Cent. Eur. J. Math. • 12(9) • 2014 • 1362-1371
DOI: 10.2478/s11533-014-0417-y

VERSITA

Central European Journal of **Mathematics**

Binary codes and partial permutation decoding sets from the odd graphs

Research Article

Washiela Fish[1*], Roland Fray[1], Eric Mwambene[1]

1 Department of Mathematics and Applied Mathematics, University of the Western Cape, Private Bag X17, Bellville 7535, South Africa

Received 25 July 2013; accepted 10 December 2013

Abstract: For $k \geq 1$, the odd graph denoted by $O(k)$, is the graph with the vertex-set $\Omega^{\{k\}}$, the set of all k-subsets of $\Omega = \{1, 2, \ldots, 2k+1\}$, and any two of its vertices u and v constitute an edge $[u, v]$ if and only if $u \cap v = \emptyset$. In this paper the binary code generated by the adjacency matrix of $O(k)$ is studied. The automorphism group of the code is determined, and by identifying a suitable information set, a 2-PD-set of the order of k^4 is determined. Lastly, the relationship between the dual code from $O(k)$ and the code from its graph-theoretical complement $\overline{O(k)}$, is investigated.

MSC: 94B05, 05B30, 05C90, 05E18

Keywords: Odd graphs • Binary codes • Automorphism group • Permutation decoding

1. Introduction

Let n, k be positive integers with $n \geq 2k$, and r a non-negative integer with $r < k$. The uniform subset graph denoted by $\Gamma(n, k, r)$ was first described by Chen and Lih in [6] and is the graph with the vertex-set the set of all k-subsets of $\{1, 2, \ldots, n\}$, and any two of its vertices u and v constitute an edge $[u, v]$ if and only if $|u \cap v| = r$. The odd graph $O(k)$ is the uniform subset graph $\Gamma(2k+1, k, 0)$. Balaban [2] encountered odd graphs in his study of carbonium ions, Cameron [5] is attributed with having introduced the term, Biggs [4] posed the question of whether it is possible to colour the edges of $O(5)$ using six colours, and Meredith and Lloyd [11] answered this question in the affirmative.

This paper focuses on the binary codes generated by the adjacency matrix of $O(k)$. This code is also the code of the $1 - \left(\binom{2k+1}{k}, k+1, k+1\right)$ design $\mathcal{D}$ of which the point set $\mathcal{P}$ is the vertex-set of $O(k)$ and the block set $\mathcal{B}$ the set of supports of the incidence vectors of its adjacency matrix. It is known (see [2, Chapter 3]) that the automorphism group of $O(k)$ is S_{2k+1}, and it is shown in Proposition 3.11 that the automorphism group of the code is also S_{2k+1}.

* *E-mail: wfish@uwc.ac.za*

The code from $O(k)$ can also be viewed from the perspective of the primitive action of the alternating group A_{2k+1} on $\Omega^{\{k\}}$. The orbits of the stabilizer $(A_{2k+1})_{\{a_1,a_1,\ldots,a_k\}}$ of the point $\{a_1, a_2, \ldots, a_k\}$ have lengths $\binom{k}{i}\binom{k+1}{k-i}$, for $0 \leq i \leq k$. Define the point set to be $\Omega^{\{k\}}$, and for each point $\{a_1, a_2, \ldots, a_k\}$ define a block $\overline{\{a_1, a_2, \ldots, a_k\}}$ by

$$\overline{\{a_1, a_2, \ldots, a_k\}} = \left\{\{x_1, x_2, \ldots, x_k\} \in \Omega^{\{k\}} : \{x_1, x_2, \ldots, x_k\} \subseteq \Omega \backslash \{a_1, a_2, \ldots, a_k\}\right\},$$

i.e. the orbit of length $k+1$. Then the points and blocks form the $1-\left(\binom{2k+1}{k}, k+1, k+1\right)$ design described above.

This paper is organized as follows: In Section 2 the preliminary ideas related to codes, designs and graphs are discussed, in Section 3 some lemmas which describe the code from $O(k)$ are proven, in Section 4 a 2-PD-set is determined for the code, and in Section 5 the relationship between the dual code from $O(k)$ and the code from $\overline{O(k)}$ is investigated.

2. Preliminaries

A *linear code* C of length n over a finite field of order q, denoted by F_q, is a subspace of F_q^n. The elements of C are called *codewords*. The *support* of a codeword is its set of non-zero coordinate positions. The *minimum weight* of C is the least number of elements in the support of any codeword of C. If the dimension of C is k and its minimum weight is d, then C is an $[n, k, d]_q$ code, or simply an $[n, k, d]$ code if $q = 2$. A *generator matrix* for C is a $k \times n$ matrix of which the rows form a basis for C. The *dual code* of C, denoted by $C^\perp$, is the orthogonal space under the standard inner product, i.e. $C^\perp = \{v \in F_q^n : (v, c) = 0 \text{ for all } c \in C\}$. A *check matrix* for C is a generator matrix H for $C^\perp$; the *syndrome* of a vector $y \in F^n$ is Hy^T. C is *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$. Two codes are *isomorphic* if the one can be obtained from the other by permuting the coordinate positions. An *automorphism* of C is an isomorphism of C onto itself. The automorphisms of C, denoted by $\mathrm{Aut}(C)$, form a group under composition.

A *graph* $\Gamma = (V, E)$ comprises a *vertex-set* V and an *edge-set* E, where the edge $[u, v]$ is an association of the vertices $u, v \in V$. If $[u, v] \in E$, then u and v are *adjacent*. The *degree* or the *valency* of a vertex v is the number of edges with which v is incident. If all the vertices of Γ are incident with the same number of vertices, then Γ is *regular*, and its valency is the valency of each of its vertices. The *complement* of $\Gamma = (V, E)$ is the graph $\overline{\Gamma} = (\overline{V}, \overline{E})$, where $\overline{V} = V$ and for $u, v \in V$, $[u, v] \in \overline{E}$ if and only if $[u, v] \notin E$. An *isomorphism* from $\Gamma = (V, E)$ to $\Gamma' = (V', E')$ is a bijection $\phi\colon V \to V'$ such that $[u, v] \in E$ if and only if $[\phi(u), \phi(v)] \in E'$. An isomorphism of Γ onto itself is an *automorphism* of Γ. The automorphisms of Γ, denoted by $\mathrm{Aut}(\Gamma)$, form a group under composition.

A *finite incidence structure*, denoted by $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with *point-set* $\mathcal{P}$, *block-set* $\mathcal{B}$ and *incidence* $\mathcal{I}$, is a $t-(v, k, \lambda)$ *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. $\mathcal{D}$ is *symmetric* if it has the same number of points as it has blocks.

An *adjacency matrix* of a graph $\Gamma = (V, E)$, where $V = \{u_1, u_2, \ldots, u_n\}$, is an $n \times n$ matrix $A = (a_{ij})$ for which $a_{ij} = 1$ if u_i and u_j are adjacent, and $a_{ij} = 0$ otherwise. A is clearly symmetric. A is also an *incidence matrix* of a $1-(v, k, k)$ design $(\mathcal{P}, \mathcal{B}, \mathcal{I})$, where $\mathcal{P} = \{p_1, p_2, \ldots, p_v\}$ and $\mathcal{B} = \{B_1, B_2, \ldots, B_v\}$, defined by $a_{ij} = 1$ if $(p_j, B_i) \in \mathcal{I}$, and $a_{ij} = 0$ otherwise.

The identification of a basis for a code C implies the identification of a set of *information positions* for C: when a generator matrix for C is reduced to *standard form*, i.e. to the form $[I_k|A]$, the first k coordinates constitute the *information positions* and the last $n-k$ coordinates the *check positions*. The choice of information positions plays a critical role in *permutation decoding* which entails the determination of a set of automorphisms of the code which exploits the full error-correcting capability of the code. More precisely, a *PD-set* for a t-error-correcting code is a set $\mathcal{S}$ of automorphisms of C which is such that for any set of t coordinate positions, there is an element of $\mathcal{S}$ which maps it into the check positions. The size of $\mathcal{S}$ is restricted by the *Gordon bound* given in Huffman [7, Theorem 8.2]. PD-sets that exploit the full error-correcting capability of the code may not even exist, and hence partial PD-sets may be resorted to (see Kroll and Vincenti [8]): An *s-PD-set* for a t-error-correcting code maps any set of $s \leq t$ coordinate positions into the check positions. This method of decoding was first developed by MacWilliams [9], and is fully described in MacWilliams and Sloane [10, Chapter 15] and Huffman [7, Section 8]. In brief, suppose that C is a t-error-correcting code with check matrix H, and that $S = \{g_1, g_2, \ldots, g_s\}$ is a PD-set for C. If x is sent and y is received and at most t errors occur, then compute the weights of the syndromes $H(yg_i)^T$ for each i until $\mathrm{weight}\left(H(yg_i)^T\right) \leq t$. y is then decoded as cg_i^{-1}, where c corresponds with yg_i in the information positions.

3. Binary codes from $O(k)$

Let k be a positive integer and $O(k)$ the odd graph which has as its vertex-set $\mathcal{P}$, the $\binom{2k+1}{k}$ k-subsets of $\Omega = \{1, 2, \ldots, 2k+1\}$. $\mathcal{P}$ also forms the point set of the 1-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ in which each point $\{a_1, a_2, \ldots, a_k\} \in \Omega^{\{k\}}$ has a block $\overline{\{a_1, a_2, \ldots, a_k\}}$ corresponding to it which is defined as follows:

$$\overline{\{a_1, a_2, \ldots, a_k\}} = \left\{\{x_1, x_2, \ldots, x_k\} \in \Omega^{\{k\}} : \{x_1, x_2, \ldots, x_k\} \subseteq \Omega \backslash \{a_1, a_2, \ldots, a_k\}\right\}.$$

The block set $\mathcal{B}$ is then defined by

$$\mathcal{B} = \left\{\overline{\{a_1, a_2, \ldots, a_k\}} : \{a_1, a_2, \ldots, a_k\} \in \Omega^{\{k\}}\right\},$$

and the incidence vector of the block $\overline{\{a_1, a_2, \ldots, a_k\}}$ by

$$v^{\overline{\{a_1, a_2, \ldots, a_k\}}} = \sum_{\{x_1, x_2, \ldots, x_k\} \subseteq \Omega \backslash \{a_1, a_2, \ldots, a_k\}} v^{\{x_1, x_2, \ldots, x_k\}}. \tag{1}$$

Throughout this paper it is assumed that $k \geq 2$. Let C denote the binary code from the adjacency matrix of $O(k)$ and $C^{\perp}$ its dual.

Lemma 3.1.
Let $S = \left\{v^{\overline{\{a_1, a_2, \ldots, a_k\}}} : \{a_1, a_2, \ldots, a_k\} \subseteq \Omega \backslash \{1\}\right\}$. *Then* S *is a basis for* C.

Proof. By equation (1), for $\{a_1, a_2, \ldots, a_k\} \in \Omega \backslash \{1\}$,

$$v^{\overline{\{a_1, a_2, \ldots, a_k\}}} = \sum_{\{x_1, x_2, \ldots, x_{k-1}\} \subseteq \Omega \backslash \{1, a_1, a_2, \ldots, a_k\}} v^{\{1, x_1, x_2, \ldots, x_{k-1}\}} + v^{\Omega \backslash \{1, a_1, a_2, \ldots, a_k\}}. \tag{2}$$

$\Omega \backslash \{1, a_1, a_2, \ldots, a_k\}$ is uniquely determined for each $\{a_1, a_2, \ldots, a_k\} \in \Omega \backslash \{1\}$. Hence S is linearly independent. By equation (2), it is easily seen that

$$\sum_{x \in \Omega \backslash \{1, a_1, a_2, \ldots, a_{k-1}\}} v^{\overline{\{a_1, a_2, \ldots, a_{k-1}, x\}}} = \sum_{x \in \Omega \backslash \{1, a_1, a_2, \ldots, a_{k-1}\}} v^{\Omega \backslash \{1, a_1, a_2, \ldots, a_{k-1}, x\}} = \sum_{\{x_1, x_2, \ldots, x_k\} \subseteq \Omega \backslash \{1, a_1, a_2, \ldots, a_{k-1}\}} v^{\{x_1, x_2, \ldots, x_k\}} = v^{\overline{\{1, a_1, a_2, \ldots, a_{k-1}\}}}.$$

Hence S spans C. Clearly, $|S| = \left|\left\{v^{\overline{\{a_1, a_2, \ldots, a_k\}}} : \{a_1, a_2, \ldots, a_k\} \subseteq \Omega \backslash \{1\}\right\}\right| = \binom{2k}{k}$. □

Lemma 3.2.
C has minimum weight $k+1$.

Proof. Each basis vector $v^{\overline{\{a_1, a_2, \ldots, a_k\}}}$, where $\{a_1, a_2, \ldots, a_k\} \subseteq \Omega \backslash \{1\}$, has weight $k+1$. Also, since two vectors $v^{\overline{\{a_1, a_2, \ldots, a_k\}}}$ and $v^{\overline{\{a'_1, a'_2, \ldots, a'_k\}}}$ are incident at a common point if and only if $\left|\{a_1, a_2, \ldots, a_k\} \cap \{a'_1, a'_2, \ldots, a'_k\}\right| = k-1$, the minimum weight vectors will be obtained by taking linear combinations of the basis vectors $\left\{v^{\overline{\{a_1, a_2, \ldots, a_{k-1}, x\}}} : x \in \Omega \backslash \{1, a_1, a_2, \ldots, a_{k-1}\}\right\}$. Suppose that a linear combination of r such vectors yields a weight of less than $k+1$. Then

$$r(k+1) - 2\binom{r}{2} < k+1, \tag{3}$$

i.e. $r < 1$ or $r > k+1$. Clearly, both possibilities for r are invalid, the second being so since $r \leq \left|\left\{v^{\overline{\{a_1, a_2, \ldots, a_{k-1}, x\}}} : x \in \Omega \backslash \{1, a_1, a_2, \ldots, a_{k-1}\}\right\}\right| = k+1$. □

Equality in (3) implies that any minimum weight vector is either a basis vector, or the sum of basis vectors of the form $\left\{v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}} : x \in \Omega\backslash\{1,a_1,a_2,\ldots,a_{k-1}\}\right\}$. Since such a linear combination results in the incidence vector $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-1}\}}}$, the following result is deduced.

Lemma 3.3.
C has a minimum weight basis. The incidence vectors $\left\{v^{\overline{\{a_1,a_2,\ldots,a_k\}}} : \{a_1,a_2,\ldots,a_k\} \subseteq \Omega\right\}$ constitute the $\binom{2k+1}{k}$ minimum words in C.

The following notation is introduced to explore analogous results for $C^\perp$. For $\{y_1,y_2,\ldots,y_{k-1}\} \subseteq \Omega$, define $v(\{y_1,y_2,\ldots,y_{k-1}\})$ by

$$v(\{y_1,y_2,\ldots,y_{k-1}\}) = \sum_{y\in\Omega\backslash\{y_1,y_2,\ldots,y_{k-1}\}} v^{\{y_1,y_2,\ldots,y_{k-1},y\}}. \tag{4}$$

Lemma 3.4.
Let $R = \left\{v(\{b_1,b_2,\ldots,b_{k-1}\}) : \{b_1,b_2,\ldots,b_{k-1}\} \subseteq \Omega\backslash\{1\}\right\}$. Then R is a basis for $C^\perp$.

Proof. Suppose $v^{\overline{\{a_1,a_2,\ldots,a_k\}}} \in S$, $v(\{b_1,b_2,\ldots,b_{k-1}\}) \in R$. The inner product $\left(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v(\{b_1,b_2,\ldots,b_{k-1}\})\right) \equiv 0 \pmod 2$ irrespective of whether $\{a_1,a_2,\ldots,a_k\} \cap \{b_1,b_2,\ldots,b_{k-1}\} = \emptyset$ or not. Hence $R \subseteq C^\perp$. Now by equation (4), for $\{b_1,b_2,\ldots,b_{k-1}\} \subseteq \Omega\backslash\{1\}$,

$$v(\{b_1,b_2,\ldots,b_{k-1}\}) = v^{\{1,b_1,b_2,\ldots,b_{k-1}\}} + \sum_{y\in\Omega\backslash\{1,b_1,b_2,\ldots,b_{k-1}\}} v^{\{b_1,b_2,\ldots,b_{k-1},y\}}.$$

$\{1,b_1,b_2,\ldots,b_{k-1}\}$ is uniquely determined for each $\{b_1,b_2,\ldots,b_{k-1}\} \subseteq \Omega\backslash\{1\}$. Hence R is linearly independent, and since $|R| = \left|\left\{v(\{b_1,b_2,\ldots,b_{k-1}\}) : \{b_1,b_2,\ldots,b_{k-1}\} \subseteq \Omega\backslash\{1\}\right\}\right| = \binom{2k}{k-1} = \binom{2k+1}{k} - \dim(C)$, R is a basis for $C^\perp$. □

Lemma 3.5.
$C^\perp$ has minimum weight $k+2$.

Proof. Each basis vector $v(\{b_1,b_2,\ldots,b_{k-1}\})$ has weight $k+2$. Consider the vectors $v(\{b_1,b_2,\ldots,b_{k-1}\})$ and $v(\{b'_1,b'_2,\ldots,b'_{k-1}\})$. If $\left|\{b_1,b_2,\ldots,b_{k-1}\} \cap \{b'_1,b'_2,\ldots,b'_{k-1}\}\right| < k-2$, then these vectors are not commonly incident at any point. Hence the minimum weight vectors will be obtained by taking linear combinations of the basis vectors $\left\{v(\{b_1,b_2,\ldots,b_{k-2},y\}) : y \in \Omega\backslash\{1,b_1,b_2,\ldots,b_{k-2}\}\right\}$. Suppose that a vector of weight less than $k+2$ can be obtained by taking a linear combination of r such vectors. Then

$$r(k+2) - 2\binom{r}{2} < k+2, \tag{5}$$

i.e. $r < 1$ or $r > k+2$. The restriction on r, namely, that $1 \le r \le k+2$, renders both solutions for (5) invalid. □

The above argument, in conjunction with Lemma 3.4, shows that the minimum words are either the basis vectors or the sum of basis vectors of the form $\left\{v(\{b_1,b_2,\ldots,b_{k-2},y\}) : y \in \Omega\backslash\{1,b_1,b_2,\ldots,b_{k-2}\}\right\}$ resulting in the vector $\{v(\{1,b_1,b_2,\ldots,b_{k-2}\})$. Hence the following result is implied.

Lemma 3.6.
$C^\perp$ has a basis of minimum weight vectors. The vectors $\left\{v(\{b_1,b_2,\ldots,b_{k-1}\}) : \{b_1,b_2,\ldots,b_{k-1}\} \subseteq \Omega\right\}$ constitute the $\binom{2k+1}{k-1}$ minimum words in $C^\perp$.

Lemmas 3.1, 3.2, 3.4 and 3.5 can be summarised as follows.

Theorem 3.7.
The binary code generated by the incidence matrix of the $1-\left(\binom{2k+1}{k}, k+1, k+1\right)$ *design or the adjacency matrix of the odd graph* $O(k)$ *where* $k \geq 2$*, is a* $\left[\binom{2k+1}{k}, \binom{2k}{k}, k+1\right]$ *code, and its dual a* $\left[\binom{2k+1}{k}, \binom{2k}{k-1}, k+2\right]$ *code.*

Lemma 3.8.
If k *is even, then* $\boldsymbol{j} \in C$*; otherwise* $\boldsymbol{j} \in C^{\perp}$*.* C *is neither self-dual nor self-orthogonal for any* $k \geq 2$*. In fact,* $C \oplus C^{\perp} = F_2^{\binom{2k+1}{k}}$ *for all* $k \geq 2$*.*

Proof. If k is even, then each basis vector $v(\{b_1, b_2, \ldots, b_{k-1}\})$, where $\{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{1\}$, in $C^{\perp}$ has even weight and hence $\boldsymbol{j} \in C$. Similarly, if k is odd, then $\boldsymbol{j} \in C^{\perp}$. Clearly, $\boldsymbol{j} \notin C \cap C^{\perp}$, since it would imply that $\boldsymbol{j}$ is orthogonal to vectors of odd weight.

The inner product $\left(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v^{\overline{\{a'_1,a'_2,\ldots,a'_k\}}}\right) \equiv 1 \pmod 2$ if $\left|\{a_1, a_2, \ldots, a_k\} \cap \{a'_1, a'_2, \ldots, a'_k\}\right| = k-1$. Hence $C \nsubseteq C^{\perp}$. Also, $C^{\perp} \nsubseteq C$, since the inner product $\left(v(\{b_1, b_2, \ldots, b_{k-1}\}), v(\{b'_1, b'_2, \ldots, b'_{k-1}\})\right) \equiv 1 \pmod 2$ if $\left|\{b_1, b_2, \ldots, b_{k-1}\} \cap \{b'_1, b'_2, \ldots, b'_{k-1}\}\right| = k-2$.

For the final statement of the lemma, for $\{a_1, a_2, \ldots, a_k\} \in \Omega^{\{k\}}$, consider the following linear combination in $C + C^{\perp}$:

$$\sum_{i=0}^{k-2} \sum_{\substack{A_i \subseteq \{a_1,a_2,\ldots,a_k\} \\ |A_i|=i}} \sum_{\substack{Y_i \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\} \\ |Y_i|=k-1-i}} v(A_i \cup Y_i) + \sum_{\{x_1,x_2,\ldots,x_k\} \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\}} v^{\overline{\{x_1,x_2,\ldots,x_k\}}} + k\boldsymbol{j}. \tag{6}$$

Now for each $0 \leq i \leq k-2$ the vector sum

$$\sum_{\substack{A_i \subseteq \{a_1,a_2,\ldots,a_k\} \\ |A_i|=i}} \sum_{\substack{Y_i \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\} \\ |Y_i|=k-1-i}} v(A_i \cup Y_i)$$

is the sum of all the vectors which are incident at points which have either i or $i+1$ elements in common with $\{a_1, a_2, \ldots, a_k\}$. Each vector of the former type occurs $k-i$ times in the sum, while each of the latter type occurs $i+1$ times. Similarly,

$$\sum_{\{x_1,x_2,\ldots,x_k\} \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\}} v^{\overline{\{x_2,x_2,\ldots,x_k\}}}$$

is the sum of vectors which are incident either at $\{a_1, a_2, \ldots, a_k\}$ or at points which have $k-1$ elements in common with $\{a_1, a_2, \ldots, a_k\}$. The vector $v^{\{a_1,a_2,\ldots,a_k\}}$ occurs $k+1$ times in the sum, while those that have $k-1$ elements in common with $\{a_1, a_2, \ldots, a_k\}$ each occurs exactly once. Hence the expression in (6) reduces to

$$(k+1)v^{\{a_1,a_2,\ldots,a_k\}} + k\sum_{i=0}^{k-1} \sum_{\substack{A'_i \subseteq \{a_1,a_2,\ldots,a_k\} \\ |A'_i|=i}} \sum_{\substack{Y'_i \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\} \\ |Y'_i|=k-i}} v^{A'_i \cup Y'_i} + k\boldsymbol{j} = (2k+1)v^{\{a_1,a_2,\ldots,a_k\}}. \qquad \square$$

Note that the expression in (6) can be simplified to $v^{\overline{\{a_1,a_2\}}} + v(\{a_1\}) + v(\{a_2\}) + \boldsymbol{j}$ when $k = 2$, and to

$$\sum_{\{x_1,x_2,x_3\} \subseteq \Omega \setminus \{a_1,a_2,a_3\}} v^{\overline{\{x_1,x_2,x_3\}}} + \sum_{\{y_1,y_2,\} \subseteq \Omega \setminus \{a_1,a_2,a_3\}} v(\{y_1, y_2\}) + \boldsymbol{j}$$

when $k = 3$.

To view C from another perspective, note that the stabilizer of the k-subset $\{a_1, a_2, \ldots, a_k\}$ in the action of a group H on $\Omega^{\{k\}}$ is the setwise stabilizer $H_{\{a_1,a_2,\ldots,a_k\}}$ in the action of H on Ω. Denote the pointwise stabilizer by $H_{(a_1,a_2,\ldots,a_k)}$. Clearly, $H_{(a_1,a_2,\ldots,a_k)} \leq H_{\{a_1,a_2,\ldots,a_k\}}$. The permutation representation of $H_{\{a_1,a_2,\ldots,a_k\}}$ with respect to its action on $\{a_1, a_2, \ldots, a_k\}$ defines a homomorphism of $H_{\{a_1,a_2,\ldots,a_k\}}$ into the symmetric group $S_{\{a_1,a_2,\ldots,a_k\}} \cong S_k$ which has as its kernel $H_{(a_1,a_2,\ldots,a_k)}$, and hence $H_{\{a_1,a_2,\ldots,a_k\}}/H_{(a_1,a_2,\ldots,a_k)}$ is isomorphic to a subgroup of S_k.

Since it is well known that the alternating groups A_n are $(n-2)$-transitive, the following result is deduced.

Lemma 3.9.
The alternating group A_{2k+1} where $k \geq 2$, acts transitively on $\Omega^{\{k\}}$.

Proposition 3.10.
The alternating group A_{2k+1} where $k \geq 2$, acts primitively as a rank $k+1$ permutation group on $\Omega^{\{k\}}$.

Proof. In view of Lemma 3.9, it is sufficient to consider the stabilizer of the subset $\{1, 2, \ldots, k\}$. Now it is easily seen that the stabilizer is $S_k \times A_{k+1}$. By the result of Ball [3], the stabilizer is maximal in A_{2k+1} and hence the action of the group is primitive. □

$O(k)$ is a highly symmetrical graph, and this is reflected in the fact that its automorphism group is large. By using the maximal independent subsets of $O(k)$ as the automorphism invariant, it can be shown that $\mathrm{Aut}(O(k)) = S_{2k+1}$. Hence $S_{2k+1} \leq \mathrm{Aut}(C)$. In fact, $\mathrm{Aut}(C) = S_{2k+1}$, as shown below.

Proposition 3.11.
The automorphism group of the binary code generated by the adjacency matrix of the odd graph $O(k)$ where $k \geq 2$, is S_{2k+1}.

Proof. Suppose that $\sigma \in \mathrm{Aut}(C)$ and $\{a_1, a_2, \ldots, a_k\} \cap \{a'_1, a'_2, \ldots, a'_k\} = \emptyset$. Then $v^{\overline{\{a_1, a_2, \ldots, a_k\}}}$ is incident at $\{a'_1, a'_2, \ldots, a'_k\}$. Since the incidence vectors constitute the minimum words and σ preserves these words, $v^{\overline{\sigma(\{a_1, a_2, \ldots, a_k\})}}$ is incident at $\sigma(\{a'_1, a'_2, \ldots, a'_k\})$. Hence $\sigma(\{a_1, a_2, \ldots, a_k\}) \cap \sigma(\{a'_1, a'_2, \ldots, a'_k\}) = \emptyset$, and $\sigma \in \mathrm{Aut}(O(k))$. □

4. Permutation decoding sets for C

In general, the automorphism group of a t-error correcting code provides the base for membership of a PD-set $\mathcal{S}$ which is such that every error vector of weight $e \leq t$ can be mapped by some member of $\mathcal{S}$ to another vector in which the e non-zero entries occur at the check positions. By Lemma 3.1, the set $\left\{\{a_1, a_2, \ldots, a_k\} : \{a_1, a_2, \ldots, a_k\} \subseteq \Omega \backslash \{1\}\right\}$ is identified as an information set for C. However, this set is found to be unsuitable for permutation decoding since if errors occur at two information positions of which the k-subsets are disjoint, then there is no automorphism of C which will map the errors into check positions. Hence an alternative basis is sought for C.

Lemma 4.1.
Let $S' = \left\{v^{\overline{\{a_1, a_2 \ldots a_{k-2}, m, n\}}} : a_1 < a_2 < \ldots < a_{k-2} < m < n \in \Omega,\ n \neq m+1\right\}$. Then S' is a basis for C.

Proof. Observe that

$$|S'| = \left|\left\{v^{\overline{\{a_1, a_2, \ldots, a_k\}}} : \{a_1, a_2, \ldots, a_k\} \in \Omega^{\{k\}}\right\} \backslash \left\{v^{\overline{\{a_1, a_2, \ldots, a_{k-2}, m, m+1\}}} : a_1 < a_2 < \ldots < a_{k-2} < m \in \Omega\right\}\right|$$

$$= \binom{2k+1}{k} - \binom{2k}{k-1} = \binom{2k}{k},$$

which concurs with the dimension of C. Recall that for $\{a_1, a_2, \ldots, a_{k-1}\} \subseteq \Omega \backslash \{1\}$,

$$v^{\overline{\{1, a_1, a_2, \ldots, a_{k-1}\}}} = \sum_{x \in \Omega \backslash \{1, a_1, a_2, \ldots, a_{k-1}\}} v^{\overline{\{a_1, a_2, \ldots, a_{k-1}, x\}}}.$$

Now suppose that

$$\sum_{\substack{a_1 < a_2 < \ldots < a_{k-2} < m < n \\ n \neq m+1}} \alpha_{\{a_1, a_2, \ldots, a_{k-2}, m, n\}} v^{\overline{\{a_1, a_2, \ldots, a_{k-2}, m, n\}}} = 0.$$

The sum above reduces to a sum of elements of S. The elements of S in the resulting sum are categorized as follows:

(i) $S_1 = \left\{ v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,m+1,m+2\}}} : a_1 < a_2 < \ldots < a_{k-3} < m \in \Omega\backslash\{1\} \right\}$,

(ii) $S_2 = \left\{ v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,n,n+1\}}} : a_1 < a_2 < \ldots < a_{k-3} < m < n \in \Omega\backslash\{1\},\ n \neq m+1 \right\}$,

(iii) $S_3 = \left\{ v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,m+1,n\}}} : a_1 < a_2 < \ldots < a_{k-3} < m < m+1 < n \in \Omega\backslash\{1\},\ n \neq m+2 \right\}$,

(iv) $S_4 = \left\{ v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,n,q\}}} : a_1 < a_2 < \ldots < a_{k-3} < m < n < q \in \Omega\backslash\{1\},\ n \neq m+1,\ q \neq n+1 \right\}$.

The vector $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,m+1,m+2\}}} \in S_1$ is not in S' and occurs only in the linear combination for $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-3},m,m+2\}}}$ in S'. Since S is linearly independent, the coefficient of $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,m+1,m+2\}}}$ in the resulting sum is zero. Hence each of the $\binom{2k-2}{k-2}$ coefficients of the form $\alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,m+2\}}$ where $1 < a_1 < a_2 < \ldots < a_{k-3} < m \in \Omega\backslash\{1\}$, in the original sum is zero.

Next, consider $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,n,n+1\}}} \in S_2$, which is also not in S'. However, $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,n,n+1\}}}$ occurs in the linear combinations for exactly two vectors in S', namely, $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-3},m,n\}}}$ and $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-3},m,n+1\}}}$. Hence the coefficient of $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,n,n+1\}}}$ in the resulting sum is $\alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,n\}} + \alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,n+1\}}$. Since $\alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,m+2\}}$ is zero for all $k-1 \leq m \leq 2k-1$, it follows that $\alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,m+3\}}$ is zero for all such m, and in general, if $\alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,p\}}$, where $m < p$ and $p \neq m+1$, is zero then $\alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,p+1\}}$ is also zero. By induction it follows that $\alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,n\}}$ is zero for all $k-1 \leq m \leq 2k-1$, where $n \neq m+1$.

Thirdly, observe that the vector $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,m+1,n\}}} \in S_3$ is in S', as well as in the linear combinations of the $k-2$ vectors in S' of the form $v^{\overline{\{1,x_1,x_2,\ldots,x_{k-3},m+1,n\}}}$, where $\{x_1, x_2, \ldots, x_{k-3}\} \subseteq \{a_1, a_2, \ldots, a_{k-3}, m\}$, and the vector $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-3},m,n+1\}}}$ in S'. Hence the coefficient of $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,m+1,n\}}}$ in the resulting sum is

$$\sum_{\{x_1,x_2,\ldots,x_{k-3}\}\subseteq\{a_1,a_2,\ldots,a_{k-3},m\}} \alpha_{\{1,x_1,x_2,\ldots,x_{k-3},m+1,n\}} + \alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,n+1\}} + \alpha_{\{a_1,a_2,\ldots,a_{k-3},m,m+1,n\}}.$$

Since each of the coefficients comprising the first $k-1$ terms above is zero by previous arguments, it follows that $\alpha_{\{a_1,a_2,\ldots,a_{k-3},m,m+1,n\}}$ is zero for all $k-1 \leq m \leq 2k-1$.

Lastly, the vector $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,n,q\}}} \in S_4$ is in S' as well as in the linear combinations for the k vectors in S' of the form $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-3},x,y\}}}$ where $\{a_1, a_2, \ldots, a_{k-3}, x, y\} \subseteq \{a_1, a_2, \ldots, a_{k-3}, m, n, q\}$. Hence the coefficient of $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,n,q\}}}$ in the resulting sum is

$$\sum_{\{a_1,a_2,\ldots,a_{k-3},x,y\}\subseteq\{a_1,a_2,\ldots,a_{k-3},m,n,q\}} \alpha_{\{1,a_1,a_2,\ldots,a_{k-3},x,y\}} + \alpha_{\{a_1,a_2,\ldots,a_{k-3},m,n,q\}}.$$

Since each of the first k coefficients is zero, the fact that S is linearly independent implies that $\alpha_{\{a_1,a_2,\ldots,a_{k-3},m,n,q\}}$ is zero for all $k-2 \leq m \leq 2k-3$, where $n \neq m+1$ and $q \neq n+1$. Since all the vectors in S' have been exhausted, the result follows. □

S' identifies the points $\left\{\{a_1, a_2, \ldots, a_{k-2}, m, n\} : a_1 < a_2 < \ldots < a_{k-2} < m < n,\ n \neq m+1\right\}$ as information positions for C. Given these information positions and the fact that C is able to correct $t = \lfloor k/2 \rfloor$ errors, the entire automorphism group S_{2k+1} is a PD-set for C. The following theorem gives a 2-PD-set for C.

Theorem 4.2.

Let $\mathcal{I}$ denote the points

$$\{1,2,\ldots,k-1,k+1\},\quad \{1,2,\ldots,k-1,k+2\},\quad \ldots,\quad \{1,2,\ldots k-1,2k+1\},\quad \{1,2,\ldots,k-2,k,k+2\},\quad \ldots,$$
$$\{1,2,\ldots,k-2,k,2k+1\},\quad \ldots,\quad \{1,2,\ldots,k-2,2k-1,2k+1\},\quad \{1,2,\ldots,k-3,k-1,k,k+2\},\quad \ldots,$$
$$\{1,k+2,k+3,\ldots,2k-1,2k+1\},\quad \ldots,\quad \{k+1,k+2,\ldots,2k-1,2k+1\},$$

where $k \geq 4$. Then $\mathcal{S} = \left\{(k-1+i,k+j)(k-1+i',k+j') : 0 \leq i \leq j \leq k+1,\ 0 \leq i' \leq j' \leq k+1\right\}$ is a 2-PD-set of size $\binom{k+3}{2}^2$ for C with $\mathcal{I}$ as information positions.

Proof. Suppose that the $2 \leq \lfloor k/2 \rfloor$ errors occur at $\mathcal{E} = \{\{e_1, e_2, \ldots, e_k\}, \{e'_1, e'_2, \ldots, e'_k\} : e_1 < e_2 < \ldots < e_k,\ e'_1 < e'_2 < \ldots < e'_k\}$.

Case (i): $\mathcal{E} \subseteq \mathcal{P} \backslash \mathcal{I}$. The identity, $1_{S_{2k+1}} \in \mathcal{S}$, and will leave $\mathcal{E}$ fixed.

Case (ii): $\{e_1, e_2, \ldots, e_k\} \in \mathcal{P} \backslash \mathcal{I}$, $\{e'_1, e'_2, \ldots, e'_k\} \in \mathcal{I}$. The following sub-cases need to be considered.

(a) $e'_{k-1} < e_{k-1} = e_k - 1 = e'_k - 1$: The permutation $(e_{k-1}, e_k)(e'_{k-1}, e_{k-1} - 1)$ will keep $\{e_1, e_2, \ldots, e_k\}$ fixed, but will map e'_k to a value which is one less than its original value, and then map e'_{k-1} to a value which is one less than the value which e'_k was mapped to.

(b) $e'_{k-1} = e_{k-1} = e_k - 1 < e'_k - 1$: The permutation $(e_{k-1}, e_k)(e'_k, e_k + 1)$ will act in a similar way as the permutation in (a).

(c) $e'_{k-1} < e'_k - 1 = e_{k-1} - 1 = e_k - 2$: The permutation $(e'_{k-1}, e'_k - 1)(e_k, e'_k - 1)$ will map e'_{k-1} to a value which is one less than e'_k, and then keep $\{e_1, e_2, \ldots, e_k\}$ and the position which $\{e'_1, e'_2, \ldots, e'_k\}$ was mapped to in check positions.

(d) $e_{k-1} = e_k - 1 = e'_{k-1} - 1 < e'_k - 2$: The permutation $(e'_k, e'_{k-1} + 1)(e_{k-1}, e'_{k-1} + 1)$ will act in a similar way as the permutation in (c).

(e) $e'_{k-1} < e_{k-1} = e_k - 1 < e'_k - 1$, $e'_{k-1} + 1 \notin \{e_1, e_2, \ldots, e_k\}$: The permutation $(e_{k-1}, e_k)(e'_k, e'_{k-1} + 1)$ will keep $\{e_1, e_2, \ldots, e_k\}$ fixed, and will map e'_k to a value which is one more than e'_{k-1}.

(f) $e'_{k-1} < e_{k-1} = e_k - 1 < e'_k - 1$, $e'_{k-1} + 1 \in \{e_1, e_2, \ldots, e_k\}$: The permutation $(e'_k, e'_{k-1} + 1)(e_k, e'_k - 1)$ will map e'_k to a value which is one more than e'_{k-1}, and since $e'_{k-1} + 1 \in \{e_1, e_2, \ldots, e_k\}$, will also map e_k to a value which is one less than the value which $e'_{k-1} + 1$ was mapped to.

(g) $e_{k-1} = e_k - 1 < e'_{k-1} - 1 < e'_k - 2$: The permutation $(e_{k-1}, e_k)(e'_k, e'_{k-1} + 1)$ will keep $\{e_1, e_2, \ldots, e_k\}$ fixed, but will map e'_k to a value which is one more than the value of e'_{k-1}.

(h) $e'_{k-1} < e'_k - 1 < e_{k-1} - 1 = e_k - 2$: The permutation $(e_{k-1}, e_k)(e'_{k-1}, e'_k - 1)$ will act in a similar way as the one in (g).

Case (iii): $\mathcal{E} \subseteq \mathcal{I}$. Again the following sub-cases are identified.

(a) $e_{k-1} = e'_{k-1} < e'_k - 1 = e_k - 1$: The permutation $(e_k, e_{k-1} + 1)(e_{k-1}, e_{k-1} + 1)$ will map $e_k = e'_k$ to a value which is one more than $e_{k-1} = e'_{k-1}$, and then keep the positions which $\{e_1, e_2, \ldots, e_k\}$ and $\{e'_1, e'_2, \ldots, e'_k\}$ were mapped to in check positions.

(b) $e'_{k-1} < e_{k-1} < e_k - 1 = e'_k - 1$: The permutation $(e_k, e_{k-1} + 1)(e'_{k-1}, e_{k-1} + 2)$ will map $e_k = e'_k$ to a value which is one more than e_{k-1}, and then map e'_{k-1} to a value which is one more than the value which e'_k was mapped to.

(c) $e'_{k-1} = e_{k-1} < e_k - 1 < e'_k - 1$: The permutation $(e_{k-1}, e_k + 1)(e'_k, e_k + 2)$ will act in a similar way to the permutation in (b).

(d) $e'_{k-1} = e'_k - 1 \leq e_{k-1} - 1 < e_k - 2$: The permutation $(e'_{k-1}, e'_k - 1)(e_k, e_{k-1} + 1)$ will map e'_{k-1} to a value which is one less than e'_k, and e_k to a value which is one more than e_{k-1}.

(e) $e'_{k-1} < e_{k-1} < e_k - 1 < e'_k - 1$, $e'_{k-1} + 1 \notin \{e_1, e_2, \ldots, e_k\}$: The permutation $(e'_k, e'_{k-1} + 1)(e_{k-1}, e_k - 1)$ will map e'_k to a value which is one more than e'_{k-1}, and since $e'_{k-1} + 1 \notin \{e_1, e_2, \ldots, e_k\}$, will also map e_{k-1} to a value which is one less than e_k.

(f) $e'_{k-1} < e_{k-1} < e_k - 1 < e'_k - 1$, $e'_{k-1} + 1 \in \{e_1, e_2, \ldots, e_k\}$: The permutation $(e'_k, e'_{k-1} + 1)(e_k, e'_k - 1)$ will map e'_k to a value that is one more than e'_{k-1}, and since $e'_{k-1} + 1 \in \{e_1, e_2, \ldots, e_k\}$, will also map e_k to a value which is one less than the value which $e'_{k-1} + 1$ was mapped to.

(g) $e'_{k-1} < e_{k-1} < e'_k < e_k$, $e'_{k-1} + 1 \notin \{e_1, e_2, \ldots, e_k\}$: The permutation $(e'_k, e'_{k-1} + 1)(e_{k-1}, e_k - 1)$ is the same as the one in (e).

(h) $e'_{k-1} < e_{k-1} < e'_k < e_k$, $e'_{k-1} + 1 \in \{e_1, e_2, \ldots, e_k\}$: The permutation $(e'_k, e'_{k-1} + 1)(e_k, e'_k + 1)$ will act in a similar way as the one in (f).

Hence $\mathcal{S} = \{(k - 1 + i, k + j)(k - 1 + i', k + j') : 0 \leq i \leq j \leq k + 1,\ 0 \leq i' \leq j' \leq k + 1\}$ is a 2-PD-set for C. Clearly, $|\mathcal{S}| = |\{(i, j) : 0 \leq i \leq j \leq k + 1\}|^2 = \binom{k+3}{2}^2$. □

Conjecture 4.3.
Let $\mathcal{I}$ be the information positions as given in Theorem 4.2. Then for $k \geq 2$,

- $\mathcal{S} = \{1_{S_{2k+1}}\} \cup \{(k-(\lfloor k/2 \rfloor - 1)+i_1, k+j_1)(k-(\lfloor k/2 \rfloor - 1)+i_2, k+j_2)\ldots(k-(\lfloor k/2 \rfloor - 1)+i_{\lfloor k/2 \rfloor}, k+j_{\lfloor k/2 \rfloor}) : 0 \leq i_1 \leq j_1 \leq k+1, 0 \leq i_2 \leq j_2 \leq k+1, \ldots, 0 \leq i_{\lfloor k/2 \rfloor} \leq j_{\lfloor k/2 \rfloor} \leq k+1\}$ *is a PD-set of size* $\binom{k+3}{2}^{\lfloor k/2 \rfloor}+1$ *for C if $\lfloor k/2 \rfloor$ is odd,*
- $\mathcal{S} = \{(k-(\lfloor k/2 \rfloor - 1)+i_1, k+j_1)(k-(\lfloor k/2 \rfloor - 1)+i_2, k+j_2)\ldots(k-(\lfloor k/2 \rfloor - 1)+i_{\lfloor k/2 \rfloor}, k+j_{\lfloor k/2 \rfloor}) : 0 \leq i_1 \leq j_1 \leq k+1, 0 \leq i_2 \leq j_2 \leq k+1, \ldots, 0 \leq i_{\lfloor k/2 \rfloor} \leq j_{\lfloor k/2 \rfloor} \leq k+1\}$ *is a PD-set of size* $\binom{k+3}{2}^{\lfloor k/2 \rfloor}$ *for C if $\lfloor k/2 \rfloor$ is even.*

The Gordon bound for a PD-set for C for $k \geq 2$ simplifies to the following:

$$\left\lceil\left\lceil\left\lceil\left\lceil\cdots\left\lceil 3\left(2+\frac{1}{k}\right)\right\rceil\left(2+\frac{1}{k}\right)\right\rceil\left(2+\frac{1}{k}\right)\right\rceil\left(2+\frac{1}{k}\right)\right\rceil\cdots\right\rceil\left(2+\frac{1}{k}\right)\right\rceil.$$

($\lfloor k/2 \rfloor - 1$ ceilings are determined in the expression above.) It is easily observed that this bound is of the order of $2^{\lfloor k/2 \rfloor + 1}$.

5. The dual code from $O(k)$ and the code from its complement $\overline{O(k)}$

The complement of the odd graph $\overline{O(k)}$, has as its vertex set $\mathcal{P}_c = \Omega^{\{k\}}$, and two vertices u and v constitute an edge $[u, v]$ if and only if $u \cap v \neq \emptyset$. The binary code generated by the adjacency matrix of $\overline{O(k)}$ is also the code obtained from the $1-\left(\binom{2k+1}{k}, \binom{2k+1}{k}-k-2, \binom{2k+1}{k}-k-2\right)$ design $\mathcal{D}_c = (\mathcal{P}_c, \mathcal{B}_c)$ where for each point $\{a_1, a_2, \ldots, a_k\} \in \Omega^{\{k\}}$ a corresponding block denoted by $\overline{\{a_1, a_2, \ldots, a_k\}}_c$ is defined as follows:

$$\overline{\{a_1, a_2, \ldots, a_k\}}_c = \{\{x_1, x_2, \ldots, x_k\} : \{x_1, x_2, \ldots, x_k\} \cap \{a_1, a_2, \ldots, a_k\} \neq \emptyset,\ \{x_1, x_2, \ldots, x_k\} \neq \{a_1, a_2, \ldots, a_k\}\}.$$

The block set $\mathcal{B}_c$ is given by

$$\mathcal{B}_c = \{\overline{\{a_1, a_2, \ldots, a_k\}}_c : \{a_1, a_2, \ldots, a_k\} \in \Omega^{\{k\}}\},$$

and the incidence vector of $\overline{\{a_1, a_2, \ldots, a_k\}}_c$ by

$$v_c^{\overline{\{a_1, a_2, \ldots, a_k\}}} = \sum_{\substack{\{x_1, x_2, \ldots, x_k\} \cap \{a_1, a_2, \ldots, a_k\} \neq \emptyset \\ \{x_1, x_2, \ldots, x_k\} \neq \{a_1, a_2, \ldots, a_k\}}} v^{\{x_1, x_2, \ldots, x_k\}}. \tag{7}$$

From equations (1) and (7), observe that

$$v_c^{\overline{\{a_1, a_2, \ldots, a_k\}}} = v^{\overline{\{a_1, a_2, \ldots, a_k\}}} + v^{\{a_1, a_2, \ldots, a_k\}} + \boldsymbol{j}. \tag{8}$$

Let C and $C^\perp$ denote the binary code and its dual from the odd graph as before, and let $\overline{C}$ denote the binary code from the adjacency matrix of $\overline{O(k)}$.

Lemma 5.1.
If k is even, or if k is odd and $k \neq 2^m - 1$ for some $m \geq 2$, then $C^\perp \subseteq \overline{C}$. However, if k is odd and $k = 2^m - 1$, then $U = \{v(\{b_1, b_2, \ldots, b_{k-1}\}) + v(\{k+3, k+4, \ldots, 2k+1\}) : \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \backslash \{1\},\ \{b_1, b_2, \ldots, b_{k-1}\} \neq \{k+3, k+4, \ldots, 2k+1\}\}$ is a basis for $C^\perp \cap \overline{C}$, and $C^\perp \cap \overline{C}$ has co-dimension 1 in $C^\perp$.

Proof. By equation (8), in $\overline{C}$ the sum

$$\sum_{x\in\Omega\setminus\{b_1,b_2,\ldots,b_{k-1}\}} v_c^{\overline{\{b_1,b_2,\ldots,b_{k-1},x\}}} = \sum_{x\in\Omega\setminus\{b_1,b_2,\ldots,b_{k-1}\}} v^{\overline{\{b_1,b_2,\ldots,b_{k-1},x\}}} + \sum_{x\in\Omega\setminus\{b_1,b_2,\ldots,b_{k-1}\}} v^{\{b_1,b_2,\ldots,b_{k-1}x\}} + (k+2)\boldsymbol{j}$$
$$= 2 \sum_{\{x_1,x_2,\ldots,x_k\}\subseteq\Omega\setminus\{b_1,b_2\ldots,b_{k-1}\}} v^{\{x_1,x_2,\ldots,x_k\}} + v(\{b_1,b_2,\ldots,b_{k-1}\}) + k\boldsymbol{j} = v(\{b_1,b_2,\ldots,b_{k-1}\}) + k\boldsymbol{j}.$$

Now if k is even, then the sum reduces to $v(\{b_1,b_2,\ldots,b_{k-1}\})$, and hence $v(\{b_1,b_2,\ldots,b_{k-1}\}) \in \overline{C}$. If k is odd and $k \neq 2^m-1$ for some $m \geq 2$, then $\binom{2k+1}{k}$ is even. The weight, $\binom{2k+1}{k} - k - 2$, of each incidence vector of $\overline{C}$ is odd, which implies that $\boldsymbol{j} \in \overline{C}$, and again, $v(\{b_1,b_2,\ldots,b_{k-1}\}) \in \overline{C}$. However, if k is odd and $k = 2^m-1$, then $\binom{2k+1}{k}$ is odd, and by a similar argument as above, it follows that $\boldsymbol{j} \in \overline{C}^{\perp}$, and since its weight is odd, $\boldsymbol{j} \notin \overline{C}$. Note that since k is odd, $\boldsymbol{j} \in C^{\perp}$ by Lemma 3.8. Hence $v(\{b_1,b_2,\ldots,b_{k-1}\}) + \boldsymbol{j} \in C^{\perp} \cap \overline{C}$ for each $\{b_1,b_2,\ldots,b_{k-1}\} \subseteq \Omega$. Clearly, $U = \{v(\{b_1,b_2,\ldots,b_{k-1}\}) + v(\{k+3,k+4,\ldots,2k+1\}) : \{b_1,b_2,\ldots,b_{k-1}\} \subseteq \Omega\setminus\{1\},\ \{b_1,b_2,\ldots,b_{k-1}\} \neq \{k+3,k+4,\ldots,2k+1\}\}$ is a linearly independent set in $C^{\perp}\cap\overline{C}$. Hence $\binom{2k}{k-1} = \dim(C^{\perp}) \geq \dim(C^{\perp}\cap\overline{C}) \geq \binom{2k}{k-1} - 1$, and since $\boldsymbol{j} \in C^{\perp}$, the final statement of the lemma follows. □

Acknowledgements

The authors are indebted to Professor Jennifer Key from the Department of Mathematics and Applied Mathematics at the University of the Western Cape for her advice and encouragement.

References

[1] Bailey R.F., Distance-Transitive Graphs, MMath thesis, University of Leeds, 2002
[2] Balaban A.T., Chemical graphs, part XII: Combinatorial patterns, Rev. Roumaine Math. Pures Appl., 1972, 17, 3–16
[3] Ball R.W., Maximal subgroups of symmetric groups, Trans. Amer. Math. Soc., 1966, 121(2), 393–407
[4] Biggs N., An edge-colouring problem, Amer. Math. Monthly, 1972, 79(9), 1018–1020
[5] Cameron P.J., Automorphism groups of graphs, In: Selected Topics in Graph Theory, 2, Academic Press, London, 1983, 89–127
[6] Chen B.L., Lih K.-W., Hamiltonian uniform subset graphs, J. Combin. Theory Ser. B, 1987, 42(3), 257–263
[7] Huffman W.C., Codes and groups, In: Handbook of Coding Theory, II, 2, North-Holland, Amsterdam, 1998, 1345–1440
[8] Kroll H.-J., Vincenti R., PD-sets for the codes related to some classical varieties, Discrete Math., 2005, 301(1), 89–105
[9] MacWilliams J., Permutation decoding of systematic codes, Bell System Tech. J., 1964, 43, 485–505
[10] MacWilliams F.J., Sloane N.J.A., The Theory of Error-Correcting Codes, North-Holland Math. Library, 16, North-Holland, Amsterdam, 1977
[11] Meredith G.H.J., Lloyd E.K., The footballers of Croam, J. Combinatorial Theory Ser. B, 1973, 15, 161–166