On some designs and codes from primitive representations of some finite simple groups

J. D. Key*
Department of Mathematical Sciences
Clemson University
Clemson SC 29634
U.S.A.

J. Moori† and B. G. Rodrigues‡
School of Mathematics, Statistics
and Information Technology
University of Natal-Pietermaritzburg
Pietermaritzburg 3209
South Africa

July 18, 2001

Abstract

We examine a query posed as a conjecture by Key and Moori [11, Section 7] concerning the full automorphism groups of designs and codes arising from primitive permutation representations of finite simple groups, and based on results for the Janko groups J_1 and J_2 as studied in [11]. Here, following that same method of construction, we show that counter-examples to the conjecture exist amongst some representations of some alternating groups, and that the simple symplectic groups in their natural representation provide an infinite class of counter-examples.

*Support of NSF grant #9730992 acknowledged.
†Support of NRF and the University of Natal (URF) acknowledged.
‡Post-graduate scholarship of DAAD (Germany) and the Ministry of Petroleum (Angola) acknowledged.

1 Introduction

In examining the codes and designs arising from the primitive representations of the first two Janko groups, Key and Moori [11] suggested in Section 7 of that paper that the computations made for these Janko groups could lead to the following conjecture: "any design $\mathcal{D}$ obtained from a primitive permutation representation of a simple group G will have the automorphism group $\mathrm{Aut}(G)$ as its full automorphism group, unless the design is isomorphic to another one constructed in the same way, in which case the automorphism group of the design will be a proper subgroup of $\mathrm{Aut}(G)$ containing G". (Here G is naturally a subgroup of $\mathrm{Aut}(\mathcal{D})$, and also of $\mathrm{Aut}(G)$, since it is simple and hence isomorphic to the (normal) subgroup of inner automorphisms. How outer automorphisms of G would define elements of $\mathrm{Aut}(\mathcal{D})$ is not clear but it did occur for those Janko groups, and in fact for most of the primitive representations; certainly the normalizer of G in $\mathrm{Aut}(\mathcal{D})$ will be a subgroup of $\mathrm{Aut}(G)$.)

While the conjecture is true for the Janko groups J_1 and J_2, and some other simple groups, we show here that it is not always true: we found examples of finite simple groups G with a primitive representation giving a design $\mathcal{D}$ (as described in Section 3) such that the automorphism group of G does not contain the automorphism group of $\mathcal{D}$. Furthermore, there are finite simple groups that have automorphisms that do not preserve the design. Specifically, we considered computationally all the primitive permutation representations of G where G is the alternating group A_6 or A_9. Using Magma [2], we constructed designs that have the group G acting primitively on points and blocks, and, for each prime dividing $|G|$, we constructed the codes of the designs over that prime field. Contradicting the conjecture in [11], we found for $G = A_6$ of degree 15, two isomorphic designs such that the automorphism group of the design is neither the group $\mathrm{Aut}(A_6)$ nor a proper subgroup of $\mathrm{Aut}(A_6)$ containing A_6. In fact if $\mathcal{D}$ denotes one of these designs then $\mathrm{Aut}(A_6) \not\leq \mathrm{Aut}(\mathcal{D})$. Similarly for $G = A_9$ we found that the orbits of length 56 and 63 respectively for A_9 of degree 120 produce designs with the property that the automorphism group is not $\mathrm{Aut}(A_9)$, nor is it a proper subgroup of $\mathrm{Aut}(A_9)$ containing A_9. Also, if $\mathcal{D}$ is either of these designs, then $A = \mathrm{Aut}(\mathcal{D})$ is the orthogonal group $O_8^+(2):2$ and $\mathrm{Aut}(A_9) \not\leq A$.

In addition to these counter-examples, the simple symplectic groups $PSp_n(q)$, for n even and at least 4, in their natural primitive rank-3 action on the points of projective $(n-1)$-space over the finite field F_q, provide an infinite set of groups that do not satisfy the conjecture, by taking the action on the symmetric design of points and hyperplanes of the $(n-1)$-space, or of its complementary design. For q odd or for q even and $n > 4$, we have the automorphism group of the group a proper subgroup of that of the design, while for $q = 2^t$ and $t \geq 2$, and $n = 4$, there are automorphisms of the group that are not automorphisms of the design.

We found other alternating groups that countered the conjecture, *viz.* A_{10} of degree 2520 using an orbit of length 144, and A_{11} of degree 462 using an orbit of length 200, and of degree 2520 using orbits of length 495 and 1584, respectively. None of these are rank-3 representations, although all the counter-examples we give in this paper are. We should point out that most the simple groups we tried did in fact satisfy the conjecture, i.e. all their primitive representations did satisfy the conjecture. These counter-examples are relatively rare, and interesting.

Aside from this issue of the conjecture made in [11], we should point out that the motivation for this study, and that in [11], is partially to find designs with good codes that have large automorphism groups. It is hoped that obtaining such codes can be of practical use in that the groups can assist in decoding. In particular, permutation decoding might be used as it is likely that PD-sets will exist for large transitive groups for at least some of the codes. With this in mind, we discuss permutation decoding in Section 2, and give an example of a PD-set for one of the codes arising from A_6 in Section 5. We also found PD-sets for some of the other codes obtained from the primitive representations of A_9, and we refer to these in Section 7.

We outline our notation in Section 2, and describe the construction in Section 3. The description of the symplectic groups as counter-examples is given in Section 4. Computations for A_6 are given in Section 5 and those for A_9 in Section 6. The appendices have a full list of computational results, and Section 7 has some observations on some of the more interesting codes obtained from the computations for A_9.

2 Terminology and notation

For the structure of groups and their maximal subgroups we follow the notation of the ATLAS [5]. The groups $G.H$, $G : H$, and $G \cdot H$ denote a general extension, a split extension and a non-split extension respectively. Also, $A.B$ or AB denotes any group having a normal subgroup of structure A, for which the corresponding quotient has structure B. For a prime p, p^n denotes the elementary abelian group of order p^n. We also denote the particular cases of an extraspecial group by p^{1+2n}, p_+^{1+2n} or p_-^{1+2n}.

Our notation for designs and codes will be standard and as in [1]. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. A design is **trivial** if every k-set of points is incident with a block of the design. The **dual** structure of $\mathcal{D}$ is $\mathcal{D}^t = (\mathcal{B}, \mathcal{P}, \mathcal{I})$. Thus the transpose of an incidence matrix for $\mathcal{D}$ is an incidence matrix for $\mathcal{D}^t$. We will say that the design is **symmetric** if it has the same number of points and blocks, and **self-dual** if it is isomorphic to its dual.

The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field F_p, in which case we write also C_p for C_F, and refer to the dimension of C_p as the **p-rank** of $\mathcal{D}$. If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.

All our codes here will be **linear codes**, i.e. subspaces of the ambient vector space. If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to show this information. A **generator matrix** matrix for the code is a $k \times n$ matrix made up of a basis for C. The **dual** or **orthogonal** code $C^\perp$ is the orthogonal under the standard inner product, i.e. $C^\perp = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$. A **check matrix** or **parity-check matrix** for C is a generator matrix for $C^\perp$; the **syndrome** of a vector $y \in F^n$ is Hy^T. A code C is **self-orthogonal** if $C \subseteq C^\perp$ and is **self-dual** if $C = C^\perp$. The **hull** of a design's code over some field is the intersection $C \cap C^\perp$. If c is a codeword then the **support** of c is the set of non-zero coordinate positions of c. A **constant vector** is one for which all the coordinate entries are either 0 or 1. The all-one vector will be denoted by $\jmath$, and is the constant vector of weight the length of the code. Two linear codes of the same length and over the same field are **equivalent** if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate position by a non-zero field element. They are **isomorphic** if they can be obtained from one another by permuting the coordinate positions. Any code is isomorphic to a code with generator matrix in so-called **standard form**, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The first k coordinates are the **information symbols** and the last $n-k$ coordinates are the **check symbols.** An **automorphism** of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\mathrm{Aut}(C)$. Any automorphism clearly preserves each weight class of C.

Permutation decoding uses so-called PD-sets: a **PD-set** for a code is a set $\mathcal{S}$ of automorphisms of the code which is such that, if the code can correct t errors, then every possible error vector of weight t or less can be moved by some member of $\mathcal{S}$ out of the information positions. That such a set will fully use the error-correction potential of the code follows from a result quoted in [9, Theorem 8.1]. There is a also a bound on the minimum size that the set $\mathcal{S}$ may have, due to Gordon [8]:

Result 1 *If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n,k,d]_q$code C, and $r = n - k$, then*

$$|\mathcal{S}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil .$$

The algorithm for permutation decoding then is as follows: we have a t-error-correcting $[n,k,d]_q$ code C with check matrix H in standard form. Thus the generator matrix G for C that is used for encoding has I_k as the first k columns, and hence the first k coordinate positions correspond to the information symbols. Any k-tuple v is encoded as vG. Suppose x is sent and y is received and at most t errors occur. Let $\mathcal{S} = \{g_1, \ldots, g_s\}$ be the PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \ldots, s$ until an i is found such that the weight of this vector is t or less. Now look at the information symbols in this vector, and obtain the codeword c that has these information symbols. Now decode y as cg_i^{-1}. Note that this is valid since permutations of the coordinate positions correspond to linear transformations of F^n, so that if $y = x + e$, where $x \in C$, then $yg = xg + eg$ for any $g \in S_n$, and if $g \in Aut(C)$, then $xg \in C$.

3 Methods and preliminary results

Our computations for the designs and codes are based on Result 2 from [11, Proposition 1] and Result 3 from [11, Lemma 2], and quoted below.

Result 2 *Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α. If*

$$\mathcal{B} = \{\Delta^g : g \in G\},$$

then $\mathcal{B}$ forms a self-dual 1-$(n, |\Delta|, |\Delta|)$ design with n blocks, with G acting as an automorphism group on this structure, primitive on the points and blocks of the design.

Note that if we form any union of orbits of the stabilizer of a point, including the orbit consisting of the single point, and orbit this under the full group, we will still get a self-dual symmetric 1-design with the group operating. Thus the orbits of the stabilizer can be regarded as building blocks. Because of the maximality of the point stabilizer, there is only one orbit of length 1: see [11]. In fact this will give us all possible designs on which the group acts primitively on points and blocks:

Result 3 *If the group G acts primitively on the points and the blocks of a symmetric 1-design $\mathcal{D}$, then the design can be obtained by orbiting a union of orbits of a point-stabilizer, as described in Result 2.*

It is clear that, if $\mathcal{D}$ is any design obtained from the construction in the manner described above, then the automorphism group of $\mathcal{D}$ will contain G. Further, if C is the code of $\mathcal{D}$ over a field F, then the automorphism group of $\mathcal{D}$ is contained in the automorphism group of C.

In this paper, in a manner similar to the study in [11], we examine the designs and codes from all the primitive representations of A_6 and A_9, the alternating groups of degree 6 and 9, respectively. Note that $\text{Aut}(A_6) = A_6 : 2^2$, A_6 being the only alternating group whose full automorphism group is not the symmetric group; $\text{Aut}(A_9) = S_9$. We looked first at A_6, of order 360, and its maximal subgroups and primitive permutation representations via the coset action on these subgroups: see [5]. There are five distinct primitive permutation representations of degrees 6, 6, 10, 15 and 15, respectively, and only the representations of degree 15 gave non-trivial designs. We then considered A_9, of order 181440, which has eight primitive permutation representations of degrees 9, 36, 84, 120, 120, 126, 280 and 840 respectively. For each of these groups, using Magma [2], we found the corresponding designs as described in Result 2, and computed the full automorphism group of the design. We also constructed each design's associated code for the primes p that divide the order of the simple group. The computations list the p-rank of the design and the dimension of the hull in each case. Where possible we have also computed the automorphism group of the code.

4 Symplectic groups

The simple symplectic group $PSp_n(q)$, where n is even and at least 4, and q is any prime power, acts as a primitive rank-3 group of degree $\frac{q^n-1}{q-1}$ on the points of the projective $(n-1)$-space $PG_{n-1}(F_q)$: see, for example, Huppert[10, p. 221]. The orbits of the stabilizer of a point P consist of $\{P\}$ and one of length $\frac{q^{n-1}-1}{q-1} - 1$ and the other of length q^{n-1}. The point P together with the points of the orbit of length $\frac{q^{n-1}-1}{q-1} - 1$ form a hyperplane, which is, in fact, the image of the absolute point P under the symplectic polarity. The symmetric 1-$(\frac{q^n-1}{q-1}, q^{n-1}, q^{n-1})$ design $\mathcal{D}$ formed following the method of Result 2 by orbiting the orbit of length q^{n-1} is the complement of the design of points and hyperplanes obtained by taking the union of the other two orbits. This latter design is of course a symmetric 2-design, i.e. a 2-$(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1})$ design and hence the complement $\mathcal{D}$ is also a 2-design, with parameters 2-$(\frac{q^n-1}{q-1}, q^{n-1}, q^{n-1} - q^{n-2})$.

The automorphism group of the design of points and planes, and hence also of its complementary design, is the full projective semi-linear group $P\Gamma L_n(q)$, by the fundamental theorem of projective geometry (see, for example, [1, Chapter 3]). The automorphism group of $PSp_n(q)$ for $n \geq 2$ is discussed in Dieudonné [7, Chapter 4], but completely determined for the case where $n = 4$ and q is even, by Steinberg [13]: see also Carter [4] for a description. Essentially, the automorphism group is $P\Gamma Sp_n(q)$ except when $n = 4$ and $q > 2$ is even, in which case it is this group extended by an involution σ that is not in $P\Gamma L_4(q)$. Thus the automorphism group of the simple group is a proper subgroup of that of the design in the case of odd q or the case of $n > 4$; for $n = 4$ and $q > 2$ even, it is not a subgroup of the automorphism group of the design. Either way, we have an infinite class of counter-examples to the conjecture in [11].

The above discussion has thus proved the following proposition:

Proposition 1 *Let G be the simple symplectic group $PSp_n(q)$, where $n \geq 4$ and even, and q is any prime power, acting as a primitive rank-3 group of degree $\frac{q^n-1}{q-1}$, and let $\mathcal{D}$ be the 1-$(\frac{q^n-1}{q-1}, q^{n-1}, q^{n-1})$ design formed from the longer orbit of a point-stabilizer. Then $\mathcal{D}$ is a symmetric 2-design with automorphism group $P\Gamma L_n(q)$ which properly contains the automorphism group of $PSp_n(q)$ unless $n = 4$ and $q = 2^t$ where $t \geq 2$. For all cases,* $\mathrm{Aut}(\mathcal{D}) \not\leq \mathrm{Aut}(G)$.

Note: 1. The case $PSp_4(2)$ is somewhat different and does not fit into the above class: see the results for A_6 below.
2. The codes of the designs in Proposition 1 are well known and are p-ary subcodes of the projective generalized Reed-Muller codes: see [1, Chapter 5].

5 Computations for A_6

Of the five primitive permutation representations of A_6, only the representations of degree 15 give non-trivial designs. The representations and orbit lengths are shown in Table 1: the first column gives the ordering of the primitive representations as given by Magma (or the ATLAS [5]) and as used in our computations (see the appendix); the second gives the maximal subgroups; the third gives the degree (the number of cosets of the point stabilizer); the fourth gives the number of orbits, and the remaining columns give the size of the non-trivial orbits of the point-stabilizer.

The first three representations give trivial designs. We used Magma to construct the permutation group and form the orbits of the stabilizer of a point for each of the representations of degree 15. For each of the non-trivial orbits, we formed the symmetric 1-design as described in Result 2. We found that the designs obtained with the same parameters for these two representations were isomorphic. Thus in all there are four non-isomorphic

No.	Max. sub.	Deg.	#	length	
1	A_5	6	2	5	
2	A_5	6	2	5	
3	$3^2:4$	10	2	9	
4	S_4	15	3	6	8
5	S_4	15	3	6	8

Table 1: Orbits of the point-stabilizer of A_6

symmetric designs for A_6 formed using single orbits. Note that none of the designs has A_6 acting as the full automorphism group, and neither was there a design whose automorphism group was $\mathrm{Aut}(A_6) = A_6 : 2^2$, since the trivial designs have the symmetric group of degree 6 or 10, respectively, as automorphism group, and those on 15 points have either A_8 or the symmetric group S_6: see Section 8.2.

Considering either of the representations of degree 15, an orbit of length 8 produces a 1-(15, 8, 8) design with automorphism group of order 20160. This representation is similar to that described for the symplectic groups, since $A_6 \cong Sp_4(2)'$, the derived group of $Sp_4(2)$. We have a rank-3 group acting on points of the projective 3-space $PG_3(F_2)$.

Proposition 2 *For $G = A_6$ of degree 15, the automorphism group A of the design $\mathcal{D}$ with parameters 1-(15, 8, 8) is $PGL_4(2) \cong A_8$ and does not contain* $\mathrm{Aut}(G)$.

Proof: Since A_6 is a subgroup of $Sp_4(2)$, this action is that on the points of $PG_3(F_2)$ and the 1-(15, 8, 8) design is actually a symmetric 2-(15, 8, 4) design, and the complement of the 2-(15, 7, 3) design of points and planes. Its automorphism group A is thus $PGL_4(2)$, by the fundamental theorem of projective geometry. That this is isomorphic to A_8 can be found in Dickson [6].

Since $\mathrm{Aut}(A_9) = A_6 : 2^2$ and since A_8 has no subgroup of index 14 (see [5]), we deduce that $\mathrm{Aut}(A_6)$ is not a subgroup of A_8. In addition, computation of the normalizer $N_A(G)$ showed that it has order 720, and is thus S_6. Furthermore, since $|A_8| > |A_6 : 2^2|$, A_8 cannot be a subgroup of $\mathrm{Aut}(A_6) = A_6 : 2^2$. □

Example 1 As an illustration of permutation decoding, we obtained a PD-set for the binary code of the 2-(15, 8, 4) design: the code is the simplex code of length 15, i.e. a [15, 4, 8] code, dual to the binary Hamming code of length 15. A generator matrix in standard form is

```
[1 0 0 0 1 1 1 0 1 0 1 0 0 1 1]
[0 1 0 0 0 1 1 1 0 0 0 1 1 1 1]
[0 0 1 0 1 1 0 0 0 1 1 1 1 0 1]
[0 0 0 1 0 1 1 1 1 1 1 0 1 0 0]
```

The group $PGL_4(2)$ contains Singer cycles, and hence the code is cyclic. According to the bound mentioned in Result 1, at least five permutations are needed for a PD-set. In addition, according to the analysis in MacWilliams [12], a PD-set might be found in a Singer group. We found the following seven elements that form a PD-set for this code in a Singer group in $PGL_4(2)$:

```
Id,
(1, 13, 10, 9, 8)(2, 5, 14, 7, 6)(3, 11, 15, 12, 4),
(1, 15, 2, 13, 12, 5, 10, 4, 14, 9, 3, 7, 8, 11, 6),
(1, 2, 12, 10, 14, 3, 8, 6, 15, 13, 5, 4, 9, 7, 11),
(1, 11, 7, 9, 4, 5, 13, 15, 6, 8, 3, 14, 10, 12, 2),
(1, 8, 9, 10, 13)(2, 6, 7, 14, 5)(3, 4, 12, 15, 11),
(1, 6, 11, 8, 7, 3, 9, 14, 4, 10, 5, 12, 13, 2, 15).
```

This gives an algorithm for correcting three errors.

6 Computations for A_9

From the eight primitive permutation representations, we obtained in all 25 non-isomorphic symmetric designs formed using Result 2 from single orbits, on which A_9 acts primitively. The full list of designs and codes is given in Section 8.2. From the list of designs and codes produced by our computations we have singled out for discussion a case where the automorphism groups of both design and code were distinct from A_9 or $\mathrm{Aut}(A_9)$. This arose for A_9 of degree 120 where the orbits of length 56 and 63 yield designs and codes with the orthogonal group $O_8^+(2):2$ as automorphism group.

Table 2 gives the same information for A_9 as Table 1 gives for A_6. The numbers appearing in parenthesis represent the number of orbits of the point stabilizer in case there is more than one of that length.

Writing $G = A_9$, there are precisely 25 non-isomorphic self-dual 1-designs obtained by taking all the images under G of single non-trivial orbits of the point stabilizer in any of G's primitive representations, and on which G acts primitively on points and blocks. Our computations show that the full automorphism groups of the designs are either A_9, $S_9 = \mathrm{Aut}(A_9)$ or the orthogonal group $O_8^+(2):2$.

No.	Max. sub.	Deg.	#	len.					
1	A_8	9	2	8					
2	S_7	36	3	14	21				
3	$(A_6 \times 3) : 2$	84	4	18	20	45			
4	$L_2(8) : 3$	120	3	56	63				
5	$L_2(8) : 3$	120	3	56	63				
6	$(A_5 \times A_4) : 2$	126	5	5	20	40	60		
7	$3^3 : S_4$	280	5	27	36	54	162		
8	$3^2 : 2A_4$	840	12	8	24(2)	27	36	72(4)	216(2)

Table 2: Orbits of the point-stabilizer of A_9

6.1 The 1-$(120, 56, 56)$ design

Our results for A_9 show that for A_9 of degree 120, the fourth or fifth rank-3 representation, an orbit of length 56 gives a 1-$(120, 56, 56)$ design. Since the representation is of rank 3, the orbits also define strongly regular graphs on 120 vertices, of valency 56 and 63 respectively: these graphs are well-known and appear in the list of Brouwer[3, page 675]. This design yields a $[120, 8]_2$ self-orthogonal doubly-even code.

Proposition 3 *For $G = A_9$ of degree 120, the automorphism group of the design $\mathcal{D}$ with parameters 1-$(120, 56, 56)$ is the orthogonal group $O_8^+(2) : 2$, which neither contains nor is contained in* Aut(G).

Proof: Let $G = A_9$ and $\overline{G}$ denote Aut$(\mathcal{D})$ where $\mathcal{D}$ is constructed from an orbit of length 56 for A_9 of degree 120. Magma computations show that $\overline{G}$ is a non-abelian group of order 348364800 generated by the permutations which we denote by a, b, c, d, e, f, g and h listed in the appendix (see Section 8.1). Computations with Magma show that there exists a non-abelian subgroup N of $\overline{G}$ of order 174182400. Since $[\overline{G} : N] = 2$ we have that $N \trianglelefteq \overline{G}$. We claim that $N \cong O_8^+(2)$. A composition series for $\overline{G}$ found by using Magma is $\overline{G} \geq N \geq 1_{\overline{G}}$; this is in fact a chief series for $\overline{G}$. Thus N is a non-abelian chief factor of $\overline{G}$. Since $|N| = 174182400 = |O_8^+(2)|$, we have that $N \cong O_8^+(2)$, as asserted.

It follows that $\overline{G} \cong O_8^+(2).2$. The permutation $\alpha =$

```
(1,84)(2,31)(5,62)(8,83)(10,26)(11,113)(12,103)(13,75)(14,38)
(15,67)(17,37)(22,72)(23,102)(24,82)(25,70)(27,52) (29,120)
(41,90)(45,117)(47,59)(48,104)(50,94)(58,89)(63,101)(64,108)
(71,85)(78,97)(87,112)
```

is in $\overline{G} - N$ and $o(\alpha) = 2$. Hence $\overline{G}$ is a split extension of N by $\langle \alpha \rangle$.

We know that $\mathrm{Aut}(A_9) = S_9$, and since the normalizer $N_{\overline{G}}(G) = G$, we have $\mathrm{Aut}(G) \not\leq \mathrm{Aut}(\mathcal{D})$, as asserted. Note however that from the ATLAS [5] we know that S_9 is a maximal subgroup of $O_8^+(2){:}2$ of index 960, so $\overline{G}$ does contain isomorphic copies of $\mathrm{Aut}(A_9)$. □

This provides another counter-example to the conjecture.

6.2 The $[120, 8, 56]_2$ code

We found that the 1-(120, 56, 56) design yields a $[120, 8]_2$ binary code whose automorphism group has order 348364800. This leads to:

Proposition 4 *The orthogonal group $O_8^+(2){:}2$ is the automorphism group of the $[120, 8]_2$ binary code C derived from the* 1-(120, 56, 56) *design $\mathcal{D}$. The code C is self orthogonal and doubly-even, with minimum distance* 56. *Its dual is a $[120, 112, 3]_2$ with* 1120 *words of weight* 3.

Proof: The automorphism group of the $[120, 8]_2$ binary code C derived from the 1-(120, 56, 56) design constructed from A_9 of degree 120 contains $\overline{G}$, the automorphism group of the design, and has, by computation, the same order, and thus is equal to $\overline{G}$.

Since the dimension of C equals the dimension of the hull (see Section 8.2) it follows that $C \subseteq C^{\perp}$ and so C is self orthogonal. Since the incidence vectors of the blocks of the design span the code, and the vectors have weight 56, C is doubly-even. In fact Magma gives the weight distribution:

```
<0, 1>, <56, 120>, <64, 135>
```

That $C^{\perp}$ has minimum weight 3 was found using Magma. The full weight distribution can be obtained. □

7 Observations

The conjecture in [11] does thus not generally hold, although it does hold for most representations. We looked further at some of the other codes that arose in the primitive representations of A_9, and found some that had interesting parameters. In some cases we found PD-sets, and the size of the sets we found is given below in such cases. The actual codes and PD-sets can be found at the website:

`http://www.ces.clemson.edu/~keyj`

in the Magma files, under PD-sets. Notice that we have not always been able to find the automorphism group of the code as this requires longer computation. However, the original group is an automorphism group, as is the automorphism group of the design, and we have worked with these.

- The ternary code of the 1-$(120, 63, 63)$ design is a $[120, 36, 24]_3$ self-orthogonal code with $O_8^+(2):2$ acting on it.
- The binary code C of the 1-$(126, 20, 20)$ design is a $[126, 56, 6]_2$ with dual a $[126, 70, 5]_2$ code. For C the minimum size of a PD-set is 4, and we found one of size 17; for $C^\perp$ the minimum size is 7 and we found one of size 32.
- The binary code C of the 1-$(126, 40, 40)$ design is a $[126, 48, 16]_2$ and its dual is a $[126, 78, 5]_2$ code. We found a PD-set of size 43 for $C^\perp$, the minimum size being 8.
- The hull of the 1-$(126, 60, 60)$ design is a $[126, 26, 32]_2$ doubly-even self-orthogonal code with automorphism group of order 3628800, which is isomorphic to S_{10}. This is also the automorphism group of the 1-(126,60,60) design's code, a $[126, 74, d]_2$, where $d \leq 12$ and its dual, a $[126, 52, 14]_2$ code. This then provides an example of the automorphism group of the code being larger than that of the design. The weight distribution of the hull is as follows:

```
> WeightDistribution(hull);
[<0,1>,<32,1575>,<36,2520>,<40,630>,<44,119700>,<48,278775>,
<52,2926350>,<56,9239940>,<60,16352280>,<64,17803800>,
<68,13894650>,<72,5005350>,<76,1313172>,<80,114345>,<84,55650>,
<100,126> ]
```

  The words of weight 100 form a 1-(126,100,100) design with S_{10} as automorphism group, and with the code of the design the hull found above. The design can also be formed by orbiting the union of an orbit of length 40 with one of length 60. The complementary design is a 1-(126,26,26) whose code is a $[126, 27, 26]_2$ that contains the code of the hull shown above, and is obtained from that code by adding the all-one vector.
- The binary code of the 1-$(280, 36, 36)$ design is a $[280, 42, 36]_2$ self-orthogonal doubly-even code.

8 Appendix

8.1 Generators Prop. 3

a = (1,2)(5,93)(6,89)(7,11)(8,65)
(10,100)(12,63)(13,116)(14,53)
(16,34)(17,40)(18,21)(19,38)(20,30)
(22,111)(24,46)(25,45)(26,115)(27,52)
(28,101)(29,69)(31,43)(32,97)(33,60)
(35,88)(36,50)(37,44)(39,104)(41,99)
(42,81)(47,94)(48,105)(49,95)(51,108)
(54,118)(56,73)(57,120)(58,112)(59,62)
(61,64)(66,113)(67,83)(70,87)(71,79)
(75,102)(76,84)(78,91)(80,103)(82,110)
(85,119)(92,98)(107,114), order 2;

b = (2,3)(5,93)(6,29)(7,60)(8,70)
(10,58)(11,66)(12,30)(13,100)(14,53)
(15,104)(16,21)(17,40)(18,19)(20,98)
(22,111)(24,109)(25,45)(26,115)(27,78)
(28,101)(32,97)(33,113)(34,38)(35,57)
(36,44)(37,85)(41,99)(42,73)(43,74)
(48,52)(50,119)(51,69)(54,118)(56,67)
(59,106)(61,64)(63,92)(65,82)(68,95)
(71,79)(72,94)(75,102)(76,120)(80,103)
(81,83)(84,88)(87,110)(89,108)(91,105)
(112,116)(114,117), order 2;

c = (3,29)(4,97)(6,24)(7,76)(8,93)
(10,50)(11,62)(13,16)(14,103)(15,26)
(17,74)(18,52)(19,95)(21,49)(22,90)
(23,55)(25,77)(27,107)(28,113)(30,82)
(31,100)(33,57)(34,61)(35,101)(36,47)
(37,64)(38,105)(39,84)(40,79)(42,92)
(43,58)(44,78)(45,111)(46,108)(48,114)
(53,68)(54,91)(59,60)(63,87)(65,99)
(67,70)(71,72)(73,110)(75,115)(80,117)
(81,96)(85,112)(86,98)(94,119)(102,106)
(104,120)(116,118), order 2;

d = (5,41,93,99)(6,82,51,70)(7,76,60,
120)(8,29,65,69)(10,50,58,119)(11,84,33,
57)(12,67,30,56)(13,44,116,37)(14,80,53,
103)(15,106)(16,78,34,91)(17,79,40,71)
(18,52,19,48)(20,73,63,83)(21,27,38,105)
(22,54,111,118)(23,55)(25,64,45,61)(26,
102,115,75)(28,97,101,32)(31,47)(35,66,
88,113)(36,112,85,100)(39,62)(42,92,81,
98)(43,94)(49,107)(59,104)(68,117)(72,
74)(77,90)(86,96)(87,89,110,108)(95,114),
order 4;

e = (5,115)(7,56)(11,73)(12,76)(20,57)
(22,45)(23,77)(25,111)(26,93)(30,120)(31,
47)(33,83)(35,98)(41,75)(42,66)(43,94)(49,
107)(54,61)(55,90)(60,67)(63,84)(64,118)
(68,117)(72,74)(81,113)(88,92)(95,114)
(99,102), order 2;

f = (8,106)(10,50)(11,63)(13,44)(14,103)
(15,65)(16,78)(18,52)(22,90)(23,111)
(25,77)(26,99)(28,86)(30,60)(35,81)
(38,105)(39,110)(40,79)(45,55)(59,82)
(62,87)(67,120)(70,104)(73,84)(85,112)
(93,102)(96,101)(98,113),
order 2;

g = (4,77)(7,10)(9,55)(11,100)(13,66)
(15,72)(17,102)(22,97)(26,80)(27,84)
(28,61)(32,111)(33,112)(35,91)(39,47)
(40,75)(48,120)(49,62)(52,76)(57,105)
(58,60)(59,95)(64,101)(68,106)
(78,88)(94,104)(103,115)(113,116),
order 2;

h = (10,18)(13,16)(14,40)(17,53)(19,58)
(21,100)(22,25)(23,55)(27,36)(31,49)
(34,116)(37,91)(38,112)(43,95)(44,78)
(45,111)(47,107)(48,119)(50,52)(54,64)
(61,118)(68,74)(71,80)(72,117)(77,90)
(79,103)(85,105)(94,114), order 2.

8.2 Designs and codes from A_6 and A_9

```
//The program, where G=A6 or A9
load simgps;
g:=SimGroup(''G'');
re:=SimRecord(''G'');
ma:=re`Max;
''no. of prim. reps='',#ma;
for k:=1 to #ma do
k,''th prim. rep.'';
gk:=ma[k];
a1,a2,a3:=CosetAction(g,gk);
st:=Stabilizer(a2,1);
orbs:=Orbits(st);
''no. of orbits='',#orbs;
v:=Index(a2,st);
''degree='',v;
pr:=[2,3,5,7];
lo:=[#orbs[i]: i in [1..#orbs]];
''seq. of orbit lengths='',lo;
for j:=2 to #lo do
''orbs no'',j,''of length'',#orbs[j];
blox:=Setseq(orbs[j]^a2);
des:=Design<1,v|blox>;des;
autdes:=AutomorphismGroup(des);
''autgp of order'',Order(autdes);
for i:=1 to #pr do
p:=pr[i];
dc:=LinearCode(des,GF(p));
dl:=Dual(dc);
d1:=Dim(dc);
d2:=Dim(dl);
d3:=Dim(dc meet dl);
''p='',p,''dim='',d1,''dimdual='',
d2,''hull='',d3;
if not ({d1,d2} subset {0,1,v-1,v})
then
if i in {1} then
cau:=PermutationGroup(dc);
''perm gp of order'',Order(cau);
end if;end if;
end for;
```

```
''-----'';
end for;
''.....'';
end for;
------------
//omiting the trivial designs and
//the natural representations
//Results for G=A6, of order 360
.....
$4 th prim. rep.
no. of orbits= 3
degree= 15
seq. of orbit$ lengths= [ 1, 6, 8 ]
orbs no 2 of length 6
1-(15, 6, 6) Design with 15 blocks
autgp of order 720
p= 2 dim= 14 dimdual= 1 hull= 0
p= 3 dim= 9 dimdual= 6 hull= 0
perm gp of order 720
p= 5 dim= 15 dimdual= 0 hull= 0
-----
orbs no 3 of length 8
1-(15, 8, 8) Design with 15 blocks
autgp of order 20160
p= 2 dim= 4 dimdual= 11 hull= 4
perm gp of order 20160
p= 3 dim= 15 dimdual= 0 hull= 0
p= 5 dim= 15 dimdual= 0 hull= 0
-----
.....
5 th prim. rep.
no. of orbits= 3
degree= 15
seq. of orbit lengths= [ 1, 6, 8 ]
orbs no 2 of length 6
1-(15, 6, 6) Design with 15 blocks
autgp of order 720
p= 2 dim= 14 dimdual= 1 hull= 0
p= 3 dim= 9 dimdual= 6 hull= 0
perm gp of order 720
p= 5 dim= 15 dimdual= 0 hull= 0
-----
orbs no 3 of length 8
1-(15, 8, 8) Design with 15 blocks
autgp of order 20160
p= 2 dim= 4 dimdual= 11 hull= 4
perm gp of order 20160
p= 3 dim= 15 dimdual= 0 hull= 0
p= 5 dim= 15 dimdual= 0 hull= 0

---------------------------------
//Results for G=A9 of order 181440
//omiting trivial designs
no. of prim. reps= 8
.....
2 th prim. rep.
no. of orbits= 3
degree= 36
seq. of orbit lengths= [ 1, 14, 21 ]
orbs no 2 of length 14
1-(36, 14, 14) Design with 36 blocks
autgp of order 362880
p= 2 dim= 8 dimdual= 28 hull= 0
perm gp of order 362880
p= 3 dim= 36 dimdual= 0 hull= 0
p= 5 dim= 28 dimdual= 8 hull= 0
p= 7 dim= 35 dimdual= 1 hull= 0
-----
orbs no 3 of length 21
1-(36, 21, 21) Design with 36 blocks
autgp of order 362880
p= 2 dim= 28 dimdual= 8 hull= 0
perm gp of order 362880
p= 3 dim= 27 dimdual= 9 hull= 0
p= 5 dim= 36 dimdual= 0 hull= 0
p= 7 dim= 35 dimdual= 1 hull= 0
-----
.....
3 th prim. rep.
no. of orbits= 4
degree= 84
seq. of orbit lengths= [ 1, 18, 20, 45 ]
orbs no 2 of length 18
1-(84, 18, 18) Design with 84 blocks
autgp of order 362880
p= 2 dim= 56 dimdual= 28 hull= 0
perm gp of order 362880
p= 3 dim= 34 dimdual= 50 hull= 7
p= 5 dim= 84 dimdual= 0 hull= 0
p= 7 dim= 84 dimdual= 0 hull= 0
-----
orbs no 3 of length 20
1-(84, 20, 20) Design with 84 blocks
autgp of order 362880
p= 2 dim= 48 dimdual= 36 hull= 0
perm gp of order 362880
p= 3 dim= 84 dimdual= 0 hull= 0
p= 5 dim= 75 dimdual= 9 hull= 0
p= 7 dim= 84 dimdual= 0 hull= 0
-----
orbs no 4 of length 45
1-(84, 45, 45) Design with 84 blocks
autgp of order 362880
p= 2 dim= 76 dimdual= 8 hull= 0
perm gp of order 362880
p= 3 dim= 34 dimdual= 50 hull= 7
p= 5 dim= 75 dimdual= 9 hull= 0
p= 7 dim= 57 dimdual= 27 hull= 8
-----
.....
4 th prim. rep.
no. of orbits= 3
degree= 120
seq. of orbit lengths= [ 1, 56, 63 ]
orbs no 2 of length 56
1-(120, 56, 56) Design with 120 blocks
autgp of order 348364800
p= 2 dim= 8 dimdual= 112 hull= 8
perm gp of order 348364800
p= 3 dim= 120 dimdual= 0 hull= 0
p= 5 dim= 120 dimdual= 0 hull= 0
p= 7 dim= 119 dimdual= 1 hull= 0
-----
orbs no 3 of length 63
1-(120, 63, 63) Design with 120 blocks
autgp of order 348364800
p= 2 dim= 120 dimdual= 0 hull= 0
p= 3 dim= 36 dimdual= 84 hull= 36
```

```
p= 5 dim= 120 dimdual= 0 hull= 0
p= 7 dim= 119 dimdual= 1 hull= 0
-----
.....
5 th prim. rep.
no. of orbits= 3
degree= 120
seq. of orbit lengths= [ 1, 56, 63 ]
orbs no 2 of length 56
1-(120, 56, 56) Design with 120 blocks
autgp of order 348364800
p= 2 dim= 8 dimdual= 112 hull= 8
perm gp of order 348364800
p= 3 dim= 120 dimdual= 0 hull= 0
p= 5 dim= 120 dimdual= 0 hull= 0
p= 7 dim= 119 dimdual= 1 hull= 0
-----
orbs no 3 of length 63
1-(120, 63, 63) Design with 120 blocks
autgp of order 348364800
p= 2 dim= 120 dimdual= 0 hull= 0
p= 3 dim= 36 dimdual= 84 hull= 36
p= 5 dim= 120 dimdual= 0 hull= 0
p= 7 dim= 119 dimdual= 1 hull= 0
-----
.....
6 th prim. rep.
no. of orbits= 5
degree= 126
seq. of orbit lengths=
[ 1, 5, 20, 40, 60 ]
orbs no 2 of length 5
1-(126, 5, 5) Design with 126 blocks
autgp of order 362880
p= 2 dim= 70 dimdual= 56 hull= 0
perm gp of order 362880
p= 3 dim= 99 dimdual= 27 hull= 0
p= 5 dim= 125 dimdual= 1 hull= 0
p= 7 dim= 126 dimdual= 0 hull= 0
-----
orbs no 3 of length 20
1-(126, 20, 20) Design with 126 blocks
autgp of order 362880
p= 2 dim= 56 dimdual= 70 hull= 0
perm gp of order 362880
p= 3 dim= 126 dimdual= 0 hull= 0
p= 5 dim= 125 dimdual= 1 hull= 0
p= 7 dim= 126 dimdual= 0 hull= 0
-----
orbs no 4 of length 40
1-(126, 40, 40) Design with 126 blocks
autgp of order 362880
p= 2 dim= 48 dimdual= 78 hull= 0
p= 3 dim= 99 dimdual= 27 hull= 0
p= 5 dim= 77 dimdual= 49 hull= 27
p= 7 dim= 99 dimdual= 27 hull= 8
-----
orbs no 5 of length 60
1-(126, 60, 60) Design with 126 blocks
autgp of order 362880
p= 2 dim= 74 dimdual= 52 hull= 26
p= 3 dim= 27 dimdual= 99 hull= 0
p= 5 dim= 125 dimdual= 1 hull= 0
p= 7 dim= 126 dimdual= 0 hull= 0
-----
.....
7 th prim. rep.
no. of orbits= 5
degree= 280
seq. of orbit lengths=
[ 1, 27, 36, 54, 162 ]
orbs no 2 of length 27
1-(280, 27, 27) Design with 280 blocks
autgp of order 362880
p= 2 dim= 232 dimdual= 48 hull= 0
p= 3 dim= 68 dimdual= 212 hull= 41
p= 5 dim= 280 dimdual= 0 hull= 0
p= 7 dim= 280 dimdual= 0 hull= 0
-----
orbs no 3 of length 36
1-(280, 36, 36) Design with 280 blocks
autgp of order 362880
p= 2 dim= 42 dimdual= 238 hull= 42
p= 3 dim= 252 dimdual= 28 hull= 0
p= 5 dim= 280 dimdual= 0 hull= 0
p= 7 dim= 280 dimdual= 0 hull= 0
-----
orbs no 4 of length 54
1-(280, 54, 54) Design with 280 blocks
autgp of order 362880
p= 2 dim= 48 dimdual= 232 hull= 0
p= 3 dim= 125 dimdual= 155 hull= 84
p= 5 dim= 280 dimdual= 0 hull= 0
p= 7 dim= 280 dimdual= 0 hull= 0
-----
orbs no 5 of length 162
1-(280, 162, 162) Design with 280 blocks
autgp of order 362880
p= 2 dim= 68 dimdual= 212 hull= 68
p= 3 dim= 41 dimdual= 239 hull= 41
p= 5 dim= 280 dimdual= 0 hull= 0
p= 7 dim= 280 dimdual= 0 hull= 0
-----
.....
8 th prim. rep.
no. of orbits= 12
degree= 840
seq. of orbit lengths=
[ 1, 8, 24, 24, 27, 36, 72, 72, 72, 72,
216, 216 ]
orbs no 2 of length 8
1-(840, 8, 8) Design with 840 blocks
autgp of order 362880
p= 2 dim= 530 dimdual= 310 hull= 112
p= 3 dim= 624 dimdual= 216 hull= 189
p= 5 dim= 651 dimdual= 189 hull= 56
p= 7 dim= 651 dimdual= 189 hull= 0
-----
orbs no 3 of length 24
1-(840, 24, 24) Design with 840 blocks
autgp of order 181440
p= 2 dim= 322 dimdual= 518 hull= 224
p= 3 dim= 699 dimdual= 141 hull= 21
p= 5 dim= 840 dimdual= 0 hull= 0
p= 7 dim= 840 dimdual= 0 hull= 0
-----
orbs no 4 of length 24
1-(840, 24, 24) Design with 840 blocks
```

```
autgp of order 181440
p= 2 dim= 322 dimdual= 518 hull= 224
p= 3 dim= 699 dimdual= 141 hull= 21
p= 5 dim= 840 dimdual= 0 hull= 0
p= 7 dim= 840 dimdual= 0 hull= 0
-----
orbs no 5 of length 27
1-(840, 27, 27) Design with 840 blocks
autgp of order 362880
p= 2 dim= 616 dimdual= 224 hull= 48
p= 3 dim= 446 dimdual= 394 hull= 41
p= 5 dim= 651 dimdual= 189 hull= 56
p= 7 dim= 784 dimdual= 56 hull= 0
-----
orbs no 6 of length 36
1-(840, 36, 36) Design with 840 blocks
autgp of order 362880
p= 2 dim= 608 dimdual= 232 hull= 190
p= 3 dim= 482 dimdual= 358 hull= 77
p= 5 dim= 771 dimdual= 69 hull= 21
p= 7 dim= 798 dimdual= 42 hull= 0
-----
orbs no 7 of length 72
1-(840, 72, 72) Design with 840 blocks
autgp of order 181440
p= 2 dim= 258 dimdual= 582 hull= 160
p= 3 dim= 182 dimdual= 658 hull= 141
p= 5 dim= 258 dimdual= 582 hull= 83
p= 7 dim= 259 dimdual= 581 hull= 0
-----
orbs no 8 of length 72
1-(840, 72, 72) Design with 840 blocks
autgp of order 181440
p= 2 dim= 546 dimdual= 294 hull= 176
p= 3 dim= 587 dimdual= 253 hull= 141
p= 5 dim= 840 dimdual= 0 hull= 0
p= 7 dim= 840 dimdual= 0 hull= 0
-----
orbs no 9 of length 72
1-(840, 72, 72) Design with 840 blocks
autgp of order 181440
p= 2 dim= 546 dimdual= 294 hull= 176
p= 3 dim= 587 dimdual= 253 hull= 141
p= 5 dim= 840 dimdual= 0 hull= 0
p= 7 dim= 840 dimdual= 0 hull= 0
-----
orbs no 10 of length 72
1-(840, 72, 72) Design with 840 blocks
autgp of order 181440
p= 2 dim= 258 dimdual= 582 hull= 160
p= 3 dim= 182 dimdual= 658 hull= 141
p= 5 dim= 258 dimdual= 582 hull= 83
p= 7 dim= 259 dimdual= 581 hull= 0
-----
orbs no 11 of length 216
1-(840, 216, 216) Design with 840 blocks
autgp of order 362880
p= 2 dim= 306 dimdual= 534 hull= 160
p= 3 dim= 230 dimdual= 610 hull= 230
p= 5 dim= 595 dimdual= 245 hull= 0
p= 7 dim= 595 dimdual= 245 hull= 0
-----
orbs no 12 of length 216
1-(840, 216, 216) Design with 840 blocks
autgp of order 362880
p= 2 dim= 418 dimdual= 422 hull= 98
p= 3 dim= 446 dimdual= 394 hull= 41
p= 5 dim= 554 dimdual= 286 hull= 104
p= 7 dim= 714 dimdual= 126 hull= 0
```

References

[1] E. F. Assmus, Jr. and J. D. Key. *Designs and their Codes.* Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] Wieb Bosma and John Cannon. *Handbook of Magma Functions.* Department of Mathematics, University of Sydney, November 1994.

[3] Andries E. Brouwer. Strongly regular graphs. In Charles J. Colbourn and Jeffrey H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 667–685. CRC Press, Boca Raton, 1996. VI.5.

[4] R. W. Carter. *Simple Groups of Lie Type.* London and New York, Wiley-Interscience, 1972.

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

[6] Leonard Eugene Dickson. *Linear Groups with an Exposition of the Galois Field Theory.* New York: Dover Publications, 1958. With an introduction by Wilhelm Magnus.

[7] Jean Dieudonné. *La Géométrie des Groupes Classiques.* Ergebnisse der Mathematik und ihrer Grenzbegiete, Neue Folge, Band 5. Berlin, Göttingen, Heidelberg: Springer-Verlag, second edition, 1963.

[8] D. M. Gordon. Minimal permutation sets for decoding the binary Golay codes. *IEEE Trans. Inform. Theory*, 28:541–543, 1982.

[9] W. Cary Huffman. Codes and groups. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 17.

[10] B. Huppert. *Endliche Gruppen I.* Berlin, Heidelberg: Springer Verlag, 1967.

[11] J. D. Key and J. Moori. Designs, codes and graphs from the Janko groups J_1 and J_2. J. Combin. Math and Combin. Comput.: To appear.

[12] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43:485–505, 1964.

[13] R. Steinberg. Automorphisms of finite linear groups. *Canad. J. Math.*, 12:606–615, 1960.