On the stabilizers of the minimum-weight codewords of the binary codes from triangular graphs

B. G. Rodrigues *
School of Mathematical and Statistical Sciences
University of KwaZulu-Natal
Durban 4041
South Africa

August 6, 2004

Abstract

The stabilizers of the minimum-weight codewords of the binary codes obtained from the strongly regular graphs $T(n)$ defined by the primitive rank-3 action of the alternating groups A_n where $n \geq 5$, on $\Omega^{\{2\}}$, the set of duads of $\Omega = \{1, 2, \cdots, n\}$ are examined. For a codeword w of minimum-weight in the binary code C obtained as stated above, from an adjacency matrix of the triangular graph $T(n)$ defined by the primitive rank-3 action of the alternating groups A_n where $n \geq 5$, on $\Omega^{\{2\}}$, the set of duads of $\Omega = \{1, 2, \cdots, n\}$, we determine the stabilizer $\mathrm{Aut}(C)_w$ in $\mathrm{Aut}(C)$ and show that $\mathrm{Aut}(C)_w$ is a maximal subgroup of $\mathrm{Aut}(C)$.

1 Introduction

The simple alternating group A_n, where $n \geq 5$, acts as a primitive rank-3 group of degree $\binom{n}{2}$ on the 2-subsets, $\Omega^{\{2\}}$ where $\Omega = \{1, 2, \cdots, n\}$. The orbits of the stabilizer in A_n of a 2-subset $P = \{a, b\}$ consist of $\{P\}$ and one of length $2(n-2)$ and the other of length $\binom{n-2}{2}$. We take as points the 2-subsets of Ω and for each $P \in \Omega^{\{2\}}$ we define a block $\bar{P}$ to be $\{Q \in \Omega^{\{2\}} \mid P \cap Q \neq \emptyset, Q \neq P\}$, i.e. the members of the orbit

*The author acknowledges the hospitality of the School of Mathematics, Statistics and Information Technology at the University of KwaZulu-Natal, Pietermaritzburg during the final preparation of this article.

of length $2(n-2)$. The 2-subsets P and blocks $\bar{P}$ form a symmetric 1-$(\binom{n}{2}, 2(n-2), 2(n-2))$ design whose binary code we will be examining.

An alternative way to approach the designs, graphs and codes that we will be looking at is through the span of the adjacency matrices of the triangular graphs. For any n the triangular graph $T(n)$ is defined to be the line graph of the complete graph K_n. It is a strongly regular graph on $v = \binom{n}{2}$ vertices, i.e. on the pairs of letters $\{i,j\}$ where $i,j \in \{1,\ldots,n\}$. The binary codes formed from the span of adjacency matrices of triangular graphs have been examined by Tonchev [14, p. 171] and Haemers, Peeters and van Rijckevorsel [8, Theorem 4.1] and recently by Key, Moori and Rodrigues [11]. See also [3, 4, 1, 2]. In particular the weight enumerator of these codes are easily determined.

The code of the 1-$(\binom{n}{2}, 2(n-2), 2(n-2))$ design obtained by taking the rows of the incidence matrix as the incidence vectors of the blocks is also the code formed by the span of the adjacency matrix of the triangular graph $T(n)$; the automorphism group of this design will contain the automorphism group of the graph, the latter of which is easily seen to be S_n. Similarly, the automorphism group of the code will contain S_n. However for $n = 6$ the group of the design and code is larger than the group of the graph (S_6), and we will use the code to explain this.

In [11] we studied the binary code C obtained from an adjacency matrix of the triangular graph $T(n)$ and permutation decoding. Here for a codeword w of minimum-weight in the binary code C obtained as stated above, from an adjacency matrix of the triangular graph $T(n)$ defined by the primitive rank-3 action of the alternating groups A_n where $n \geq 5$, on $\Omega^{\{2\}}$, the set of duads of $\Omega = \{1, 2, \cdots, n\}$, we determine the stabilizer $\mathrm{Aut}(C)_w$ in $\mathrm{Aut}(C)$ and show that $\mathrm{Aut}(C)_w$ is a maximal subgroup of $\mathrm{Aut}(C)$.

In Section 2 we give the necessary definitions and background, in Section 3 we give a brief overview of the primitive rank-3 action of the alternating groups A_n on the 2-subsets, $\Omega^{\{2\}}$ where $\Omega = \{1, 2, \cdots, n\}$. In Section 4 we describe the nature of the binary codes of the triangular graphs $T(n)$ for $n \geq 5$ and the nature of the minimum-weight codewords.

Since the alternating group A_n acts as an automorphism group of C, in Section 5 we determine the stabilizer $(A_n)_w$ of a word of minimum-weight w in C and show that $(A_n)_w \cong S_{n-2}$, for $n \geq 6$ and even. Similarly we show that $(A_n)_w \cong A_{n-1}$, for $n \geq 5$ and odd. In all cases $(A_n)_w$ are maximal subgroups of A_n.

Further in Section 6 by extending the results of Section 5 to S_n we show that for $n \geq 8$ and even $(S_n)_w \cong S_{n-2} \times 2$. If $n = 6$, however $(A_8)_w \cong 2^3{:}L_3(2)$. Also for $n \geq 5$ and odd we show that $(S_n)_w \cong S_{n-1}$.

2 Background and terminology

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. The design is **symmetric** if it has the same number of points and blocks.

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. 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 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** (or **parity-check**) matrix for C is a generator matrix H 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 $C = C^\perp$. 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 j, 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 **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.

Terminology for **graphs** is standard: the graphs, $\Gamma = (V, E)$ with vertex set V and edge set E, are undirected and the **valency** of a vertex is the number of edges containing the vertex. A graph is **regular** if all the vertices have the same valency; a regular graph is **strongly regular** of type (n, k, λ, μ) if it has n vertices, valency k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices. The **line graph** of a graph $\Gamma = (V, E)$ is the graph $\Gamma^t = (E, V)$ where e and f are adjacent in Γ^t if e and f share a vertex in Γ. The **complete graph** K_n on n vertices has for E the set of all 2-subsets of V. The line graph of K_n is the **triangular graph** $T(n)$,

and it is strongly regular of type $(\binom{n}{2}, 2(n-2), n-2, 4)$. These graphs are unique for $n \neq 8$ and for $n = 8$ there are exactly three other graphs with the same parameters, the so-called Chang graphs: see [4, 8].

The codes are the binary span of the adjacency matrix of the graph. The p-rank of these has been studied by various authors; see [3, 8] for collected results.

The designs and codes in this paper come from the following standard construction, described in [9, Proposition 1] and in [10]:

Result 2.1 *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*

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

and, given $\delta \in \Delta$,

$$\mathcal{E} = \{\{\alpha, \delta\}^g : g \in G\},$$

then $\mathcal{B}$ forms a self-dual 1-$(n, |\Delta|, |\Delta|)$ design with n blocks, and $\mathcal{E}$ forms the edge set of a regular connected graph of valency $|\Delta|$, with G acting as an automorphism group on each of these structures, primitive on vertices of the graph, and on points and blocks of the design.

3 Alternating groups

For a set Ω of size n we shall use the notation $\Omega^{\{k\}}$ to denote the set of all k-subsets (a set of k unordered elements) of Ω for $1 \leq k \leq n$. If $k = 2$ we call $\Omega^{\{2\}}$ the set of all **duads** of Ω. Since $|\Omega| = n$ we have $|\Omega^{\{k\}}| = \binom{n}{k}$. If $\Lambda = \{\sigma_1, \sigma_2, \cdots, \sigma_k\}$ is a k-subset of Ω, then the stabilizer of the "point" Λ in the action of G on $\Omega^{\{k\}}$ is the setwise stabilizer G_Λ in the action of G in Ω. The pointwise stabilizer of Λ in the action of G on Ω is denoted by $G_{[\Lambda]}$. Obviously $G_{[\Lambda]} \leq G_\Lambda$. The permutation representation of G_Λ associated with its action on Λ defines a homomorphism of G_Λ into the symmetric group $S_\Lambda \cong S_k$ with kernel $G_{[\Lambda]}$ and so the factor group $G_\Lambda / G_{[\Lambda]}$ is isomorphic to a subgroup of S_k.

Lemma 3.1 *If $n \geq 3$ then the alternating group A_n acts transitively on $\Omega^{\{2\}}$ the set of duads of $\Omega = \{1, 2, \cdots, n\}$.*

Proof: For if we let $\{\sigma_1, \sigma_2\}$ and $\{\sigma_3, \sigma_4\}$ be duads in $\Omega^{\{2\}}$, then the permutation $(\sigma_1\ \sigma_3)(\sigma_2\ \sigma_4) \in A_n$ moves them accordingly. ■

We now look at the structure of the stabilizer $(A_n)_\Lambda$ of $\Lambda = \{\sigma_1, \sigma_2\} \in \Omega^{\{2\}}$ and show that $(A_n)_\Lambda \cong S_{n-2} = (S_n)_{\{\sigma_1, \sigma_2\}}$.

Theorem 3.2 *If $n \geq 5$ then the alternating group A_n, acts primitively as a rank-3 permutation group of degree $\binom{n}{2}$ on $\Omega^{\{2\}}$ where $\Omega = \{1, 2, \cdots, n\}$.*

Proof: That the action is transitive follows from Lemma 3.1. Since A_n acts on $\Omega^{\{2\}}$ and $|\Omega^{\{2\}}| = \binom{n}{2}$ we have that

$$|(A_n)_{\{\sigma_1,\,\sigma_2\}}| = \frac{n!}{2} \times \frac{2}{n(n-1)} = (n-2)!. \tag{1}$$

Now

$$\begin{aligned}(A_n)_{\{\sigma_1,\,\sigma_2\}} &= \{g \in A_n \mid \{\sigma_1,\sigma_2\}^g = \{\sigma_1,\sigma_2\}\} \\ &= \{g \in A_n \mid {\sigma_1}^g = \sigma_1, {\sigma_2}^g = \sigma_2 \text{ or } {\sigma_1}^g = \sigma_2, {\sigma_2}^g = \sigma_1\}.\end{aligned}$$

Clearly

$$(A_n)_{[\sigma_1,\sigma_2]} = A_{n-2} \leq (A_n)_{\{\sigma_1,\,\sigma_2\}}$$

and

$$K = \{(\sigma_1\ \sigma_2)\cdot\alpha \mid \alpha \in (S_n)_{[\sigma_1,\sigma_2]},\ \ \alpha \text{ is odd}\} \leq (A_n)_{\{\sigma_1,\,\sigma_2\}}.$$

Thus $A_{n-2} \cup K \leq (A_n)_{\{\sigma_1,\,\sigma_2\}}$ and

$$|A_{n-2} \cup K| = |A_{n-2}| + |K| = 2|A_{n-2}| = \frac{2(n-2)!}{2} = (n-2)! = |(A_n)_{\{\sigma_1,\,\sigma_2\}}|,$$

by (1) .

Hence $(A_n)_{\{\sigma_1,\,\sigma_2\}} = A_{n-2} \cup K$. Since

$$(A_n)_{\{\sigma_1,\sigma_2\}} \leq A_n, \quad |(A_n)_{\{\sigma_1,\,\sigma_2\}}| = 2|A_{n-2}| = |S_{n-2}|$$

and $A_{n-2} = (A_n)_{[\sigma_1,\sigma_2]} \leq (A_n)_{\{\sigma_1,\sigma_2\}}$, we can deduce that $(A_n)_{\{\sigma_1,\,\sigma_2\}} \cong S_{n-2}$.

The group $(A_n)_{\{\sigma_1,\,\sigma_2\}}$ has three orbits $\{\{\sigma_1,\,\sigma_2\}\}$, $\{\sigma_i, \gamma \mid i \in \{1,2\}, \gamma \in \Omega \setminus \{\sigma_1,\,\sigma_2\}\}$ and $\{\gamma,\mu \mid \gamma,\mu \in \Omega \setminus \{\sigma_1,\,\sigma_2\}, \gamma \neq \mu\}$. These orbits have lengths 1, $2(n-2)$ and $\frac{(n-2)(n-3)}{2}$, respectively. Now any non-trivial block for the action of A_n on $\Omega^{\{2\}}$ which contains the point $\{\sigma_1,\sigma_2\}$ must also contain one of the other orbits of $(A_n)_{\{\sigma_1,\,\sigma_2\}}$. However, a simple argument shows that for $n \neq 4$ such a block must also contain the other orbit, and so the action of A_n on $\Omega^{\{2\}}$ is primitive. Now since $(A_n)_{\{\sigma_1,\,\sigma_2\}}$ is the stabilizer of a point in the action of A_n on $\Omega^{\{2\}}$ and A_n is primitive we have that $(A_n)_{\{\sigma_1,\,\sigma_2\}}$ is maximal. ■

4 The binary codes

In all the following we will take G to be the simple alternating group A_n, where $n \geq 5$, in its natural primitive rank-3 action of degree $\binom{n}{2}$ on $\Omega^{\{2\}}$ where $\Omega = \{1, 2, \cdots, n\}$. For the orbits Δ of the stabilizer of a point, as described in Result 2.1, we take the one of length $2(n-2)$ and get a symmetric 1-$(\binom{n}{2}, 2(n-2), 2(n-2))$ design $\mathcal{D}$.

Alternatively let n be any integer and let $T(n)$ denote the triangular graph with vertex set $\mathcal{P}$ the $\binom{n}{2}$ 2-subsets of a set Ω of size n. The 1-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ will have point set $\mathcal{P}$ and for each point (2-subset) $\{a, b\} \in \mathcal{P}$, $a \neq b$, $a, b \in \Omega$, a block, which we denote by $\overline{\{a, b\}}$, is defined in the following way:

$$\overline{\{a, b\}} = \{\{a, x\}, \{b, y\} \mid x \neq a, b;\ y \neq a, b\}.$$

Then

$$\mathcal{B} = \{\ \overline{\{a, b\}} \mid a, b \in \Omega,\ a \neq b\}.$$

The incidence vector of the block $\overline{\{a, b\}}$ is then

$$v^{\overline{\{a,b\}}} = \sum_{x \neq a} v^{\{a,x\}} + \sum_{y \neq b} v^{\{b,y\}} \tag{2}$$

where, as usual with the notation from [1], the incidence vector of the subset $X \subseteq \mathcal{P}$ is denoted by v^X. Since our points here are actually pairs of elements from Ω, note that we are using the notation $v^{\{a,b\}}$ instead of $v^{\{\{a,b\}\}}$, as discussed in [1]. Clearly G acts as an automorphism group on $\mathcal{D}$ on C, $C^\perp$, and on $T(n)$. With the exception of $n = 6$ we have that the full automorphism of $\mathcal{D}$ is S_n which is in turn the automorphism group of C. When $n = 6$ the automorphism group of both design and code is the alternating group $A_8 \cong PGL_4(2)$.

To avoid trivial cases we will take $n \geq 5$. Then in all the following C will denote the binary code of $\mathcal{D}$ and of $T(n)$ and we shall henceforth refer to these binary codes as the binary codes of the triangular graphs.

First we summarize some results on these codes, the weight enumerator and their automorphism groups, that we will be needing. The proofs can be found in [11].

The following lemma follows easily and is mentioned in [8]. Note that in this lemma, the notation $< i, A(i) >$ denotes the fact that there are $A(i)$ vectors of weight i. Here we only prove the first part of the lemma. For the remaining facts, see [11].

Lemma 4.1 *Let C be the binary code obtained by the row span of an adjacency matrix for the triangular graph $T(n)$, where $n \geq 5$.*

If $n = 2m$ is even then C is a $[\binom{2m}{2}, 2m-2, 4(m-1)]_2$ code with weight distribution

Table 1
The weight distribution of C

i	$A(i)$
0	1
$4(m-1)$	$\binom{2m}{2}$
$8(m-2)$	$\binom{2m}{4}$
$\vdots$	$\vdots$
m^2	$\frac{1}{2}\binom{2m}{m}$

if m is even, and weight distribution

Table 2
The weight distribution of C

i	$A(i)$
0	1
$4(m-1)$	$\binom{2m}{2}$
$8(m-2)$	$\binom{2m}{4}$
$\vdots$	$\vdots$
m^2-1	$\binom{2m}{m-1}$

if m is odd. If n is odd, then C is a $[\binom{n}{2}, n-1, n-1]_2$ code with weight distribution

Table 3
The weight distribution of C

i	$A(i)$
0	1
$n-1$	n
$\vdots$	$\vdots$
$2i(n-2i)$	$\binom{n}{2i}$
$\vdots$	$\vdots$

where $1 \leq i \leq (n-1)/2$.
The automorphism group of C is S_n unless $n = 6$, in which case it is $PGL_4(2) \cong A_8$.

Proof: The dimension of these codes is well documented and not hard to deduce: see [3]. It is easy to see that the sum of the incidence vectors for i disjoint duads will give a vector of C of weight $2i(n-2i)$. Clearly we must have $i \leq \lfloor \frac{n}{2} \rfloor$ and for n even, at $i = \frac{n}{2}$, we get the zero vector. Thus for $n = 2m$ even we get increasing weights from a minimum of $2(n-2)$ up to a maximum when $i = \lfloor \frac{m}{2} \rfloor$, and the weight distribution is seen by simple counting to be as given in the statement, distinct cases for m even and m odd. In this case of n even the minimum-weight vectors are then the incidence vectors of the blocks of the design.

If n is odd, the maximum number of disjoint duads is $\frac{n-1}{2}$, and all the weights are distinct, with a minimum when $i = \frac{n-1}{2}$, i.e. weight $n-1$. ■

Now if w is a codeword of minimum-weight in C, in Sections 5 and 6 we determine respectively the structures of $(A_n)_w$ and $(S_n)_w$, i.e, the stabilizers of w in A_n and in the automorphism group of the code C, which is the symmetric group S_n.

Since A_n acts as an automorphism group of C, in Section 5, Lemmas 5.1 and 5.2 deal with the action of A_n on the minimum-weight codewords of C. Furthermore, since the automorphism group of C is the symmetric group S_n, in Lemmas 6.1 and 6.2 of Section 6 we consider the action of S_n.

5 Stabilizer in A_n of a minimum-weight codeword

In Lemma 5.1 and Lemma 6.1 we deal with the cases where $n \geq 8$, and even and in particular when $n = 6$. In Lemma 5.2 and Lemma 6.2 we address the cases where $n \geq 5$, and odd.

Lemma 5.1 *For $n \geq 6$ and even, the stabilizer in A_n of a word of minimum-weight w in C is a maximal subgroup of A_n of index $\binom{n}{2}$. Furthermore $(A_n)_w \cong S_{n-2}$.*

Proof: Let $C_{2(n-2)} = \{w \in C \mid \mathrm{wt}(w) = 2(n-2),$ where $n \geq 6$ and even$\}$, (where wt(w), represents de weight of a codeword w in C) denote the set of minimum weight codewords in C. Since A_n is an automorphism group of C it preserves the weight class of C, therefore it preserves $C_{2(n-2)}$. Now, from Table 1 of Lemma 4.1 we have that $A(i) = |C_{2(n-2)}| = \binom{n}{2}$ for any $n \geq 6$. Now, since A_n is $(n-2)$-transitive on n points it is transitive on $\binom{n}{2}$ points. From this we deduce that A_n is transitive on $C_{2(n-2)}$, ie, $w^{A_n} = C_{2(n-2)}$ for any $w \in C_{2(n-2)}$. Hence $|C_{2(n-2)}| = \frac{|A_n|}{|(A_n)_w|}$. So it follows that $\binom{n}{2} = \frac{\frac{n!}{2}}{|(A_n)_w|}$ and thus $|(A_n)_w| = (n-2)!$. That the index of $(A_n)_w$ in A_n is $\binom{n}{2}$ is routine.

The $\binom{n}{2}$ minimum-weight codewords are the incidence vectors of the blocks of the design $\mathcal{D}$, so the design formed by taking the words of minimum-weight as blocks is precisely the design $\mathcal{D}$. But by Result 2.1 we know that A_n acts primitively on points and blocks of $\mathcal{D}$ so the maximality of $(A_n)_w$ in A_n follows. By Lemma 3.2 we deduce that $(A_n)_w \cong S_{n-2}$. ■

Remark: From Lemma 5.1 we observe that the minimum-weight codewords are precisely the blocks of $\mathcal{D}$ and so it follows S_{n-2} is a block stabilizer in $\mathcal{D}$.

Lemma 5.2 *For $n \geq 5$ and odd, the stabilizer in A_n of a word of w of minimum-weight in C is a maximal subgroup of A_n of index n. Moreover $(A_n)_w \cong A_{n-1}$.*

Proof: Observe from Lemma 4.1 that if w is a word of minimum-weight in C the size of C_{n-1} is n. Transitivity of A_n on C_{n-1} follows using a similar argument to that in the proof of Lemma 5.1. Now $|C_{n-1}| = \frac{|A_n|}{|(A_n)_w|}$ from which follows that $|(A_n)_w| = \frac{(n-1)!}{2}$ and certainly $[A_n{:}(A_n)_w] = n$. From the previous statement we get that $(A_n)_w$ is a maximal subgroup of A_n and we can easily deduce that $(A_n)_w \cong A_{n-1}$. ■

6 Stabilizer in S_n of a minimum-weight codeword

Since the automorphism group of the code is the symmetric group S_n, for all $n \geq 5$ except when $n = 6$ in this section we deal with the stabilizers $(S_n)_w$ by extending the results of Section 5 to S_n. Notice from Lemma 4.1 that the case $n = 6$ is an exception, since the automorphism group of both design and code is not the symmetric group S_6. The automorphism group of both design and code is the alternating group $A_8 \cong PGL_4(2)$. We show then that $(A_8)_w$ is a maximal subgroup of A_8 isomorphic to $2^3{:}L_3(2)$.

Lemma 6.1 *For $n \geq 8$ and even, the stabilizer in the automorphism group of C, of a minimum-weight codeword w in C is a maximal subgroup of S_n of index $\binom{n}{2}$. Moreover $(S_n)_w \cong S_{n-2} \times 2$. If $n = 6$, then $(A_8)_w \cong 2^3{:}L_3(2)$.*

Proof: We first prove that the stabilizer in S_n of a word w of minimum weight in C, ie, $(S_n)_w$ is a maximal subgroup of S_n and finally show that for $n = 6$, $(A_8)_w$ is a maximal subgroup of A_8. From Lemma 4.1 we have that the minimum weight of C is $2(n-2)$, for either cases of m when $n \geq 8$ and even. Define $C_{2(n-2)} = \{w \in C \mid \mathrm{wt}(w) = 2(n-2),$ where $n \geq 8$ and even$\}$, to be the set of minimum weight codewords in C. Let $w \in$

$C_{2(n-2)}$, once again by Lemma 4.1 we have that there exists $g \in S_n$ such that $w^g = w'$, for $w, w' \in C_{2(n-2)}$. So, the action of $\mathrm{Aut}(C) = S_n$ on $C_{2(n-2)}$ is transitive. Therefore $|C_{2(n-2)}| = \frac{|S_n|}{|(S_n)_w|}$. Now, since $|C_{2(n-2)}| = \binom{n}{2}$ (see Table 1) for any $n \geq 8$, it follows that $\binom{n}{2} = \frac{n!}{|(S_n)_w|}$ and so $|(S_n)_w| = 2(n-2)!$. From these calculations we deduce that $[S_n{:}(S_n)_w] = \frac{n!}{2(n-2)!} = \binom{n}{2}$.

Now the $\binom{n}{2}$ minimum-weight codewords are the incidence vectors of the blocks of the design $\mathcal{D}$, so the design formed by taking the words of minimum-weight as blocks is precisely the design $\mathcal{D}$. Since S_n acts primitively on the set of duads of Ω and these are precisely the $\binom{n}{2}$ points of $\mathcal{D}$, and since the minimum-weight codewords are the blocks of $\mathcal{D}$, the maximality of $(S_n)_w$ in S_n follows. Now by the Atlas [7] we have that a maximal subgroup of S_n of index $\binom{n}{2}$ is isomorphic to the subgroup $S_{n-2} \times 2$, whenever $n \geq 8$ and even.

Finally for $n = 6$ we have that C is a $[15, 4, 8]_2$ binary code whose automorphism group is the alternating group A_8. Here the set C_8 of minimum-weight codewords consists of $\binom{6}{2} = 15$ codewords. Using the above argument we have that $15 = \frac{|A_8|}{|(A_8)_w|}$ and so $|(A_8)_w| = \frac{20160}{15} = 1344$, and hence a maximal subgroup of A_8 (see Atlas [7]). From the list of maximal subgroups of A_8 we deduce that $(A_8)_w \cong 2^3{:}L_3(2)$. ■

Remark: From Lemma 6.1 we observe that the minimum-weight codewords are precisely the blocks of $\mathcal{D}$ and so it follows that $\mathrm{Aut}(C)_w$ is a block stabilizer in $\mathcal{D}$.

Lemma 6.2 *Let w be a minimum-weight codeword in C. Then the stabilizer $(S_n)_w$ is a maximal subgroup of index n in S_n. Moreover $(S_n)_w \cong S_{n-1}$ for all $n \geq 5$ and odd.*

Proof: First notice that the support of a codeword w of minimum-weight in C is $n-1$, whenever $n \geq 5$ and odd, and that there are n such codewords. That S_n is transitive on C_{n-1} follows from Lemma 4.1. The maximality of $(S_n)_w$ follows from the fact that $|(S_n)_w| = (n-1)!$. That $(S_n)_w \cong S_{n-1}$ follows easily. ■

Lemma 6.3 *$(A_n)_w$ is a maximal normal subgroup of $(S_n)_w$, for all $n \geq 8$ and even. If $n = 6$ then S_4 is neither a maximal nor a normal subgroup of $2^3{:}L_3(2)$.*

Proof: It is obvious that $(A_n)_w \leq (S_n)_w$. Since A_n is a maximal subgroup of S_n so will $(A_n)_w$ be a maximal subgroup of $(S_n)_w$. The normality of $(A_n)_w$ in $(S_n)_w$ follows at once by finding the index of $(A_n)_w$ in $(S_n)_w$. Observe that $[(S_n)_w{:}(A_n)_w] = \frac{2\times(n-2)!}{(n-2)!} = 2$, and so the result. For $n = 6$

we have that $[(2^3{:}L_3(2)){:}S_4] = 56$ and $2^3{:}L_3(2)$ has no maximal subgroup of index 56. Also S_4 is not a normal subgroup of $2^3{:}L_3(2)$. In fact the normal subgroups of $2^3{:}L_3(4)$ are 1_H, where $H = 2^3{:}L_3(2)$, an elementary abelian group of type 2^3, and $2^3{:}L_3(2)$, respectively.■

Lemma 6.4 *$(A_n)_w$ is a maximal normal subgroup of $(S_n)_w$, for all $n \geq 5$ and odd.*

Proof: The result follows using a similar argument to the first part of the proof of Lemma 6.3. ■

7 Observations

The determination of the stabilizers of the minimum-weight codewords gives a new approach to constructing the maximal subgroups of both the alternating groups and the symmetric groups for $n \geq 5$.

References

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

[2] E. F. Assmus, Jr. and J. D. Key, *Designs and codes: an update*, Des. Codes Cryptogr. 9 (1996), 7–27.

[3] A. E. Brouwer and C. J. van Eijl, *On the p-rank of the adjacency matrices of strongly regular graphs*, J. Algebraic Combin. 1 (1992), 329–346.

[4] A. E. Brouwer and J.H. van Lint, *Strongly regular graphs and partial geometries*, Enumeration and Design (1982 In D.M. Jackson & S.A. Vanstone, Waterloo, ed.), Academic Press, Toronto, 1984, Proc. Silver Jubilee Conf. on Combinatorics, Waterloo, 1982, pp. 85–122.

[5] P. J. Cameron, *Permutation Groups*, Cambridge University Press, Cambridge, 1999, London Math. Soc. Students Text, 45.

[6] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their Links*, Cambridge University Press, Cambridge, 1991, London Mathematical Society Student Texts 22.

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

[8] W. H. Haemers, R. Peeters, and J. M. van Rijckevorsel, *Binary codes of strongly regular graphs*, Des. Codes Cryptogr. **17** (1999), 187–209.

[9] 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. **40** (2002), 143–159.

[10] J. D. Key, J. Moori, and B. G. Rodrigues, *On some designs and codes from primitive representations of some finite simple groups*, J. Combin. Math and Combin. Comput. **45** (2003), 3–19.

[11] J. D. Key, J. Moori, and B. G. Rodrigues, *Permutation decoding for the binary codes from triangular graphs*, European J. Combin. **25** (2004), 113–123.

[12] J. Moori and B. G. Rodrigues, *A self-orthogonal doubly-even code invariant under the M^cL:2 group*, J. Combin. Theory, Ser. A, To appear.

[13] B. G. Rodrigues, *Codes of Designs and Graphs from Finite Simple Groups*, Ph.D. thesis, University of Natal, Pietermaritzburg, 2002.

[14] Vladimir D. Tonchev, *Combinatorial Configurations Designs, Codes, Graphs*, Pitman Monographs and Surveys in Pure and Applied Mathematics, No. 40, Longman, New York, 1988, Translated from the Bulgarian by Robert A. Melter.