Binary codes from graphs on triples and permutation decoding

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

April 15, 2004

Abstract

We show that permutation decoding can be used, and give explicit PD-sets in the symmetric group, for some of the binary codes obtained from the adjacency matrices of the graphs on $\binom{n}{3}$ vertices, for $n \geq 7$, with adjacency defined by the vertices as 3-sets being adjacent if they have zero, one or two elements in common, respectively.

1 Introduction

MacWilliams [8] introduced an algorithm for permutation decoding, employing it mostly for cyclic codes and the Golay codes. It involves choosing appropriate information sets for the code and finding a set of automorphisms that satisfies particular conditions (see below), such a set being called a PD-set.

*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.

†Support of NRF and the University of Natal (URF) acknowledged.

‡Post-graduate scholarship of DAAD (Germany) and the Ministry of Petroleum (Angola) acknowledged.

Appropriate information sets and PD-sets for infinite classes of codes defined by some strongly regular graphs with the symmetric group as an automorphism group were found in [6, 7]. In [5] we examined the binary codes from a similar class of graphs, not strongly regular, but with the symmetric group as automorphism group, and obtained the dimension, the minimum weight, and some classes of minimum words for these codes: see Section 3, Result 1 for a statement of the main theorem obtained.

In that paper we announced that we would include the establishment of PD-sets for the interesting members of this set of codes in a further paper, and this current paper addresses that issue. Here we prove the following:

Theorem 1 *Let Ω be a set of size n, where $n \geq 7$ and n is odd. Let $\mathcal{P} = \Omega^{\{3\}}$, the set of subsets of Ω of size 3, be the vertex set of the graph $A_2(n)$ with adjacency defined by two vertices (as 3-sets) being adjacent if the 3-sets meet in two elements. Let $C_2(n)$ denote the code formed from the row span over $\mathbb{F}_2$ of an adjacency matrix for $A_2(n)$.*

The dual $C_2(n)^\perp$ is a $[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$ code with

$$\mathcal{I} = \{\{i,j,n\} \mid 1 \leq i < j < n\} \cup \{\{n-3, n-2, n-1\}\} \setminus \{\{n-2, n-1, n\}\}$$

as information set. Then $C_2(n)^\perp$ has a PD-set in S_n given by the following elements of S_n in their natural action on triples of elements of $\Omega = \{1, 2, \ldots, n\}$:

$$S = \{(n,i)(n-1,j)(n-2,k) \mid 1 \leq i \leq n, 1 \leq j \leq n-1, 1 \leq k \leq n-2\},$$

where (i,i) denotes the identity element of S_n.

Note that the size of the PD-set is of the order of n^3, as is the length of the code.

The proof of the theorem is given in Section 3. In Section 4 we mention one of the other dual codes and give a PD-set.

2 Background and terminology

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. 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 $V = F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. For any vector $w \in V$, the coordinate of w at the point $P \in \mathcal{P}$ is denoted by $w(P)$.

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** 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 $C^\perp$. 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 non-zero entries are equal to 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. An **automorphism** of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\mathrm{Aut}(C)$.

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.

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**.

Permutation decoding was first developed by MacWilliams [8]. It involves finding a set of automorphisms of a code such that the set satisfies certain conditions that allow it to be used for decoding; such a set is called a PD-set. The method is described fully in MacWilliams and Sloane [9, Chapter 15] and Huffman [3, 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 then 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 will fully use the error-correction potential of the code follows easily and is proved in Huffman [3, Theorem 8.1]. Of course such a set might not exist at all, and existence is not invariant under equivalence, nor isomorphism, of codes. Furthermore, there is a bound on the minimum size that the set $\mathcal{S}$ may have: see Gordon [2], or [3].

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. So $G = [I_k|A]$ and $H = [A^T|I_{n-k}]$, for some A 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 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 yg_i, and obtain the codeword c that has these information symbols. 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 $g \in \mathrm{Aut}(C)$, then $xg \in C$.

3 The codes and PD-sets

We describe first briefly how the codes are defined from graphs and designs. Let n be any integer and Ω a set of size n; to avoid degenerate cases we take $n \geq 7$. Taking the set $\Omega^{\{3\}}$ to be the set of all 3-element subsets of Ω, we define three non-trivial undirected graphs with vertex set $\mathcal{P} = \Omega^{\{3\}}$, and denote these graphs by $A_i(n)$ where $i = 0, 1, 2$. The edges of the graph $A_i(n)$ are defined by the rule that **two vertices are adjacent in** $A_i(n)$ if as 3-element subsets they have exactly i elements of Ω in common. For each $i = 0, 1, 2$ we define from $A_i(n)$ a 1-design $\mathcal{D}_i(n)$, on the point set $\mathcal{P}$ by defining for each point $P = \{a, b, c\} \in \mathcal{P}$ a block $\overline{\{a, b, c\}}_i$ by

$$\overline{\{a, b, c\}}_i = \{\{x, y, z\} \mid |\{x, y, z\} \cap \{a, b, c\}| = i\ \}.$$

Denote by $\mathcal{B}_i(n)$ the block set of $\mathcal{D}_i(n)$, so that each of these is a symmetric 1-design on $\binom{n}{3}$ points with block size, respectively:

- $\binom{n-3}{3}$ for $\mathcal{D}_0(n)$;
- $3\binom{n-3}{2}$ for $\mathcal{D}_1(n)$;
- $3(n-3)$ for $\mathcal{D}_2(n)$.

The incidence vector of the block $\overline{\{a,b,c\}}_i$ for $i = 0,1,2$, respectively, is then

$$v^{\overline{\{a,b,c\}}_0} = \sum_{x,y,z\in\Omega^*} v^{\{x,y,z\}}; \tag{1}$$

$$v^{\overline{\{a,b,c\}}_1} = \sum_{x,y\in\Omega^*} v^{\{a,x,y\}} + \sum_{x,y\in\Omega^*} v^{\{b,x,y\}} + \sum_{x,y\in\Omega^*} v^{\{c,x,y\}}; \tag{2}$$

$$v^{\overline{\{a,b,c\}}_2} = \sum_{x\in\Omega^*} v^{\{a,b,x\}} + \sum_{x\in\Omega^*} v^{\{a,c,x\}} + \sum_{x\in\Omega^*} v^{\{b,c,x\}} \tag{3}$$

where $\Omega^* = \Omega \setminus \{a,b,c\}$, and, 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 triples of elements from Ω, we emphasize that we are using the notation $v^{\{a,b,c\}}$ instead of the more cumbersome $v^{\{\{a,b,c\}\}}$, as mentioned in [1]. In [5] we examined the binary codes of these designs, i.e., denoting the block set of $\mathcal{D}_i(n)$ by $\mathcal{B}_i(n)$, we took

$$C_i(n) = C_2(\mathcal{D}_i(n)) = \langle v^b \mid b \in \mathcal{B}_i(n)\rangle,$$

where the span is taken over $\mathbb{F}_2$. Alternatively, this can be regarded as the row span over $\mathbb{F}_2$ of an adjacency matrix of the relevant graph. We obtained the following:

Result 1 *Let Ω be a set of size n, where $n \geq 7$. Let $\mathcal{P} = \Omega^{\{3\}}$, the set of subsets of Ω of size 3, be the vertex set of the three graphs $A_i(n)$, for $i = 0,1,2$, with adjacency defined by two vertices (as 3-sets) being adjacent if the 3-sets meet in zero, one or two elements, respectively. Let $C_i(n)$ denote the code formed from the row span over $\mathbb{F}_2$ of an adjacency matrix for $A_i(n)$. Then*

1. $n \equiv 0 \pmod 4$:
   - (a) $C_2(n) = \mathbb{F}_2^{\mathcal{P}}$;
   - (b) $C_0(n) = C_1(n)$ *is* $[\binom{n}{3}, \binom{n}{3} - n, 4]_2$ *and* $C_0(n)^\perp$ *is* $[\binom{n}{3}, n, \binom{n-1}{2}]_2$;
2. $n \equiv 2 \pmod 4$:
   $C_i(n) = \mathbb{F}_2^{\mathcal{P}}$ *for* $i = 0,1,2$;
3. $n \equiv 1 \pmod 4$:
   - (a) $C_0(n) = C_1(n) \cap C_2(n)$;
   - (b) $C_0(n)$ *is* $[\binom{n}{3}, \binom{n}{3} - \binom{n}{2}, 8]_2$ *and* $C_0(n)^\perp$ *is* $[\binom{n}{3}, \binom{n}{2}, n-2]_2$;
     $C_1(9)$ *is* $[84, 76, 3]_2$ *and* $C_1(9)^\perp$ *is* $[84, 8, 38]_2$;
     $C_1(n)$ *is* $[\binom{n}{3}, \binom{n}{3} - n + 1, 4]_2$ *and* $C_1(n)^\perp$ *is* $[\binom{n}{3}, n-1, (n-2)(n-3)]_2$ *for* $n > 9$;
     $C_2(n)$ *is* $[\binom{n}{3}, \binom{n-1}{3}, 4]_2$ *and* $C_2(n)^\perp$ *is* $[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$;

4. $n \equiv 3 \pmod 4$*:*

(a) $C_1(n) = \langle v^P + j \mid P \in \mathcal{P} \rangle$ *is* $[\binom{n}{3}, \binom{n}{3} - 1, 2]_2$*;*

(b) $C_0(n) = C_2(n)$ *is* $[\binom{n}{3}, \binom{n-1}{3}, 4]_2$ *and* $C_2(n)^\perp$ *is* $[\binom{n}{3}, \binom{n-1}{2}, n - 2]_2$*;*

For all $n \geq 7, i = 0, 1, 2,$ $C_i(n) \cap C_i(n)^\perp = \{0\}$*, and the automorphism groups of these codes are* S_n *or* $S_{\binom{n}{3}}$*.*

Notice that the code $C_2(n)^\perp$ for n odd is always $[\binom{n}{3}, \binom{n-1}{2}, n-2]_2$, and, furthermore, information sets are given in [5]. We now prove the theorem:

Proof of Theorem 1: That the information symbols can be taken as given above follows from Proposition 1 of [5], where we have replaced the point $\{n-2, n-1, n\}$ in the information set by $\{n-3, n-2, n-1\}$ in order to be able to construct a PD-set.

Let $\mathcal{I}$ denote the information positions, and $\mathcal{C}$ the check positions. Thus

$$\mathcal{I} = \{\{i, j, n\} \mid 1 \leq i < j < n\} \cup \{\{n-3, n-2, n-1\}\} \setminus \{\{n-2, n-1, n\}\}.$$

Let $P = \{n-3, n-2, n-1\} \in \mathcal{I}$ and $Q = \{n-2, n-1, n\} \in \mathcal{C}$. Notice that the code will correct $t = \frac{n-3}{2}$ errors.

Take a set $\mathcal{T}$ of t points of $\mathcal{P}$ and let $T = \bigcup_{\{a,b,c\} \in \mathcal{T}} \{a, b, c\}$. We need to exhibit an element $\sigma \in S$ such that $\mathcal{T}\sigma \subseteq \mathcal{C}$. For this we need to consider the different types of composition of $\mathcal{T}$, so the proof goes through a number of cases. Notice that if $\mathcal{T} \subseteq \mathcal{C}$ then the identity automorphism, which is in S, will do. Thus suppose $\mathcal{T} \not\subseteq \mathcal{C}$.

Let z_i denote the number of elements in Ω that occur i times in $\mathcal{T}$. Then $\sum_{i=0}^{t} z_i = n$ and $\sum_{i=0}^{t} i z_i = 3t$. Thus

$$\sum_{i=2}^{t} (2i - 3) z_i + 9 = 3z_0 + z_1. \tag{4}$$

Case (I): $\mathcal{T} \subseteq \mathcal{I}$. Then at least $t - 1$ members of $\mathcal{T}$ contain n.
(i) $P \notin \mathcal{T}$: then $|T| \leq 2t + 1 = n - 2$, so there are at least two distinct elements a and b in Ω, not equal to n, that are not in T. If $a \leq n - 3$ then $\sigma = (n, a)$ will satisfy $\mathcal{T}\sigma \subseteq \mathcal{C}$. If $\{a, b\} = \{n-2, n-1\}$ then again (n, a) will do.
(ii) $P \in \mathcal{T}$: then $|T| \leq 2(t-1) + 1 + 3 = n - 1$, so there is at least one element $a \in \Omega$ such that $a \notin T$. Clearly $a \leq n - 4$. If $|T| = n - 1$, then $n-3, n-2, n-1$ appear only in P and in no other element of $\mathcal{T}$. Thus $(n, n-3)$ will do. If $|T| < n-1$ then there are at least two elements $a, b \notin T$ with $a, b \leq n - 4$. Then $\mathcal{T}(n, a)(n-1, b) \subseteq \mathcal{C}$.

Case (II): suppose $\mathcal{T}$ meets both $\mathcal{I}$ and $\mathcal{C}$ non-trivially.
(i) Suppose first that $z_0 \neq 0$. Then if $a \in \Omega$, $a \neq n$ and $a \notin T$, the transposition $\tau = (n, a)$ will transform $\mathcal{T}$ into $\mathcal{T}\tau$ which will not contain n, so that if we find an element σ to take $\mathcal{T}\tau$ into $\mathcal{C}$, where $\sigma \in S$ but fixes n, then $\tau\sigma \in S$ will map $\mathcal{T}$ into $\mathcal{C}$.

So assume that n is absent from $\mathcal{T}$. Then $P \in \mathcal{T}$ and the number of points of the form $\{i, n-2, n-3\}$ with $i \neq n, n-1$ is $n-4 = 2t-1$, so there is an element $b \leq n-4$ such that $\{b, n-2, n-3\} \notin \mathcal{T}$. Then $\mathcal{T}(n, a)(n-1, b) \subseteq \mathcal{C}$.

(ii) Now suppose that $T = \Omega$, and thus $z_0 = 0$, and $n \geq z_1 \geq 9$ from Equation (4). For $a \in \Omega$, let $x(a)$ denote the number of times a appears in points in $\mathcal{T}$. So $1 \leq x(a) \leq t$ for each $a \in \Omega$ and $3t = \sum_{i=1}^{n} x(i) = \sum_{i=1}^{t} iz_i$. For any $a \in \Omega$, $x(a) = 3t - \sum_{b \neq a} x(b) \leq 3t - (n-1) = t-2$, and so $z_i = 0$ for $i \geq t-1$.

We will now show that we can find a point $\{a, b, c\} \in \mathcal{T}$ such that $x(a) = x(b) = 1$, $a, b \leq n-4$, and $c \neq n$. Suppose $x(n) = m$, and that $1 < m \leq t-2$. Then

$$3t = z_1 + m + \sum_{x(i) \geq 2, i \neq n} x(i) \geq z_1 + m + 2(n-1-z_1),$$

which simplifies to $z_1 \geq t+4+m$. If $m = 1$ then this inequality still applies if we take z_1 to be the number of elements with $x(a) = 1$ excluding n. Suppose that as many pairs with $x(a) = 1$ as possible occur as part of a triple with n in $\mathcal{T}$. This uses $2m$ elements, leaving $z_1 - 2m \geq t+4-m$ elements with $x(a) = 1$ (always excluding n from the count). We want to exclude $n-3, n-2, n-1$, which still leaves at least $z_1 - 2m - 3 \geq t-m+1$ elements. The number of points of $\mathcal{T}$ available is $t-m$ so we must have at least one point $X = \{a, b, c\}$ with two elements a and b with $x(a) = x(b) = 1$, $a, b \leq n-4$, and $c \neq n$.

Finally we show how this point $X = \{a, b, c\}$ can be used to define group elements that will map $\mathcal{T}$ into $\mathcal{C}$. We need to look at the various possibilities for c.

1. $c \leq n-4$: then $\sigma = (n, a)(n-1, b)(n-2, c)$ will satisfy $\mathcal{T}\sigma \subseteq \mathcal{C}$, since $\{d, e, n\}\sigma \in \mathcal{C}$, $\{a, b, c\}\sigma = \{n, n-1, n-2\} \in \mathcal{C}$, and $\{n-3, n-2, n-1\}\sigma^{-1} = \{b, c, n-3\} \notin \mathcal{T}$, since $x(b) = 1$ and $a \neq n-3$.

2. $c = n-1$: then $\sigma = (n, a)(b, n-2)$ will work as above, noting that $\{n-3, n-2, n-1\}\sigma^{-1} = \{b, n-1, n-3\} \notin \mathcal{T}$, since $x(b) = 1$ and $a \neq n-3$.

3. $c = n-2$: then $\sigma = (n, a)(b, n-1)$ will work as in the previous case.

4. $c = n-3$: then $\{a,b,c\} = \{a,b,n-3\}$ and take $\sigma = (n,a)(b,n-1)(n-2,n-3)$. Then $\{a,b,c\}\sigma = \{n,n-1,n-2\} \in \mathcal{C}$, and $\{n-3,n-2,n-1\}\sigma^{-1} = \{b,n-2,n-3\} \notin \mathcal{T}$, since $x(b) = 1$ and $a \neq n-2$.

We have shown that every t-tuple, and hence every s-tuple for $s \leq t$ can be moved by an element of S into the error positions. Thus S is a PD-set for $C_2(n)^{\perp}$. ■

4 Conclusion

Note: 1. We expect that a similar sort of construction can be made for PD-sets for the other codes from these graphs, but one requires suitable information sets. In particular, taking the code $C_0(n)^{\perp}$ for $n \equiv 1 \pmod 4$ and $n \geq 9$, we have a $[\binom{n}{3}, \binom{n}{2}, n-2]_2$ code that will correct $\frac{n-3}{2}$ errors. From Lemma 10 of [5] we can take as the $\binom{n}{2}$ information positions the points $\{i,j,n\}$ for $1 \leq i,j \leq n-1$, $\{i,n-2,n-1\}$ for $1 \leq i \leq n-3$ and two extra points: $\{n-4,n-3,n-1\}$ and $\{n-4,n-3,n-2\}$. To construct a PD-set we need to switch one of these points with a point from the check positions, and it is easy to verify that the following will form an information set: if

$$\begin{aligned}
\mathcal{I}_1 &= \{\{i,j,n\} \,|\, 1 \leq i < j \leq n-1\} \setminus \{\{n-2,n-1,n\}\}; \\
\mathcal{I}_2 &= \{\{i,n-2,n-1\} \,|\, 1 \leq i \leq n-3\}; \\
\mathcal{I}_3 &= \{\{n-4,n-3,n-2\}, \{n-4,n-3,n-1\}, \{n-5,n-4,n-3\}\}
\end{aligned}$$

then

$$\mathcal{I} = \mathcal{I}_1 \cup \mathcal{I}_2 \cup \mathcal{I}_3$$

is an information set for $C_0(n)^{\perp}$ for $n \equiv 1 \pmod 4$ and $n \geq 9$. The set $\{(n,i)(n-1,j)(n-2,k)(n-3,l) \mid 1 \leq i \leq n, 1 \leq j \leq n-1, 1 \leq k \leq n-2, 1 \leq l \leq n-3\}$, where (i,i) denotes the identity element of S_n, can be shown to be a PD-set for the code, the proof following the lines of the proof for the code we have given, but having more cases to be dealt with separately.

2. The existence of a PD-set for a code is not invariant under equivalence, and part of the problem of finding PD-sets is to find suitable information sets: for example, in the theorem, the points

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

can be taken as information symbols, but if they are, the code will not have a PD-set to correct all the allowed errors, since, for $n = 9$, the $[84,28,7]_2$ code corrects $t = 3$ errors but there is no element in S_9 that move the three points

$$\{1,2,9\}, \{3,4,5\}, \{6,7,8\}$$

into the check positions. However, if $\{7, 8, 9\}$ is placed in the check positions and $\{6, 7, 8\}$ in the information positions, then it can be done: in this example, $(6, 9)$ will do it.
3. A bound found in Gordon [2] (and quoted and derived in Huffman [3]) for the smallest size a PD-set can be, when compared with the order of the group of the code, shows that for some well-known codes from geometries, PD-sets will not exist beyond a certain code length: see [4] for details.

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

[3] 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.

[4] J. D. Key, T. P. McDonough, and V. C. Mavron. Partial permutation decoding of codes from finite planes. To appear: European J. Combin.

[5] J. D. Key, J. Moori, and B. G. Rodrigues. Binary codes from graphs on triples. *Discrete Math.*, To appear.

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

[7] J. D. Key and P. Seneviratne. Permutation decoding of binary codes from lattice graphs. *Discrete Math.*, To appear.

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

[9] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1983.