Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®
European Journal of Combinatorics 25 (2004) 113–123

European Journal of Combinatorics

www.elsevier.com/locate/ejc

Permutation decoding for the binary codes from triangular graphs

J.D. Key[a], J. Moori[b], B.G. Rodrigues[b]

[a]*Department of Mathematical Sciences, Clemson University, Clemson SC 29634, USA*
[b]*School of Mathematics, Statistics and Information Technology, University of Natal-Pietermaritzburg, Pietermaritzburg 3209, South Africa*

Received 2 April 2003; received in revised form 7 August 2003; accepted 7 August 2003

Abstract

By finding explicit PD-sets we show that permutation decoding can be used for the binary code obtained from an adjacency matrix of the triangular graph $T(n)$ for any $n \geq 5$.

1. Introduction

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 [12, p. 171] and Haemers et al. [7, Theorem 4.1] (see also [1, 2, 4, 5]). Note that the dimension and weight enumerator are easily determined. Here we examine the codes and their duals further, and in particular show how the case $n = 6$ distinguishes itself. We prove (Proposition 3.4) that S_n is the full automorphism group of the code for $n \geq 5$ except in the case $n = 6$. We also look at the question of minimum-weight generators for the code, and for its dual, and use these to obtain explicit permutation-decoding sets for the code:

Theorem 1.1. *Let $\mathcal{I}$ denote the subset*

$$P_1 = \{1, n\}, P_2 = \{2, n\}, \ldots, P_{n-1} = \{n-1, n\}$$

of vertices of the triangular graph $T(n)$ where $n \geq 5$, and let C denote a binary code of $T(n)$ with $\mathcal{I}$ in the first $n-1$ positions. Then

E-mail address: keyj@ces.clemson.edu (J.D. Key).

0195-6698/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2003.08.001

(1) *C is a $\left[\binom{n}{2}, n-1, n-1\right]_2$ code for n odd and, with $\mathcal{I}$ as the information positions,*

$$\mathcal{S} = \{1_G\} \cup \{(i,n) \mid 1 \le i \le n-1\}$$

is a PD-set for C of n elements in S_n;

(2) *C is a $\left[\binom{n}{2}, n-2, 2(n-1)\right]_2$ code for n even, and with $\mathcal{I}$ excluding P_{n-1} as the information positions,*

$$\mathcal{S} = \{1_G\} \cup \{(i,n) \mid 1 \le i \le n-1\} \cup \{[(i,n-1)(j,n)]^{\pm 1} \mid 1 \le i, j \le n-2\}$$

is a PD-set for C of $n^2 - 2n + 2$ elements in S_n.

The code formed by the span of the adjacency matrix is also the code of the 1-$\left(\binom{n}{2}, 2(n-2), 2(n-2)\right)$ design obtained by taking the rows of the adjacency matrix as the incidence vectors of the blocks; 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 words of weight-3 in the dual code to explain this: see Lemma 3.2 and Proposition 3.4.

In Section 2 we give the necessary definitions and background, in Section 3 we prove Proposition 3.4 and a number of lemmas concerning the codes, and finally, in Section 4, we prove Theorem 1.1.

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** 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. $C^\perp = \{v \in F^n \mid (v,c) = 0 \text{ for all } c \in C\}$. 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** in a code C over F is one for which all the coordinate entries are either 0 or take a constant non-zero value $a \in F$. The **all-one vector** will be denoted by $\boldsymbol{j}$, and is the constant vector of weight the length of the code and all entries equal to 1. 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 $\left(\binom{n}{2}, 2(n-2), n-2, 4\right)$.

An alternative way to approach the designs, graphs and codes that we will be looking at is through the primitive rank-3 action of the simple alternating group A_n, for $n \geq 5$, on the 2-subsets, $\Omega^{\{2\}}$, of a set Ω of size 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 of length $2(n-2)$. The 2-subsets P and blocks $\bar{P}$ form a symmetric 1-$\left(\binom{n}{2}, 2(n-2), 2(n-2)\right)$ design whose binary code we will be examining.

Permutation decoding was first developed by MacWilliams [9]. The method is described fully in MacWilliams and Sloane [10, Chapter 15] and Huffman [8, Section 8]. A **PD-set** for a t-error-correcting code C is a set $\mathcal{S}$ of automorphisms of C which is such that every possible error vector of weight $s \leq t$ can be moved by some member of $\mathcal{S}$ to another vector where the s non-zero entries have been moved out of the information positions. In other words, every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ to a t-set consisting only of check-position coordinates. That such a set, should it exist, will fully use the error-correction potential of the code follows easily and is proved in Huffman [8, Theorem 8.1]. Furthermore, there is a bound on the minimum size that the set $\mathcal{S}$ may have, due to Gordon [6] (using a result of Schönheim [11]), and quoted and proved in [8, Theorem 8.2]:

Result 2.1. If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n, k, d]_q$ code C, and $r = n-k$, then

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

Note that this is simply the smallest possible size of a PD-set and computations indicate that this bound is only met for some rather small cases.

The algorithm for permutation decoding is as follows: given a t-error-correcting $[n, k, d]_q$ code C with generator matrix $G = [I_k \mid A]$ and check matrix $H = [A^T \mid I_{n-k}]$, for some A, the first k coordinate positions correspond to the information symbols and any vector v of length k 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 weights of the syndromes $H(yg_i)^T$ for $i = 1, \ldots, s$ until an i is found such that the weight is t or less. Find the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

3. The binary codes

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:

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

Thus

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

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

$$v^{\overline{\{a,b\}}} = \sum_{x \neq a} v^{\{a,x\}} + \sum_{y \neq b} v^{\{b,y\}} \tag{1}$$

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]. Further, if a, b, c are distinct points in Ω, we write

$$v^{\overline{\{a,b,c\}}} = v^{\{a,b\}} + v^{\{b,c\}} + v^{\{a,c\}} \tag{2}$$

to denote this vector of weight 3 in the ambient space. Notice also that for any distinct a, b, c,

$$v^{\overline{\{a,b\}}} + v^{\overline{\{a,c\}}} = v^{\overline{\{b,c\}}}. \tag{3}$$

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 $C^\perp$ will be its dual code.

We first quote from [7] the following result, which is easy to obtain, as is the full weight enumerator:

Result 3.1. If n is odd, then C is a $\left[\binom{n}{2}, n-1, n-1\right]_2$ code and if n is even, C is a $\left[\binom{n}{2}, n-2, 2(n-2)\right]_2$ code.

Lemma 3.2. *The minimum weight of $C^\perp$ for $n \geq 5$ is 3 and any word of the form $v^{\overline{\{a,b,c\}}}$, where a, b, c are distinct, is in $C^\perp$. If $n \neq 6$, these are all the words of weight 3 in $C^\perp$, and the number of words of weight 3 is thus $\binom{n}{3}$. If $n = 6$, further words of weight 3 have the form $v^{\{a,b\}} + v^{\{c,d\}} + v^{\{e,f\}}$ where $\Omega = \{a, b, c, d, e, f\}$; in this case there are 35 words of weight 3.*

Proof. First check that the minimum weight cannot be smaller: suppose $w = v^{\{a,b\}} + v^{\{c,d\}}$ where a, b, c, d are all distinct. If $e \in \Omega$ is distinct from all these (such an element will

exist since we are taking $n \geq 5$), then $(w, v^{\overline{\{a,e\}}}) = 1$. If $w = v^{\{a,b\}} + v^{\{a,d\}}$, then $(w, v^{\overline{\{a,b\}}}) = 1$. So the minimum weight is at least 3, and precisely this since it is easy to check that any vector $w = v^{\overline{\{a,b,c\}}}$ as defined in Eq. (2), is in $C^\perp$. Looking for other possible vectors of weight 3 in $C^\perp$, the only case that is not immediately ruled out is $w = v^{\{a,b\}} + v^{\{c,d\}} + v^{\{e,f\}}$ where a, b, c, d, e, f are all distinct (so $n \geq 6$). If there is another element $g \in \Omega$, then $(w, v^{\overline{\{a,g\}}}) = 1$, but if $n = 6$ then $w \in C^\perp$, giving 15 additional weight-3 vectors in $C^\perp$. □

Lemma 3.3. *If n is even then $C \subseteq C^\perp$ and C is doubly-even; if n is odd, $C \oplus C^\perp = F_2^{\mathcal{P}}$. For any n, $\jmath \in C^\perp$.*

Proof. Since blocks are of even size $2(n-2)$, that $\jmath \in C^\perp$ is immediate. For the first statement, consider $(v^{\overline{\{a,b\}}}, v^{\overline{\{c,d\}}})$. If $\{a,b\} = \{c,d\}$ then this is zero. If $d = a$, then the inner product is $n + 2 = 0$ if n is even. If a, b, c, d are all distinct, then the inner product is $4 \equiv 0 \pmod 2$.

For any $a, b \in \Omega$, we have

$$\sum_{c \neq a,b} v^{\overline{\{a,b,c\}}} = \sum_{c \neq a,b} v^{\{a,b\}} + \sum_{c \neq a,b} v^{\{a,c\}} + \sum_{c \neq a,b} v^{\{b,c\}} = (n-2)v^{\{a,b\}} + v^{\overline{\{a,b\}}}.$$

Thus if n is odd, $v^{\{a,b\}} \in C + C^\perp$ for any a, b, while for n even we obtain once again that $v^{\overline{\{a,b\}}} \in C^\perp$. Clearly C is doubly-even when n is even. □

Proposition 3.4. *For $n \geq 5$, the automorphism group of the binary code C of the triangular graph $T(n)$ is S_n unless $n = 6$, in which case the automorphism group of the code is $PGL_4(2) \cong A_8$.*

Proof. In all cases, any automorphism of the graph will define an automorphism of the design and of the code. Since the group of the complete graph is obviously S_n, and the group of its line graph is the same (by a theorem of Whitney [13]), the automorphism group of the code will contain S_n. We now use the fact that, for $n \neq 6$, the automorphism group preserves (and is transitive on) both pairs of letters of Ω and triples of letters of Ω to show that any automorphism of C induces a permutation on Ω. Indeed, for $g \in G = \mathrm{Aut}(C)$, g preserves the words of weight 3 in $C^\perp$, and thus, for $n \neq 6$, g maps pairs of elements to pairs of elements, and triples of elements to triples of elements; this will be used to define an action of g on Ω.

Let $g \in G$. Then g is given as an element of $S_{\binom{n}{2}}$. We wish to define an action of g on Ω. Let $x \in \Omega$. For arbitrary $a, b \in \Omega$, a, b, x distinct, suppose $g : v^{\overline{\{a,b,x\}}} \mapsto v^{\overline{\{a_1,b_1,x_1\}}}$. So a map is induced on triples of elements of Ω by $g : \{a,b,x\} \mapsto \{a_1,b_1,x_1\}$. Since g preserves incidence of points of $\mathcal{D}$ on words of $C^\perp$, i.e. g preserves incidence of pairs of elements of Ω on triples, we have, without loss of generality,

$$g : \begin{cases} \{a,b,x\} & \mapsto \{a_1,b_1,x_1\} \\ \{a,b\} & \mapsto \{a_1,b_1\} \\ \{a,x\} & \mapsto \{a_1,x_1\} \\ \{b,x\} & \mapsto \{b_1,x_1\}. \end{cases}$$

To preserve incidence then we will attempt to define g on Ω by $g : \{a, x\} \cap \{b, x\} \mapsto \{a_1, x_1\} \cap \{b_1, x_1\}$, i.e. $g : x \mapsto x_1$ (and $a \mapsto a_1$, $b \mapsto b_1$).

We need to check that this is indeed well-defined. Take first another triple of the form $\{a, c, x\}$ where $c \neq b$. Since $g : \{a, x\} \mapsto \{a_1, x_1\}$ we must have $\{a_1, x_1\}$ incident with $(\{a, c, x\})^g$, and so $g : \{a, c, x\} \mapsto \{a_1, c_1, x_1\}$. Thus $g : \{c, x\} \mapsto \{c_1, x_1\}$ or $\{a_1, c_1\}$. Suppose $g : \{c, x\} \mapsto \{a_1, c_1\}$ and hence also $g : \{a, c\} \mapsto \{x_1, c_1\}$. Then $(\{b, c, x\})^g$ must contain b_1, x_1, a_1, c_1, and so we must have $b_1 = c_1$. But then $(\{a, b, x\})^g = \{a_1, b_1, x_1\} = \{a_1, c_1, x_1\} = (\{a, c, x\})^g$, which is impossible since g is a permutation on triples. Thus $g : \{c, x\} \mapsto \{x_1, c_1\}$ and again we get $g : x \mapsto x_1$, and $g : c \mapsto c_1$. If we now take any triple $\{x, y, z\}$ containing x, we look first at $\{a, y, x\}$ as above, and then at $\{z, y, x\}$ and have $g : x \mapsto x_1$, as required. Therefore g is defined in S_n, and $\mathrm{Aut}(C) = S_n$.

In case $n = 6$, there are more words of weight 3 in $C^\perp$, so we cannot use this argument since we cannot assume that the vectors of the form $v^{\overline{\{a,b,c\}}}$ are mapped to one another. In this case C is a $[15, 4, 8]_2$ code and its dual is a $[15, 11, 3]_2$ code. A generator matrix for C must thus have every pair of columns linearly independent, i.e. distinct, and so C is the dual of the Hamming code of length 15. Its automorphism group is well known to be $PGL_4(2)$. □

Now we look for bases of minimum-weight vectors for C and $C^\perp$. Clearly if n is even then C has a basis of minimum-weight vectors since the incidence vectors of the blocks are the minimum-weight vectors and span C by definition.

Lemma 3.5. *Let $\Omega = \{a_1, a_2, \ldots, a_n\}$. The set of $n - 1$ vectors*

$$\mathcal{S} = \{v^{\overline{\{a_i, a_{i+1}\}}} \mid 1 \leq i \leq n - 1\}$$

is a spanning set for C. For n odd $\mathcal{S}$ is a basis; for n even $\mathcal{S} \backslash \{v^{\overline{\{a_{n-1}, a_n\}}}\}$ is a basis of minimum-weight vectors.

Proof. Note that for $2 \leq i \leq n$, $v^{\overline{\{a_1, a_i\}}} = \sum_{j=1}^{i-1} v^{\overline{\{a_j, a_{j+1}\}}}$, and thus $v^{\overline{\{a_i, a_j\}}} = v^{\overline{\{a_1, a_i\}}} + v^{\overline{\{a_1, a_j\}}}$ can be written as a sum of vectors in $\mathcal{S}$ and so $\mathcal{S}$ spans C. Since for n odd the size of $\mathcal{S}$ is the dimension of C, the set $\mathcal{S}$ gives a basis for C when n is odd.

If $n = 2m$ we know that $\sum v^{\overline{\{a,b\}}} = 0$, where the sum ranges over a set of m disjoint pairs of elements of Ω. Hence for n even we have, from $\sum_{j=1}^{n-1} v^{\overline{\{a_j, a_{j+1}\}}} = v^{\overline{\{a_1, a_n\}}}$, and $v^{\overline{\{a_1, a_n\}}} + \sum_{j=1}^{m-1} v^{\overline{\{a_{2j}, a_{2j+1}\}}} = 0$, a non-trivial linear relation amongst the vectors in $\mathcal{S}$, from which it follows that the vectors are linearly dependent. Since

$$v^{\overline{\{a_1, a_2\}}} + v^{\overline{\{a_3, a_4\}}} + \cdots + v^{\overline{\{a_{n-1}, a_n\}}} = v^{\overline{\{a_2, a_3\}}} + v^{\overline{\{a_4, a_5\}}} + \cdots + v^{\overline{\{a_{n-2}, a_{n-1}\}}},$$

we can omit $v^{\overline{\{a_{n-1}, a_n\}}}$ from the spanning set. □

Lemma 3.6. *C has a basis of minimum-weight vectors.*

Proof. For n even, this follows from Lemma 3.5. For n odd, the minimum weight of C is $n - 1$ and there are exactly n minimum-weight vectors, which have the form, for

each $a \in \Omega$,

$$w_a = \sum v^{\overline{\{a_i, a_j\}}},$$

where the sum is over a set of $(n-1)/2$ disjoint pairs of elements of $\Omega\backslash\{a\}$. Then for $a \neq b$, we can write

$$w_a + w_b = v + v^{\overline{\{b,c\}}} + v + v^{\overline{\{a,c\}}} = v^{\overline{\{a,b\}}},$$

showing that the w_a span C, and hence C is also spanned by minimum-weight vectors when n is odd. Notice that

$$\begin{aligned}\sum_{i=1}^{n} w_{a_i} &= (w_{a_1} + w_{a_2}) + \cdots + (w_{a_{n-2}} + w_{a_{n-1}}) + w_{a_n} \\ &= v^{\overline{\{a_1,a_2\}}} + \cdots + v^{\overline{\{a_{n-2},a_{n-1}\}}} + w_{a_n} \\ &= w_{a_n} + w_{a_n} = 0,\end{aligned}$$

and thus $\{w_{a_i} \mid 1 \leq i \leq n-1\}$ is a basis for C. □

Lemma 3.7. *$C^{\perp}$ has a basis of minimum-weight vectors for n odd, but not for n even.*

Proof. Take $\Omega = \{1, 2, \ldots, n\}$. For $n \neq 6$, the minimum-weight vectors of $C^{\perp}$ are of the form

$$v^{\overline{\{a,b,c\}}} = v^{\{a,b\}} + v^{\{a,c\}} + v^{\{b,c\}}.$$

Let S be the following set of these vectors:

$$S = \{v^{\overline{\{i,j,j+1\}}} \mid 1 \leq i < j \leq n-1\}.$$

Notice that S has size $\binom{n-1}{2}$. We order the points of $\mathcal{P}$ in the following way:

$$\{1,2\}, \{1,3\}, \ldots, \{1,n-1\}, \{2,3\}, \ldots, \{2,n-1\}, \ldots, \{n-2,n-1\}, \tag{4}$$

followed by the remaining points

$$\{1,n\}, \{2,n\}, \ldots, \{n-1,n\}. \tag{5}$$

We show that for $n \neq 6$ every vector of weight 3 is in the span of S. Using the ordering of the points as given above, it will follow that the vectors in S span a space of dimension $\binom{n-1}{2} = \binom{n}{2} - (n-1)$. Thus for n odd the span of S is the dual code $C^{\perp}$, whereas for n even it is not. In the even case the all-one vector $\boldsymbol{j}$ needs to be adjoined. If this is done at the bottom of the generator matrix for $C^{\perp}$ then the points from Eq. (5) up to $\{n-2, n\}$ can be taken as the last $n-2$ coordinates, while the position corresponding to $\{n-1, n\}$ can be placed in front of this set.

For this, we have, for $1 \leq i < j < j+1 < k \leq n$,

$$v^{\overline{\{i,j,k\}}} = v^{\overline{\{i,j,j+1\}}} + v^{\overline{\{i,j+1,k\}}} + v^{\overline{\{j,j+1,k\}}},$$

and induction will show that every vector of the form $v^{\overline{\{i,j,k\}}}$ is in the span of S. Further, ordering the points as given, and the vectors of S in the same way, by the smallest two elements, produces an upper triangular matrix which clearly has the rank given above. □

Note. The generator matrix obtained for $C^\perp$ in the above ordering can be reduced to the form $[I_k \mid A]$ where k is the dimension of $C^\perp$. If the points are re-ordered with the first k put at the end then the matrix is $[A \mid I_k]$. This is now standard form for the code C, and the corresponding generator matrix for C has the form $[I_{N-k} \mid A^T]$ where $N = \binom{n}{2}$.

4. PD-sets

In this section we prove Theorem 1.1.

In order to get our generator matrix into standard form, as described above, we order the point set $\mathcal{P}$ by taking the set from Eq. (5), i.e.

$$P_1 = \{1, n\}, P_2 = \{2, n\}, \ldots, P_{n-1} = \{n-1, n\}, \tag{6}$$

first, followed by the set from Eq. (4), i.e.

$$P_n = \{1, 2\}, P_{n+1} = \{1, 3\}, \ldots, P_{2n-2} = \{2, 3\}, \ldots, P_{\binom{n}{2}} = \{n-2, n-1\}. \tag{7}$$

The generator matrix for $C^\perp$, using the words of weight 3 (with $\jmath$ if n is even), is then a check matrix for C in standard form. Thus the generator matrix for C will also be in standard form, with the first $n-1$ coordinates the information symbols for n odd, and the first $n-2$ for n even.

Proof of Theorem 1.1. Suppose first that n is odd. Order the points of the coordinate set $\mathcal{P}$ as described in Eqs. (6) and (7) so that the first $n-1$ points are in the information positions.

Now C can correct $t = (n-3)/2$ errors. We need a set $\mathcal{S}$ of elements of $G = S_n = \mathrm{Aut}(C)$ such that every t-set of elements of $\mathcal{P}$ is moved by some element of $\mathcal{S}$ into the check positions. If the $s \leq t$ positions are all in the check positions, then we can use the identity element, 1_G, to keep these in the check positions.

Suppose the $s \leq t$ positions occur at

$$\{a_1, n\}, \{a_2, n\}, \ldots, \{a_r, n\},$$

distinct points in the information positions, and at

$$\{b_1, c_1\}, \{b_2, c_2\}, \ldots, \{b_m, c_m\},$$

distinct points in the check positions, where $r + m = s \leq t$. The number of elements of Ω in the set

$$\mathcal{T} = \{a_1, \ldots, a_r\} \cup \{b_1, \ldots, b_m\} \cup \{c_1, \ldots, c_m\} \subseteq \Omega \backslash \{n\}$$

is at most $r + 2m$. Since $r + m \leq t = (n-3)/2$, we have $2r + 2m \leq n - 3$, and so $r + 2m \leq n - 3$. Thus there are elements other than n in Ω that are not in $\mathcal{T}$; let d be one of these. The transposition $\sigma = (d, n)$ will map the r elements

$$\{a_1, n\}, \{a_2, n\}, \ldots, \{a_r, n\}$$

out of the information positions, as required, and fix the m elements already in the check positions.

It follows that the given set $\mathcal{S} = \{1_G\} \cup \{(i, n) \mid 1 \leq i \leq n-1\}$ forms a PD-set of n group elements for the code. This completes the proof for the case n odd.

Now suppose n is even. Again we order the points as in Eqs. (6) and (7) so that now the points $P_1, P_2, \ldots, P_{n-2}$ are in the information positions, $\mathcal{I}$, and the remaining points of $\mathcal{P}$, starting with $P_{n-1} = \{n-1, n\}$, then followed by $P_n, \ldots, P_{\binom{n}{2}}$, are in the check positions, $\mathcal{E}$. In this case we need to correct $t = n-3$ errors, since the minimum weight is $2(n-2)$.

We claim that

$$\mathcal{S} = \{1_G\} \cup \{(i, n) \mid 1 \leq i \leq n-1\} \cup \{[(i, n-1)(j, n)]^{\pm 1} \mid 1 \leq i, j \leq n-2\}$$

is a PD-set for C. Note that $|\mathcal{S}| = 1 + n - 1 + 2(n-2) + (n-2)(n-3) = n^2 - 2n + 2$.

We need to show that every t-tuple T of points of $\mathcal{P}$ can be moved into the check positions $\mathcal{E}$ by some member of $\mathcal{S}$. Consider the various cases for the members of T:

(i) if all the t positions are in $\mathcal{E}$ then 1_G will do;

(ii) if all the t positions are in $\mathcal{I}$ then $(n-1, n)$ will do;

(iii) if some $a \in \Omega \backslash \{n\}$ does not occur in any member of T then (a, n) will do.

We can thus restrict attention to those sets T for which every $a \in \Omega$ appears in some 2-subset in T. We show that if $\{a, b\} \in T$ and a does not occur again in any element of T, then an element of $\mathcal{S}$ can be found to map T into $\mathcal{E}$. Consider the possible cases:

(iv) $a = n$ and $b = n-1$, then 1_G will do; if $b \neq n-1$, then $(b, n-1)$ will do;

(v) $a \neq n$ and $b = n$ then if $a = n-1$, $(n, n-1)$ will do and if $a \neq n-1$ then $(a, n, n-1) = (a, n)(a, n-1)$ will do;

(vi) $a \neq n$ and $b \neq n$ then if $a = n-1$, $(b, n-1)(b, n)$ will do; if $a \neq n-1$, then if $b = n-1$, (a, n) will do and if $b \neq n-1$, $(a, n)(b, n-1)$ will do.

So if there is a 2-subset $\{a, b\} \in T$ such that a occurs only once, our set of permutations will form a PD-set. Now every $a \in \Omega$ occurs and if every element appears more than once we would have $2n$ elements to place in $2t = 2(n-3)$ positions, which is impossible. □

Note. (1) The computational complexity of the decoding by this method may be quite low, of the order $n^{1.5}$ if the elements of the PD-set are appropriately ordered. The codes are low density parity check (LDPC) codes.

(2) The permutations given in the set $\mathcal{S}$ need to be written as permutations on the points $P_1, P_2, \ldots, P_{\binom{n}{2}}$. Thus, for example, if $n = 6$, then with the ordering of the points as given in Eqs. (6) and (7),

$$(1, 6) \equiv (P_2, P_6)(P_3, P_7)(P_4, P_8)(P_9, P_5)$$

$$(1, 5)(1, 6) \equiv (P_1, P_9, P_5)(P_2, P_6, P_{12})(P_3, P_7, P_{14})(P_4, P_8, P_{15}).$$

(3) For $n \geq 5$ odd the lower bound in Result 2.1 has an explicit form, i.e. $(n-1)/2$. This follows directly from the given formula.

(4) For n even the lower bound of Result 2.1 is not as easily simplified. From computations (using Magma [3]) up to a large value of n, the following formula appears

to hold for this bound for $n \geq 18$ (smaller values of n seem to be unrepresentative of the general rule): writing $k \equiv \frac{n-18}{2} \pmod 6 \in \{0, 1, 2, 3, 4, 5\}$, the lower bound for n is

$$n - 2 + 10\left\lfloor \frac{n-6}{12} \right\rfloor + k + \left\lfloor \frac{k}{2} \right\rfloor.$$

In this case the size of the PD-sets we have found are of the order of n^2; some Magma output below illustrates the comparison of this with the lower bound. The first column gives the value of n, the second the code length, the third the number of errors corrected, the fourth the value of the lower bound, and the fifth the size of the PD-set we constructed.

```
n,  length,  n-3,  bound,  PDset
 6     15      3      5        26
 8     28      5      8        50
10     45      7     11        82
12     66      9     15       122
14     91     11     18       170
16    120     13     22       226
18    153     15     26       290
20    190     17     29       362
22    231     19     33       442
24    276     21     36       530
26    325     23     40       626
28    378     25     43       730
30    435     27     48       842
32    496     29     51       962
34    561     31     55      1090
36    630     33     58      1226
38    703     35     62      1370
40    780     37     65      1522
```

Acknowledgements

The first author thanks the School of Mathematics, Statistics and Information Technology at the University of Natal-Pietermaritzburg for their hospitality. This work was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research under Grant N00014-00-1-0565, and NSF grant #9730992. The second author acknowledges the support of NRF and the University of Natal (URF). The third author acknowledges the post-graduate scholarship of DAAD (Germany) and the Ministry of Petroleum (Angola).

References

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

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

[3] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, November 1994. Available from http://www.maths.usyd.edu.au:8000/u/magma/.
[4] A.E. Brouwer, C.J. van Eijl, On the p-rank of the adjacency matrices of strongly regular graphs, J. Algebraic Combin. 1 (1992) 329–346.
[5] A.E. Brouwer, J.H. van Lint, Strongly regular graphs and partial geometries, in: D.M. Jackson, S.A. Vanstone (Eds.), Enumeration and Design, Proc. Silver Jubilee Conf. on Combinatorics, Waterloo, 1982, Academic Press, Toronto, 1984, pp. 85–122.
[6] D.M. Gordon, Minimal permutation sets for decoding the binary Golay codes, IEEE Trans. Inform. Theory 28 (1982) 541–543.
[7] W.H. Haemers, R. Peeters, J.M. van Rijckevorsel, Binary codes of strongly regular graphs, Des. Codes Cryptogr. 17 (1999) 187–209.
[8] W.C. Huffman, Codes and groups, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, part 2, vol. 2, Elsevier, Amsterdam, 1998, pp. 1345–1440 (Chapter 17).
[9] F.J. MacWilliams, Permutation decoding of systematic codes, Bell System Tech. J. 43 (1964) 485–505.
[10] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1983.
[11] J. Schönheim, On coverings, Pacific J. Math. 14 (1964) 1405–1411.
[12] V.D. Tonchev, Combinatorial Configurations, Designs, Codes, Graphs, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 40, Longman, New York, 1988 (translated from the Bulgarian by R.A. Melter).
[13] H. Whitney, Congruent graphs and the connectivity of graphs, Amer. J. Math. 54 (1932) 154–168.