

# New constructions of groups without semiregular subgroups

Michael Giudici  
School of Mathematics and Statistics  
The University of Western Australia  
35 Stirling Highway  
Crawley, WA 6009  
Australia  
giudici@maths.uwa.edu.au

## Abstract

An *elusive* permutation group is a transitive permutation group with no fixed point free elements of prime order, or equivalently, no nontrivial semiregular subgroups. We provide several new constructions of elusive groups, some of which enable us to build elusive groups with new degrees.

## 1 Introduction

A transitive permutation group on a set  $\Omega$  is called *elusive* if it does not contain a fixed point free element of prime order, or equivalently, no nontrivial semiregular subgroups. The first elusive groups were constructed in [6] and were the affine groups  $\text{AGL}(1, p^2)$ , where  $p$  is a Mersenne prime, acting on the set of lines of the affine plane  $\text{AG}(2, p)$ . Further examples and constructions were provided in [3]. It was determined in [9] that the only elusive groups with a transitive minimal normal subgroup are the wreath products  $M_{11} \text{ wr } K$ , of the Mathieu group  $M_{11}$  and a transitive subgroup  $K$  of  $S_k$ , acting on  $12^k$  points. Despite the existence of elusive groups, every transitive permutation group of degree at least two has a fixed point free element of prime power order [6, Theorem 1].

Let  $G$  be a permutation group on a set  $\Omega$ . The *2-closure*  $G^{(2)}$  of  $G$  is the largest subgroup of  $\text{Sym}(\Omega)$  which has the same orbits on ordered pairs as  $G$ .

For example, the 2-closure of a 2-transitive group is the full symmetric group. We say that  $G$  is *2-closed* if  $G = G^{(2)}$ . Given a graph  $\Gamma$ , any permutation of the vertices of  $\Gamma$  which preserves the orbits of  $\text{Aut}(\Gamma)$  on ordered pairs preserves adjacency and hence must be an automorphism of  $\Gamma$ . Thus  $\text{Aut}(\Gamma)$  is a 2-closed permutation group.

In 1981, Marušič [15] asked if every vertex-transitive digraph has a fixed point free automorphism of prime order. This question was later reposed by Jordan [13]. The existence of such an automorphism reveals much information about the structure of the digraph and allows it to be represented in a compact way, see [2]. Semiregular automorphisms have been particularly useful in constructing Hamiltonian paths [16, 17] and cycles [1] in families of vertex-transitive graphs, and in the classification of vertex-transitive graphs of small orders [14]. Cubic arc-transitive graphs whose quotient with respect to a semiregular automorphism is a tree have been classified in [11]. Marušič and Scapellato [18, Theorem 3.3] proved that all vertex-transitive cubic graphs have a fixed point free automorphism of prime order and more recently it has been shown that so do all vertex-transitive graphs of valency 4 [5]. It was shown in [10] that all vertex-transitive, locally quasiprimitive graphs have a semiregular automorphism. This includes all 2-arc-transitive graphs and all arc-transitive graphs of prime valency.

Klin [4] extended the question of Marušič and Jordan to a more general setting and asked if every transitive 2-closed group contains a fixed point free element of prime order. The conjecture that every transitive 2-closed group contains a fixed point free element of prime order is now referred to as the *polycirculant conjecture*, for more discussion see [3]. The results of [9] imply that all minimal normal subgroups of a counterexample are intransitive.

Let  $\mathcal{E}$  be the set of degrees for which elusive groups occur. Marušič [15, Theorems 3.3 and 3.4] showed that prime powers do not belong to  $\mathcal{E}$  and nor do integers of the form  $mp$  where  $p$  is a prime and  $m \leq p$ . The  $\text{AGL}(1, p^2)$  examples given in [6] have degree  $p(p+1)$  where  $p$  is a Mersenne prime while elusive groups of degree  $7^k \cdot 12$  and  $p^k \cdot 2^n$  where  $p$  is a Mersenne prime and  $2^n > p$  were constructed in [3, Pages 328, 329]. It was also shown in [3, Theorem 4.1(c)] that  $\mathcal{E}$  is closed under multiplication and the question of whether or not  $\mathcal{E}$  has density zero was posed.

In Section 2 we provide a new construction of elusive groups which proves the following.

**Theorem 1.1.** *Let  $p = 2^\ell - 1$  be a Mersenne prime and  $q_1, \dots, q_r$  be distinct odd primes dividing  $p - 1$ . Then for every  $k \geq 1, n \geq \ell$  and  $j_1, \dots, j_r \geq 0$ , there exists an elusive group of degree  $p^k 2^n q_1^{j_1} \dots q_r^{j_r}$ .*

We will see in Lemma 2.7 that the set of all degrees provided by The-

orem 1.1 has density zero. In Section 3, we provide a new construction of elusive groups using the permutation module for  $\text{AGL}(1, p^2)$ . Example 3.4 is particularly interesting as it is the first known example of an elusive group with an elementary abelian minimal normal subgroup  $N$  such that the stabiliser in  $N$  of point is not a hyperplane and  $G$  is not the wreath product in product action of an elusive group. In Section 4, we give a degree doubling construction. Neither of these two constructions give us new degrees but we see in Section 5 that they allow us to describe all elusive groups of degree at most 30. We also show that none of the examples constructed in this paper are 2-closed and so do not provide counterexamples of the polycirculant conjecture.

### Acknowledgements

The author would like to thank Cheryl Praeger and Tim Penttila for several helpful discussions. Part of the work appears in the author's PhD thesis completed under the supervision of Peter Cameron to whom he is also grateful. The author is currently supported by a Australian Postdoctoral Fellowship.

## 2 New degrees

The following theorem [3, Theorem 3.1] gives a general basis from which to construct elusive groups.

**Theorem 2.1.** *Let  $G_1$  be a subgroup of  $\text{GL}(V)$  for some finite vector space  $V$ , and suppose that  $G_1$  has order coprime to the characteristic of  $V$ . Let  $H_1$  be a subgroup of  $G_1$ , and  $W$  be an  $H_1$ -invariant proper subspace of  $V$ . Then the action of  $V \rtimes G_1$  on the set of right cosets of  $W \rtimes H_1$  is elusive if and only if*

- (a) *the images of  $W$  by  $G_1$  cover  $V$ ; and*
- (b) *every conjugacy class of elements of prime order in  $G_1$  meets  $H_1$ .*

Theorem 2.1 does not hold in the case where the characteristic of  $V$  divides  $|G_1|$ . For example, if  $V = \text{GF}(3)^2$ ,  $G_1 = \text{GL}(2, 3)$ ,  $W$  is a 1-space and  $H_1$  is the stabiliser in  $G_1$  of  $W$ , then conditions (a) and (b) hold but the action of  $V \rtimes G_1$  on the set of right cosets of  $W \rtimes H_1$  is not elusive. We have the following theorem in the noncoprime case.

**Theorem 2.2.** *Let  $G_1$  be a subgroup of  $\text{GL}(V)$  for some finite vector space  $V$  over a field of characteristic  $p$ , and suppose that  $p$  divides  $|G_1|$ . Let  $H_1$  be a subgroup of  $G_1$  and  $W$  be an  $H_1$ -invariant proper subspace of  $V$ . Then the action of  $V \rtimes G_1$  on the set of right cosets of  $W \rtimes H_1$  is elusive if and only if*

- (a) the images of  $W$  by  $G_1$  cover  $V$ ;
- (b) every conjugacy class of elements of prime order in  $G_1$  meets  $H_1$ ; and
- (c) for each element  $vh$  of order  $p$ , with  $v \in V$  and  $h \in H_1$ , there is an image  $U$  of  $W$  under  $G_1$  which is fixed by  $h$  such that  $vh$  fixes some translate of  $U$ .

*Proof.* Let  $G = V \rtimes G_1$  and  $H = W \rtimes H_1$ . Note that the elements of prime order in  $G$  are of three types:

1. elements of  $V$ ,
2. elements of order  $r \neq p$ ,
3. elements of order  $p$  which are not in  $V$ .

All elements in  $V$  fix a point (that is, a right coset) if and only if the images of  $W$  under  $G_1$  cover  $V$ . Since  $r \neq p$ , a Sylow  $r$ -subgroup of  $G_1$  is also a Sylow  $r$ -subgroup of  $G$  and so by Sylow's Theorem, all elements of prime order  $r \neq p$  are conjugate to an element of  $G_1$  and all elements of order  $r$  in  $H$  are conjugate to an element of  $H_1$ . Hence all elements of prime order  $r \neq p$  in  $G$  fix a point if and only if all conjugacy classes of elements of order  $r$  in  $G_1$  meet  $H_1$ .

If  $wg \in G$  with  $v \in V$  and  $g \in G_1$  has order  $p$  then  $g$  has order  $p$ . Moreover, the conjugates of  $vg$  are of the form  $vg'$  for some  $v \in V$  and  $g'$  conjugate in  $G_1$  to  $g$ . Note that if (b) holds then every element  $wg$  of order  $p$  is conjugate to an element  $vh$  for some  $h \in H_1$ . The element  $vh$  fixes a coset  $Huk$  with  $u \in V$  and  $k \in G_1$  if and only if  $vh$  fixes the translate  $W^k + u^k$ , that is  $(W^k + u^k + v)^h = W^k + u^k$ . Note that this requires  $W^k$  to be fixed by  $h$ . Hence all elements of order  $p$  fix a coset of  $H$  in  $G$  if and only if all conjugacy classes of  $G_1$  of elements of order  $p$  meet  $H_1$  and (c) holds.  $\square$

We also require the following lemma which determines when an action is faithful.

**Lemma 2.3.** *Let  $G_1$  be a subgroup of  $\text{GL}(V)$  for some finite vector space  $V$ . Let  $H_1$  be a subgroup of  $G_1$ , and  $W$  be an  $H_1$ -invariant proper subspace of  $V$ . Then the action of  $V \rtimes G_1$  on the set of right cosets of  $W \rtimes H_1$  is faithful if and only if  $\bigcap_{g \in G_1} W^g = \{0\}$ .*

*Proof.* Let  $K$  be the kernel of the action of  $V \rtimes G_1$  on the set of right cosets of  $W \rtimes H_1$ . Then  $K = \bigcap_{g \in G} (W \rtimes H_1)^g$  and so  $K \cap V = \bigcap_{g \in G_1} W^g$ .

Suppose that  $K \cap V$  is trivial. Then since  $V$  and  $K$  are normal subgroups of  $G$  they commute. However,  $G_1 \leq \text{GL}(V)$  and so  $V$  is self-centralising in

$V \rtimes G_1$ . Hence  $K = 1$ . Thus  $K \neq 1$  if and only if  $K \cap V$  is nontrivial and the result follows.  $\square$

We will often use the following result.

**Theorem 2.4.** ([3, Theorem 5.3]) *Let  $E$  be a half-transitive permutation group with orbits  $\mathcal{O}_i$  having the following properties:*

- (a) *The action of  $E$  on each  $\mathcal{O}_i$  is regular.*
- (b) *If  $\alpha_i \in \mathcal{O}_i$  and  $\alpha_j \in \mathcal{O}_j$  for  $i \neq j$ , then either  $E_{\alpha_i} = E_{\alpha_j}$  or  $E_{\alpha_i}E_{\alpha_j} = E$ .*

*Then  $E^{(2)}$  contains a semiregular permutation.*

Note that if  $E$  is an elementary abelian  $p$ -group and each  $E_{\alpha_i}$  has codimension 1 then the hypotheses of Theorem 2.4 hold.

Using Theorem 2.1, a doubling construction was provided in [3, Theorem 3.3], whereby given a certain elusive group of degree  $p2^n$  for some Mersenne prime  $p$  such that  $2^n > p$ , a new elusive group of degree  $2^{n+1}p$  was constructed. The following construction allows us to multiply the degree by certain primes and in the case where this prime is 2 gives us a more general doubling construction than that in [3].

**Construction 2.5 (A priming construction).** We start with an elusive permutation group  $G = V \rtimes \langle a \rangle$  of degree  $p^m \ell$  with point stabiliser  $H = W \rtimes \langle b \rangle$ , where

1.  $V$  is a finite dimensional vector space over the field  $\text{GF}(p)$ ,
2.  $a \in \text{GL}(V)$  of order  $k$ , such that  $k$  is coprime to  $p$ ,
3.  $W$  is a codimension  $m$  subspace of  $V$  whose stabiliser in  $\langle a \rangle$  is  $\langle b \rangle$ .

We then take  $q$  to be a prime which divides  $k$ .

Let

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

and let  $g$  be the linear transformation of the vector space  $V'$  given by  $(1, \dots, 1, a)\tau$  where  $\tau = (123 \dots q)$  permutes the  $q$  copies of  $V$ . Next let  $Y = \langle g \rangle$  and

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

Then  $M = \langle (b, \dots, b) \rangle$  is the stabiliser of  $W'$  in  $Y$ . Finally, let  $G^* = V' \rtimes Y$  and  $H^* = W' \rtimes M$ .

**Theorem 2.6.** *Let  $G^*$  and  $H^*$  be as obtained from Construction 2.5. Then the action of  $G^*$  on the set of right cosets of  $H^*$  is elusive of degree  $p^m \ell q$ .*

*Proof.* By Theorem 2.1, the images of  $W$  under  $\langle a \rangle$  cover  $V$ , and so the images of  $W'$  under  $Y$  cover  $V'$ . Note that Lemma 2.3 implies that  $\cap_i W^{a^i} = \{0\}$ . Thus  $\cap_{y \in Y} (W')^y = \{0\}$  and so by Lemma 2.3, the action of  $G^*$  on the set of right cosets of  $H^*$  is faithful.

Now

$$g^i = \begin{cases} (a^{(i-1)/q}, \dots, a^{(i-1)/q}, a^{(i-1)/q+1})\tau & \text{for } i \equiv 1 \pmod{q} \\ \vdots & \\ (a^{(i+1)/q-1}, a^{(i+1)/q}, \dots, a^{(i+1)/q})\tau^{q-1} & \text{for } i \equiv q-1 \pmod{q} \\ (a^{i/q}, \dots, a^{i/q}) & \text{for } i \equiv 0 \pmod{q} \end{cases}$$

Hence  $g$  has order  $qk$ . Let  $g^i$  be an element of  $Y$  of prime order  $r$ . Suppose first that  $i \not\equiv 0 \pmod{q}$ . Then  $q$  divides the order of  $g^i$  and so  $r = q$ . The only elements of order  $q$  in  $Y$  are  $g^k, g^{2k}, \dots, g^{(q-2)k}$  and  $g^{(q-1)k}$ . However,  $q$  divides  $k$ , which contradicts  $i \not\equiv 0 \pmod{q}$ . Hence if  $g^i$  has prime order then  $i \equiv 0 \pmod{q}$  and so

$$g^i = (a^{i/q}, \dots, a^{i/q}).$$

Then  $a^{i/q}$  is an element of  $\langle a \rangle$  of prime order and so by Theorem 2.1,  $a^{i/q}$  lies in  $\langle b \rangle$ . Hence  $g^i \in M$ . Thus Theorem 2.1 implies that  $G^*$  acts elusively on the set of right cosets of  $H^*$  of index  $p^m q \ell$ .  $\square$

Note that  $V'$ ,  $g$ , any prime dividing  $k$ ,  $W'$ ,  $G^*$  and  $H^*$  satisfy the initial conditions of Construction 2.5 and so we can apply the construction recursively.

For each Mersenne prime  $p$ , the elusive groups  $\text{AGL}(1, p^2) \cong C_p^2 \rtimes C_{p^2-1}$  of degree  $p(p+1)$  give us a starting point from which to use Construction 2.5. For example, when  $p = 7$  we can construct examples of degree  $7 \cdot 2^i \cdot 3^j$  for all  $i \geq 3$  and  $j \geq 0$ . In general, for any Mersenne prime  $p = 2^\ell - 1$  such that  $p - 1 = 2q_1^{\alpha_1} \dots q_r^{\alpha_r}$  we can use Construction 2.5 to build elusive groups of degree  $p2^n q_1^{j_1} \dots q_r^{j_r}$  for any  $n \geq \ell$  and  $j_1, \dots, j_r \geq 0$ . We can then use the construction of [3, Theorem 3.2] to find elusive groups of degree  $p^k 2^n q_1^{j_1} \dots q_r^{j_r}$  for all  $k \geq 1$ . Thus we have proved Theorem 1.1. For each of the examples constructed, note that  $W'$  has codimension 1 in  $V'$  and so we can use Theorem 2.4 to find fixed point free elements of order  $p$  in their 2-closures. Thus none of the examples constructed are 2-closed and their 2-closures are not elusive.

We now look at the density of the set of all degrees provided by Theorem 1.1. All logarithms are to the base 2.

**Lemma 2.7.** *The set of all degrees given in Theorem 1.1 has density zero.*

*Proof.* Let  $S(x)$  be the set of all degrees given in Theorem 1.1 which are less than  $x$ , that is, all integers of the form  $p^k 2^n q_1^{j_1} \dots q_r^{j_r}$  where  $p$  is a Mersenne prime,  $k \geq 1$ ,  $p < 2^n$ , each  $q_i$  is an odd prime dividing  $p - 1$  and  $j_i \geq 0$ . We divide  $S(x)$  into two disjoint subsets  $S_1(x)$  and  $S_2(x)$  such that  $S_1(x)$  contains all integers of the form  $p^k 2^n q_1^{j_1} \dots q_r^{j_r}$  with  $p \leq \log(x)$  while  $S_2(x)$  contains all integers of the form  $p^k 2^n q_1^{j_1} \dots q_r^{j_r}$  with  $p > \log(x)$ .

Let  $p$  be a Mersenne prime such that  $p \leq \log(x)$ . Then  $p$  contributes at most  $\log(x)^{r+2}$  integers to  $S_1(x)$ . Now the number of prime divisors of  $p - 1$  is less than  $\log(p - 1)$  which in turn is at most  $\log(\log(x))$ . An upper bound for the number of Mersenne primes less than or equal to  $\log(x)$  is  $\log(\log(x))$  and this allows us to show that

$$\lim_{x \rightarrow \infty} \frac{|S_1(x)|}{x} = 0.$$

Next let  $p$  be a Mersenne prime such that  $p > \log(x)$ . Then there are at most  $x/\log(x)$  multiples of  $p$  which are less than  $x$ . Furthermore, if  $2^l - 1$  is prime then  $l$  is prime and so there are at most  $\pi(\log(x))$  Mersenne primes less than  $x$ , where  $\pi(t)$  is the number of primes less than  $t$ . Since  $\pi(t) \sim \frac{t}{\log(t)}$ , we see that

$$\lim_{x \rightarrow \infty} \frac{|S_2(x)|}{x} = 0.$$

Hence

$$\lim_{x \rightarrow \infty} \frac{|S(x)|}{x} = \lim_{x \rightarrow \infty} \frac{|S_1(x)| + |S_2(x)|}{x} = 0.$$

□

### 3 Permutation module examples

First we note the following lemma.

**Lemma 3.1.** *Let  $S$  be a subset of the points of the affine plane  $\text{AG}(2, q)$ , with  $q$  odd, which meets every line in an odd number of points. Then  $S$  is the whole plane.*

*Proof.* Let  $V$  be the set of all functions  $f : \text{GF}(q)^2 \cup \{\infty\} \rightarrow \text{GF}(2)$ . Then  $V \cong \text{GF}(q)^{q^2+1}$  and has a codimension 1 subspace  $W$  given by the set of all functions  $f \in V$  such that the sum of  $f(v)$  over all  $v \in \text{GF}(q)^2 \cup \{\infty\}$  is equal to 0. For each  $P \subseteq \text{GF}(q)^2$ , let  $f_P \in V$  be the function given by

$$f_P(v) = \begin{cases} 1 & v \in P \cup \{\infty\} \\ 0 & \text{otherwise} \end{cases}$$

Since each line  $l$  of  $\text{AG}(2, q)$  has  $q$  points and  $q$  is odd, we have  $f_l \in W$ . Moreover, since  $W$  has dimension  $q^2$  it follows from [19, Theorem 6] that  $W$  is spanned by the set of all such  $f_l$ . Now as  $S$  meets every line of  $\text{AG}(2, q)$  in an odd number of points, it follows that

$$\sum_{v \in \text{GF}(q)^2 \cup \{\infty\}} f_S(v) f_l(v) = 0$$

for each line  $l$ . Thus  $f_S \in W^\perp$ . Since  $W^\perp$  is the set of constant functions we have that  $S$  is the whole plane.  $\square$

We now have the following construction.

**Construction 3.2.** Let  $p$  be a Mersenne prime and let  $X$  be the set of all functions  $f : \text{GF}(p^2) \rightarrow \text{GF}(2)$ . Note that  $X$  is a  $p^2$ -dimensional vector space over  $\text{GF}(2)$  and  $G_1 = \text{AFL}(1, p^2)$  acts on  $X$  via the action  $f^g(v) = f(v^{g^{-1}})$  for all  $f \in X$  and  $g \in G_1$ . The vector space  $X$  is the permutation module for the action of  $G_1$  on  $\text{GF}(p^2)$ . Now  $G_1$  acts irreducibly on the codimension one subspace  $V$  of  $X$  given by

$$V = \{f \in X \mid \sum_{v \in \text{GF}(p^2)} f(v) = 0\}.$$

See for example [19, p 7]. Let  $H_1$  be the stabiliser in  $G_1$  of  $\text{GF}(p)$  and let

$$W = \{f \in V \mid \sum_{v \in \text{GF}(p)} f(v) = 0\},$$

a codimension one subspace of  $V$ . Now let  $G = V \rtimes G_1$  and  $H = W \rtimes H_1$ , and consider the action of  $G$  on the set of right cosets of  $H$ .

**Theorem 3.3.** *Let  $G$  and  $H$  be as given by Construction 3.2. Then the action of  $G$  on the set of right cosets of  $H$  is elusive of degree  $2p(p+1)$ .*

*Proof.* Since  $G_1$  is irreducible on  $V$ , Lemma 2.3 implies that the action of  $G$  on the set of right cosets of  $H$  is faithful. Since the action of  $G_1$  on the set of lines of the affine plane  $\text{AG}(2, p)$  is elusive (by Theorem 2.1), it follows that all elements of  $G_1$  of prime order are conjugate to an element of  $H_1$ . Let  $f \in V$  and let  $S = \{v \in \text{GF}(p^2) \mid f(v) \neq 0\}$ . Since  $p$  is odd, and  $\sum_{v \in \text{GF}(p^2)} f(v) = 0$  it follows that  $S \neq \text{GF}(p^2)$ . Thinking of  $\text{GF}(p^2)$  as a  $\text{GF}(p)$  vector space, Lemma 3.1 implies that there is some line  $l$  of the affine plane  $\text{AG}(2, p)$  such that  $S$  meets  $l$  in an even number of points and so  $\sum_{v \in l} f(v) = 0$ . Hence  $f$  lies in some image of  $W$  under  $G_1$ . It remains to check condition (c) of

Theorem 2.2. If  $fh$ , for  $f \in V$  and  $h \in H_1$ , has order 2 with both  $f$  and  $h$  nontrivial then  $h$  has order 2 and  $f^h = f$ . Now  $H_1 \cong C_{p-1} \times C_2$  and has only three involutions  $h_1, h_2, h_3$  where  $h_1$  is multiplication by  $-1$ ,  $h_2$  is the  $p^{\text{th}}$  power map, and  $h_3 = h_1 h_2$ . The involution  $h_1$  fixes setwise  $\text{GF}(p^2) \setminus \text{GF}(p)$  and is fixed point free on this set. Thus if  $f \in V$  is fixed by  $h_1$  then for each orbit  $\{v_1, v_2\}$  of  $\langle h_1 \rangle$  on  $\text{GF}(p^2) \setminus \text{GF}(p)$  we have  $f(v_1) = f(v_2) = 1$  or  $f(v_1) = f(v_2) = 0$ . Thus  $\sum_{v \notin \text{GF}(p)} f(v) = 0$  and since  $f \in V$  we have  $\sum_{v \in \text{GF}(p)} f(v) = 0$  and so  $f \in W$ . Hence  $fh_1$  fixes  $W$  and (c) is satisfied for  $fh_1$ . Similarly,  $h_2$  is also fixed point free on  $\text{GF}(p^2) \setminus \text{GF}(p)$  and so any  $f \in V$  fixed by  $h_2$  also lies in  $W$  and again (c) is satisfied for  $fh_2$ . The element  $h_3$  fixes a unique 1-dimensional  $\text{GF}(p)$ -space  $l$  of  $\text{GF}(p^2)$  pointwise and is fixed point free on the remaining points. Hence if  $f \in V$  is fixed by  $h_3$  then  $\sum_{v \notin l} f(v) = 0$ . Thus  $f$  lies in the image  $\{f' \in V \mid \sum_{v \in l} f'(v) = 0\}$  of  $W$ , and this image is fixed by  $h_3$  and  $fh_3$ . Hence condition (c) of Theorem 2.2 holds for all involutions  $fh$  for  $h \in H_1$  and so the action of  $G$  on the set of right cosets of  $H$  is elusive.  $\square$

We note that the examples yielded by Construction 3.2 do not give us any new degrees. Moreover, since  $W$  is a hyperplane of  $V$ , Theorem 2.4 implies that the 2-closure of  $G$  contains a fixed point free element of order 2.

In the case where  $p = 3$  we also obtain the following example.

**Example 3.4.** Let  $X$  be the set of all functions  $f : \text{GF}(3^2) \rightarrow \text{GF}(2)$ . Note that  $X$  is a 9-dimensional vector space over  $\text{GF}(2)$  and  $G_1 = \text{AGL}(1, 9)$  acts on  $X$  via the action  $f^g(v) = f(v^{g^{-1}})$  for all  $f \in X$  and  $g \in G_1$ . Now  $G_1$  acts irreducibly on the codimension one subspace  $V$  of  $X$  given by

$$V = \{f \in X \mid \sum_{v \in \text{GF}(3^2)} f(v) = 0\}.$$

Let  $H_1$  be the stabiliser in  $G_1$  of  $\text{GF}(3)$  and so  $H_1$  stabilises the subspace

$$U = \{f \in V \mid f \text{ is constant on } \text{GF}(3)\}$$

of  $V$  of codimension two. Now let  $G = V \rtimes G_1$  and  $H = U \rtimes H_1$ , and consider the action of  $G$  on the set of right cosets of  $H$ .

**Lemma 3.5.** *Let  $G$  and  $H$  be as given by Example 3.4. Then the action of  $G$  on the set of right cosets of  $G$  on  $H$  is elusive of degree 48.*

*Proof.* Since the action of  $G_1$  on the set of lines of  $\text{AG}(2, 3)$  is elusive, every conjugacy class of elements of prime order in  $G_1$  meets  $H_1$ . Note that the images of  $U$  under  $G_1$  correspond to the lines of  $\text{AG}(2, 3)$  with each image

of the form  $\{f \in V \mid f \text{ constant on } l'\}$  for some line  $l'$ . Let  $f \in V$ . Then a quick check sees that there is some line  $l'$  such that  $f$  is constant on  $l'$  and so the set of images of  $U$  under  $G_1$  covers  $V$ . It remains to verify condition (c) of Theorem 2.2. If  $fh$ , for  $f \in V$  and  $h \in H_1$ , has order 2 with both  $f$  and  $h$  nontrivial then  $h$  has order 2 and  $f^h = f$ . Moreover, if  $f \in U$  then  $fh$  clearly fixes  $U$  and so it suffices to just look at the elements  $f \in V \setminus U$  fixed by  $h$ . There are three involutions  $h_1, h_2, h_3$  of  $H_1$ , where  $h_1$  is multiplication by  $-1$ ,  $h_2$  is the cube map and  $h_3 = h_1h_2$ . We define three functions  $f_1, f_2, f_3 \in V$  with  $f_i(v) = 0$  for all  $v \notin \text{GF}(p)$ . On  $\text{GF}(3)$  we define the functions as follows:

$$\begin{aligned} f_1(0) &= 0, f_1(1) = 1, f_1(2) = 1 \\ f_2(0) &= 1, f_2(1) = 1, f_2(2) = 0 \\ f_3(0) &= 1, f_3(1) = 0, f_3(2) = 1 \end{aligned}$$

Note that  $f_1, f_2, f_3$  provide a set of representatives for the translates of  $U$  in  $V$ . If  $h_1$  fixes  $f \in V \setminus U$  then  $f(1) = f(2)$  and so  $f \in U + f_1$ . Moreover,  $fh_1$  interchanges  $U$  and  $U + f_1$  while fixing  $U + f_2$  and  $U + f_3$ . Hence condition (c) holds for  $fh_1$ . Similarly, for  $h_3 = h_1h_2$ . However, if  $f \in V \setminus U$  is fixed by  $h_2$  then  $fh_2$  may not fix any of the translates of  $U$ . Instead, let  $\xi$  be a primitive element of  $\text{GF}(9)$  and let  $l = \{0, \xi^2, \xi^6\}$ . Then  $l$  is a 1-dimensional  $\text{GF}(3)$ -space which is fixed by  $h_2$  and  $h_2$  interchanges  $\xi^2$  and  $\xi^6$ . Then  $h_2$  fixes the image  $U' = \{f : f \in V \mid f \text{ constant on } l\}$  of  $U$  and similar arguments as above show that if  $f \in V$  is fixed by  $h_2$  then  $fh_2$  fixes a translate of  $U'$ . Thus condition (c) of Theorem 2.2 holds for all involutions  $fh$  with  $h \in H_1$  and so  $G$  is elusive.  $\square$

Let  $G$  be an elusive permutation group with elementary abelian minimal normal subgroup  $N$ . If all orbits of  $N$  have length  $p$  then the hypotheses of Theorem 2.4 automatically hold while they may not necessarily hold if they have length  $p^2$ . Note that in the unique minimal normal subgroup  $V$  of the group  $G$  given by Example 3.4, the stabiliser of a point has codimension 2 and hence all orbits of  $V$  have length 4. In this case we see that the intersection of any two images of  $U$  has codimension 2 in  $U$  and so the hypotheses of Theorem 2.4 still hold, and the 2-closure contains a fixed point free element of order 2. The only other known construction of elusive permutation groups where the orbits of an elementary abelian minimal normal subgroup do not have length  $p$  is as follows: Let  $G$  be an elusive permutation group on a set  $\Omega$  with minimal normal elementary abelian  $p$ -subgroup  $N$  such that the orbits of  $N$  have length  $p$ . Then [3, Theorem 4.1] implies that  $G \text{ wr } S_k$  acts elusively on  $\Omega^k$ . Moreover,  $N^k$  is an elementary abelian minimal normal subgroup of  $G \text{ wr } S_k$  and has orbits of length  $p^k$ . The fact that  $G \text{ wr } S_k$  is not 2-closed

and its 2-closure contains fixed point free elements of order  $p$  follows from the fact that the 2-closure of  $G$  contains fixed point free elements of order  $p$  and [3, Theorem 5.2].

If we attempt to generalise Example 3.4 to higher primes the obvious choice for  $U$  would be

$$U = \{f \in V \mid f \text{ is constant on } \text{GF}(p)\}.$$

However, this has codimension  $p - 1$  in  $V$  while  $|G_1 : H_1| = p(p + 1)$ . Hence for Mersenne primes  $p > 3$ , the images of  $U$  under  $G_1$  do not cover  $V$ .

## 4 Generalised doubling construction

In [3] a degree doubling construction was given for certain elusive groups which is encompassed by our priming construction (Construction 2.5). The following construction places the doubling construction in a wider context.

**Construction 4.1.** Let  $p = 2^l - 1$  be a Mersenne prime and let  $V = \text{GF}(p)^4$  with basis vectors  $e_1, e_2, e_3, e_4$ . For  $a, b \in \text{GF}(p)$ , not both 0, let

$$\chi_{1,a,b} = \begin{pmatrix} a & b & 0 & 0 \\ -b & a & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \chi_{2,a,b} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & -b & a \end{pmatrix}$$

Also let

$$\tau_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \sigma = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Then  $X = \langle \chi_{1,a,b}, \chi_{2,a,b}, \sigma, \tau_1, \tau_2 \mid a, b \in \text{GF}(p) \rangle \cong \text{GL}(1, p^2) \text{ wr } C_2$  and preserves the decomposition  $V = \langle e_1, e_2 \rangle \oplus \langle e_3, e_4 \rangle$ . Let  $W = \langle e_1, e_2, e_3 \rangle$ . Then  $X_W = \langle \tau_1, \tau_2, \chi_{1,a,b}, \chi_{2,c,0} \mid c \in \text{GF}(p)^*, a, b \in \text{GF}(p) \rangle$  and so  $|X : X_W| = 2^{l+1}$ . Moreover, since  $\langle \chi_{2,a,b} \mid a, b \in \text{GF}(p) \rangle$  acts transitively on the set of nonzero vectors of  $\langle e_3, e_4 \rangle$  it follows that the set  $\mathcal{W}$  of images of  $W$  under  $X$  covers  $V$ . Let  $S \leq X$  such that  $S$  acts transitively on  $\mathcal{W}$  and every element of order 2 in  $S$  fixes some element of  $\mathcal{W}$ . Then by Theorem 2.1, the action of  $G = V \rtimes S$  on the set of right cosets of  $W \rtimes S_W$  is elusive of degree  $p \cdot 2^{l+1}$ .

Note that we cannot choose  $S = X$  as the element  $\sigma$  does not fix an element of  $\mathcal{W}$ . One possible choice for  $S$  is  $\langle \chi_{1,a,b}, \chi_{2,a,b}, \tau_2 \sigma \mid a, b \in \text{GF}(p) \rangle$ ,

which has index 2 in  $X$ . The doubling construction given in [3, Theorem 3.3] is the case where  $S = \langle \chi_{2,x_1,x_2} \sigma \rangle$  with  $x_1, x_2$  chosen so that  $\chi_{2,x_1,x_2}$  has order  $p^2 - 1$ .

We note here that Construction 4.1 can be generalised in the following manner which allows repeated doubling. It also encompasses all the doubling constructions in [8].

**Construction 4.2.** Let  $V$  be a vector space over a field of characteristic  $p$ ,  $G_1 \leq \text{GL}(V)$  of order coprime to  $p$ , and  $W$  a subspace of  $V$  with stabiliser  $H_1$  in  $G_1$  such that  $V \rtimes G_1$  acts elusively on the set of right cosets of  $W \rtimes H_1$ . Let  $X = G_1 \text{ wr } C_2$  preserve the decomposition  $\bar{V} = V \oplus V$  and let  $\bar{W} = V \oplus W$ . Then since the set of images of  $W$  under  $G_1$  covers  $V$ , it follows that the set  $\mathcal{W}$  of images of  $\bar{W}$  covers  $\bar{V}$  and has size  $2|G_1 : H_1|$ . Moreover, each element of  $X$  of prime order  $r \neq 2$  is conjugate to an element of  $X_W = G_1 \times H_1$ . Thus by Theorem 2.1, if there exists  $S \leq X$  which is transitive on  $\mathcal{W}$  and such that every element of order two in  $S$  is conjugate in  $S$  to an element of  $S_W$  then  $\bar{V} \rtimes S$  acts elusively on the set of right cosets of  $\bar{V} \rtimes S_W$ .

## 5 The elusive groups of degree up to 30

All transitive permutation groups of degree up to 30 have been determined by Hulpke [12] and are available in GAP [7]. Using the results of Marušič [15, Theorems 3.3 and 3.4] that there are no elusive groups of degree  $p^k$  or  $mp$ , where  $p$  is a prime and  $m \leq p$ , the only possible degrees less than or equal to 30 for elusive groups are 12, 18, 24 and 30. All elusive groups of degree 12 were given in [3, Figure 1] and they are the transitive subgroups of  $M_{11}$  in its action on 12 points. Searching through the GAP database we see that there are no elusive groups of degree 18 or 30 and that there are 19 elusive groups of degree 24. The elusive groups of degree 24 fall into three families:

1. Fifteen groups of the form  $G = C_3^4 \rtimes S$  where  $S$  is a 2-group of order  $2^4, 2^5, 2^6, 2^7$  or  $2^8$  acting faithfully on  $C_3^4$ , and  $G_\alpha = C_3^3 \rtimes S_\alpha$ . Since a Sylow 2-subgroup of  $\text{GL}(4, 3)$  is isomorphic to  $\Gamma\text{L}(1, 9) \text{ wr } C_2$ , all these examples arise from Construction 4.1.
2. Three groups of the form  $G = C_2^8 \rtimes K$  where  $K = \text{A}\Gamma\text{L}(1, 9), \text{A}\Gamma\text{L}(1, 9)$  or  $C_3^2 \rtimes Q_8$ , and  $G_\alpha = C_2^7 \rtimes K_\alpha$  where  $K_\alpha$  is the stabiliser in  $K$  of a point in its elusive action of degree 12. When  $K = \text{A}\Gamma\text{L}(1, 9)$ , this is the example we get from Construction 3.2 with  $p = 3$  and the remaining two are transitive subgroups.

3. An index two subgroup of  $M_{10} \text{ wr } S_2 = (A_6 \cdot C_2) \text{ wr } C_2$  in its imprimitive action of degree 24.

Theorem 2.4 shows that the groups in the first two families are not 2-closed while [3, Theorems 5.1 and 5.5] can be used to show that the 2-closure of the last example contains  $A_6^4$  and hence is not elusive.

## References

- [1] B. Alspach, *Lifting Hamilton cycles of quotient graphs*, Discrete Math. **78** (1989), 25–36.
- [2] N. Biggs, *Three remarkable graphs*, Can. J. Math. **25** (1973), 397–411.
- [3] P. J. Cameron, M. Giudici, G. A. Jones, W. M. Kantor, M. H. Klin, D. Marušič, and L. A. Nowitz, *Transitive permutation groups without semiregular subgroups*, J. London Math. Soc. **66** (2002), 325–333.
- [4] P. J. Cameron(ed.), *Problems from the Fifteenth British Combinatorial Conference*, Discrete Math. **167/168** (1997), 605–61.
- [5] E. Dobson, A. Malnič, D. Marušič and L. A. Nowitz, *Semiregular automorphisms of vertex-transitive graphs of certain valencies*, to appear in J. Combin. Theory Ser. B.
- [6] B. Fein, W. M. Kantor and M. Schacher, *Relative Brauer groups. II*, J. Reine Angew. Math. **328** (1981), 39–57.
- [7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002, (<http://www.gap-system.org>).
- [8] M. Giudici, *Fixed point free elements of prime order in permutation groups*, PhD Thesis, Queen Mary, University of London (2002).
- [9] M. Giudici, *Quasiprimitive permutation groups with no fixed point free elements of prime order*, J. London Math. Soc. **67** (2003), 73–84.
- [10] M. Giudici and J. Xu, *All vertex-transitive locally quasiprimitive graphs have a semiregular automorphism*, to appear in J. Algebraic Combin.
- [11] J. D. Horton and I. Z. Bouwer, *Symmetric Y-graphs and H-graphs*, J. Combin. Theory Ser. B **53** (1991), 114–129.

- [12] A. Hulpke, *Constructing transitive permutation groups*, J. Symb. Comp. **39** (2005), 1–30.
- [13] D. Jordan, *Eine symmetrieeigenschaft von graphen, graphentheorie und ihre anwendungen (Stadt Wehlen, 1988), 17–20*, Dresdner Reihe Forsch. **9** (1988).
- [14] B. D. McKay and G. F. Royle, *The transitive graphs with at most 26 vertices*. Ars Combin. **30** (1990), 161–176.
- [15] D. Marušič, *On vertex symmetric digraphs*, Discrete Math. **36** (1981), 69–81.
- [16] D. Marušič and T. D. Parsons, *Hamiltonian paths in vertex-symmetric graphs of order  $5p$* , Discrete Math. **42** (1982), 227–242.
- [17] D. Marušič and T. D. Parsons, *Hamiltonian paths in vertex-symmetric graphs of order  $4p$* , Discrete Math. **43** (1983), 91–96.
- [18] D. Marušič and R. Scapellato, *Permutation groups, vertex-transitive digraphs and semiregular automorphisms*, Eur. J. Comb. **19** (1998), 707–712.
- [19] B. Mortimer, *The modular permutation representations of the known doubly transitive groups*, Proc. London Math. Soc. (3) **41** (1980), 1–20.