive permutation group such that $G = N \rtimes G_1$ for N an elementary abelian minimal normal p -subgroup and G_1 cyclic. Then $p = 2^l - 1$ is a Mersenne prime, $|N : N_\alpha| = p$ and the degree of G is $p^{2^{j_0} r_1^{j_1} \dots r_t^{j_t}}$ where $j_0 \geq l, j_1, \dots, j_t \geq 0$ and r_1, \dots, r_t are distinct odd primes dividing $p - 1$.*

In [10], a construction of Kantor is given as a possible source of elusive permutation groups. These groups are of the form $G = N \rtimes G_1$ where $N \cong C_p^d$ and G_1 is a 2-subgroup of the multiplicative group of $\text{GF}(p^d)$. It was shown in [10] that when $p = 3$ this does in fact produce elusive permutation groups while the doubling construction in [2] shows that it produces examples for any Mersenne prime p . Theorem 1.1 shows that these are the only primes for which the construction produces elusive groups.

The *2-closure* of a permutation group G acting on a set Ω is the largest subgroup of $\text{Sym}(\Omega)$ with the same set of orbits as G on the set Ω^2 . We say that G is *2-closed* if it is equal to its 2-closure. The *polycirculant conjecture* (see [2]) states that every 2-closed transitive permutation group has a fixed point free element of prime order. The automorphism group of a digraph is 2-closed, and Marusič [12] originally asked if every vertex transitive digraph has a fixed point free automorphism of prime order. This was later extended to 2-closed groups by Klin [3] and has recently received a lot of attention, for example [2, 4, 5, 8, 9, 13]. It was shown in [7, p 2723] that the elusive permutation groups in Theorem 1.1 are not 2-closed and that their 2-closures are not elusive.

2 Priming and depriming

We will need the following result about the representation theory of cyclic groups which follows from Schur's Lemma.

Lemma 2.1. *Let V be a d -dimensional vector space over $\text{GF}(q)$ and G_1 a cyclic irreducible group of linear transformations of V . Then we can identify V with $\text{GF}(q^d)$ such that G_1 acts on V as a subgroup of $\text{GF}(q^d)^*$ with G_1 not contained in any proper subfield of $\text{GF}(q^d)$. In particular, $|G_1|$ is prime to q .*

If G is an elusive permutation group acting on the set Ω then every element g of prime order fixes a point. Hence if $\alpha \in \Omega$, then g is conjugate to an element of G_α . The following result is an application of this observation.

Theorem 2.2 ([2] Theorem 3.1). *Let G be a subgroup of $\text{GL}(V)$ for some finite vector space V , and suppose that G has order prime to the characteristic of V . Let H be a subgroup of G , and U be an H -invariant proper subspace of V . Then the action of $V \rtimes G$ on the set of right cosets of $U \rtimes H$ is elusive if and only if the following hold:*

(i). The images of U by G cover V .

(ii). Every conjugacy class of elements of prime order in G meets H .

We have the following priming construction from [7].

Construction 2.3 (A priming construction). Let $G = V \rtimes \langle a \rangle$ be an elusive permutation group of degree $p^s l$ with point stabiliser $H = U \rtimes \langle b \rangle$, where

- (i). V is a finite dimensional vector space over $\text{GF}(p)$,
- (ii). $a \in \text{GL}(V)$ of order k , such that k is prime to p ,
- (iii). U is a codimension s subspace of V which is $\langle b \rangle$ -invariant.

Let r be a prime which divides k . Let

$$V' = \underbrace{V \oplus V \oplus \cdots \oplus V}_{r \text{ copies}}$$

and let g be the linear transformation in $\text{GL}(V)$ wr S_r of the vector space V' given by $(1, \dots, 1, a)\tau$ where $\tau = (123 \dots r)$ permutes the r copies of V . Next let

$$U' = U \oplus \underbrace{V \oplus V \oplus \cdots \oplus V}_{r-1 \text{ copies}}.$$

Then U' is M -invariant, where $M = \langle (b, \dots, b) \rangle$. Finally, let $G^* = V' \rtimes \langle g \rangle$ and $H^* = U' \rtimes M$.

Theorem 2.4. [7, Theorem 2.6] *Let G^* and H^* be as obtained from Construction 2.3. Then the action of G^* on the set of right cosets of H^* is elusive of degree $p^s l r$.*

An important part of our proof of Theorem 1.1 is the following depriming theorem.

Theorem 2.5. *Suppose that $G = V \rtimes G_1$ is an elusive permutation group with point stabiliser $H = U \rtimes H_1$ such that $V \cong \text{GF}(q)^d$ and $G_1 = \langle g \rangle$ is a cyclic irreducible subgroup of $\text{GL}(d, q)$. Suppose that there is a decomposition $V = V_1 \oplus \cdots \oplus V_t$ preserved by G_1 such that $U = U_1 \oplus V_2 \oplus \cdots \oplus V_t$. Then $V_1 \rtimes \langle g^t \rangle$ acts elusively on the set of right cosets of $U_1 \rtimes H_1$. Moreover, G can be reconstructed from the elusive action of $V_1 \rtimes \langle g^t \rangle$ via Construction 2.3.*

Proof. Let $e_{11}, e_{12}, \dots, e_{1r}$ be a basis for V_1 and for $j = 2, \dots, t$, let $e_{ji} = e_{1i}^{g^{j-1}}$ for each $i = 1, \dots, r$. Then $\{e_{ji} \mid i = 1, \dots, r, j = 1, \dots, t\}$ is a basis for V . Moreover, with respect to this basis $g = (1, \dots, 1, a)\tau$ where $a \in \text{GL}(r, q)$ and $\tau = (12 \dots t)$ cyclically permutes the V_i . Then $g^t = (a, \dots, a)$ and since G_1 is irreducible we have that $\langle a \rangle$ is an irreducible subgroup of $\text{GL}(r, q)$. Thus $\langle g^t \rangle$ acts faithfully and irreducibly on V_1 . Moreover, since H_1 fixes U , it follows that $H_1 \leq \langle g^t \rangle$. As G_1 is cyclic and irreducible, Lemma 2.1 implies that $|G_1|$ is coprime to p and so by Theorem 2.2, every element of prime order in G_1 is in H_1 . Thus every element of prime order in $\langle g^t \rangle$ lies in H_1 . Let $v \in V_1$. Then $v' = (v, \dots, v) \in V$ and so by Theorem 2.2, there exists g^i such that $(v')^{g^i} \in U$. Thus $U_1 \neq \{0\}$ and there exists j such that $v^{a^j} \in U_1$. Hence $(v')^{g^{tj}} \in U$. Thus the set of images of U_1 under $\langle g^t \rangle$ covers V_1 and so by Theorem 2.2, the action of $V_1 \rtimes \langle g^t \rangle$ on the set of right cosets of $U_1 \rtimes H_1$ is elusive. The fact that G can be reconstructed from $V_1 \rtimes \langle g^t \rangle$ using Construction 2.3 follows from the representation of g as $(1, \dots, 1, a)\tau$. \square

3 Proof of main theorem

We will have the following setup throughout this section and as such, these will be referred to collectively as Hypothesis 1.

Hypothesis 1. *Let $G = V \rtimes G_1$ be an elusive permutation group with point stabiliser $H = U \rtimes H_1$, where*

- (i). $V = \text{GF}(q)^d$ with $q = p^f$ for some prime p and positive integer $d \geq 2$,
- (ii). $G_1 = \langle g \rangle \leq \text{GF}(q^d)^*$ and is irreducible,
- (iii). $|G_1| = n$ and the primes dividing n also divide $q - 1$,
- (iv). $U < V$ and $\dim U = e \geq 1$,
- (v). $H_1 \leq \text{GF}(q)^*$,
- (vi). $H_1 < G_1$ with $m = |H_1|$ and U is H_1 -invariant.

We begin by showing that an elusive permutation group satisfying the conditions of Theorem 1.1 is of the form given in Hypothesis 1.

Lemma 3.1. *Let G be an elusive permutation group such that $G = N \rtimes G_1$ for N an elementary abelian minimal normal subgroup and G_1 cyclic. Then G satisfies Hypothesis 1.*

Proof. Let Ω be the set upon which G acts and $\alpha \in \Omega$. Suppose that $|N| = p^r$ for some prime p . Then N is an r -dimensional vector space over $\text{GF}(p)$. Since $N \triangleleft G$, there exists a homomorphism $\phi : G_1 \rightarrow \text{GL}(r, p)$. Let K be the kernel of ϕ . Suppose that $K \neq 1$ and let r be a prime dividing $|K|$ and $h \in K$ be an element of order r . Since G_1 is cyclic, $\langle h \rangle \triangleleft G_1$ and as h centralises N , we also have $\langle h \rangle \triangleleft G$. Since G is elusive, all elements of prime order in G are conjugate to an element of G_α , and so $h \in G_\alpha$. Thus G_α contains a normal subgroup of G , contradicting G acting faithfully on Ω . Thus $K = 1$ and so G_1 is isomorphic to a subgroup of $\text{GL}(r, p)$. Since N is a minimal normal subgroup of G it follows that G_1 is irreducible.

By Lemma 2.1, we can identify N with $\text{GF}(p^r)$ such that $G_1 \leq \text{GF}(p^r)^*$. Since all nontrivial elements of N are conjugate to an element of G_α and hence of N_α it follows that $N_\alpha \neq 1$ and by the faithfulness of G we have that $N_\alpha \neq N$. Moreover, since the elements of G_1 of prime order are conjugate to elements of G_α , and these elements do not have order p , it follows that $G_\alpha = N_\alpha \rtimes H_1$ for some nontrivial subgroup H_1 of G_1 such that every prime dividing $|G_1|$ divides $|H_1|$.

Let $V = N$ and $U = N_\alpha$. Now N_α is a $\text{GF}(p)$ -subspace of V invariant under H_1 (vi). Let $\text{GF}(p^f)$ be the largest subfield of $\text{GF}(p^r)$ such that U is invariant under $\text{GF}(p^f)^*$ and let $q = p^f$ and $d = r/f$. As G_1 is irreducible, $d \geq 2$. Then V is a d -dimensional vector space over $\text{GF}(q)$ (i) and U is an e -dimensional $\text{GF}(q)$ -subspace with $e \geq 1$ (iv). Moreover, $G_1 \leq \text{GF}(q^d)^*$ (ii) and the stabiliser in $\text{GF}(q^d)^*$ of U is $\text{GF}(q)^*$. Since U is H_1 invariant, we have $H_1 \leq \text{GF}(q)^*$ (v) and so has order dividing $q - 1$. By Theorem 2.2, every prime dividing $|G_1|$ divides $|H_1|$, and so only primes dividing $q - 1$ divide $|G_1|$ (iii). Thus G is as in Hypotheses 1. \square

We now deal with the case where $d = 2$.

Proposition 3.2. *Suppose Hypothesis 1 holds. If $d = 2$ then q is a Mersenne prime and G is an FKS-group.*

Proof. The dimension e of U is necessarily 1 and so we can assume $U = \text{GF}(q)$ and $V = \text{GF}(q)^2$. By Theorem 2.2, V is covered by the images of U under G_1 so G_1 is transitive on the set of 1-spaces of V (of which there are $q + 1$)

and so $q+1$ divides $n = |G_1|$. Moreover, by Hypothesis 1, all primes dividing n divide $q-1$. Thus if r is a prime dividing $q+1$, it divides $q-1$ and so $r=2$. Since r was arbitrary we have $q+1=2^i$ and so $q=2^i-1$. It follows from [11] that q is prime and so G is an FKS-group. \square

In the remaining part of this section we will have cause to refer to the largest power of some integer a that divides another integer b . This quantity will be denoted $\mu_a(b)$.

Lemma 3.3. *Let q be a positive integer and let r be an odd prime dividing $q-1$. Then*

$$\mu_r(q^d - 1) = \mu_r(q - 1)\mu_r(d)$$

Proof. First suppose $\mu_r(d) = 1$. Since $r|(q-1)$ we have $q \equiv 1 \pmod{r}$ and so $1+q+\dots+q^{d-1} \equiv d \pmod{r}$. But $\mu_r(d) = 1$ so $r \nmid d$ giving $r \nmid 1+q+\dots+q^{d-1}$ and so $\mu_r(q^d - 1) = \mu_r(q - 1) = \mu_r(q - 1)\mu_r(d)$.

Now we show that $\mu_r\left(\frac{q^{r^{i+1}}-1}{q^{r^i}-1}\right) = r$ for $i \geq 0$. We can expand the fraction to $\frac{q^{r^{i+1}}-1}{q^{r^i}-1} = 1 + q^{r^i} + q^{2r^i} + q^{3r^i} + \dots + q^{(r-1)r^i}$ and since $q \equiv 1 \pmod{r}$ we see that r divides $\frac{q^{r^{i+1}}-1}{q^{r^i}-1}$. To see that r^2 does not divide $\frac{q^{r^{i+1}}-1}{q^{r^i}-1}$ note that if $a, b < r$ then $(ar + b)^r \equiv b^r \pmod{r^2}$ (using binomial expansion). Since $q \equiv 1 \pmod{r}$ we have $q^r \equiv 1 \pmod{r^2}$ and so $\frac{q^{r^{i+1}}-1}{q^{r^i}-1} \equiv r \pmod{r^2}$.

Now let $\nu = \mu_r(d)$ and $\delta = d/\nu$. We have

$$(q^d - 1) = (q - 1) \frac{q^r - 1}{q - 1} \frac{q^{r^2} - 1}{q^r - 1} \frac{q^{r^3} - 1}{q^{r^2} - 1} \cdots \frac{q^\nu - 1}{q^{\nu/r} - 1} \frac{(q^\nu)^\delta - 1}{q^\nu - 1}$$

and so the lemma follows from the previous two cases. \square

Lemma 3.4. *Let q be an odd integer. Then*

$$\mu_2(q^d - 1) = \begin{cases} \mu_2(q - 1) & \text{if } d \text{ is odd} \\ \mu_2(q^2 - 1) \frac{\mu_2(d)}{2} & \text{if } d \text{ is even} \end{cases}$$

Proof. We have $q^d - 1 = (q - 1)(q^{d-1} + \dots + q + 1)$. If d is odd then $q^{d-1} + \dots + q + 1 \equiv 1 \pmod{2}$ and so $\mu_2(q^d - 1) = \mu_2(q - 1)$. Suppose d is even. First note that since q is odd and -1 is not a square mod 4 we have $\mu_2(q^{2^i} + 1) = 2$ for all $i > 0$.

Now let $\nu = \mu_2(d)$ and $\delta = d/\nu$. We have

$$\begin{aligned} q^d - 1 &= (q^2 - 1) \frac{q^4 - 1}{q^2 - 1} \frac{q^8 - 1}{q^4 - 1} \cdots \frac{q^\nu - 1}{q^{\nu/2} - 1} \frac{(q^\nu)^\delta - 1}{q^\nu - 1} \\ &= (q^2 - 1)(q^2 + 1)(q^4 + 1)(q^8 + 1) \cdots (q^{\nu/2} + 1) \frac{(q^\nu)^\delta - 1}{q^\nu - 1} \end{aligned}$$

and so the result follows from the previous two cases. \square

We can now eliminate the case where d is a prime.

Lemma 3.5. *Suppose Hypothesis 1 holds. Then d is not an odd prime dividing $q - 1$.*

Proof. Suppose to the contrary. Then by Lemmas 3.3 and 3.4, $\mu_d(q^d - 1) = d\mu_d(q - 1)$ and $\mu_2(q^d - 1) = \mu_2(q - 1)$. Thus there are at most $d \leq q - 1$ images of U under G_1 . Since U contains at most $q^{d-1} - 1$ nonzero vectors, the images of U under G_1 do not cover V . This contradicts Theorem 2.2 and so the result holds. \square

We also show that if d is twice a prime then U is a hyperplane.

Lemma 3.6. *Suppose that Hypothesis 1 holds and $d = 2r$ for some prime r dividing $q - 1$. Then U is a hyperplane.*

Proof. Since n is only divisible by primes dividing $q - 1$, Lemmas 3.3 and 3.4 imply that the only primes dividing n/m are 2 and r . Moreover, $\mu_2(q^{2r} - 1) = \mu_2(q^2 - 1)\mu_2(r)$, while if r is odd then $\mu_r(q^{2r} - 1) = r\mu_r(q - 1)$. It follows that U has at most $r\mu_2(q + 1) \leq q^2 - 1$ images under G_1 . Suppose that U is not a hyperplane. Then the images of U under G_1 cover at most

$$(q^2 - 1)(q^{2r-2} - 1) = q^{2r} - q^{2r-2} - q^2 + 1 < q^d - 1$$

non-zero vectors of V . This contradicts the fact that the images of U under G_1 cover V (Theorem 2.2) and so U is a hyperplane. \square

Next we obtain some results concerning decompositions of V .

Lemma 3.7. *Let $g \in \text{GL}(d, q)$ act irreducibly on the vector space $V = \text{GF}(q)^d$ and suppose that all primes dividing $n = |g|$ also divide $q - 1$. If there is an odd prime r dividing $q - 1$ such that $\mu_r(n)$ does not divide $q - 1$ then there is a decomposition*

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

preserved by $\langle g \rangle$. Furthermore, $\langle g^r \rangle$ is the stabiliser in $\langle g \rangle$ of V_1 .

Proof. By Lemma 2.1, $\langle g \rangle$ can be considered as a subgroup of the multiplicative group $\text{GF}(q^d)^*$ acting on $V \cong \text{GF}(q^d)$. Thus n divides $q^d - 1$. Since r divides $q - 1$ but $\mu_r(n)$ does not, it follows from Lemma 3.3 that r divides d . Moreover,

$$\mu_r(q^d - 1) = \mu_r(q - 1)\mu_r(d) = r\mu_r(q - 1)\mu_r(d/r) = r\mu_r(q^{d/r} - 1)$$

Now for every prime divisor $r' \neq r$ of n , it also follows from Lemma 3.3 that $\mu_{r'}(q^d - 1) = \mu_{r'}(q^{d/r} - 1)$. So $n/r = |g^r|$ divides $q^{d/r} - 1$ and therefore $\langle g^r \rangle$ is a subgroup of $\text{GF}(q^{d/r})^*$.

Now still identifying V with the additive group of $\text{GF}(q^d)$ we see that there is a $\langle g^r \rangle$ -invariant $\text{GF}(q)$ -subspace, namely the subfield $V_1 = \text{GF}(q^{d/r})$. The images V_1, V_2, \dots, V_r of V_1 under $\langle g \rangle$ are also $\langle g^r \rangle$ -invariant since $\langle g^r \rangle$ is a normal subgroup of $\langle g \rangle$. Furthermore, the V_i span a $\langle g \rangle$ -invariant subspace of V . Since $\langle g \rangle$ is irreducible it follows that the V_i span V . By considering their dimensions we see that they form the required decomposition. \square

Lemma 3.8. *Let $g \in \text{GL}(d, q)$ act irreducibly on the vector space $V = \text{GF}(q)^d$ and suppose that all primes dividing $n = |g|$ also divide $q - 1$. Furthermore, suppose that $d > 2$ and $n = 2^i n' > 2$ with n' odd and dividing $q - 1$. Then there is a decomposition*

$$V = V_1 \oplus V_2$$

preserved by G_1 . Furthermore, $\langle g^r \rangle$ is the stabiliser in $\langle g \rangle$ of V_1 .

Proof. By Lemma 2.1, $\langle g \rangle$ can be considered as a subgroup of the multiplicative group $\text{GF}(q^d)^*$ acting on $V \cong \text{GF}(q^d)$. Thus n divides $q^d - 1$. Moreover, by Lemmas 3.3 and 3.4, if r is an odd prime dividing d then n divides $q^{d/r} - 1$, contradicting $\langle g \rangle$ being irreducible. Thus d is a power of 2. For every odd prime divisor r of n , it also follows from Lemma 3.3 that $\mu_r(q^d - 1) = \mu_r(q^{d/2} - 1)$. Since d is a power of 2, Lemma 3.4 implies that

$$\mu_2(q^d - 1) = \mu_2(q^2 - 1) \frac{\mu_2(d)}{2} = 2\mu_2(q^2 - 1)\mu_2(d/4) = 2\mu_2(q^{d/2} - 1)$$

So $n/2 = |g^2|$ divides $q^{d/2} - 1$ and therefore $\langle g^2 \rangle$ is a subgroup of $\text{GF}(q^{d/2})^*$.

The rest of the proof then follows along exactly the same lines as the proof for Lemma 3.7. \square

Lemma 3.9. *Let $\nu r = d$ and let q, ν, r, d all be natural numbers with $\nu > 2$ and $q > 1$. Then*

$$\frac{q^d - 1}{q^\nu - 1} (q^{\nu-1} - 1) > q^{d-2} - 1$$

Proof. Let $Q = q^\nu$. Then

$$\begin{aligned}
\frac{q^d - 1}{q^\nu - 1}(q^{\nu-1} - 1) &> q^{d-2} - 1 \\
\iff \frac{Q^r - 1}{Q - 1}(Qq^{-1} - 1) &> Q^r q^{-2} - 1 \\
\iff \left(\sum_{i=0}^{r-1} Q^i \right) Qq^{-1} - \left(\sum_{i=0}^{r-1} Q^i \right) &> Q^r q^{-2} - 1 \\
\iff Q^r q^{-1} + \left(\sum_{i=0}^{r-2} Q^i \right) Qq^{-1} - \left(\sum_{i=1}^{r-1} Q^i \right) - 1 &> Q^r q^{-2} - 1 \\
\iff \left(\sum_{i=1}^{r-1} Q^i \right) q^{-1} - \left(\sum_{i=1}^{r-1} Q^i \right) &> Q^r q^{-2} - Q^r q^{-1} \\
\iff \left(\sum_{i=1}^{r-1} Q^i \right) (q^{-1} - 1) &> Q^r q^{-1} (q^{-1} - 1) \\
\iff \sum_{i=1}^{r-1} Q^i &< Q^r q^{-1} \\
\iff 1 + \sum_{i=1}^{r-1} Q^i &\leq Q^r q^{-1} \\
\iff \frac{q^d - 1}{q^\nu - 1} &\leq q^{d-1} \\
\iff q^d - 1 &\leq q^{d-1}(q^\nu - 1) \\
\iff \frac{q^d - 1}{q - 1} &\leq q^{d-1} \frac{q^\nu - 1}{q - 1} \\
\iff \sum_{i=0}^{d-1} q^i &\leq \sum_{i=d-1}^{d-2+\nu} q^i \\
\iff \frac{q^{d-1} - 1}{q - 1} &\leq q^d + q^{d+1} + \dots + q^{d-2+\nu}
\end{aligned}$$

The last inequality holds as the left hand side is less than q^{d-1} which is less than each term on the right hand side. Thus the result holds. \square

A *secundum* of a vector space is a subspace of codimension two.

Lemma 3.10. *Suppose that U is a secundum of $V = \text{GF}(q^d)$ considered as a $\text{GF}(q)$ -vector space and that V has a decomposition $V_1 \oplus \cdots \oplus V_r$ with each V_i invariant under $\text{GF}(q^{d/r})^*$ for some prime divisor r of d with $d/r > 2$. Then there is a (possibly different) decomposition $V'_1 \oplus V'_2 \oplus \cdots \oplus V'_r$ with each V'_i invariant under $\text{GF}(q^{d/r})^*$ such that $U = U'_1 \oplus V'_2 \oplus \cdots \oplus V'_r$ where U'_1 has codimension 2 in V'_1 .*

Proof. Since $\text{GF}(q^d)^*$ is transitive on the set of nonzero vectors of V the images of V_1 under $\text{GF}(q^d)^*$ cover V . Since $\text{GF}(q^{d/r})^*$ is the stabiliser of V_1 in $\text{GF}(q^d)^*$, the number of images of V_1 is $\frac{q^d-1}{q^{\nu}-1}$, where $\nu = \frac{d}{r}$. As V_1 contains $q^\nu - 1$ non-zero vectors, it follows that every non-zero vector of V lies in a unique image of V_1 under $\text{GF}(q^d)^*$. We denote this set of images by \mathcal{S} .

Since U has codimension 2 in V and $\nu > 2$, it follows that each element of \mathcal{S} meets U in a nontrivial subspace of dimension ν , $\nu - 1$ or $\nu - 2$. We wish to show that there is at least one element of \mathcal{S} that intersects U in a subspace of codimension 2. Suppose that there is no such subspace. Then each element of $\{U \cap W : W \in \mathcal{S}\}$ contains at least $q^{\nu-1} - 1$ non-zero vectors. Since $|\mathcal{S}| = \frac{q^d-1}{q^\nu-1}$ and each non-zero vector of V lies in a unique element of \mathcal{S} , this gives $\frac{q^d-1}{q^\nu-1}(q^{\nu-1} - 1)$ non-zero vectors. By Lemma 3.9 this is greater than $q^{d-2} - 1$, the number of non-zero vectors in U , a contradiction. Thus there must be at least one image V_1^h of V_1 under $\text{GF}(q^d)^*$ that intersects U in a subspace of codimension 2. Setting $V'_i = V_i^h$ we obtain the required decomposition. \square

Proposition 3.11. *Suppose Hypothesis 1 holds with $d \geq 3$ and suppose that there is a prime r dividing $q-1$ with $\mu_r(n)$ not dividing $q-1$ with the following conditions:*

- (a) *if $r = 2$ then r is the only prime divisor of n with $\mu_r(n)$ not dividing $q - 1$;*
- (b) *if $d/r = 2$ then U is a hyperplane.*

Then there is a dimension d/r subspace V_1 of V containing another subspace U_1 such that $V_1 \rtimes \langle g^r \rangle$ acts elusively on the set of cosets of $U_1 \rtimes H_1$. Moreover, if $e < d - 1$ then we can take U_1 to be an H_1 -invariant secundum of V , while if $e = d - 1$ then U_1 is a hyperplane of V_1 and the elusive permutation group G can be reconstructed from $V_1 \rtimes \langle g^r \rangle$ via Construction 2.3.

Proof. By Lemma 3.5, $d/r \geq 2$. It follows from Lemmas 3.7 or 3.8 that there is a decomposition $V = V_1 \oplus \cdots \oplus V_r$ preserved by $\langle g \rangle$ with each V_i invariant under $\langle g^r \rangle$. First suppose that U is a hyperplane and let $U' = U_1 \oplus V_2 \oplus \cdots \oplus V_r$, where U_1 is a hyperplane of V_1 . Now $G_1 \triangleleft \text{GF}(q^d)^*$ and $\text{GF}(q^d)^*$ is transitive on hyperplanes and so there exists $h \in \text{GF}(q^d)^*$ which maps U to U' . Moreover, h induces an automorphism of G which maps $U \rtimes H_1$ to $U' \rtimes H_1$. Thus the action of G on the set of cosets of $U \rtimes H_1$ is equivalent to the action of G on the set of cosets of $U' \rtimes H_1$. Thus without loss of generality we may replace U with U' . Then by Theorem 2.5, $V_1 \rtimes \langle g^r \rangle$ acts elusively on the set of cosets of $U_1 \rtimes \langle h \rangle$ and G can be reconstructed from $V_1 \rtimes \langle g^r \rangle$ via Construction 2.3.

Now suppose that U is not a hyperplane. Then U is contained in a secandum U' . Moreover, since $H_1 \leq \text{GF}(q)^*$, we have that U' is H_1 -invariant and since the set of images of U under G_1 covers V , so does the set of images of U' under G_1 . Hence by Theorem 2.2, $G = V \rtimes G_1$ also acts elusively on the set of cosets of $U' \rtimes H_1$. By Lemma 3.10, we may assume that (changing the decomposition if necessary) $U' = U_1 \oplus V_2 \oplus \cdots \oplus V_r$ where U_1 has codimension 2 in V_1 . By Theorem 2.5, it follows that $V_1 \rtimes \langle g^r \rangle$ acts elusively on the set of cosets of $U_1 \rtimes \langle h \rangle$. \square

We can now prove Theorem 1.1.

Proof of Theorem 1.1. By Lemma 3.1, we may take G as in Hypothesis 1. The theorem is proved by induction on d . If $d = 2$ then G is an FKS-group by Proposition 3.2. Suppose $d > 2$. Since the images of U under G_1 cover V , it follows that n does not divide $q - 1$. Thus we are in one of the following two cases.

- (i). There is an odd prime r' such that $\mu_{r'}(n)$ does not divide $q - 1$.
- (ii). $n = 2^i n'$ with n' odd and dividing $q - 1$ and 2^i not dividing $q - 1$.

If (i) holds let $r = r'$ while if (ii) holds let $r = 2$. By Lemma 3.5 and the fact that $d > 2$, we have $d \neq r$ and so $d/r \geq 2$. By Lemma 3.6 we may assume that if $d = 2r$ then U is a hyperplane. Thus we can apply Proposition 3.11 to obtain a new elusive group $G' = V_1 \rtimes \langle g^r \rangle$ with point stabiliser $U_1 \rtimes H_1$ satisfying Hypothesis 1 such that V_1 has dimension d/r and $U_1 < V_1$. Since $d/r < d$, the inductive hypothesis implies that G' can be obtained by repeatedly applying Construction 2.3 to an FKS-group and that U_1 is a hyperplane of V_1 . Thus by Proposition 3.11, G can be reconstructed

from G' by applying Construction 2.3 using the prime r and hence is obtained by repeatedly applying Construction 2.3 to an FKS-group. This completes the proof. \square

References

- [1] P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts 45 (1999).
- [2] Peter J. Cameron, Michael Giudici, Gareth A. Jones, William M. Kantor, Mikhail H. Klin, Dragan Marušič, and Lewis A. Nowitz, *Transitive permutation groups without semiregular subgroups*, J. London Math. Soc. 66 (2002) 325–333.
- [3] Peter J. Cameron(ed.), *Problems from the Fifteenth British Combinatorial Conference*, Discrete Math. 167/168 (1997) 605–61.
- [4] E. Dobson, A. Malnič, D. Marušič and L. A. Nowitz, *Semiregular automorphisms of vertex-transitive graphs of certain valencies*, J. Combin. Theory Ser. B 97 (2007) 371–380.
- [5] E. Dobson, A. Malnič, D. Marušič and L. A. Nowitz, *Minimal normal subgroups of transitive permutation groups of square-free degree*, Discrete Math. 307 (2007) 373–385.
- [6] Burton Fein, William M. Kantor, and Murray Schacher, *Relative Brauer groups. II*, J. Reine Angew. Math. 328 (1981) 39–57.
- [7] Michael Giudici, *New constructions of groups without semiregular subgroups*, Comm. Algebra. 35 (2007) 2719–2730.
- [8] Michael Giudici, *Quasiprimitive permutation groups with no fixed point free elements of prime order*, J. London Math. Soc. 67 (2003) 73–84.
- [9] M. Giudici and J. Xu, *All vertex-transitive locally quasiprimitive graphs have a semiregular automorphism*, J. Algebraic Combin. 25 (2007) 217–232.
- [10] G. Jones and M. Klin, *On polycirculant graphs and groups*, preprint N340, University of Southampton, 2000.

- [11] S. Ligh and L. Neal, *A note on Mersenne numbers*, *Math. Mag.* 47 (1974) 231–233.
- [12] Dragan Marušič, *On vertex symmetric digraphs*, *Discrete Math.* 36 (1981) 69–81.
- [13] Dragan Marušič and Raffaele Scapellato, *Permutation groups, vertex-transitive digraphs and semiregular automorphisms*, *Eur. J. Comb.* 19 (1998) 707–712.