

## On the reconstruction index of permutation groups: semiregular groups\*

PHILIP MAYNARD AND JOHANNES SIEMONS

**Summary.** The reconstruction index of all semiregular permutation groups is determined. We show that this index satisfies  $3 \leq \rho(G, \Omega) \leq 5$  and we classify the groups in each case.

**Mathematics Subject Classification (2000).** Permutation groups 20B05; Reconstruction 05C60, 05C65.

**Keywords.** Regular and semiregular permutation actions, reconstruction.

### 1. Introduction

The subject of this paper is an invariant which one may define for an arbitrary group action. So let  $G$  be a group and let  $(G, \Omega)$  be an action. Then  $G$  acts naturally on  $\{\Delta : \Delta \subseteq \Omega\}$  by setting  $G \ni g : \Delta \mapsto \Delta^g := \{\delta^g : \delta \in \Delta\}$ . Two sets  $\Delta, \Gamma \subseteq \Omega$  are called *isomorphic*, denoted  $\Delta \approx \Gamma$ , if they are in the same  $G$ -orbit and they are called *hypomorphic*, denoted  $\Delta \sim \Gamma$ , if there exists a bijection  $h : \Delta \rightarrow \Gamma$  so that for all  $\delta \in \Delta$  we have  $\Delta \setminus \{\delta\} \approx \Gamma \setminus \{h(\delta)\}$ . Then  $\Delta$  is *reconstructible*, if all sets hypomorphic to  $\Delta$  are isomorphic to  $\Delta$ . The *reconstruction index*  $\rho(G, \Omega)$  now is the least integer  $r$  so that every finite  $\Omega$ -subset of  $r$  or more elements is reconstructible. If no such  $r$  exists, put  $\rho(G, \Omega) = \infty$ . The ideas which motivate this definition are discussed in Section 2.

It is clear that we may assume that the permutation action is faithful and so we can restrict ourselves to permutation groups. In this paper we determine the reconstruction index for all semiregular permutation groups. To state the result for finite groups let  $\mathcal{L}_0$  denote the collection of all subgroups of the following:

- (i) extensions of an elementary abelian 2-group  $V$  by a cyclic group of order 3 or 5 acting fix-point-freely on  $V$ ,
- (ii) the holomorph of a cyclic group of order 3, 4 or 5,
- (iii) the symmetric group  $\text{Sym}_4$ , or the alternating group  $\text{Alt}_5$ .

---

\*We acknowledge support from the Leverhulme Foundation for a Project on Reconstruction Indices.

Let also  $\mathcal{Q}$  denote the quaternion group of order 8.

**Theorem 1.1.** *Let  $(G, \Omega)$  with  $1 < |G|$  be a finite semiregular permutation group with  $6 \leq |\Omega| \leq \infty$ . Then  $3 \leq \rho(G, \Omega) \leq 5$  and the following holds:*

- (i) *If  $G$  contains a subgroup isomorphic to  $\mathcal{Q}$ , then  $\rho(G, \Omega) = 5$ .*
- (ii) *If  $G$  belongs to  $\mathcal{L}_0$ , then  $\rho(G, \Omega) = 3$ .*
- (iii) *In all other cases  $\rho(G, \Omega) = 4$ .*

For infinite groups a similar result holds. We denote by  $\mathcal{L}$  the family of all infinite groups  $G$  for which

- (i) every element in  $G$  has finite order,
- (ii) every finite subgroup of  $G$  belongs to  $\mathcal{L}_0$ , and
- (iii) if  $g, h \in G$  satisfy  $g^2 = h^2 \neq Id$ , then  $g = h^{-1}$  and  $g, h$  have order 4.

**Theorem 1.2.** *Let  $(G, \Omega)$  be an infinite semiregular permutation group. Then  $3 \leq \rho(G, \Omega) \leq 5$  and the following holds:*

- (i) *If  $G$  contains a subgroup isomorphic to  $\mathcal{Q}$ , then  $\rho(G, \Omega) = 5$ .*
- (ii) *If  $G$  belongs to  $\mathcal{L}$ , then  $\rho(G, \Omega) = 3$ .*
- (iii) *In all other cases  $\rho(G, \Omega) = 4$ .*

The proofs of Theorems 1.1 and 1.2 are completed in Section 6. In Section 3 we discuss the main bounds for the reconstruction index of a semiregular group. The same basic theorem applies also to subgroups of Frobenius groups or Zassenhaus groups. Here the reconstruction index can be bounded above by 10 and 16, respectively, but we have no further classification in these cases. Several recent papers [14, 19, 20, 10] deal with reconstruction problems closely related to semiregular groups. Many of these results follow directly from Theorems 1.1 and 1.2. Some reconstruction problems more generally deal with *decks*. In many situations the main results here can be adapted to deck reconstruction, see the comments in the following section.

## 2. Some remarks on the reconstruction index

The reconstruction index belongs to the less well-known invariants of permutations groups, with general references restricted to Cameron's 'Open problems in permutation groups' in [4] and Babai's article in the Handbook of Combinatorics [2]. A few words about the reconstruction index may therefore be useful. The term itself refers to the famous 1942 reconstruction problem of Ulam and Kelly about reconstructing a graph from the isomorphism classes of its vertex deleted subgraphs. Since then many reconstruction problems have been proposed, and as we shall see, many can be treated in terms of reconstruction indices. The idea of interpreting such problems more generally as a property of permutation groups, as far as we are aware, has been formalized first in Mnukhin's 1987 paper [12].

The process of translating a particular combinatorial reconstruction problem into the permutation group problem is not entirely obvious and will be best illustrated by some examples.

We start with the original Ulam and Kelly problem. Let  $\Omega$  be the countably infinite vertex set of the random graph  $\mathcal{R}$ . Then every subset  $\Delta \subset \Omega$  inherits from  $\mathcal{R}$  the structure of a graph, and it is a fact that every finite graph occurs in this fashion. The fundamental property of  $G_{\mathcal{R}} := \text{Aut}(\mathcal{R})$  is that any two  $k$ -element subsets of  $\Omega$  belong to the same  $G_{\mathcal{R}}$ -orbit, if and only if the two sets are isomorphic as graphs on  $k$  vertices. In particular, two hypomorphic subsets of  $\Omega$  are exactly the same thing as two abstract graphs which satisfy the assumption of Ulam's conjecture. The graph  $\Delta$  therefore is reconstructible from its vertex deleted subgraphs if and only if  $\Delta \subset \Omega$  is reconstructible, as defined here, with regards to  $G_{\mathcal{R}}$ . Ulam's conjecture is the statement that  $\rho(G_{\mathcal{R}}, \Omega) = 3$ . Note in contrast that  $G_{\mathcal{R}}$  has  $\rho(G_{\mathcal{R}}, G_{\mathcal{R}}) = 5$  in the regular action: a short argument due to David Evans shows that the symmetric group on a countably infinite set can be embedded into  $G_{\mathcal{R}}$ . In particular,  $\mathcal{Q} \subseteq G_{\mathcal{R}}$  and so  $\rho = 5$  by Theorem 1.2 (i).

The reconstructibility of a graph from the isomorphism classes of its edge deleted subgraphs translates as follows. Let  $V$  be a set of vertices and let  $V^{\{2\}}$  be the collection of all unordered pairs from  $V$ . Let  $G$  be  $\text{Sym}(V)$  acting naturally on  $V^{\{2\}}$ . Then every graph with vertex set  $V$  can be identified as a suitable  $E \subseteq V^{\{2\}}$  representing its edges. Furthermore, two graphs  $(V, E)$  and  $(V, E^*)$  are isomorphic, if and only if  $E$  and  $E^*$  are in the same  $G$ -orbit. Therefore two graphs satisfying the hypothesis for edge reconstruction correspond to hypomorphic subsets, and so the edge reconstruction conjecture is that  $\rho(\text{Sym}(V), V^{\{2\}}) = 4$  for all  $|V| \geq 4$ . As a general reference for results on graph reconstruction see Bondy's article [3]. We mention also that often there is more than one way to translate the reconstruction problem into a permutation group problem.

Other reconstruction problems occur naturally in design theory and coding theory, for the latter see also [9]. Several papers ([19, 20, 14, 10, 6]) consider the reconstruction of configurations, sequences or of sets of group elements and often one can identify these as group reconstruction problems.

We now consider a characterisation of the reconstruction index in terms of orbits on the power set of  $\Omega$ . Let  $(G, \Omega)$  be a permutation group with  $\Omega$  finite. Then  $G$  acts naturally on the collection  $\Omega^{\{k\}}$  of all  $k$ -element subsets of  $\Omega$ . List the  $G$ -orbits as  $\{O_{i,k} : 1 \leq i \leq n_k\}$  on  $\Omega^{\{k\}}$  where  $n_k$  denotes the number of such orbits. For  $\Delta \in \Omega^{\{k\}}$  with  $1 < k < |\Omega|$  define the vectors  $c^+(\Delta) = (c_1^+, \dots, c_i^+, \dots, c_{n_{k+1}}^+)$  and  $c^-(\Delta) = (c_1^-, \dots, c_j^-, \dots, c_{n_{k-1}}^-)$  by

$$c_i^+ := |\{\Gamma \in O_{i, k+1} : \Delta \subseteq \Gamma\}| \quad \text{and} \quad c_j^- := |\{\Gamma \in O_{j, k-1} : \Delta \supseteq \Gamma\}|.$$

A *deck*, more generally, is a function such as  $c^-(\Delta)$  which records the containment in  $\Delta$  of subsets from  $O_{j, k^*}$  for various  $k^* < |\Delta|$ . While decks will play no further role here some of the following results, and in particular Proposition 2.1, are easily adapted to decks.

Clearly  $c^+$  and  $c^-$  are invariant on each  $O_{i,k}$  and for certain  $k$ 's are even *full* invariants:

**Proposition 2.1.** (*Theorem 4.2 in [21]*) *Let  $\Delta, \Delta^* \in \Omega^{\{k\}}$  where  $2k + 1 \leq |\Omega|$ . Then  $\Delta$  and  $\Delta^*$  are isomorphic, if and only if  $c^+(\Delta) = c^+(\Delta^*)$ .*

*Proof.* The idea is that the  $c^+(\Delta)$ , with  $\Delta \in O_{i,k}$  and  $1 \leq i \leq n_k$ , form the rows of a matrix of size  $n_k \times n_{k+1}$  which can be shown to have rank  $n_k$ . In particular, all rows are different.  $\square$

By definition  $\Delta \subseteq \Omega$  is hypomorphic to  $\Delta^* \subseteq \Omega$ , if and only if  $c^-(\Delta) = c^-(\Delta^*)$ . On the other hand, by giving a  $k$ -set and its complement the same orbit index, it is also clear that the  $O_{i,k}$  can be indexed such that  $c^+(\Delta) = c^-(\Omega \setminus \Delta)$ . Hence

**Proposition 2.2.** *Let  $\Delta, \Delta^* \in \Omega^{\{k\}}$  with  $|\Omega| < 2k$  be hypomorphic. Then  $\Delta$  and  $\Delta^*$  are isomorphic. In particular,  $\rho(G, \Omega) \leq \frac{|\Omega|}{2} + 1$ .*

This bound is best possible in general. The quaternion group of order 8 is remarkable in several respects. First of all, it meets this bound with  $\rho(\mathcal{Q}, \mathcal{Q}) = 5$  in its regular representation, the details are given after the proof of Theorem 4.2. It is also a counter example to Theorem 7.6 in [2] and to Theorem 6.1 in [4] which give bounds for  $\rho(G, \Omega)$  which are similar to the one above. Livshiz [7] has examples of intransitive 2-groups of arbitrarily large degree with  $\rho = \frac{n}{2} + 1$ .

Now suppose that the orbits  $\{O_{i,r} : 1 \leq i \leq n_r\}$  are given for some fixed  $r$  with  $2r \leq |\Omega| + 1$ . Using Proposition 2.1 one can use the  $c^+$ -vectors to work out successively  $\{O_{i,r-1}\}$ ,  $\{O_{i,r-2}\}$ ,  $\dots$  and so on. If  $r \geq \rho(G, \Omega) - 1$ , then  $\{O_{i,r+1}\}$ ,  $\{O_{i,r+2}\}$ ,  $\dots$  etc. can be determined from the  $c^-$ -vectors. Hence the orbits on all subsets can be reconstructed from  $\{O_{i,r} : 1 \leq i \leq n_r\}$  by this simple counting procedure, as long as  $\rho(G, \Omega) - 1 \leq r \leq |\Omega|/2$ . Thus  $\rho(G, \Omega) - 1$  is the least value for which this is possible and this may serve as an additional characterisation of the reconstruction index.

This paper is based almost exclusively on an extension of Nash-Williams' Lemma [18] due Alon *et al.* [1], see also the paper of Müller [17].

**Proposition 2.3.** *Let  $(G, \Omega)$  be a permutation group. Suppose that  $\Delta \subseteq \Omega$  is not reconstructible and that for some  $S \subseteq \Delta$  the setwise stabilizer  $G_S$  is finite. Then for every set  $K$  with  $S \subseteq K \subseteq \Delta$  and  $|K| \equiv |\Delta| \pmod{2}$  there is some  $g \in G$  with  $\Delta \cap \Delta^g = K$ .*

Little appears to be known about the reconstruction index in general. Indeed, it is rather difficult to link this invariant to other permutational properties. Apart from the case of abelian groups dealt with in [13] the classification here, as far as we are aware, is the only general class of permutation groups for which the reconstruction index is known.

### 3. The main bounds

From now on we assume that  $(G, \Omega)$  is an arbitrary permutation group and, unless stated otherwise, we do not assume that  $G$  is finite. From Proposition 2.3 we first obtain a general bound for semiregular permutation groups.

In [13] it was conjectured that the reconstruction index for a regular group is at most 5. This is true even more generally for semiregular groups:

**Theorem 3.1.** *Let  $(G, \Omega)$  be semiregular with  $1 < |G|$  and  $4 \leq |\Omega|$ . Then  $3 \leq \rho(G, \Omega) \leq 5$ .*

*Proof.* Suppose that  $\Delta \subseteq \Omega$  with  $m := |\Delta| \geq 5$  is not reconstructible. In Proposition 2.3 take  $S := \{\delta\}$  for some  $\delta \in \Delta$ . Then  $G_S$  is finite and for any  $K$  with  $S \subseteq K \subseteq \Delta$  and  $|K| \equiv |\Delta| \pmod{2}$  there is a  $g \in G$  with  $\Delta \cap \Delta^g = K$ , by Proposition 2.3. For any such  $K$  we have  $\delta \in K$  and so  $|g \in G : \delta \in \Delta^g| \geq 2^{m-2}$ . The number on the right is the number of sets  $K$  with  $S \subseteq K \subseteq \Delta$  and  $|K| \equiv |\Delta| \pmod{2}$ . The number on the left is at most  $|\Delta| = m$ , a contradiction. Hence  $\rho(G, \Omega) \leq 5$ .

Assume first that  $G$  is regular and so is not 2-homogeneous. Since  $G$  is 1-homogeneous all 2-element subsets are hypomorphic and so the lower bound follows in this case. Next assume that  $G$  is intransitive with orbits  $\Omega_1, \Omega_2, \dots$  and let  $\alpha \neq \beta \in \Omega_1$  and  $\gamma \in \Omega_2$ . Then  $\{\alpha, \gamma\}$  and  $\{\beta, \gamma\}$  are hypomorphic, but not isomorphic. This completes the proof.  $\square$

In the next two sections we shall examine these bound more closely and classify groups accordingly. First however we note that the same principle can be applied to two other important classes of permutation groups.

**Theorem 3.2.** *Let  $G$  be a permutation group on  $\Omega$ . If the pointwise stabilizer  $G$  of every two points is 1, then  $\rho(G, \Omega) \leq 10$ . If the pointwise stabilizer in  $G$  of every three points is 1, then  $\rho(G, \Omega) \leq 16$ .*

*Proof.* If the stabilizer in  $G$  of every two points is 1, suppose that  $\Delta$  with  $|\Delta| = m \geq 10$  is not reconstructible. In Proposition 2.3 take  $S := \{\alpha, \beta\} \subseteq \Delta$ . Then  $G_S$  is finite and for any  $K$  satisfying  $S \subseteq K \subseteq \Delta$  and  $|K| \equiv |\Delta| \pmod{2}$  there is a  $g \in G$  with  $\Delta \cap \Delta^g = K$ . Since  $S \subseteq K$  for any such  $K$  it follows that  $|g \in G : S \subseteq \Delta^g| \geq 2^{m-3}$ . Further, since  $m \geq 10$  it follows that  $2^{m-3} > 2^{\binom{\Delta}{2}}$ . But this implies that the pointwise stabilizer of  $\{\alpha, \beta\}$  is not trivial, a contradiction. A similar argument can be used for the case when the stabilizer in  $G$  of every three points is 1.  $\square$

This theorem applies for instance to all Frobenius and Zassenhaus groups and it would be interesting to evaluate the index for such groups. Moreover, it would

be interesting to decide when the bounds are sharp, if at all. In the manuscript [14] the indices are computed for many small linear groups in their natural representation. Such computations are quite involved and, with the kind permission of the author, we will record some of his findings to make these more widely available. For instance, it is shown that  $AGL(1, 16)$  has reconstruction index 7 in the natural representation, while  $AGL(1, 16)$ ,  $AGL(1, 11)$ ,  $AGL(1, 23)$  and subgroups of index 2 in  $AGL(1, 16)$  all have index 6. The projective linear groups  $PSL(2, 11)$ ,  $PGL(2, 11)$ ,  $PGL(2, 16)$ ,  $PGL(2, 17)$ ,  $PSL(2, 19)$  have index 7 in their natural representations,  $PSL(2, 17)$  has index 6 while  $PGL(2, 13)$  and  $PSL(2, 13)$  have index 5. These examples show that any classification for the affine and projective linear groups will not be quite as straightforward as the main theorems here.

#### 4. The case $\rho = 5$

Let  $G$  be a permutation group on  $\Omega$ . Following Wielandt, a subset  $B$  of  $\Omega$  is a *block* of  $G$  if for each  $g \in G$  either  $B^g = B$  or  $B^g \cap B = \emptyset$ .

**Lemma 4.1.** *Let  $G$  be semiregular on  $\Omega$  and let  $\Delta, \Delta' \subseteq \Omega$  be hypomorphic and non-isomorphic sets of cardinality 4. Then there exists a block  $B$  with  $\Delta \subset B \subseteq \Omega$  of size 7 or 8 such that the setwise stabilizer  $G_B$  is regular on  $B$ . Furthermore, there exists some  $g \in G$  such that  $\Delta, \Delta'^g \subseteq B$  are hypomorphic under the action of  $G_B$ .*

*Proof.* Let  $\Delta = \{\alpha, \beta, \gamma, \delta\}$ . It follows from Proposition 2.3 that:

$$\forall S \subseteq \Delta \text{ with } |S| = 2 \text{ there exists } g \in G \text{ such that } \Delta \cap \Delta^g = S. \quad (*)$$

For  $\alpha \in \Omega$  set  $S_\alpha := \{\Delta^* \in \Delta^G : \alpha \in \Delta^*\}$ . As  $G$  is semiregular it follows that  $|S_\alpha| \leq 4$ . Also, if  $|S_\alpha| \neq 0$ , then  $|S_\alpha| \geq 4$  by (\*). Therefore  $|S_\alpha| = 0$  or 4 for any  $\alpha \in \Omega$ . It is not difficult to see that

$$S_\alpha = \{\{\alpha, \beta, \gamma, \delta\}, \{\alpha, \beta, x, y\}, \{\alpha, \gamma, x, z\}, \{\alpha, \delta, y, z\}\}$$

for some distinct  $x, y, z \in \Omega \setminus \Delta$ . Let  $M := \{\Delta^g : g \in G \text{ and } \Delta^g \cap \{\alpha, \beta, \gamma, \delta, x, y, z\} \neq \emptyset\}$ . By (\*)  $M$  contains sets  $X_1, X_2, X_3$  with  $\{\beta, \gamma\} = \Delta \cap X_1$ ,  $\{\beta, \delta\} = \Delta \cap X_2$  and  $\{\gamma, \delta\} = \Delta \cap X_3$ . Hence  $|M| \geq 7$ . Now if  $X_1, X_2, X_3 \subseteq \{\alpha, \beta, \gamma, \delta, x, y, z\}$ , then  $|M| = 7$  since each  $a \in \{\alpha, \beta, \gamma, \delta, x, y, z\}$  must then occur in exactly 4 sets from  $M$ . Assume now without loss of generality that  $X_1 = \{\beta, \gamma, w, v\} \not\subseteq \{\alpha, \beta, \gamma, \delta, x, y, z\}$ . If  $v \notin \{\alpha, \beta, \gamma, \delta, x, y, z\}$ , then by (\*) there exist  $f \neq h \in G$  such that  $\{\beta, w\} = X_1 \cap \Delta^f$  and  $\{\beta, v\} = X_1 \cap \Delta^h$ . This gives  $|S_\beta| \geq 5$ , a contradiction. Hence  $v \in \{\alpha, \delta, x, y, z\}$  and a similar argument shows that every set from  $S_w$  is contained in  $\{\alpha, \beta, \gamma, \delta, x, y, z, w\}$ . Therefore  $S_\alpha \cup S_w \subseteq M$ . But since each  $a \in \{\alpha, \beta, \gamma, \delta, x, y, z, w\}$  must then occur in exactly 4 sets from  $M$  we have  $M = S_\alpha \cup S_w$  and so  $|M| = 8$ .

Now  $|M| = n \in \{7, 8\}$  and we set

$$B := \{\alpha, \beta, \gamma, \delta, x, y, z\} \text{ or } B := \{\alpha, \beta, \gamma, \delta, x, y, z, w\}$$

correspondingly. Write  $M = \{\Delta_1 = \Delta, \Delta_2, \dots, \Delta_n\}$ . Let  $g_i \in G$  be the permutation with  $\Delta^{g_i} = \Delta_i$  for  $i \in \{1, \dots, n\}$  and put  $G^* = \{I_d = g_1, \dots, g_n\}$ . We note two simple facts: firstly, since  $G$  is semiregular and  $|G^*| = |B|$  it follows that for  $a \in \{\alpha, \beta, \gamma, \delta\}$  and  $g \in G$  we have  $a^g \in B$  if and only if  $g \in G^*$ . Secondly, for all  $s \in B \setminus \{\alpha, \beta, \gamma, \delta\}$  there exist  $a, b \in \{\alpha, \beta, \gamma, \delta\}$  and  $g \in G^*$  such that  $a^g = s$  and  $b^g \in \{\alpha, \beta, \gamma, \delta\}$ . (Looking at the  $S_\alpha$  and  $X_1, X_2, X_3$  it follows that at most one of the sets in  $M$  does not contain at least two elements from  $\{\alpha, \beta, \gamma, \delta\}$ ).

We now show that  $B^g = B$  for all  $g \in G^*$ . Thus, assume that  $s^g \notin B$  for some  $g \in G^*$  and  $s \in B \setminus \{\alpha, \beta, \gamma, \delta\}$ . Then, as we have just shown, there exist  $h \in G^*$  and  $a, b \in \{\alpha, \beta, \gamma, \delta\}$  such that  $a^h = s$  and  $b^h \in \{\alpha, \beta, \gamma, \delta\}$ . Then  $b^{hg} \in B$  implies that  $hg \in G^*$ . However,  $a^{hg} = s^g \notin B$ , a contradiction. In particular,  $B^{g_i} = B$  for all  $g_i \in G^*$  and so  $G^*$  is a group of order  $|B|$  acting regularly on the points of  $B$ .

Thus  $B^g = B$  for  $g \in G^*$  where  $|G^*| = |B|$ . So for all  $h \in G \setminus G^*$  we must have  $B \cap B^h = \emptyset$ . So indeed  $B$  is a block. Further,  $G_{\{B\}}$  is a regular on  $B$ , (since  $|G^*| = |B|$ ).

The fact that there exists  $g \in G$  with  $\Delta^{g^2} \subseteq B$  is easy: clearly, there exists  $h \in G$  with  $\Delta^{h^2} = \{\alpha, \beta, \gamma, t\}$  for some  $t \in \Omega \setminus \Delta$ . If  $t \notin B$ , then  $\{\alpha, \beta, t\}$  is not contained in  $B$  but all maximal subsets of  $\Delta$  are contained in a block, a contradiction.  $\square$

**Theorem 4.2.** *Let  $(G, \Omega)$  be semiregular with  $1 < |G| \leq \infty$  and  $4 \leq |\Omega| \leq \infty$ . Then  $\rho(G, \Omega) = 5$ , if and only if  $G$  contains a subgroup isomorphic to  $\mathcal{Q}$ .*

*Proof.* By Theorem 3.1 it follows that  $\rho(G, \Omega) = 5$ , if and only if  $G$  has non-reconstructible sets of cardinality 4.

Let  $G$  be semiregular on  $\Omega$  with hypomorphic sets  $\Delta \not\cong \Delta'$  of cardinality 4. Then determine  $B$  and  $g$  as in Lemma 4.1 and so  $\Delta, \Delta^{g^2} \subseteq B$  are hypermorphic, but not isomorphic under the regular action of  $G_B$  on  $B$ . Since  $|B| = 7$  or  $8$  we need just inspect the regular groups of degree 7 and 8. The only one with such orbits is  $\mathcal{Q}$ . Hence, if  $\rho(G, \Omega) = 5$ , then  $G$  must contain  $\mathcal{Q}$  as a subgroup.

Conversely, let  $G$  contain a copy of  $\mathcal{Q}$ . Then, see page 29 of [5], there exist distinct  $g, h, k \in G$  with  $g^2 = h^2 = k^2 = ghk \neq Id$ . Then  $g, h$  and  $k$  have some cycles which contain at least three points, say  $g = \begin{pmatrix} \alpha & 1 & \dots \\ 1 & \beta & \dots \end{pmatrix}$  from which it follows that  $h = \begin{pmatrix} \alpha & 2 & \dots \\ 2 & \beta & \dots \end{pmatrix}$  and  $k = \begin{pmatrix} \alpha & 3 & \dots \\ 3 & \beta & \dots \end{pmatrix}$  for some  $1, 2, 3, \alpha, \beta \in \Omega$ . The conditions imply that  $g^2 = ghk = kgh = hkg$  and hence  $g = \begin{pmatrix} \alpha & 1 & 3 & \dots \\ 1 & \beta & 2 & \dots \end{pmatrix}$ ,  $h = \begin{pmatrix} \alpha & 2 & 1 & \dots \\ 2 & \beta & 3 & \dots \end{pmatrix}$  and  $k = \begin{pmatrix} \alpha & 3 & 2 & \dots \\ 3 & \beta & 1 & \dots \end{pmatrix}$ . It is a simple matter to check that  $\Delta := \{1, 2, 3, \alpha\}$  and  $\Delta' := \{1, 2, 3, \beta\}$  are hypomorphic, but not isomorphic under the action of  $G$ .  $\square$

The quaternion group of order 8 is quite special and it may be worth to write out the details for  $\mathcal{Q}$  in its regular action on itself. Let its generators be  $g, h, k :=$

$gh$  with  $g^4 = 1 = h^4 = k^4$  and  $g^{-1}hg = h^3$ . Then it is easy to check that  $\Delta := \{g, h, k, ghk\}$  and  $\Delta' := \{g, h, k, 1\}$  are hypomorphic, but not isomorphic. Each set has 8 images under  $\mathcal{Q}$  and together these 16 sets form the facets of a hyperoctahedron (or cross-polytope) in dimension 4.

Furthermore, for any integer  $j > 0$  let  $M_j$  denote the vector space over the rationals whose basis vectors are the  $j$ -element subsets from  $\mathcal{Q}$ . We may then consider the linear map  $\partial : M_j \rightarrow M_{j-1}$  which maps each set  $\Gamma$  onto the formal sum of its subsets of cardinality  $|\Gamma| - 1$ . If we regard  $\underline{\Delta}^{\mathcal{Q}} := \sum_{a \in \mathcal{Q}} \Delta^a$  and  $\underline{\Delta}'^{\mathcal{Q}} := \sum_{a \in \mathcal{Q}} \Delta'^a$  as elements in  $M_4$ , then  $0 \neq \underline{\Delta}^{\mathcal{Q}} - \underline{\Delta}'^{\mathcal{Q}}$  is in the kernel of  $\partial : M_4 \rightarrow M_3$ . (This property, suitably stated, is indeed equivalent in general to saying that two sets are hypomorphic, but not isomorphic.) In addition, one can show that the minimum weight in the kernel of  $\partial : M_k \rightarrow M_{k-1}$  is  $2^k$  and so we see that  $\underline{\Delta}^{\mathcal{Q}} - \underline{\Delta}'^{\mathcal{Q}}$  is a *minimum weight vector* in this kernel. For more details see Theorem 2.2 in [16].

**5. The case  $\rho = 3$**

We begin with a simple lemma.

**Lemma 5.1.** *If  $(G, \Omega)$  is semiregular and if there is some  $g \in G$  with  $5 < |g|$ , then  $4 \leq \rho(G, \Omega)$ .*

*Proof.* Since  $G$  is semiregular  $g$  contains a cycle of the kind  $(123456\dots)$ . Then  $\Delta := \{1, 2, 4\} \sim \Delta' := \{1, 3, 4\}$  since  $\{1, 2\} \approx \{3, 4\}$ ,  $\{1, 4\} \approx \{1, 4\}$  and  $\{2, 4\} \approx \{1, 3\}$ . Further, if  $\Delta^h = \Delta'$  for some  $h \in G$ , then  $h = g^2$  or  $g^3$  but this is not the case. □

For the proof of the next result the following notation will be useful. Let  $g$  be a permutation of  $\Omega = \{1, 2, \dots\}$ . Then we write, for example,  $g = (123 - 79-)$  to indicate that the only known information about  $g$  is  $1^g = 2, 2^g = 3$  and  $7^g = 9$ . Also,  $g = (123)*$  means that  $g$  is the product of the 3-cycle  $(123)$  and some permutation  $*$  of  $\Omega \setminus \{1, 2, 3\}$ .

**Lemma 5.2.** *Let  $(G, \Omega)$  be semiregular with  $6 \leq |\Omega|$  and suppose that  $|g| \leq 5$  for all  $g \in G$ . Then there are non-reconstructible sets of cardinality 3, if and only if there exist distinct elements  $1 \neq g, h \in G$  for which one of the following holds:*

- (i)  $g^2 = h^2 \neq Id$  and  $g \neq h^{-1}$ , or
- (ii)  $gh = hg$  with  $|g| \cdot |h| > 4$  and  $\langle g \rangle \cap \langle h \rangle = Id$ .

*Proof.* We begin with the 'only if' part of the lemma and assume that  $\Delta := \{\alpha, \beta, \gamma\} \sim \Delta' := \{\alpha, \beta, \delta\}$  are hypomorphic, but not isomorphic sets of cardinality 3.



Since  $\Delta \sim \Delta'$  there exist  $g, h \in G$  which perform the isomorphisms between  $\{\alpha, \gamma\}, \{\beta, \gamma\}$  and  $\{\alpha, \delta\}, \{\beta, \delta\}$ . There are 5 possibilities:

- A)  $g = (\gamma\alpha\delta-), h = (\gamma\beta\delta-),$
- B)  $g = (\alpha\beta - \gamma\delta-), h = (\beta\alpha - \gamma\delta-),$
- C)  $g = (\alpha\beta - \gamma\delta-), h = (\beta\delta - \gamma\alpha-),$
- D)  $g = (\alpha\delta - \gamma\beta-), h = (\beta\alpha - \gamma\delta-),$  or
- E)  $g = (\alpha\delta - \gamma\beta-), h = (\beta\delta - \gamma\alpha-).$

In CASE A it is clear that  $g^2 = h^2 \neq Id$ . Further, if  $g = h^{-1}$ , then it follows that  $g = (\gamma\alpha\delta\beta)*$ . But then  $\Delta^{g^2} = \Delta'$ , a contradiction.

In CASE B we must have  $g = (\alpha\beta)(\gamma\delta)*$  and then  $\Delta^g = \Delta'$ , a contradiction.

In CASE C it can be seen that  $h^g = h^{g^{-1}} = h^{-1}$ . It follows that  $hg^2 = g^2h$ . Now assume that  $|h| = |g^2| = 2$ . Then  $h = (\beta\delta)(\gamma\alpha)*$  and  $g = (\alpha\beta xy)(\gamma\delta ab)*$  for certain  $x, y, a, b \in \Omega$ . Then  $g^2 = (\alpha x)(\beta y)(\gamma a)(\delta b)*$ . The condition  $hg^2 = g^2h$  implies that  $h = (\beta\delta)(\gamma\alpha)(xa)(yb)*$ . Then  $hg = gh$  and  $|g| \neq 2$ . Hence either  $g^2h = hg^2$  with  $|g^2| \neq 2$  or  $gh = hg$  with  $|g| \neq 2$ . We now show that  $\langle g \rangle \cap \langle h \rangle = Id$  and so also  $\langle g^2 \rangle \cap \langle h \rangle = 1$ . If  $\langle g \rangle \cap \langle h \rangle \neq Id$ , it follows that  $\beta$  and  $\delta$  are in the same cycle of  $g$  since they are in the same cycle of  $h$ . Also, since  $|k| \leq 5$  for all  $k \in G$  it follows that one of the following three cases holds:

- i)  $g = (\alpha\beta\gamma\delta)*,$
- ii)  $g = (\alpha\beta x\gamma\delta)*$  for some  $x \in \Omega,$  or
- iii)  $g = (\alpha\beta\gamma\delta y)*$  for some  $y \in \Omega.$

In case i)  $\Delta^{g^{-1}} = \Delta'$ , a contradiction. In the last two cases it follows that  $g^2 = h = g^3$ , a contradiction. We note also that CASE D is the same as CASE C on interchanging  $\alpha$  and  $\beta$ .

In CASE E it is clear that  $gh = hg$ . Also if  $|g| = |h| = 2$ , then  $g = (\alpha\delta)(\gamma\beta)*$  and  $h = (\beta\delta)(\gamma\alpha)*$ . It follows that  $\Delta^{gh} = \Delta'$ , a contradiction. Finally, in a similar way to the last case we can show that  $\langle g \rangle \cap \langle h \rangle = Id$ .

Now consider the converse. First assume that there exist distinct  $g, h \in G$  with  $g^2 = h^2 \neq Id$  and  $g \neq h^{-1}$ . It follows that  $g = (1\alpha 2-)$  and  $h = (1\beta 2-)$  for some  $1, 2, \alpha, \beta \in \Omega$ . It is clear that the sets  $\Delta := \{1, \alpha, \beta\}$  and  $\Delta' := \{2, \alpha, \beta\}$  are hypomorphic. We show that they are not isomorphic. If  $\Delta^k = \Delta'$  for some  $k \in G$ , then  $\alpha^k = 2$  or  $\beta$ . The first case implies  $k = g$ , but this would require that  $\beta^g = \beta$ , a contradiction. The second case implies  $k = g^{-1}h$ . Under the action of  $k$  we have  $\beta^k = 2$  or  $\alpha$ . In the former case we would require that  $\beta^{g^{-1}} = \beta$ , a contradiction. The latter case requires  $1^k = 2$ , i.e.  $1^{g^{-1}} = \beta$ , but then  $g = h^{-1}$ , a contradiction.

Next assume that there exist  $g, h \in G$  with  $gh = hg$  with at least one of  $g$  and  $h$  not having order 2. Further,  $\langle g \rangle \cap \langle h \rangle = Id$ . We assume without loss of generality that  $|g| \neq 2$ , say  $g = (\alpha_1\alpha_2\alpha_3 \dots \alpha_n)(\alpha_{n+1}\alpha_{n+2}\alpha_{n+3} \dots \alpha_{2n})*$  for  $3 \leq n \leq 5$  and  $\alpha_i \in \Omega$ . We may assume also that  $\alpha_{n+1}^h = \alpha_1$ . The condition  $hg = gh$  then implies that  $h = (\alpha_{n+1}\alpha_1 - \alpha_{n+2}\alpha_2-)$ . It is an easy matter to check that  $\Delta = \{\alpha_1, \alpha_2, \alpha_{n+1}\} \sim \Delta' = \{\alpha_2, \alpha_{n+1}, \alpha_{n+2}\}$ . If  $\Delta^k = \Delta'$  for some  $k \in G$ , then  $\alpha_2^k$  is equal to  $\alpha_{n+1}$  or  $\alpha_{n+2}$ , i.e.  $k = g^{-1}h^{-1}$  or  $k = h^{-1}$ . But  $\alpha_3^{g^{-1}h^{-1}} = \alpha_{n+2}$  and so  $k \neq g^{-1}h^{-1}$ . Furthermore, if  $k = h^{-1}$ , then for  $\Delta^{h^{-1}} = \Delta'$

we would need that  $h = (\alpha_{n+2}\alpha_2\alpha_{n+1}\alpha_1-)$  and so  $g = h^{-2}$ . Clearly then  $|h| \geq 6$ , a contradiction.  $\square$

Let  $\mathcal{T}_0$  be the class of all finite groups for which the following three properties hold:

- $\mathcal{T}_0$ (i) If  $G$  belongs to  $\mathcal{T}_0$ , then  $|G|$  divides  $2^a \cdot 3 \cdot 5$ , for some  $a \in \mathbb{N}$ .
- $\mathcal{T}_0$ (ii) The elements belonging to a group in  $\mathcal{T}_0$  have order at most 5.
- $\mathcal{T}_0$ (iii) If  $g \neq h$  belong to a group in  $\mathcal{T}_0$  and satisfy  $g^2 = h^2 \neq Id$ , then  $g = h^{-1}$  and  $g, h$  have order 4.

So  $\mathcal{T}_0$  is closed under subgroups. Elementary abelian 2-groups are in  $\mathcal{T}_0$ , so are  $Alt_5$  and the dihedral group of order 8. The precise nature of  $\mathcal{T}_0$  will be analysed in the last chapter where we show that  $\mathcal{T}_0$  is indeed the family  $\mathcal{L}_0$  mentioned in the Introduction.

**Theorem 5.3.** *Let  $(G, \Omega)$  be a finite semiregular permutation group with  $1 < |G|$  and  $6 \leq |\Omega|$ . Then  $\rho(G, \Omega) = 3$ , if and only if  $G \in \mathcal{T}_0$ .*

*Proof.* Suppose that  $\rho(G, \Omega) = 3$  with  $G$  finite. Then  $|G| = 2^a \cdot 3^b \cdot 5^c$  for some  $a, b, c \in \mathbb{N}$  by Lemma 5.1. Now we show that  $b, c \in \{0, 1\}$ . Assume for example that  $b \geq 2$ . Let  $P_3$  be a Sylow 3-subgroup of  $G$ , so  $Z(P_3) \neq 1$ . Let  $g \in Z(P_3)$ , so  $|g| = 3^l$  for some integer  $l$ . By Lemma 5.1 it follows that  $|g| = 3$ . Now take  $h \in P_3 \setminus \langle g \rangle$ , so  $|h| = 3$  also. Then  $gh = hg$  and clearly  $\langle g \rangle \cap \langle h \rangle = Id$ , contradicting Lemma 5.2.

Therefore  $|G|$  divides  $2^a \cdot 3 \cdot 5$  for some  $a \in \mathbb{N}$ . Lemma 5.1 implies that all elements in  $G$  have order at most 5. Then it follows from Lemma 5.2 that there does not exist elements  $g, h \in G$  with  $g^2 = h^2 \neq Id$  and  $g \neq h^{-1}$ , and this gives the property  $\mathcal{T}_0$ (iii). Hence  $G \in \mathcal{T}_0$ .

Conversely, let  $G \in \mathcal{T}_0$  be semiregular on  $\Omega$ . First we show that all  $\Omega$ -subsets of cardinality 3 are reconstructible. For assume the contrary. Then by Lemma 5.2 there exist distinct  $g, h \in G$  with at least one of the following cases holding:

- 1)  $g^2 = h^2 \neq Id$  with  $g \neq h^{-1}$ , or
- 2)  $gh = hg$  with at least one of  $g$  and  $h$  not having order 2, and  $\langle g \rangle \cap \langle h \rangle = Id$ .

We need to consider only the second case. Let  $H := \langle g, h \rangle$  and suppose that  $g$  has order 3, 4 or 5. As  $H = C_{|g|} \times C_{|h|}$  we have that  $|g||h|$  divides  $2^a \cdot 3 \cdot 5$ , and as each element in  $H$  has order at most 6, only the possibilities  $|g| = 4 = |h|$  or  $|g| = 4, |h| = 2$  remain. In the first case note that  $g^2 = (gh^2)^2 \neq 1$  so that  $g = (gh^2)^{-1}$ , a contradiction. Similarly, in the second case,  $g^2 = (gh)^2 \neq 1$  so that  $g = (gh)^{-1}$ , contradicting  $\langle g \rangle \cap \langle h \rangle = Id$ .

So  $\rho(G, \Omega) \neq 4$ . We know that if  $\rho(G, \Omega) = 5$ , then  $G$  contains a copy of  $\mathcal{Q}$  acting regularly, on say  $\Omega_1 \subseteq \Omega$ . It can be checked that  $\mathcal{Q}$  acting regularly has non-reconstructible set of cardinality 3. Thus we must have  $\rho(G, \Omega) = 3$ .  $\square$

Finiteness of the group is not really essential and infinite semiregular groups

can be dealt with in a similar fashion. For this let  $\mathcal{T}$  be the class of all infinite groups  $G$  for which

- $\mathcal{T}$ (i) every element in  $G$  has finite order,
- $\mathcal{T}$ (ii) every finite subgroup of  $G$  belongs to  $\mathcal{T}_0$ , and
- $\mathcal{T}$ (iii) if  $g, h \in G$  satisfy  $g^2 = h^2 \neq Id$ , then  $g = h^{-1}$  and  $g, h$  have order 4.

(So any element belonging to a group in  $\mathcal{T}$  has order at most 5, by  $\mathcal{T}$ (ii), and it may be that  $\mathcal{T}$ (iii) is already contained in  $\mathcal{T}$ (ii) though this is not immediately clear.)

**Theorem 5.4.** *Let  $(G, \Omega)$  be an infinite semiregular permutation group. Then  $\rho(G, \Omega) = 3$ , if and only if  $G \in \mathcal{T}$ .*

*Proof.* If  $G \in \mathcal{T}$  acts semiregularly on  $\Omega$ , then the second part of the proof of Theorem 5.3 applies verbatim and so we have  $\rho(G, \Omega) = 3$ .

Suppose therefore that  $\rho(G, \Omega) = 3$ . Then  $\mathcal{T}$ (i) and  $\mathcal{T}$ (iii) follow identically as in the proof of Theorem 5.3. It remains to consider the case when  $H$  is a finite subgroup of  $G$ . Here select some union  $\Omega^*$  of  $H$ -orbits with  $6 < |\Omega^*| < \infty$  and regard  $(H, \Omega^*)$  as a finite semiregular permutation group. Then  $3 \leq \rho(H, \Omega^*) \leq 5$ . If  $3 = \rho(H, \Omega^*)$ , then apply Theorem 5.3 and the result follows. Hence it remains to rule out that  $4 \leq \rho(H, \Omega^*) \leq 5$ .

This can be done as follows. Consider the possibility  $\rho(H, \Omega^*) = 4$  first. Suppose that  $\Gamma, \Gamma^* \subseteq \Omega^*$  are  $H$ -hypomorphic sets of size 4. Then  $\Gamma, \Gamma^*$  are  $G$ -hypomorphic and hence  $G$ -isomorphic. Without loss of generality we can assume that  $\Gamma = \{1, 2, \alpha\}$ ,  $\Gamma^* = \{1, 2, \beta\}$  and that the  $G$ -isomorphism is afforded by  $g \in G$  where  $g = (12)(\alpha\beta)^*$  or  $g = (\alpha 21\beta^-)$ . In either case there are then  $h_i \in H$ ,  $1 \leq i \leq 2$  which afford the maps  $h_i : \Gamma \setminus \{i\} \rightarrow \Gamma^*$ . Each of them is fixed-point-free and each pair has fixed-point-free quotient. Going through the various possibilities, check that each time there is some expression  $h$  in the  $h_i$ 's for which  $g^{-1}h$  or  $gh$  has a fixed point. Hence  $g^{-1}h = 1$  or  $gh = 1$  so that  $g \in H$  and  $\Gamma, \Gamma^*$  are  $H$ -isomorphic. This shows that  $\rho(H, \Omega^*) \neq 4$ . The possibility  $\rho(H, \Omega^*) = 5$  can be ruled out in a similar fashion or by using Theorem 4.2.  $\square$

## 6. Conclusion and applications

We begin by examining  $\mathcal{T}_0$  more closely. Let  $G$  be in  $\mathcal{T}_0$  and let  $g \in G$  have order  $\neq 2$ . Suppose there is some  $c \in C_G(g) \setminus \langle g \rangle$ . Then by  $\mathcal{T}_0$ (ii) the only possibilities are  $|g| = 4$  and  $|c| = 2$  or  $|c| = 4$ . In the first case  $g^2 = (gc)^2 \neq 1$  so that  $g^{-1} = gc$  by  $\mathcal{T}_0$ (iii) which is a contradiction. In the second case apply  $\mathcal{T}_0$ (iii) to  $g^2 = (gc^2)^2 \neq 1$  resulting in  $g^{-1} = gc^2$ , thus  $g^2 = c^2$  whereby  $\mathcal{T}_0$ (iii) gives  $g^{-1} = c$ , again a contradiction. Hence

**Lemma 6.1.** *Let  $G$  belong  $\mathcal{T}_0$  and suppose that  $g \in G$  has order  $\neq 2$ . Then  $C_G(g) = \langle g \rangle$ .*

**Lemma 6.2.** *A 2-group belonging to  $\mathcal{T}_0$  is elementary abelian, cyclic of order 4 or dihedral of order 8.*

*Proof.* Let  $S \in \mathcal{T}_0$  be a 2-group and let  $g \in S$  have order 4. If  $S$  is abelian, we are done,  $S = \langle g \rangle$  by Lemma 6.1. In the other case, when  $z \in Z(S) \neq S$  is an involution, Lemma 6.1 implies  $z = g^2$ . Hence any two elements of order 4 have the same square and  $\mathcal{T}_0$ (iii) says that there is only one subgroup  $C$  of order 4. The remainder is clear,  $S/C$  acts faithfully on  $C$  and so  $|S| = 8$ .  $\square$

**Lemma 6.3.** *Let  $G$  be solvable. Then  $G$  is in  $\mathcal{T}_0$ , iff  $G$  is a subgroup of one of the following:*

- (i) *the semi-direct product  $V \cdot C$  where  $V$  is elementary abelian of order  $2^n$  for some  $n \in \mathbb{N}$  and  $C$  has order 3 or 5 acting fix-point-freely on  $V$ ;*
- (ii) *the holomorph  $\text{Hol}(C)$  with  $C$  cyclic of order 3, 4 or 5, thus  $|\text{Hol}(C)| = 6, 12$  or  $20$ ;*
- (iii) *the symmetric group  $\text{Sym}(4)$ .*

*Proof.* It is evident that the groups in (i)–(iii) satisfy  $\mathcal{T}_0$ (i)– $\mathcal{T}_0$ (iii). So consider the converse and suppose that  $G$  belongs to  $\mathcal{T}_0$ . If  $|G|$  is not divisible by all three primes, then it is easy to check from Lemma 6.1 and Lemma 6.2 that  $G$  is contained in one of the groups under (i)–(iii).

To rule out the case when  $|G| = 2^n \cdot 3 \cdot 5$  with  $n > 0$  select a composition series of  $G$  and select in it the largest subgroup  $H$  whose order is divisible by two primes only. Then  $H$  is one of the groups mentioned under (i)–(iii) and without loss we may assume that  $H$  is normal in  $G$  with  $|G : H| = p$  being the remaining prime. The case when  $H \subseteq \text{Hol}(C)$  or  $\text{Sym}_4$  can be ruled out easily. Similarly, when  $H = V \cdot C$  then it is easy to show that the Sylow- $p$ -subgroup does not act fix-point-freely on  $V$ .  $\square$

It remains to consider the case when  $G$  in  $\mathcal{T}_0$  is not solvable, of order  $|G| = 2^n \cdot 3 \cdot 5$  with  $n \geq 2$ . Let  $S$  be the Sylow-2-subgroup of  $G$ . The cases where  $S$  is cyclic or dihedral can be ruled out easily and so  $S$  is elementary abelian by Lemma 6.2. It follows from Lemma 6.1 and Burnside's transfer lemma that  $N := N_G(S) \supset S$ . So  $G$  has a representation of degree  $|G : N| = 3$  or  $5$ . From the insolubility of  $G$  it follows that  $|G : N| = 5$  and  $G/K = \text{Alt}_5$  where  $K$  is the kernel of this representation. Thus  $K$  is elementary abelian of order  $2^{n-2}$ . Consider  $C := C_G(K)$ , a normal subgroup of  $G$ . As  $K \subset S \subseteq C$  we have  $C = G$ . This contradicts Lemma 6.1 unless  $C = 1$ . Hence in fact  $G = \text{Alt}_5$  and we have proved

**Lemma 6.4.** *Suppose that  $G$  in  $\mathcal{T}_0$  is not solvable. Then  $G$  is isomorphic to  $\text{Alt}_5$ .*

*Proof of Theorem 1.1 and 1.2.* Lemmas 6.3 and 6.4 show that the groups in  $\mathcal{T}_0$

are in fact those of  $\mathcal{L}_0$  mentioned in the introduction. The result therefore follows from Theorems 4.2, 5.3 and 5.4.

We note two corollaries. The first concerns Hamiltonian groups and is due to Mnukhin [13]. The non-abelian Hamiltonian groups are all of the form  $\mathcal{Q} \times U \times C_2^m$  for  $0 \leq m$  and an abelian group  $U$  of odd order, see [5].

**Corollary 6.5.** *The reconstruction index of an abelian group of order at least 6 acting faithfully is equal to 4, unless the group is an elementary abelian 2-group in which case the index is equal to 3. The reconstruction index of a non-abelian Hamiltonian group is equal to 5 in any faithful representation.*

**Corollary 6.6.** *If  $G$  has odd order  $> 6$  and acts semiregularly on  $\Omega$ , then  $\rho(G, \Omega) = 4$ .*

**Acknowledgement.** We wish to thank Valeriy Mnukhin for helpful discussions, many suggestions and bringing the manuscripts [7, 14] to our attention. Many thanks also to Andreas Pilsak who read our manuscript very carefully.

## References

- [1] N. ALON, Y. CARO, I. KRASIKOV AND Y. RODITTY, *Combinatorial reconstruction problems*, J. Combin. Theory Ser. B 47 (1989), 153–161.
- [2] L. BABAI, *Automorphism groups, isomorphism, reconstruction*, in: R. L. Graham, M. Grötschel and L. Lovász (eds.), *Handbook of Combinatorics 2*, ch. 27, North Holland, Amsterdam, 1995.
- [3] J. A. BONDY, *A Graph reconstructor's manual*, in: K. L. Lloyd (ed.), *Surveys in Combinatorics*, 221–251, London Math. Soc. Lecture Note Ser. 116, Cambridge University Press, 1991.
- [4] P. J. CAMERON, *Some open problems on permutation groups*, in: M. W. Liebeck and J. Saxl (eds.), *Groups, Combinatorics and Geometry*, 340–350, London Math. Soc. Lecture Note Ser. 165, Cambridge University Press, 1992.
- [5] H. S. M. COXETER AND W. O. MOSER, *Generators and Relations for Discrete Groups*, 4th Edition, Ergebnisse der Mathematik, Springer-Verlag, Heidelberg, New York, 1980.
- [6] I. KRASIKOV AND Y. RODITTY, *On a reconstruction problem for sequences*, J. Combin. Theory Ser. A 77 (1997), 344–348.
- [7] E. M. LIVSHIZ, *On the reconstruction of configurations from their maximum fragments*, Manuscript, Tbilisi, 1983.
- [8] P. M. MAYNARD, *On orbit reconstruction problems*, Ph.D. Thesis, University of East Anglia, Norwich, 1996.
- [9] P. M. MAYNARD AND J. SIEMONS, *On the reconstruction of linear codes*, J. Combin. Des. 6 (1998), 285–291.
- [10] P. M. MAYNARD, *Square-celled animal reconstruction problems*, Ars Combin. 56 (2000), 81–87.
- [11] V. B. MNUKHIN, *Combinatorial Properties of Partially Ordered Sets and Group Actions*, in: J. Siemons (ed.), *Discrete Mathematics and Applications*, TEMPUS Lecture Notes Vol. 8, University of East Anglia, Norwich, 1993.
- [12] V. B. MNUKHIN, *Reconstruction of  $k$ -orbits of a permutation group*, Math. Notes 42 (1987), 975–980.

- [13] V. B. MNUKHIN, *The  $k$ -orbit reconstruction for Abelian and Hamiltonian groups*, Acta Appl. Math. 52 (1998), 149–162.
- [14] V. B. MNUKHIN, *The  $k$ -orbit reconstruction for Abelian and Hamiltonian groups II*, Manuscript, Taganrog, 1996.
- [15] V. B. MNUKHIN, *The  $k$ -orbit reconstruction and the orbit algebra*, Acta Appl. Math. 29 (1992), 83–117.
- [16] V. B. MNUKHIN AND I. J. SIEMONS, *On the modular homology in the Boolean algebra*, J. Algebra, 179 (1996), 191–199.
- [17] V. MÜLLER, *The edge reconstruction conjecture is true for graphs with more than  $n \log_2 n$  edges*, J. Combin. Theory Ser. B 22 (1977), 281–283.
- [18] C. NASH-WILLIAMS, *The reconstruction problem*, in: L. W. Beineke and R. J. Wilson (eds.), *Selected Topics in Graph Theory*, 205–236, Academic Press, London–New York, 1978.
- [19] A. J. RADCLIFFE AND A. D. SCOTT, *Reconstructing subsets of  $\mathbb{Z}/n$* , J. Combin. Theory Ser. A 83 (1998), 169–187.
- [20] A. J. RADCLIFFE AND A. D. SCOTT, *Reconstructing subsets of the reals*, Electron. J. Combin. 6 (1999).
- [21] J. SIEMONS, *On partitions and permutation groups on unordered sets*, Arch. Math. (Basel) 38 (1982), 391–403.

Ph. Maynard and J. Siemons  
School of Mathematics  
University of East Anglia  
Norwich, NR4 7TJ  
United Kingdom  
e-mail: j.siemons@uea.ac.uk  
philip\_maynard@hotmail.com

Manuscript received: May 22, 2000 and, in final form, February 25, 2002.



To access this journal online:  
<http://www.birkhauser.ch>

---