Codes from Uniform Subset Graphs and Cycle Products

by

Washiela Fish

A thesis submitted in fulfilment of the requirements for the degree of Ph.D. in the Department of Mathematics and Applied Mathematics, University of the Western Cape

Supervisor: Prof. R. Fray
Co-supervisor : Dr. E. Mwambene

April 2007

Declaration

I declare that *Codes from Uniform Subset Graphs and Cycle Products* is my own work, that it has not been submitted before for any degree or assessment to any other university, and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

. . . . . .

Washiela Fish

April 2007

Acknowledgements

All praise and thanks is due to Almighty God for bringing me to this stage of my journey towards knowledge and understanding.

I would like to thank my supervisor, Prof. Fray, for allowing me to embark on this journey in the first place. His advice and willingness to provide resources, even if it meant getting help from outside, will always be appreciated.

I would also like to thank my co-supervisor, Dr. Mwambene, for accompanying me for much of the way, and then watching anxiously from a distance, as I continued on my way. His encouragement, and commitment to his subject serve as shining examples for any educator.

In fact, I would like to express my sincerest gratitude to all the members of the Mathematics Department for their concern about my well-being on this journey.

Of course, any journey undertaken requires the cooperation of those who will be most affected by it. In this regard, I am eternally indebted to my dear parents, Rugaya and Ismail, for their unconditional love and support. I am also greatly indebted to my husband, Achmat, and my children, Maryam, Abdul-Aziz and Amina, for their endless patience and understanding, especially when the route was mostly uphill. Lastly, I would like to thank my sister, Fatima, and my "brother", Abraham Prins, whose love for laughter and life in general, made the mountains that I have had to climb on the journey appear a little less high, and the rivers I have had to cross, a little less wide.

I acknowledge the financial assistance in the form of a Scarce Skills scholarship that I have received from the NRF.

I would also like to thank Lauretta Adams from the Department of Mathematical Sciences, Mathematics Division at the University of Stellenbosch who assisted so ably with the typing of this thesis.

Abstract

In [17] Key et al. described the binary codes generated by the adjacency matrix of the Triangular graph $T(n)$. Although the parameters for these codes were known from [13] and [40], the perspective was new, and on the basis of a set of information positions which had been identified for the code, the authors determined PD-sets for the code of the order of n when n is odd, and of the order of n^2 when n is even. In [35] a similar treatment was given to the binary codes from the graphs generated by the 3-subsets of $\Omega = \{1, 2, \ldots, n\}$, in which adjacency was determined by the size of the intersection of any two 3-subsets.

Now both of the classes of graphs described above constitute subclasses of the huge class of distance-transitive graphs known as the Uniform Subset graphs, and denoted in the literature by $G(n, k, r)$. $G(n, k, r)$ is defined to be the graph of which the vertex-set is the set of k-subsets of $\Omega = \{1, 2, \ldots, n\}$, and any two vertices u and v constitute an edge $[u, v]$ if and only if $|u \cap v| = r$. $G(n, k, r)$ is regular, and $\binom{k}{r}\binom{n-k}{k-r}$-connected. It is strongly regular only in the case of the Triangular graph $T(n)$, and its complement $\overline{T(n)}$. Moreover, the automorphism groups for $G(n, k, r)$ for various values of n, k and r are both well-known and large, thereby increasing the potential for determining PD-sets from amongst these group elements. The most important subclasses of $G(n, k, r)$ are the Odd graphs $O(k)$, the Johnson graphs $J(n, k)$, of which the Triangular graphs are a further subclass, and the Kneser graphs $K(n, k)$.

In this thesis only binary codes are studied. Firstly, the codes generated over the field $GF(2)$ by the adjacency matrix of the complement, $\overline{T(n)}$, of the Triangular graph, are

examined. It is shown that the code obtained is the full space $F_2^{\binom{n}{2}}$ when $n \equiv 0(\text{mod } 4)$, and the dual code of the space generated by the $\boldsymbol{j}$-vector when $n \equiv 2(\text{mod } 4)$. The codes from the other two cases are less trivial: when $n \equiv 1(\text{mod } 4)$ the code is an $[\binom{n}{2}, \binom{n}{2}-n+1, 3]$ code, and when $n \equiv 3(\text{mod } 4)$ it is an $[\binom{n}{2}, \binom{n}{2}-n, 4]$ code. Furthermore, a set of information positions is identified for $C^{\perp}$ in the non-trivial cases, and PD-sets of the order of n and n^2 are determined.

A similar treatment is given to the codes generated by $O(k)$. It is shown that the code generated by the adjacency matrix of $O(k)$ is a $[\binom{2k+1}{k}, \binom{2k}{k}, k+1]$ code, and its dual a $[\binom{2k+1}{k}, \binom{2k}{k-1}, k+2]$ code. The automorphism group of $O(k)$ is known to be S_{2k+1}, and by an explicit argument, the automorphism group of the code is also shown to be S_{2k+1}. A 2-PD-set of the order of k^4 is determined with a set of information positions alternative to that identified from a natural basis for the code.

The results pertaining to the codes generated by $J(n,k)$ are generalisations of the results obtained in [17] and [35]. In fact, it is shown that if k is odd, and $n = 2k+1$ then the code from $J(n,k)$ is identical to the code from $O(k)$.

Codes generated by the cartesian, categorical, and lexicographic products of the n-cycles are also given attention. Amongst the results obtained are that the categorical product of m copies of C_n generate an $[n^m, (n-1)^m, 2^m]$ code if n is odd, and an $[n^m, (n-2)^m, 2^m]$ code if n is even. If $n = 8$ then the cartesian product of m copies of C_8 generate an $[8^m, 6.8^{m-1}, 2m]$ code, and on the evidence of the deduction that the cartesian product of m copies of C_4 generate a $[4^m, 2.4^{m-1}, 2m]$ code, it is conjectured that if $n = 2^k$, where $k \geq 2$, then the cartesian product of m copies of C_n generate an $[n^m, (n-2).n^{m-1}, 2m]$ code. For the codes generated by the cartesian product of m copies of C_2, where $m \geq 6$, a 2-PD-set is determined, and for those generated by the categorical product of m copies of C_n, m-PD-sets are determined.

List of Symbols

$\subseteq$	is a subset of
$\cong$	is isomorphic to
$\equiv$	is equivalent to
$\emptyset$	the empty set
$\leq$	less than or equal to
$\in$	is an element of
$\cup$	the union of
$\cap$	the intersection of
$\sum$	the sum of
$\lceil\ \rceil$	the ceiling of
$\lfloor\ \rfloor$	the floor of
$d(u, v)$	the distance between the vertices u and v
$[u, v]$	the edge joining the vertices u and v
(v, w)	the standard inner product of the vectors v and w
$[n, k, d]_q$	a q-ary code of length n, dimension k, and minimum weight d
I_k	the $k \times k$ identity matrix
A^T	the transpose of the matrix A
$C^\perp$	the dual code of C
$F_q, GF(q)$	the Galois field of order q
F_q^n	the n-dimensional vector space over F_q
C_n	the n-cycle

$G(n,k,r)$	the Uniform Subset graph
$T(n)$	the Triangular graph
$\overline{T(n)}$	the complement of the Triangular graph
$O(k)$	the Odd graph
$J(n,k)$	the Johnson graph
S_n	the symmetric group on n letters
A_n	the alternating group on n letters
D_{2n}	the dihedral group on n letters
$A \times B$	the direct product of A and B
$A \wr B$	the wreath product of A and B
$A \rtimes B$	the semi-direct product of A and B
$\|X\|$	the cardinality of a set X
$\binom{n}{k}$	n choose k
$\Omega^{\{k\}}$	the k-subsets of Ω
$C \oplus C^{\perp}$	the direct sum of a code C and its dual
1_G	the identity element of a group G
$\dim(C)$	the dimension of a code C
$\mathrm{Aut}(C)$	the automorphism group of a code C
$\mathrm{Aut}(G)$	the automorphism group of a graph G
$H \leq G$	H is a subgroup of G
$\square_{i=1}^{m} C_n$	the cartesian product of m copies of C_n
$\prod_{i=1}^{m} C_n$	the categorical product of m copies of C_n
$[\ ]_{i=1}^{m} C_n$	the lexicographic product of m copies of C_n
$\boxtimes_{i=1}^{m} C_n$	the strong product of m copies of C_n

Contents

Chapter 1

Introduction

There are many instances in everyday life when information has to be transmitted from a sender to a receiver via a channel. A channel may take various forms. Telephone lines, radio and television, audio and video recorders, compact disks and flash drives are examples of channels. The information transmitted via a channel is prone to interference, termed noise, which may be the result of adverse weather conditions in the case of radio and television, damage such as scratches in the case of a compact disk or competing telephone messages in the case of telephone lines. The issues of reliability and accuracy, coupled with efficiency, are thus fundamental issues in information transmission. Coding theory has been developed to address the problem of detecting and correcting transmission errors caused by noise in a channel. In particular, coding schemes have to be designed which will facilitate relatively simple and fast encoding of the original information by the addition of redundancy, which can in turn be used to recover the original information. The more redundancy is added, the more reliably and accurately errors can be detected and corrected, but the less efficiently information is transmitted. Hence any solution to the problem is necessarily a trade-off between these core issues. The historical account that follows is an amalgamation of information in [14], [34], [41], [44] and [36].

In 1948 Claude Shannon proved the *Noisy Coding Theorem* which states the following:

Every channel has an associated channel capacity $\mathcal{C}$. Furthermore, there exist codes such that information can be transmitted across the channel at rates less than $\mathcal{C}$ with arbitrarily small probability of error. Unfortunately, Shannon's proof, nor any proof given since, showed how such codes could be constructed, but merely established their existence. Besides, even if codes that satisfied Shannon's criteria were discovered, their implementation may be highly impractical: since the probability of error has to be small, the lengths of such codes may be unwieldy, or the encoding and decoding may be very complex. In their quest to find codes that are relatively easy to implement, coding theorists have turned their attention to codes that have rich algebraic and geometric structure.

In 1950 Hamming introduced the first major class of linear codes that were specifically designed for error correction. Hamming codes are perfect $[2^m - 1, 2^m - m - 1, 3]$ binary codes and since they are single-error correcting, they can be decoded using syndrome decoding.

Cyclic codes were the next important class of codes that were discovered. In 1957 E. Prange introduced cyclic codes which he identified with ideals. Cyclic codes are of practical importance since, amongst others, they facilitate fast and efficient encoding and decoding using high-speed shift registers. Hadamard codes are cyclic codes which result from the decomposition of Hadamard matrices which were first introduced in 1893. These include both linear and non-linear codes, the smaller non-linear ones having especially agreeable properties. In 1958 Prange introduced quadratic residue codes. These are linear cyclic codes with large minimum distances and information rates approximately $\frac{1}{2}$. The interest in decoding algorithms for quadratic residue codes has made them widely applicable.

In 1948 Shannon also described Hamming's perfect $[7, 4, 3]$ code. In 1949, in a quest for similar codes, Golay extended this code to a class of p-ary codes of length $\dfrac{p^m - 1}{p - 1}$ where p is a prime. Furthermore, Golay described a perfect binary triple-error-correcting code and a perfect ternary double-error-correcting code. The Golay codes were derived from an inspection of Pascal's triangle and the recognition of the connection between the

entries in the triangle to perfect codes. Golay codes have been used in the space program of the USA. In particular, the extended binary Golay code was used to provide clear colour photographs of Jupiter and Saturn between 1979 and 1981. The "error-trapping" decoding algorithm described in 1964 by Kasami is one of the many efficient decoding algorithms for the Golay codes.

In 1954 Muller described the codes that are now called the Reed-Muller codes by using Boolean functions. Reed identified Muller's codes as multinomials over $GF(2)$, and the resulting Reed-Muller codes had an advantage over Hamming and Golay codes in that varying numbers of errors per codeword could be corrected. An application of the Reed-Muller codes has been the use of a first-order code of length thirty-two in the Mariner space probes flown between 1969 and 1977. An investigation into the theory on which the Reed-Muller codes are based has led to the discovery of new codes such as the Kerdock and the Preparata codes. Reed-Muller codes also have the benefit of a fast maximum likelihood decoding algorithm.

BCH (Bose-Hocquenghem-Chaudhuri) codes were first proposed in 1959 as a generalization of the Hamming codes. They were shown to be cyclic by Petersen in 1960 who also devised a decoding algorithm for them. The Reed-Solomon codes are maximum distance separable codes that were introduced by Reed and Solomon in 1969. They were shown to be closely related to BCH codes - they could be characterized as non-binary BCH codes. When an efficient decoding algorithm was discovered for BCH codes in 1968, coupled with the recognition that long BCH and Reed-Solomon codes performed better than Reed-Muller codes, the use of the latter fell out of favour.

Convolutional codes were first introduced by Elias in 1969. Whereas in the case of block codes, information divided into streams of some fixed length k are converted to codewords of some fixed length n, in the case of convolutional codes the entire information stream is converted into a single codeword. Redundancy was introduced through the use of a shift register, and the resulting codes were found to be capable of detecting and correcting errors fairly accurately and reliably, thereby giving credence to Shannon's *Noisy Coding Theorem*

of 1948. Various decoding algorithms were described for convolutional codes, the first of these being that of Wozencraft and Reiffen. Massey described majority logic decoding algorithms for both block and convolutional codes. In 1967 Viterbi described another approach to decoding convolutional codes, and it was later shown that this algorithm was in fact a maximum-likelihood decoding algorithm for convolutional codes.

The historical account above describes some of the ways in which the problem of designing codes that had rich algebraic and geometric structure and therefore facilitated relatively simple encoding and decoding, was addressed. Another approach to the problem is the construction of codes from combinatorial structures such as designs, projective geometries and graphs. (See [35] for a detailed discussion on the interplay between these structures.) The primary focus of this thesis is the description of some codes which have been constructed from certain classes of graphs. The codes obtained are the span over $GF(2)$ of the rows of the adjacency matrix of the graphs under consideration, and important parameters such as their dimension and minimum weight are determined. Other important issues considered are whether the code has a basis comprising minimum weight vectors, the identification of its minimum words, and whether it is self-orthogonal, self-dual, or whether the direct sum of the code and its dual is the full vector space. Recent examples appearing in the literature of codes constructed in this way are the codes from the line graphs of complete bipartite graphs in [16], the codes from the line graphs of complete multipartite graphs in [18], the codes from Triangular graphs in [17], and the codes from the graphs on 3-subsets in which adjacency is determined by the size of the intersection of any two 3-subsets in [35].

The code generated by the rows of the adjacency matrix of a graph is also the code of the $1-(v,k,k)$ design in which the rows constitute the incidence vectors of the blocks of the design. Codes generated by the incidence vectors of designs have been used to construct new designs, to extend designs, and to refute the existence of particular designs. On the other hand, coding theory has benefited from the existence of certain designs in that the rich geometric structure of a design impacts on the weight distribution of a code, and facilitates comparatively simple encoding and decoding.

Codes can also be constructed from algebraic structures such as simple groups and near-rings, but such constructions will not be delved into in this thesis. ([35] can be consulted for some information on codes from simple groups.) In Chapter 2 then, only the preliminaries relating to codes, designs and graphs are discussed.

A similar sentiment applies to the theory presented in Chapter 3 - despite the fact that there are other important decoding algorithms such as maximum likelihood decoding and majority logic decoding, only permutation decoding is detailed so as not to sidetrack from the line of discussion and to arrive at the research topics as quickly as possible.

Chapter 4 sets the stage for the research that follows in Chapters 5, 6 and 7. A historical account, as well as some of the graph-theoretical properties of the important class of distance-transitive graphs, the Uniform Subset graphs, is given in detail. The focus on the Uniform Subset graphs was motivated by the observation that the Triangular graphs discussed in [17], as well as the graphs on 3-subsets discussed in [35], form part of this large class of highly symmetric graphs of which the automorphism groups were both well-known and large. The Uniform Subset graph $G(n,k,r)$ has as its vertex-set the k-subsets of $\Omega = \{1,2,\ldots,n\}$, and any two vertices u and v constitute an edge $[u,v]$ if and only if $|u \cap v| = r$. $G(n,k,r)$ is shown to be regular (strongly regular only in the case of the Triangular graph $T(n)$ and its complement $\overline{T(n)}$) and $\binom{k}{r}\binom{n-k}{k-r}$-connected. This chapter concludes with the characterization of vertex-transitive graphs as subgraphs induced by the orbits of Uniform Subset graphs under some group action as discussed in [33].

In Chapter 5 the codes generated by the adjacency matrix of the complement, $\overline{T(n)}$, of the Triangular graph, are examined. Trivially, the code obtained is the full space $F_2^{\binom{n}{2}}$ when $n \equiv 0(\text{mod } 4)$, and the dual code of the span of the $\boldsymbol{j}$-vector when $n \equiv 2(\text{mod } 4)$. However, when $n \equiv 1(\text{mod } 4)$ the code is an $[\binom{n}{2}, \binom{n}{2} - n + 1, 3]$ code, and when $n \equiv 3(\text{mod } 4)$, it is an $[\binom{n}{2}, \binom{n}{2} - n, 4]$ code. Furthermore, in the former case both the code and its dual are shown to have bases comprising minimum weight vectors, whereas in the latter case only the code has a minimum weight basis since the $\boldsymbol{j}$-vector has to be adjoined to any set of minimum weight basis vectors in the dual code. The code generated by the rows of the

adjacency matrix of $\overline{T(n)}$ is also the code of the $1-\left(\binom{n}{2},\binom{n-2}{2},\binom{n-2}{2}\right)$ design $\mathcal{D}$ of which the point set $\mathcal{P}$ is the vertex-set of $\overline{T(n)}$, and the block set $\mathcal{B}$ the supports of the set of incidence vectors of its adjacency matrix. It is shown explicitly that for the non-trivial codes, the automorphism group is the symmetric group S_n. In a similar manner as in [17], a set of information positions are identified for the dual code and permutation decoding sets of the order of n and n^2 are determined in the non-trivial cases.

In Chapter 6 a similar treatment is given to the Odd graph $O(k), O(k)$ being the Uniform Subset graph $G(2k+1,k,0)$. It is shown that the code generated by the adjacency matrix of $O(k)$ is a $[\binom{2k+1}{k},\binom{2k}{k},k+1]$ code, and its dual a $[\binom{2k+1}{k},\binom{2k}{k-1},k+2]$ code. Moreover, the incidence vectors are shown to constitute the minimum words, and hence the code has a basis consisting of minimum weight vectors. The dual is also shown to have a minimum weight basis. It is shown explicitly that the automorphism group of the code is S_{2k+1}. Using an alternative information set to the one derived from the natural basis, a 2-PD-set of the order of k^4 is determined for this code.

In Chapter 7 the codes and their duals generated by the adjacency matrix of the Johnson graphs $J(n,k)$ i.e. the Uniform Subset graphs $G(n,k,k-1)$, are discussed. It is shown that in each case, the code has a basis comprising minimum weight vectors. The same does not apply to the dual codes, however, for if both n and k are even, then the minimum weight vectors do not span the dual code. In all the non-trivial cases it is shown that the automorphism group of the code is S_n. The work in this chapter is an extension of the work in [17] since $T(n)$ is the Johnson graph $J(n,2)$, and the codes derived from it as given in [17] are a specific case of the codes derived from $J(n,k)$ when k is even. A similar statement applies to the codes from $J(n,3)$ as described in [35] in relation to the codes from $J(n,k)$ when k is odd. Furthermore, it is observed that the code from $J(n,k)$ equals the code from $O(k)$ when k is odd and $n=2k+1$.

Chapter 8 is a discussion on the codes generated by the various graph products of the n-cycle C_n. The graph products considered are the cartesian product, the categorical product and the lexicographic product. (The other important product, the strong product,

is also introduced, although the codes generated by it are not elaborated on.) It is shown that the code generated by the categorical and the lexicographic product of m copies of C_2 is the full space $F_2^{2^m}$. Insofar as the cartesian product is concerned, this is only the case when m is odd - when m is even then the code is a $[2^m, 2^{m-1}, m]$ self-dual code. Further results obtained are that the categorical product of m copies of C_n generate an $[n^m, (n-1)^m, 2^m]$ code of which the dual is an $[n^m, n^m-(n-1)^m, n]$ code if n is odd, and an $[n^m, (n-2)^m, 2^m]$ code of which the dual is an $[n^m, n^m-(n-2)^m, \frac{n}{2}]$ code if n is even. It is shown explicitly that the cartesian product of m copies of C_8 generate an $[8^m, 6.8^{m-1}, 2m]$ code, and in conjunction with an earlier observation that the cartesian product of m copies of C_4 generate a $[4^m, 2.4^{m-1}, 2m]$ code, it is conjectured that if $n = 2^k$, where $k \geq 2$, then the cartesian product of m copies of C_n generate an $[n^m, (n-2).n^{m-1}, 2m]$ code which contains its dual.

Magma [6] version 2.9 running on a 1.5 GHz Pentium M processor was used for all the computations. Some of the programmes especially written for the research in this thesis are given in the Appendices.

Chapter 2

The Preliminaries relating to Codes, Designs and Graphs

This chapter deals with some introductory definitions and results relating to codes, designs and graphs which will be required in subsequent chapters. The treatment is not claimed to be complete nor is it claimed to be extensive, but merely sets the stage for subsequent chapters, and the interested reader is referred to [1], [42] and [36] for further details.

2.1 Codes

Some general notions about codes introduce the discussion.

Definition 2.1.1. *Let F be a finite set, termed an* **alphabet**, *of q elements. A* **q-ary** *code C is a set of finite sequences of elements of F, called* **codewords**. *If all the sequences in C have the same length n, then C is called a* **block code** *of length n.*

All the codes studied in this thesis are block codes - they are generated by the rows of the adjacency matrix of various graphs. Depending on the definition of adjacency of the

points of the graph, these rows will generally differ.

Definition 2.1.2. *Let C be a q-ary code, and c and c' codewords in C. The* **Hamming distance** *between c and c', denoted by $d(c, c')$, is the number of positions in which they differ.*

The Hamming distance is usually referred to as the **distance** between two codewords. It defines a metric on the set of all sequences of length n over the alphabet F.

Definition 2.1.3. *The* **minimum distance** *d of a code C is the minimum of the distances between any two distinct codewords in C i.e.*

$$d = \min\{d(c, c') : c, c' \in C,\ c \neq c'\}.$$

The minimum distance impacts on both the error-detecting and error-correcting capabilities of the code, as proclaimed below.

Theorem 2.1.4. **[1, Theorem 2.1.1]** *Let C be a code with minimum distance d, and let s and t be the maximum number of errors that C can detect and correct respectively. Then $s \leq d - 1$ and $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$.*

From Theorem 2.1.4 it is evident that the larger the minimum distance, the more errors C is able to detect and correct. However, a large minimum distance is usually attained at the expense of a long block length, and encoding and decoding may be inefficient. Ideally, C should consist of many codewords in order that a variety of messages can be transmitted. The number of codewords of length n can clearly not exceed the number of sequences over F of length n. There are further restrictions on the number of codewords in C, and these are given below.

Theorem 2.1.5. **[1, Theorem 2.1.2]** *Let C be a q-ary code of length n (i.e. the code-*

words all have length n) and minimum distance d. Then

$$|C| \leq q^{n-d+1}.$$

The bound above is termed the **Singleton bound**. Another important bound, which is considered to be better than the Singleton bound, is the **Sphere-packing bound** given below.

Theorem 2.1.6. [1, Theorem 2.1.3] *Let C be a q-ary code of length n and minimum distance d. Then*

$$|C| \leq \frac{q^n}{1 + n(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{\lfloor \frac{d-1}{2} \rfloor}(q-1)^{\lfloor \frac{d-1}{2} \rfloor}}.$$

The number $\left\lfloor \frac{d-1}{2} \right\rfloor$ is referred to in the literature as the **sphere-packing radius** of C. Letting $\left\lfloor \frac{d-1}{2} \right\rfloor = t$, C is called a **perfect t-error-correcting code** if the Sphere-packing bound is met. Furthermore, if C is a binary code, then the bound above is termed the **Hamming bound**.

Now let the alphabet F be a finite field of order q, which will be denoted by F_q, and let F_q^n denote the n-dimensional vector space over F_q. Of primary interest in this thesis are the subspaces of F_q^n.

Definition 2.1.7. *A* **linear code** *of length n over the field F_q is a subspace of F_q^n. If $\dim(C) = k$, then C is written $[n,k]_q$, or simply $[n,k]$ if $q = 2$. The* **information rate** *is $\frac{k}{n}$, and the* **redundancy** *is $n - k$.*

Every linear code C contains the all-zero vector $0 \in F_q^n$, and this fact is used in the following definition:

Definition 2.1.8. *Let C be an $[n,k]_q$ code. The* **weight** *of a codeword $c \in C$ is given by $weight(c) = d(0,c)$.*

Now if $c, c' \in C$, then since C is a subspace, $c - c' \in C$. Since in addition, $d(c, c') = d(0, c - c')$, it follows that the **minimum weight** of a linear code C is its minimum distance d. If the minimum weight of C is known and equals d, then C is an $[n, k, d]_q$ code, or simply an $[n, k, d]$ code if $q = 2$. Since the number of words in C is now q^k, the Singleton bound and the Sphere-packing bound reduce to $d \leq n - k + 1$ and $\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i \leq q^{n-k}$ respectively. C is said to be **doubly-even** if the weight of all its codewords are divisible by 4.

Definition 2.1.9. *Let C and C' be linear codes of length n over F_q. Then C and C' are* **equivalent** *if each can be obtained from the other by permuting the coordinate positions of F_q^n and multiplying each coordinate by a non-zero field element. They are* **isomorphic** *if the one can be obtained from the other by merely permuting the coordinate positions.*

For C an $[n, k, d]_q$ code and $c \in C$, let

$$A_i(c) = |\{c' \in C : \ d(c, c') = i\}|.$$

Clearly, for $0 \leq i \leq n, A_i(c) \geq 0$. Also, $A_0(c) = 1$, and $\sum_{i=0}^{n} A_i(c) = q^k$. The linearity of C implies that $A_i(c) = A_i(c')$ for any $c, c' \in C$, and any $0 \leq i \leq n$, and hence the reference to c in $A_i(c)$ may be dropped. The sequence (as given in Magma outputs) $(< A_i, i >: 0 \leq i \leq n)$ is called the **weight distribution** of C.

Definition 2.1.10. *Let C be an $[n, k, d]_q$ code. The* **weight enumerator** *of C is the polynomial*

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i.$$

Note that the above polynomial can also be written in the form

$$W_C(x, y) = \sum_{c \in C} x^{n - \text{weight(c)}} y^{\text{weight(c)}}.$$

Definition 2.1.11. *Let C be an $[n,k]_q$ code. The* **dual code** *of C, denoted by $C^\perp$, is given by*

$$C^\perp = \{v \in F_q^n : (v,c) = 0, \text{ for all } c \in C\},$$

where $(\ ,\ )$ denotes the standard inner product on F_q^n. Furthermore, if $C \subseteq C^\perp$, then C is said to be **self-orthogonal**, *and if $C = C^\perp$, then C is said to be* **self-dual**. *The* **hull** *of C is the subspace $C \cap C^\perp$ of F_q^n.*

The above definition provides another way of specifying a linear code. Before elaborating further on the relationship between C and $C^\perp$, it should be noted that the famous result of MacWilliams [28] gives a relationship between the weight enumerator of $C^\perp$ and that of C. To be explicit,

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(y-x, y+(q-1)x).$$

Since an $[n,k]_q$ code is a subspace of F_q^n, it can be described in terms of a basis for that subspace.

Definition 2.1.12. *Let C be an $[n,k]_q$ code. A* **generator matrix** *$\mathcal{G}$ for C is a $k \times n$ matrix obtained from any set of k linearly independent vectors in C.*

Since the dual code $C^\perp$ is the null space of $\mathcal{G}$, the following result is deduced:

Proposition 2.1.13. [1, Proposition 2.3.1] *Let C be an $[n,k]_q$ code. Then*

$$\dim(C) + \dim(C^\perp) = n.$$

Now if $\mathcal{G}$ is a generator matrix for C, then a generator matrix $\mathcal{H}$ for $C^\perp$ is an $(n-k) \times n$ matrix that satisfies $\mathcal{G}\mathcal{H}^T = 0$. The generator matrix for $C^\perp$ thus provides a mechanism of checking whether or not a codeword is in C.

Definition 2.1.14. *Any generator matrix $\mathcal{H}$ for $C^\perp$ is called a* **parity-check matrix** *or simply a* **check matrix** *for C.*

If the generator matrix $\mathcal{G}$ is written in **standard form** i.e. $\mathcal{G} = [I_k|A]$, where A is a $k \times (n-k)$ matrix over F_q, then $H = [-A^T|I_{n-k}]$ is a check matrix for C. The first k coordinates are called the **information positions** and the rest the **check positions** or the **redundancy positions**. Any generator matrix $\mathcal{G}$ for C can be Gauss-reduced to a matrix $\mathcal{G}'$ which is in standard form and which is the generator matrix of a code C' which is isomorphic to C.

The generator matrix facilitates the encoding of the original information. A generator matrix in standard form will clearly simplify the encoding: if one of the original messages is $[u] \in F_q^k$, and $\mathcal{G} = [I_k|A]$, then the encoded message is $[u|uA]$, where uA represents the redundancy.

The $\boldsymbol{j}$**-vector** is the vector in F_q^n of which the coordinates are all equal to one. The presence of the $\boldsymbol{j}$-vector in $C^\perp$ implies that all the vectors in C must have even weight if $q = 2$, and can hence prove useful in determining the minimum weight of C. A similar statement applies to the presence of the $\boldsymbol{j}$-vector in C. In general, the weights of C and $C^\perp$ are not easily determined. Of course, amongst the vectors resulting from the generator matrix of C are those of minimum weight. The parity-check matrix for C can be used to determine its minimum weight, as asserted below.

Theorem 2.1.15. [1, Theorem 2.3.1] *Let C be an $[n,k]_q$ code and $\mathcal{H}$ a parity-check matrix for C. Then C has minimum weight d if and only if every set of $d-1$ columns of $\mathcal{H}$ is linearly independent, and there exists a set of d columns of $\mathcal{H}$ which is linearly dependent.*

Another concept that will feature prominently in this thesis is that of an automorphism of a code.

Definition 2.1.16. *Let C be an $[n,k,d]_q$ code. Then any isomorphism of C onto itself is called an* **automorphism** *of C. The set of all automorphisms of C form a group, the* **automorphism group** *of C, denoted by $Aut(C)$.*

An automorphism of C is thus a permutation on the coordinate positions which maps codewords to codewords. Hence any automorphism of C preserves its weight classes, and this idea is useful in determining $\mathrm{Aut}(C)$ in the first place. With specific reference to the codes generated by the adjacency matrix of graphs as is the case in this thesis, the automorphism group of the graph is contained in the automorphism group of the code.

So even if the full automorphism group of the code has not been determined but the automorphism group of the graph is known, then permutations which map errors occurring at the information positions into the check positions may still be identified. In fact, the full automorphism group of the graph may not even need to be known - all that may be required are sets of automorphisms of the graph.

2.2 Designs

A **finite incidence structure** denoted by $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, consists of two finite disjoint sets $\mathcal{P}$ and $\mathcal{B}$ together with a relation $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. The elements of $\mathcal{P}$ are called **points**, and those of $\mathcal{B}$ are called **blocks**. In the case that the points and the blocks are related by set membership, the incidence structure is denoted by $\mathcal{T} = (\mathcal{P}, \mathcal{B})$. If $(p, B) \in \mathcal{I}$, then it is said that p is **incident** with B, or that B contains the point p, or that p is on B.

As is the case for most other structures, incidence structures are identified by the concept of isomorphism.

Definition 2.2.1. *Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $\mathcal{T}' = (\mathcal{P}', \mathcal{B}', \mathcal{I}')$ be incidence structures, and let ϕ be a bijection from $\mathcal{P} \cup \mathcal{B}$ to $\mathcal{P}' \cup \mathcal{B}'$. Then ϕ is an* **isomorphism** *from $\mathcal{T}$ to $\mathcal{T}'$ if and only if $\phi(\mathcal{P}) = \mathcal{P}', \phi(\mathcal{B}) = \mathcal{B}'$, and $p \in \mathcal{P}$ is incident with $B \in \mathcal{B}$ if and only if $\phi(p) \in \mathcal{P}'$ is incident with $\phi(B) \in \mathcal{B}$. Furthermore, if $\mathcal{T} = \mathcal{T}'$, then ϕ is an* **automorphism**.

Those incidence structures that possess a high degree of regularity are singled out below:

Definition 2.2.2. *An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a* $\boldsymbol{t-(v,k,\lambda)}$ *design, or simply a* **t-design**, *where t, k, v and λ are non-negative integers, if*

(1) $|\mathcal{P}| = v$;

(2) every block B is incident with exactly k points; and

(3) every t distinct points are together incident with exactly λ blocks.

It may be the case that two distinct blocks are incident with the same k points, so that blocks are repeated. A design is **simple** if it has no repeated blocks. A design is **trivial** if each set of k points is incident with a block - the number of blocks will then be $\binom{v}{k}$. In this thesis only simple, non-trivial designs will be considered.

Theorem 2.2.3. [1, Theorem 1.2.1] *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $t-(v,k,\lambda)$ design. Then for each integer $0 \leq s \leq t$ the number λ_s of blocks incident with s points is independent of these points, and is given by*

$$\lambda_s = \lambda \, \frac{(v-s)(v-s-1)\dots(v-t+1)}{(k-s)(k-s-1)\dots(k-t-1)}. \tag{2.1}$$

$\mathcal{D}$ is an $s-(v,k,\lambda_s)$ design for each $1 \leq s \leq t$.

In keeping with the above notation, let λ_i be the number of blocks incident with i points where $0 \leq i \leq t$. Then by definition, $\lambda_t = \lambda, \lambda_0 = |\mathcal{B}|$, and λ_1 is the number of blocks incident with any point, termed the **replication number** of the design. A counting argument can be used to prove the recursion formula

$$\lambda_i = \lambda_{i+1} \, \frac{(v-i)}{(k-i)}, \tag{2.2}$$

and letting $\lambda_0 = b$ and $\lambda_1 = r$, it can be deduced that

$$bk = vr, \tag{2.3}$$

and if $t = 2$, then

$$r(k-1) = \lambda(v-1). \tag{2.4}$$

From a given design $\mathcal{D}$, new designs may be constructed. These may result from, amongst others, taking the complements or the duals of the original design, and will be useful in determining properties of the linear codes that will be constructed from the original design.

Definition 2.2.4. *Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. Then the structure $\mathcal{T}^t = (\mathcal{P}^t, \mathcal{B}^t, \mathcal{I}^t)$, where $\mathcal{P}^t = \mathcal{B}$, $\mathcal{B}^t = \mathcal{P}$, and $(B, p) \in \mathcal{I}^t$ if and only if $(p, B) \in \mathcal{I}$, is called the* **dual** *of $\mathcal{T}$.*

A design is **symmetric** if it has the same number of points as it has blocks. Symmetric designs are therefore designs of which the duals have the same parameters as the original designs. A design is **self-dual** if it is isomorphic to its dual.

Definition 2.2.5. *Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. Then the structure $\overline{\mathcal{T}} = (\overline{\mathcal{P}}, \overline{\mathcal{B}}, \overline{\mathcal{I}})$, where $\overline{P} = \mathcal{P}, \overline{\mathcal{B}} = \mathcal{B}$, and $\overline{\mathcal{I}} = \mathcal{P} \times \mathcal{B} \setminus \mathcal{I}$, is called the* **complement** *of $\mathcal{T}$.*

Theorem 2.2.6. **[1, Theorem 1.3.1]** *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a $t - (v, k, \lambda)$ design with $v - k \geq t$. Then $\overline{\mathcal{D}}$ is a $t - (v, v - k, \overline{\lambda})$ design, where*

$$\overline{\lambda} = \lambda \, \frac{(v-k)(v-k-1)\cdots(v-k-t+1)}{k(k-1)\cdots(k-t+1)}. \tag{2.5}$$

Another important concept that will be needed is that of an automorphism of a design.

Definition 2.2.7. *An* **automorphism** *of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a permutation σ of the points $\mathcal{P}$ which preserves the blocks $\mathcal{B}$.*

The automorphisms of $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ form a group under group composition, and induce a permutation on the block set $\mathcal{B}$.

The designs that will be focused on in this thesis are the symmetric $1 - (v, k, k)$ designs. Linear codes will be constructed from them, and their automorphism groups will be determined.

In the introduction it has been mentioned that codes that had a rich algebraic and geometric structure were the ones of interest since they would facilitate comparatively easy encoding and decoding. From the above discussion it becomes evident that designs are good candidates for the construction of such codes because of the degree of regularity that they possess. The other important combinatorial structures that could be used to construct codes are graphs, and a similar sort of regularity needs to be investigated for graphs which will identify those that are candidates for the construction of good codes. All the graphs considered in this thesis will be finite.

2.3 Graphs

Definition 2.3.1. *A* **graph** $G = (V, E)$ *consists of a* **vertex-set** V *and an* **edge-set** E*, where the edge, denoted by* $[u, v]$*, is an association of the vertices* $u, v \in V$*. If* $[u, v] \in E$*, then* u *and* v *are said to be* **adjacent***, and are called the* **endpoints** *of* $[u, v]$*.*

A graph in which the vertices $[u, v]$ and $[v, u]$ are distinct is called a **directed graph**. An edge of the form $[u, u]$ is called a **loop**. Edges which have the same endpoints are called **multiple edges**. Graphs which have neither loops nor multiple edges are called **simple graphs**. Only simple, undirected graphs will be focused on in this thesis.

Definition 2.3.2. *A* **path** *between* u *and* v *is a sequence of distinct vertices* $u = u_0 u_1 \dots u_n = v$ *such that* $[u_i, u_{i+1}]$ *is an edge. The length of the path is* n*.*

Definition 2.3.3. *The* **distance** *between* u *and* v*, denoted by* $d(u, v)$*, is the minimum length of all paths between* u *and* v*, if such paths exist. Otherwise,* $d(u, v) = \infty$*.*

Definition 2.3.4. *A* **subgraph** *of a graph* $G = (V, E)$ *is a graph* $G' = (V', E')$*, where* $V' \subseteq V$ *and* $E' \subseteq E$*.*

In the following definition paths are viewed as subgraphs of any graph G.

Definition 2.3.5. *A graph G is* **connected** *if and only if any two vertices $u, v \in V$ are vertices of a path in G. Otherwise, G is* **disconnected**.

Definition 2.3.6. *The* **components** *of a graph G are its maximal connected subgraphs.*

Clearly, the vertex-sets of the components of a graph are disjoint. The same applies to the edge-sets. Hence if each component has the same number of vertices, then the number of components can easily be found. Furthermore, with regard to later observations, there appears to be a relationship between the number vertices in such components and the number of errors that a code generated by such a graph is capable of correcting. This relationship has however not been explored further.

Definition 2.3.7. *The* **degree** *or the* **valency** *of a vertex v of G is the number of edges with which v is incident. If all the vertices of G are incident with the same number of edges, then G is said to be* **regular**, *and the common valency is the valency of the graph.*

The following are some familiar results relating the degrees of the vertices of a graph to its number of edges:

Proposition 2.3.8. [**42, Proposition 1.3.3**] *The sum of the degrees of all the vertices of a graph is equal to twice the number of edges of the graph.*

Corollary 2.3.9. [**42, Corollary 1.3.5**] *Every graph has an even number of vertices of odd degree.*

Corollary 2.3.10. [**42, Corollary 1.3.6**] *A graph having n vertices and valency k has $\frac{nk}{2}$ edges.*

It is clear that the maximum valency that any graph having n vertices can have is $n-1$, when every vertex is adjacent to every other vertex. Hence the maximum number of edges that such a graph can have is $\binom{n}{2}$. Such a graph is called a **complete** graph, and is denoted by K_n. In the language of design theory then, a graph is a $t-(v,2,\lambda)$ design where the vertices are the points of the design and the edges its blocks. The graph is regular if $t \geq 1$, and complete if $t = 2$. At the other extreme to the complete graph is the **null graph**, the graph which has no vertices nor edges.

The concepts of a dual structure (see [42] for further details) and a complementary structure are both applicable to graphs, although the former will not be discussed at all in this thesis.

Definition 2.3.11. *The* **complement** *of a graph $G = (V, E)$ is the graph $\overline{G} = (\overline{V}, \overline{E})$, where $\overline{V} = V$ and for $u, v \in V, [u, v] \in \overline{E}$ if and only if $[u, v] \notin E$.*

Graph complements will be used to construct codes in this thesis, and of particular interest has been the study of the relationship between the dual code generated by a graph and the code generated by its complement.

A property which if possessed by a graph, is also possessed by its dual, is that of strong regularity.

Definition 2.3.12. *A graph G is* **strongly regular** *with parameters (n, k, λ, μ) if it has n vertices, its valency is k, any two adjacent vertices are commonly adjacent to λ vertices, and any two non-adjacent vertices are commonly adjacent to μ vertices.*

Another graph that reference will be made to is a line graph.

Definition 2.3.13. *A* **line graph** *of a graph $G = (V, E)$ is the graph $L(G) = (E, V)$ where $e, e' \in E$ are adjacent in $L(G)$ if and only if there exists $v \in V$ such that e and e' are commonly incident with v.*

In the case of codes, an automorphism is a permutation of the coordinate positions of a code which preserves codewords. Likewise, an automorphism of a design is a permutation on the points which preserves blocks. The analogy in the case of a graph is as follows:

Definition 2.3.14. *An* **isomorphism** *from a graph $G = (V, E)$ to a graph $G' = (V', E')$ is a bijection $\phi : V \to V'$ such that $[u, v] \in E$ if and only if $[\phi(u), \phi(v)] \in E'$. An isomorphism from G onto itself is called an* **automorphism** *of G.*

An automorphism of G is thus a permutation on its vertices which preserves its edges. The automorphisms of G form a group called the **automorphism group** of G denoted by $\mathrm{Aut}(G)$. A result of Whitney in [43] states that if a graph G is connected and it has more than four vertices, then $\mathrm{Aut}(G) \cong \mathrm{Aut}(L(G))$. Similarly, if $\overline{G}$ is the complement of G, then $\mathrm{Aut}(G) \cong \mathrm{Aut}(\overline{G})$. (See [37, Proposition 3.7] for details.)

2.4 Codes from Designs

As mentioned in the introduction, the codes constructed from designs have enriched the theory of designs in that new designs have been constructed, existing designs have been extended, and certain designs have been shown not to exist. Knowledge about the design from which a code was constructed could facilitate efficient encoding and decoding. On the other hand, not all codes yield designs, and the Assmus-Mattson Theorem (see [1, Theorem 2.11.2]) gives criteria for determining whether the supports of the vectors of a certain weight yield a t-design. The step from a design to a code can be taken via the incidence matrix of the design.

Definition 2.4.1. *Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a $t - (v, k, \lambda)$ incidence structure, where $\mathcal{P} = \{p_1, p_2, \ldots, p_v\}$, and $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$. An* **incidence matrix** *for $\mathcal{T}$ is a $b \times v$ matrix*

$A = (a_{ij})$ *such that*

$$a_{ij} = \begin{cases} 1 & \text{if } (p_j, B_i) \in \mathcal{I}, \\ 0 & \text{if } (p_j, B_i) \notin \mathcal{I}. \end{cases}$$

If $t \neq 0$, then any incidence matrix for $\mathcal{T}$ will have k 1's in each row and r 1's in each column. Any matrix consisting of 0's and 1's of which the number of 1's in each row and the number of 1's in each column are constants, is the incidence matrix of a 1-design. The 1-designs that will be encountered in this thesis have the additional property that the row constant and the column constant are equal, in other words, the incidence matrices are symmetric.

The definition of the incidence matrix is not confined to the one given above - another definition is that of A^T, where A is as given above. In fact, the core idea is not that of a matrix, but of characteristic functions from which incidence vectors are constructed.

Definition 2.4.2. *Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure, F any field, and $F^{\mathcal{P}}$ the vector space of functions from $\mathcal{P}$ to F. For any $X \subseteq \mathcal{P}$, let v^X denote the* **characteristic function** *on X i.e.*

$$v^X(p) = \begin{cases} 1 & \text{if } p \in X, \\ 0 & \text{if } p \notin X. \end{cases}$$

The standard basis for $F^{\mathcal{P}}$ is $\{v^{\{p\}} : p \in \mathcal{P}\}$. If no confusion arises, the accurate use of notation may be sacrificed for the sake of readability - the braces around the point p may be dropped as will be the case in this thesis, where the points are either k-subsets or m-tuples.

Definition 2.4.3. *Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure, F any field, and $F^{\mathcal{P}}$ the vector space of functions from $\mathcal{P}$ to F. For a block $B \in \mathcal{B}$, where $B \subseteq \mathcal{P}$, the* **incidence vector** *v^B is the vector associated with the characteristic function on B and will be written*

$$v^B = \sum_{p:(p,B)\in\mathcal{I}} v^{\{p\}}. \tag{2.6}$$

Note that if the block $B \not\subset \mathcal{P}$, then in order to define v^B, B first has to be identified with the set of points which are incident with it.

Definition 2.4.4. *Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure. The* **code** *of $\mathcal{T}$ over a field F is the subspace of $F^{\mathcal{P}}$ generated by the incidence vectors associated with the blocks of $\mathcal{T}$ i.e.*

$$C_F(\mathcal{T}) = span\{v^B : B \in \mathcal{B}\}.$$

The above definition is not dependent on an ordering of the incidence vectors, since any ordering of the incidence vectors will generate codes that are isomorphic.

If p is any prime and F is the field F_p, then $C_F(\mathcal{T})$ can be written $C_p(\mathcal{T})$.

Definition 2.4.5. *Let $\mathcal{T} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure, and $C_p(\mathcal{T})$ the code of $\mathcal{T}$ over F_p. Then the* **p-rank** *of $\mathcal{T}$ is the dimension of $C_p(\mathcal{T})$ and is written*

$$\text{rank}_p(\mathcal{T}) = \dim(C_p(\mathcal{T})).$$

With regard to automorphism groups, the automorphism group of an incidence structure will be contained in the automorphism group of the code generated by the incidence structure. Clearly, if the code generated is the full vector space or the dual of the code generated by the $\boldsymbol{j}$-vector, then the code's automorphism group is the full symmetric group on the points $\mathcal{P}$. The converse is also true (see [20, Lemma 4]).

2.5 Codes from Graphs

An alternative method of constructing codes that have a rich geometric structure is to resort to graphs which have a high degree of regularity. Similar constructions to those in [16], [17], [18] and [35] have been carried out in this thesis, and these hinge on the concept of an adjacency matrix for a graph.

Definition 2.5.1. *Let $G = (V, E)$ be a graph with vertex-set $V = \{u_1, u_2, \ldots, u_n\}$. An* **adjacency matrix** *for G is an $n \times n$ matrix $A = (a_{ij})$ where*

$$a_{ij} = \begin{cases} 1 & \text{if } [u_i, u_j] \in E, \\ 0 & \text{if } [u_i, u_j] \notin E. \end{cases}$$

Now an adjacency matrix as defined above is also an incidence matrix for a $1-(v, k, k)$ design, and hence characteristic functions, incidence vectors, and ultimately codes, can be defined in much the same way as has been the case for incidence structures. The automorphism group of the graph will be contained in the automorphism group of the code generated by its adjacency matrix.

In this thesis the complements of the Triangular graphs $G(n, 2, 0)$, the Odd graphs $G(2k+1, k, 0)$, the Johnson graphs $G(n, k, k-1)$, and certain graph products of the n-cycle C_n have been given the treatment described above as in the case of binary codes. Important properties of the resulting codes and their duals, such as the identification of a basis and the subsequent dimension, the minimum weight, the identification of the minimum words, the existence of a minimum weight basis, as well as whether the codes are self-dual, self-orthogonal or whether the direct sum of the codes and their duals is the full space, have been studied.

For the sake of completeness, it is mentioned that there are alternative ways of constructing codes from graphs. By defining codes as the non-empty subsets of the vertex-set V, and then partitioning the vertices according to their distance from a code C, Guidici and Praeger [11] have obtained codes of which the cells of the distance partition are the orbits of some group of automorphisms of the graph. This definition of a code from a graph has also been used to describe perfect codes in direct products of cycles in [22]. In [10] Curtis and Morris describe the construction of a code from the adjacency matrix of a bipartite graph $\tilde{G}$ derived from a graph G. No further details will be provided on the above-mentioned constructions, since they have no direct bearing on the research that follows, and the interested reader is referred to the references indicated.

Chapter 3

Permutation Decoding

The idea of permutation decoding was first introduced by MacWilliams in [27]. Although permutation decoding was originally developed for the decoding of the Hamming and Golay codes, it is applicable to all codes which have large automorphism groups. The main problem involves finding a set of automorphisms of the code which satisfies certain conditions, and which facilitates the full use of the error-correcting capability of the code. The problem is exacerbated by the fact that such a set is dependent on the choice of the information positions for the code. A complete description of the method is given in MacWilliams and Sloane [26, Chapter 16], and in Huffman [15, Section 8].

3.1 Some results on PD-sets

Definition 3.1.1. *A* **PD-set** *for a t-error-correcting code is a set of automorphisms $\mathcal{S}$ of the code 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.*

A PD-set may not even exist for a given code and a given set of information positions. From the following result in [15], it can be deduced that, should such a set exist, it will

use the full error-correcting capability of the code.

Theorem 3.1.2. [15, Theorem 8.1] *Let C be an $[n,k,d]_q$ t-error-correcting code, and $\mathcal{H}$ a check matrix for C i.e. I_{n-k} is in the redundancy positions. Let $y = c+e$ be a vector, where $c \in C$, and weight $(e) \leq t$. Then the information positions in y are correct if and only if weight (Syndrome(y)) = weight$(\mathcal{H}y^T) \leq t$.*

Proof: Suppose that the generator matrix $\mathcal{G}$ for C is in standard form i.e. $\mathcal{G} = [I_k|A]$. The first k positions are the information positions and the check matrix $\mathcal{H}$ is of the form $\mathcal{H} = [-A^T|I_{n-k}]$. If the information positions of y are correct, then

$$\mathcal{H}y^T = \mathcal{H}(c+e)^T = \mathcal{H}c^T + \mathcal{H}e^T = 0 + e^T = e^T,$$

and hence weight $(\mathcal{H}y^T) \leq t$.

Conversely, suppose that the information symbols are not all correct, and that errors occur in the information positions. Let $e = (e_1, e_2, \ldots, e_n)$ where $e' = (e_1, e_2, \ldots, e_k)$, and $e'' = (e_{k+1}, e_{k+2}, \ldots, e_n)$. Then

$$\begin{aligned}
\text{weight}(\mathcal{H}y^T) &= \text{weight}(\mathcal{H}e^T) = \text{weight}(-A^T(e')^T + (e'')^T) \\
&\geq \text{weight}(-A^T(e')^T) - \text{weight}((e'')^T) \\
&= \text{weight}(e'A) - \text{weight}(e'') \\
&= \text{weight}(e'A) + \text{weight}(e') - \text{weight}(e') - \text{weight}(e'') \\
&= \text{weight}(e'\mathcal{G}) - \text{weight}(e) \\
&\geq d - t \geq t + 1,
\end{aligned}$$

and the result follows. □

The algorithm for permutation decoding then proceeds as follows: If $\mathcal{H}$ is a check matrix for an $[n,k,d]_q$ code C in standard form, then the generator matrix $\mathcal{G}$ for C has I_k as the first k columns thereby identifying the first k positions as information positions. If x is sent, then x is encoded as xG. If y is received and at most t errors have occurred during

transmission, then compute the syndromes $\mathcal{H}(\sigma_i(y))^T$ for $i \in \{1, 2, \ldots, s\}$, where $\mathcal{S} = \{\sigma_1, \sigma_2, \ldots, \sigma_s\}$ is a PD-set for C. For $i \in \{1, 2, \ldots, s\}$ such that weight $(\mathcal{H}(\sigma_i(y))^T) \leq t$, let c be the codeword of which the information positions agree with those of the syndrome. Then y is decoded as $\sigma_i^{-1}(c)$.

The following is a bound proposed by Gordon on the basis of a result in Schönheim [39], for the minimum size of a PD-set and is proved in [15]:

Theorem 3.1.3. *Let $\mathcal{S}$ be a PD-set for a t-error-correcting $[n, k, d]_q$ code, and let $r = n - k$. Then*

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

If the minimum weight of a code C is 3 or 4, then C is capable of correcting one error, and syndrome decoding will suffice: multiples of the columns of the check matrix will yield all the possible syndromes, and the received vector only needs to be compared with columns of the check matrix.

The following lemma is given in [35]:

Lemma 3.1.4. [35, Lemma 3.5.6] *Let C be an $[n, k, d]_q$ t-error-correcting code, and let $r = n - k$. Let $X = \{(x_1, x_2, \ldots, x_t) : x_i \in \{1, 2, \ldots, n\}$, for all $i \in \{1, 2, \ldots, t\}\}$, and let $\mathcal{E} = \{(e_1, e_2, e_3, \ldots, e_t) : e_i \in \{k+1, k+2, \ldots, n\}$, for all $i \in \{1, 2, \ldots, t\}\}$, where the positions from $k+1$ to n have been identified as check positions. Then $\mathcal{S} = \{\sigma_1, \sigma_2, \ldots, \sigma_s\}$ is a PD-set for C if*

$$\bigcup_{i=1}^{s} \sigma_i^{-1}(\mathcal{E}) = X.$$

Furthermore, for any $\alpha \in Aut(C)$, the set $\alpha\mathcal{S} = \{\alpha\sigma_1, \alpha\sigma_2, \ldots, \alpha\sigma_s\}$ is also a PD-set for C.

For permutation decoding of cyclic codes in [27], if C is an $[n, k, d]_q$ t-error-correcting cyclic code, then $\tau \in S_n$ where τ is defined by $\tau : i \mapsto i + 1$, for all $i \in \{1, 2, \ldots, n\}$, is an automorphism of C. If e is the error-vector and t errors occur such that there is a

sequence of k zeros between two error positions, then there exists $j \in \{1, 2, \ldots, n\}$ such that τ^j will map e into the check positions. Hence $< \tau >$ is a PD-set for C if $k < \frac{n}{2}$.

The following definition in [19] and used in Kroll and Vincenti [24] was motivated by the fact that full PD-sets may not exist for some codes, and so-called partial PD-sets may be resorted to.

Definition 3.1.5. *An* ***s*-PD-set** *for a t-error-correcting code is a set of automorphisms $\mathcal{S}$ of the code which is such that for any set of $s \leq t$ coordinate positions, there is an element of $\mathcal{S}$ which maps it into the check positions.*

Due to the fact that the codes investigated in this thesis are very general, full PD-sets have only been found in the case of the duals of the codes generated by the complements of the Triangular graph. For the codes generated by the Odd graphs, a 2-PD-set has been found, and for those generated by the Johnson graphs, 3-PD-sets have been found. Partial PD-sets have also been found for the codes generated by the cartesian and the categorical products of n-cycles.

Chapter 4

An Introduction to Uniform Subset Graphs

In Key et al. [17] the binary codes and permutation decoding sets generated by the adjacency matrix of the Triangular graphs were studied. The Triangular graph $T(n)$ is the line graph of the complete graph on n vertices, K_n. From an alternative perspective, the **Triangular graph** is the graph of which the vertices are the 2-subsets of the set $\Omega = \{1, 2, 3, \ldots, n\}$, and two vertices u and v constitute an edge $[u, v]$ if and only if $|u \cap v| = 1$. In [35] the binary codes generated from the graphs of which the vertices are the 3-subsets of Ω, with two vertices u and v now constituting an edge $[u, v]$ if and only if $|u \cap v| = 0$, or $|u \cap v| = 1$, or $|u \cap v| = 2$, were studied. Permutation decoding sets were described for the codes generated by these graphs in the case that $|u \cap v| = 0$, and $n \equiv 1 (\text{mod } 4)$, and for the dual codes in the case that $|u \cap v| = 2$, and $n \geq 7$ is odd. Since the primary objective of this study is to describe binary codes from graphs using similar methods as had been used in [16], [17], [18] and [35], focusing on the class of graphs of which the Triangular graphs and the graphs on 3-subsets constituted important subclasses seemed the obvious starting point. Furthermore, the automorphism groups of these classes of graphs were both well-known and large, and it was thought that the potential for successful permutation decoding would also exist for other subclasses of this

large class of graphs.

In this chapter a brief account will be given of this large class of graphs as it appears in the literature. Some of its basic properties will also be described, and finally, its relationship to vertex-transitive graphs in general will be explored.

4.1 Historical Overview

The **Uniform Subset graphs**, denoted by $G(n, k, r)$, constitute the large class of graphs of which the Triangular graphs and the graphs on 3-subsets are subclasses. In their general form they were first introduced by Chen and Lih in [9], who described them as follows: Let $\Omega = \{1, 2, 3, \ldots, n\}$, and let $\Omega^{\{k\}}$ denote the k-subsets of Ω . The graph $G(n, k, r)$ has $\Omega^{\{k\}}$ as its vertex-set, and any two vertices u and v constitute an edge $[u, v]$ if and only if $|u \cap v| = r$. Clearly, $G(n, k, r)$ is a large class of graphs. However, it is not as large as it appears as it can be assumed that $n \geq 2k$, based on the following observation:

Lemma 4.1.1. [2, Lemma 3.1.3] *For $n \geq k \geq r, G(n, k, r) \cong G(n, n-k, n-2k+r)$.*

Proof: Suppose that $u \in \Omega^{\{k\}}$. Define a function $f : \Omega^{\{k\}} \to \Omega^{\{n-k\}}$ by

$$f(u) = \Omega \setminus u.$$

If $[u, v]$ is an edge in $G(n, k, r)$, then $|u \cap v| = r$, and so

$$\begin{aligned} |f(u) \cap f(v)| &= |(\Omega \setminus u) \cap (\Omega \setminus v)| \\ &= |\Omega \setminus (u \cup v)| \\ &= n - |u \cup v| \\ &= n - (2k - r) \\ &= n - 2k + r. \end{aligned}$$

Hence $[f(u), f(v)]$ is an edge in $G(n, n-k, n-2k+r)$, and since f is clearly a bijection,

the result follows. □

For $n \geq 2k$, the class of graphs $G(n, k, k-1)$ is known as the Johnson graphs, the Triangular graphs $G(n, 2, 1)$ being an important subclass. The class of graphs $G(n, k, 0)$ is known as the Kneser graphs, the Odd graphs $G(2k+1, k, 0)$ being an important subclass. These classes of graphs had been investigated before the general definition had been given. The Odd graphs, which will be denoted by $O(k)$, were studied by Balaban [3] who encountered them in his study of shifts in carbonium ions and subsequently dubbed them ($O(k-1)$) "k-valent halved combination graphs". The term "Odd graph" appears to have originated from Cameron [8]. Biggs [4] described $O(5)$ in a novel way, albeit unrealistically, as follows: In the English hamlet of Croam the eleven members of the football team were so consumed by the idea of winning that they had no option but to organise matches amongst themselves with two teams each consisting of five men and the eleventh man serving as referee. Each possible choice of teams and referee plays only one match resulting in a total of 1386 possible games. He concludes by posing the question about the possibility of each team playing its six games on different weekdays. Biggs' problem above reduces to the question about whether it is possible to colour the edges of $O(5)$ using six colours. Meredith and Lloyd [30] answered this question in the affirmative. To shed more light on their results, the following definitions and observation are needed.

Definition 4.1.2. *A graph G is* **Hamiltonian** *if and only if it contains a cycle which passes through every vertex exactly once.*

Definition 4.1.3. **[30]** *A graph G is* **m-ply Hamiltonian** *if and only if it contains m edge-disjoint Hamiltonian cycles.*

Definition 4.1.4. *An* **m-colouring** *of a graph G is a function from the vertices of G to the set $\{1, 2, \ldots, m\}$ such that if $[u, v]$ is an edge of G then the image of u is not equal to the image of v.*

Lemma 4.1.5. **[30]** *Let G be a graph with an even number of vertices and that is m-ply Hamiltonian. Then $2m$ colours are sufficient to colour the edges in the Hamiltonian cycles.*

Proof: Since each Hamiltonian cycle has an even number of edges, two colours are sufficient to colour the edges. □

Earlier, Meredith and Lloyd [31] had shown that $O(3)$ is doubly Hamiltonian, and that $O(4), O(5)$ and $O(6)$ are Hamiltonian. In [30] they show that $O(5)$ is triply Hamiltonian, and since $O(5)$ has an even number of edges ($\binom{11}{5}$), it follows from Lemma 4.1.4 that six colours are sufficient to colour the edges. They argued using the quotient graph Q obtained by factoring $O(k)$ by a subgroup H of its automorphism group which is essentially a subgroup of S_{2k+1}, since any permutation of Ω induces a permutation of the vertices of $O(k)$ which also preserves their disjointness. The orbits of the vertices of $O(k)$ under the action of H form the vertex-set of Q, and two vertices $\overline{u}$ and $\overline{v}$ are adjacent if and only if there exists $w \in \overline{v}$ such that u and w are adjacent in $O(k)$. Evidently, Q may not be a simple graph. The Hamiltonian cycles in Q are then lifted back to Hamiltonian cycles in $O(k)$. By factoring $O(5)$ by the cycle $(1, 2, 3, 4, 5, 6, 7)$, a triply Hamiltonian graph is obtained, the Hamiltonian cycles of which are then lifted to Hamiltonian cycles in $O(5)$. Subsequently, in "The rugby footballers of Croam" [29], Mather obtains a Hamiltonian cycle in $O(7)$ by using the methods described above. Still with reference to $O(k)$, Biggs [5] posed another question, namely whether there were any values of k for which $O(k)$ is a Cayley graph, the definition of which is given below.

Definition 4.1.6. *Let A be a group and S a subset of A such that $1_A \in S$ and $S = S^{-1}$. A graph G is a* **Cayley graph** *if and only if its vertex-set is A, and any two vertices u and v constitute an edge $[u, v]$ in G if and only if $v = us$ for some $s \in S$.*

Godsil [12] showed that none of the Odd graphs are Cayley graphs by using the fact that a graph G is Cayley if and only if its automorphism group $\mathrm{Aut}(G)$ contains a subgroup which acts regularly on the vertices of G. In fact, he used this fact to prove that the

Kneser graphs $G(n,k,0)$ are not Cayley except when $k=2$ and n is a prime power and $n \equiv 3 (\text{mod } 4)$, or when $k=3$ and $n=8$ or 32. The former case was initially settled by Sabidussi [38].

The Kneser graphs $G(n,k,0)$ originated from the following context: In 1955 Kneser [23] conjectured that if the k-subsets of a $2k+m$ set are partitioned into $m+1$ classes, then one of the classes will contain two disjoint k-subsets. Lovász [25] proved Kneser's conjecture by constructing the graphs $G(2k+m,k,0)$ associated with it, and by reformulating it to that which claimed that $m+2$ colours are necessary to colour the vertices of $G(2k+m,k,0)$.

One of the properties of the class of Uniform Subset graphs is that it is **distance-regular** (see Bailey [2, Chapter 2] for further details), by which is meant that for any two vertices u and v such that $d(u,v)=i$, the number of vertices w such that $d(u,w)=j$ and $d(w,v)=k$, is independent of u and v. Moon [32] focused on this property of graphs in relation to the class of Johnson graphs which he denoted by $J(n,k)$. He, along with others, investigated whether a distance-regular graph which has the parameters of $J(n,k)$ is in fact isomorphic to it. He shows that $J(n,k)$ is unique for $n \geq 20$, so in particular $J(n,k)$ is characterized by its parameters for all but finitely many pairs (n,k).

The motivation of Chen and Lih [9] for defining the Uniform Subset graphs $G(n,k,r)$ was to investigate the triples (n,k,r) for which $G(n,k,r)$ would be Hamiltonian, thereby broadening the work of Meredith and Lloyd [30], and Mather [29] who had focused on determining which of the Odd graphs were Hamiltonian. They introduced the notion of an admissible triple, and conjectured that $G(n,k,r)$ was Hamiltonian for all admissible triples except $(5,2,0)$ and $(5,3,1)$. They succeeded in proving the conjecture for $(n,k,k-1),(n,k,k-2),(n,k,k-3)$, and for suitably large n when k is given and $r=0$ or 1.

Now that some of the less obvious properties of the Uniform Subset graphs have become apparent from the above discussion, the more mundane ones will be focused on.

4.2 Some basic properties

The first few properties pertain to the order and the valency of $G(n, k, r)$.

Proposition 4.2.1. [2, Proposition 3.1.2]

(a) $G(n, k, r)$ *has* $\binom{n}{k}$ *vertices.*

(b) $G(n, k, r)$ *is regular, each vertex having valency* $\binom{k}{r}\binom{n-k}{k-r}$.

(c) $G(n, k, r)$ *is not strongly regular.*

Proof:

(a) The number of vertices of $G(n, k, r)$ is just the number of k-subsets of $\Omega = \{1, 2, 3, \ldots, n\}$, of which there are $\binom{n}{k}$.

(b) Suppose that u is a vertex of $G(n, k, r)$. Any vertex v adjacent to u consists of r of the k elements of u, as well as $k-r$ elements of $\Omega \setminus u$. Hence u has valency $\binom{k}{r}\binom{n-k}{k-r}$.

(c) Suppose that $u = \{x_1, x_2, x_3, \ldots, x_r, x_{r+1}, \ldots, x_k\}$ and $v = \{x_1, x_2, x_3, \ldots, x_r, x_{k+1}, \ldots, x_{2k-r}\}$ are vertices of $G(n, k, r)$ having r elements in common. Then u and v are adjacent, and any vertex commonly adjacent to u and v consists either of $\{x_1, x_2, x_3, \ldots, x_r\}$ and $k - r$ elements of $\Omega \setminus (u \cup v)$, or of $r - 1$ elements of $\{x_1, x_2, x_3, \ldots, x_r\}$, one each of $\{x_{r+1}, x_{r+2}, \ldots, x_k\}$ and $\{x_{k+1}, x_{k+2}, \ldots, x_{2k-r}\}$ and $k - r$ elements of $\Omega \setminus (u \cup v)$, or $r - 2$ elements of $\{x_1, x_2, x_3, \ldots, x_r\}$, and so on. Hence u and v are commonly adjacent to $\sum_{i=0}^{r} \binom{r}{r-i}\binom{k-r}{i}^2\binom{n-2k+r}{k-r-i}$ vertices. However, if any two vertices u and v are not adjacent and $r \neq 0$ nor 1, then u and v are commonly adjacent to $\binom{k}{r}^2\binom{n-2k}{k-2r}$ vertices if $|u \cap v| = 0$, and to

$$\binom{k-1}{r-1}^2\binom{n-2k+1}{k-2r+1} + \binom{k-1}{r}^2\binom{n-2k+1}{k-2r}$$

vertices if $|u \cap v| = 1$. Hence $G(n, k, r)$ is not strongly regular. □

The distance-regularity of $G(n,k,r)$ has already been alluded to in Section 4.1 above. Distance-regularity is a purely combinatorial property of a graph. A stronger property which involves the automorphism group of a graph is that of distance-transitivity, which is defined as follows:

Definition 4.2.2. *A graph G is* **distance-transitive** *if and only if for any vertices s,t,u,v such that $d(s,t)=d(u,v)$, there exists $\sigma \in Aut(G)$ such $\sigma(s)=u$ and $\sigma(t)=v$.*

Proposition 4.2.3. *$G(n,k,r)$ is distance-transitive.*

Whilst the above proposition is not shown in this thesis for the entire class of Uniform Subset graphs, in subsequent chapters it will be shown explicitly that $\overline{T(n)}$, the complement of the Triangular graph $T(n), O(k)$, as well as $J(n,k)$, are all distance-transitive. **Edge-** and **vertex-transitivity** are defined analogously, and are implied by distance-transitivity: with reference to Definition 4.2.2 above, $d(s,t)=d(u,v)=1$ in the former case, and 0 in the latter case.

The next property deals with the connectivity of $G(n,k,r)$, by which is meant the following:

Definition 4.2.4. *A graph G is* ***t*-connected** *if and only if a minimum number of t vertices need to be removed from G to result in a disconnected graph or a trivial graph.*

Proposition 4.2.5. [9, Proposition 3] *$G(n,k,r)$ is $\binom{k}{r}\binom{n-k}{k-r}$ -connected.*

Proof: Suppose that $u=\{x_1,x_2,x_3,\ldots,x_{k-m},x_{k-m+1},\ldots,x_k\}$ and $v=\{x_1,x_2,x_3,\ldots,x_{k-m},y_1,\ldots,y_m\}$ are vertices of $G(n,k,r)$ having $k-m$ elements in common. (By Lemma 4.1.1 it can be assumed that $n \geq 2k$.) Define a sequence of vertices $w_i = \{x_1,x_2,x_3,\ldots,x_{k-i},y_1,\ldots,y_i\}$ for $i=0,1,2,\ldots,m$. Now any two consecutive elements of the sequence $u=w_0,w_1,\ldots,w_m=v$ have $k-1$ elements in common. Hence $G(n,k,r)$ will

be connected if any two vertices s and t such that $|s \cap t| = k-1$ are connected. So suppose that s and t are vertices of $G(n,k,r)$ and $s \cap t = \{a_1, a_2, \ldots, a_{k-1}\}$. Then s and t are commonly adjacent to $\{a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_{k-r}\}$ for any $\{b_1, b_2, \ldots, b_{k-r}\} \subseteq \Omega \setminus (s \cup t)$. The result follows by Proposition 4.2.1(b) and a theorem of Lovász in [26] which states that a connected simple graph which has an edge-transitive automorphism group and valency at least t, is t-connected. □

The discussion above underlines the fact that Uniform Subset graphs possess a high degree of symmetry, being vertex-, edge- and distance-transitive. A question that comes to mind is the following: Do Uniform Subset graphs in any way characterize graphs that are vertex-, edge- or distance-transitive? In [33] this question is answered in the affirmative in the case of vertex-transitive graphs. The main ideas in [33] are outlined in the following section.

4.3 Vertex-transitive graphs as subgraphs induced by the orbits of Uniform Subset graphs

Since the vertices of $G(n,k,r)$ are just the elements of $\Omega^{\{k\}}$, any permutation $\alpha \in S_n$ induces a permutation σ_α of the vertices of $G(n,k,r)$ which preserves the size of the intersection i.e. $\alpha \in S_n$ induces an automorphism σ_α of $G(n,k,r)$, and hence α can be identified with σ_α.

Now let H be a subgroup of S_n, and consider a fixed orbit $\triangle^k$ of H as it acts on $\Omega^{\{k\}}$. Let K be the subgraph of $G(n,k,r)$ induced by $\triangle^k$: K has $\triangle^{\{k\}}$ as its vertex-set, and any two vertices u and v constitute an edge $[u,v]$ if and only if $|u \cap v| = r$. Clearly, H acts transitively on K, and hence K is vertex-transitive.

The above observation can be summed up in the following definition:

Definition 4.3.1. [33, Definition 1] *A graph K is an* **Orbit Uniform Subset graph** *if and only if it is a subgraph of $G(n,k,r)$ induced by an orbit of $\Omega^{\{k\}}$ when a permutation group acts on it.*

By Cayley's theorem which states that every group is isomorphic to a subgroup of a group of permutations, the following result is obtained:

Theorem 4.3.2. [33, Theorem 2] *Every finite group is isomorphic to a transitive subgroup of an automorphism group of a graph.*

The discussion now proceeds to identifying vertex-transitive graphs with Orbit Uniform Subset graphs.

Let G be a vertex-transitive graph which has m edges. The edges of G can be identified with the set $M = \{1, 2, 3, \ldots, m\}$. So for any vertex u of G, let

$$\overline{u} = \{i \in M : i \text{ is incident with } u\},$$

and consider the family of such subsets of M,

$$\mathcal{F} = \{\overline{u} : \ u \text{ is a vertex of } G\}.$$

Let K be the intersection graph which has $\mathcal{F}$ as its vertex-set, and any two vertices $\overline{u}$ and $\overline{v}$ constitute an edge if and only if $|\overline{u} \cap \overline{v}| \neq 0$. It is well-known that the intersection graph K is isomorphic to G, so it remains to be shown that K is an Orbit Uniform Subset graph. Since G is vertex-transitive, it is regular with valency say p. Hence for each vertex u of G, $|\overline{u}| = p$, which implies that $\mathcal{F}$ is a family of p-subsets of M. Moreover, for any edge $[\overline{u}, \overline{v}]$ of K, $|\overline{u} \cap \overline{v}| = 1$, since exactly one edge is incident with any two adjacent vertices. Hence K is a subgraph of $G(m, p, 1)$.

Now let H be a transitive subgroup of $\mathrm{Aut}(K)$. Any $\sigma \in \mathrm{Aut}(K)$ induces a permutation f_σ of M given by

$$f_\sigma(i) \in \sigma(\overline{u}) \cap \sigma(\overline{v}), \text{ whenever } i \in \overline{u} \cap \overline{v}.$$

f_σ is both well-defined and injective, since the intersection of any two vertices is unique, and σ preserves the uniqueness. Hence H is a subgroup of S_m, and K an Orbit Uniform Subset graph.

The above observations are summarized in the following result:

Theorem 4.3.3. [33, Theorem 3] *A vertex-transitive graph G is the subgraph of a Uniform Subset graph induced by an orbit of its vertex-set when a subgroup of $Aut(G)$ acts transitively on the vertices of G.*

This, in conjunction with the observation that any Orbit Uniform Subset graph is vertex-transitive, yields the following general result:

Theorem 4.3.4. [33, Theorem 4] *A graph G is vertex-transitive if and only if it is a subgraph induced by an orbit of a Uniform Subset graph under the action of some group.*

It should be noted that there are other sources of distance-transitive graphs besides the Uniform Subset graphs such as the Hamming graphs and the Grassman graphs. Nonetheless, Moon [32] showed that any distance-regular graph having the parameters of a Johnson graph is indeed a Johnson graph, and in [33] it is shown that any vertex-transitive graph is an Orbit Uniform Subset subgraph. In conclusion then, given that edge-transitivity is completely independent of vertex-transitivity, the question is posed whether there is a class of graphs which is the source of all edge-transitive graphs.

Chapter 5

Binary Codes and Permutation Decoding sets from the complements of the Triangular graphs

In Section 4.1 the Triangular graph $T(n)$ has been defined as the graph of which the vertex-set is the set of all 2-subsets of $\Omega = \{1, 2, \ldots, n\}$, and any two vertices u and v constitute an edge $[u, v]$ if and only if $|u \cap v| = 1$. As documented in Section 4.1, these graphs have received widespread attention. More recently, the codes generated by the rows of the adjacency matrix of these graphs have also received attention, notably by Tonchev [40], Haemers, Peeters and van Rijckenvorsel [13], Brouwer and van Eijl [7], and Key et al. [17]. In [17] it is shown that the code obtained thus is an $[\binom{n}{2}, n-1, n-1]$ code when n is odd, and an $[\binom{n}{2}, n-2, 2(n-2)]$ code when n is even. Moreover, in [17] it is shown that permutation decoding sets of the order of n^2 (when n is even) and of n (when n is odd) exist for these codes.

In this chapter the codes generated by the rows of the adjacency matrix of $\overline{T(n)}$, the complement of the Triangular graph $T(n)$, are studied. It is shown that the code obtained thus is the full space $F_2^{\binom{n}{2}}$ when $n \equiv 0 (\text{mod } 4)$, and the dual code of the span of the $\boldsymbol{j}$-

vector when $n \equiv 2(\text{mod } 4)$. The codes from the other two cases are less trivial: when $n \equiv 1(\text{mod } 4)$ the code is an $[\binom{n}{2}, \binom{n}{2} - n + 1, 3]$ code, and when $n \equiv 3(\text{mod } 4)$ it is an $[\binom{n}{2}, \binom{n}{2} - n, 4]$ code. Furthermore, in the former case both the code and its dual are shown to have bases comprising minimum weight vectors, whereas in the latter case only the code has a minimum weight basis since the $\boldsymbol{j}$-vector has to be adjoined to any set of minimum weight basis vectors in the dual code. The basis elements of C are used to identify an appropriate set of information positions for $C^{\perp}$ which make possible the determination of a permutation decoding set for $C^{\perp}$ of the order of n^2 when $n \equiv 3(\text{mod } 4)$, and of n when $n \equiv 1(\text{mod } 4)$.

The code generated by the rows of the adjacency matrix of $\overline{T(n)}$ is also the code of the $1 - (\binom{n}{2}, \binom{n-2}{2}, \binom{n-2}{2})$ design $\mathcal{D}$ of which the point set $\mathcal{P}$ is the vertex-set of $\overline{T(n)}$, and the block set $\mathcal{B}$ the supports of the set of incidence vectors of its adjacency matrix. It is well-known that $\text{Aut}(T(n))$ is the symmetric group S_n, and since the automorphism group of a graph equals that of its complement (see [37], Proposition 3.7), $\text{Aut}(\overline{T(n)})$ is also S_n, and hence S_n is contained in the automorphism group of both the design and the code. It is shown in Theorem 5.2.12 that for the non-trivial codes of $\overline{T(n)}$, the automorphism group is in fact S_n.

The primitive action of the alternating group $A_n, n \geq 5$, provides an alternative perspective on the codes described above. In [33, Theorem 2.4.12] it has been shown that the stabilizer $(A_n)_{\{a,b\}}$ of a 2-subset $P = \{a, b\}$ of Ω has as orbits P, and two others of lengths $2(n-2)$ and $\binom{n-2}{2}$. Consider as points the 2-subsets of Ω, and for each $P \in \Omega^{\{2\}}$, define $\overline{P}$ by $\overline{P} = \{Q \in \Omega^{\{2\}} : P \cap Q = \emptyset\}$ i.e. the orbit of length $\binom{n-2}{2}$. Then the points and blocks defined thus form a $1 - (\binom{n}{2}, \binom{n-2}{2}, \binom{n-2}{2})$ design of which the binary code is exactly that resulting from $\overline{T(n)}$.

The discussion proceeds with a few brief observations about $\overline{T(n)}$, notably its distance-transitivity.

5.1 Some basic properties of the complements of the Triangular graphs

$\overline{T(n)}$ has $\binom{n}{2}$ vertices and valency $\binom{n-2}{2}$. It is a strongly regular graph : if any two vertices u and v are adjacent, then they are commonly adjacent to $\binom{n-4}{2}$ vertices, and if they are non-adjacent, then they are commonly adjacent to $\binom{n-3}{2}$ vertices. The best-known of the graphs $\overline{T(n)}$ is the Petersen graph $\overline{T(5)}$.

$\overline{T(n)}$ is also distance- (and hence vertex- and edge-) transitive as shown below.

Proposition 5.1.1. *$\overline{T(n)}$ is distance-transitive.*

Proof: Suppose that $\{x_1, x_2\}, \{y_1, y_2\}, \{w_1, w_2\}$ and $\{z_1, z_2\}$ are vertices of $\overline{T(n)}$ such that $d(\{x_1, x_2\}, \{y_1, y_2\}) = d(\{w_1, w_2\}, \{z_1, z_2\}) = 1$. Then $\{x_1, x_2\} \cap \{y_1, y_2\} = \{w_1, w_2\} \cap \{z_1, z_2\} = \emptyset$, and there is a permutation $\alpha \in S_n$ such that $\alpha(x_i) = w_i$ and $\alpha(y_i) = z_i$, for all $i \in \{1, 2\}$, and which induces an automorphism σ_α of $\overline{T(n)}$ such that $\sigma_\alpha(\{x_1, x_2\}) = (\{w_1, w_2\})$ and $\sigma_\alpha(\{y_1, y_2\}) = (\{z_1, z_2\})$. If on the other hand, $d(\{x_1, x_2\}, \{y_1, y_2\}) = d(\{w_1, w_2\}, \{z_1, z_2\}) \neq 1$, then $d(\{x_1, x_2\}, \{y_1, y_2\}) = d(\{w_1, w_2\}, \{z_1, z_2\}) = 2$, since any two non-adjacent vertices are commonly adjacent to a third vertex (in fact, to $\binom{n-3}{2}$ vertices), and an automorphism of $\overline{T(n)}$ which maps the vertices appropriately is induced as before. □

Now that some of the basic properties of $\overline{T(n)}$ have been mentioned, the focus shifts to the main issue at hand in this chapter.

5.2 Binary Codes from $\overline{T(n)}$

Let n be a positive integer and $\overline{T(n)}$ the complement of the Triangular graph which has as its vertex-set $\mathcal{P}$, the set of all 2-subsets of $\Omega = \{1, 2, \ldots, n\}$. Now $\mathcal{P}$ also forms the

point set of the 1-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ where for each point $\{a, b\} \in \Omega^{\{2\}}$, a corresponding block denoted by $\overline{\{a, b\}}$ is defined as follows:

$$\overline{\{a, b\}} = \{\{x, y\} : \{x, y\} \subseteq \Omega \setminus \{a, b\}\}.$$

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

$$\mathcal{B} = \{\overline{\{a, b\}} : \{a, b\} \in \Omega^{\{2\}}\},$$

and the incidence vector of the block $\overline{\{a, b\}}$ by

$$v^{\overline{\{a,b\}}} = \sum_{\{x,y\} \subseteq \Omega \setminus \{a,b\}} v^{\{x,y\}}, \tag{5.1}$$

where the incidence vector of $X \subseteq \mathcal{P}$ is denoted by v^X. As had been explained in [17], the elements of $\mathcal{P}$ are themselves subsets of Ω, and hence v^X should in all correctness be denoted by $v^{\{X\}}$. However, the less pedantic notation does not diminish the arguments that follow, and has thus been adopted.

In all the results that follow it is assumed that $n \geq 5$ in order to avoid trivial cases. C denotes the binary code of $\mathcal{D}$ (and hence of $\overline{T(n)}$), and $C^\perp$ its dual.

The codes obtained in the case that n is even will first be described.

Lemma 5.2.1. *If $n \equiv 0 (\mathrm{mod}\ 4)$, then $C = F_2^{\binom{n}{2}}$.*

Proof: It suffices to show that each unit vector $v^{\{a,b\}}, \{a, b\} \in \Omega^{\{2\}}$, is in C. So suppose that $\{a, b\} \in \Omega^{\{2\}}$, and consider the set $\{v^{\overline{\{x,y\}}} : \{x, y\} \in \Omega^{\{2\}}$ and $v^{\overline{\{x,y\}}}$ is incident at $\{a, b\}\}$. Then

$$\begin{aligned}\sum_{\{x,y\} \subseteq \Omega \setminus \{a,b\}} v^{\overline{\{x,y\}}} &= \tbinom{n-2}{2} v^{\{a,b\}} + \tbinom{n-3}{2} \sum_{x \in \Omega \setminus \{a,b\}} v^{\{a,x\}} + \tbinom{n-3}{2} \sum_{y \in \Omega \setminus \{a,b\}} v^{\{b,y\}} \\ &\quad + \tbinom{n-4}{2} \sum_{\{x,y\} \subseteq \Omega \setminus \{a,b\}} v^{\{x,y\}},\end{aligned}$$

and since $n \equiv 0 (\text{mod } 4)$, $\sum_{\{x,y\} \subseteq \Omega \setminus \{a,b\}} v^{\overline{\{x,y\}}} = v^{\{a,b\}}$. $\square$

Lemma 5.2.2. *If $n \equiv 2(\text{mod } 4)$, then the set S consisting of the $\binom{n}{2} - 1$ vectors $\{v^{\{a,b\}} + v^{\{n-1,n\}} : \{a,b\} \in \Omega^{\{2\}}, \{a,b\} \neq \{n-1,n\}\}$ is a basis for C.*

Proof: The first step is to show that the vectors in S are indeed in C. So consider the following sum of incidence vectors:

$$\begin{aligned} & v^{\overline{\{a,b\}}} + \sum_{x \in \Omega \setminus \{a,b\}} v^{\overline{\{a,x\}}} + \sum_{y \in \Omega \setminus \{a,b\}} v^{\overline{\{b,y\}}} \\ = \; & (n-3) \sum_{x \in \Omega \setminus \{a,b\}} v^{\{a,x\}} + (n-3) \sum_{y \in \Omega \setminus \{a,b\}} v^{\{b,y\}} + (2n-7) \sum_{\{x',y'\} \subseteq \Omega \setminus \{a,b\}} v^{\{x',y'\}}. \end{aligned}$$

Since $n \equiv 2(\text{mod } 4)$, the vector sum above is incident at all the points $\{x,y\} \in \Omega^{\{2\}}, \{x,y\} \neq \{a,b\}$. Similarly for the vector sum

$$v^{\overline{\{n-1,n\}}} + \sum_{x \in \Omega \setminus \{n-1,n\}} v^{\overline{\{x,n-1\}}} + \sum_{y \in \Omega \setminus \{n-1,n\}} v^{\overline{\{y,n\}}},$$

and hence the combination of these sums yield

$$\begin{aligned} & v^{\overline{\{a,b\}}} + \sum_{x \in \Omega \setminus \{a,b\}} v^{\overline{\{a,x\}}} + \sum_{y \in \Omega \setminus \{a,b\}} v^{\overline{\{b,y\}}} + v^{\overline{\{n-1,n\}}} + \sum_{x' \in \Omega \setminus \{n-1,n\}} v^{\overline{\{x',n-1\}}} \\ & + \sum_{y' \in \Omega \setminus \{n-1,n\}} v^{\overline{\{y',n\}}} \\ = \; & v^{\{a,b\}} + v^{\{n-1,n\}}. \end{aligned}$$

In order to show that S spans C, it is sufficient to show that any incidence vector $v^{\overline{\{c,d\}}}, \{c,d\} \in \Omega^{\{2\}}$, is a sum of vectors in S. So consider the sum

$$\sum_{\substack{\{x,y\} \subseteq \Omega \setminus \{c,d\} \\ \{x,y\} \neq \{n-1,n\}}} (v^{\{x,y\}} + v^{\{n-1,n\}}).$$

Now if $\{c,d\} \neq \{n-1,n\}$, then

$$\sum_{\substack{\{x,y\} \subseteq \Omega \setminus \{c,d\} \\ \{x,y\} \neq \{n-1,n\}}} (v^{\{x,y\}} + v^{\{n-1,n\}}) = \sum_{\substack{\{x,y\} \subseteq \Omega \setminus \{c,d\} \\ \{x,y\} \neq \{n-1,n\}}} v^{\{x,y\}} + (\tbinom{n-2}{2} - 1) v^{\{n-1,n\}},$$

and since $n \equiv 2(\text{mod } 4)$, this sum reduces to $\sum_{\{x,y\}\subseteq\Omega\setminus\{c,d\}} v^{\{x,y\}}$ i.e. to $v^{\overline{\{c,d\}}}$. On the other hand, if $\{c,d\} = \{n-1,n\}$ then

$$\sum_{\substack{\{x,y\}\subseteq\Omega\setminus\{c,d\}\\ \{x,y\}\neq\{n-1,n\}}} (v^{\{x,y\}} + v^{\{n-1,n\}}) = \sum_{\{x,y\}\subseteq\Omega\setminus\{n-1,n\}} v^{\{x,y\}} + \tbinom{n-2}{2} v^{\{n-1,n\}},$$

and since $n \equiv 2(\text{mod } 4)$, this sum reduces to $\sum_{\{x,y\}\subseteq\Omega\setminus\{n-1,n\}} v^{\{x,y\}}$ i.e. to $v^{\overline{\{n-1,n\}}}$ in this case. Linear independence follows easily from the observation that any two vectors in S are commonly incident only at $\{n-1,n\}$. Clearly,

$$|S| = |\{v^{\{a,b\}} + v^{\{n-1,n\}} : \{a,b\} \in \Omega^{\{2\}}, \{a,b\} \neq \{n-1,n\}\}| = \tbinom{n}{2} - 1.$$

□

Lemma 5.2.3. *If $n \equiv 2(\text{mod } 4)$, then the minimum weight of C is 2. The vectors in S, together with the $\binom{\binom{n}{2}-1}{2}$ vectors $\{v^{\{a,b\}} + v^{\{c,d\}} : \{a,b\},\{c,d\} \in \Omega^{\{2\}}, \{a,b\} \neq \{c,d\} \neq \{n-1,n\}\}$ constitute the $\binom{\binom{n}{2}}{2}$ minimum words in C.*

Proof: Since each incidence vector $v^{\overline{\{a,b\}}}, \{a,b\} \in \Omega^{\{2\}}$, has weight $\binom{n-2}{2}$, which is even if $n \equiv 2(\text{mod } 4)$, the $\boldsymbol{j}$ vector is in $C^\perp$ - in fact, $C^\perp = \text{span}\{\boldsymbol{j}\}$ since the dimension of C is $\binom{n}{2} - 1$. Hence C has no vectors of odd weight, and since the vectors in S each has a weight of 2, the minimum weight of C is 2. Clearly, the only other vectors of weight 2 in C result from the sum of any two vectors in S, and since there are $\binom{\binom{n}{2}-1}{2}$ of these, C has $\binom{\binom{n}{2}-1}{2} + \binom{n}{2} - 1 = \binom{\binom{n}{2}}{2}$ minimum words. □

The codes for n odd are somewhat less trivial, and are described next. As before, the identification of basis vectors for C and $C^\perp$ takes priority. To facilitate the discussion in the case of $C^\perp$, the following notation is introduced:

For $\{c\} \in \Omega^{\{1\}}$, define a vector $v(\{c\})$ by

$$v(\{c\}) = \sum_{z\in\Omega\setminus\{c\}} v^{\{c,z\}}. \tag{5.2}$$

Lemma 5.2.4. *If n is odd, then the set of vectors $\{v(\{c\}) : \{c\} \in \Omega^{\{1\}}\}$ is in $C^{\perp}$. $R = \{v(\{c\}) : \{c\} \in \Omega^{\{1\}}, c \neq 1\}$ is a linearly independent set in $C^{\perp}$. If in addition, $n \equiv 3 (\mathrm{mod}\ 4)$, then $R \cup \{\boldsymbol{j}\}$ is linearly independent in $C^{\perp}$.*

Proof: Suppose that n is odd, and for any incidence vector $v^{\overline{\{a,b\}}} \in C$, consider the inner product $(v^{\overline{\{a,b\}}}, v(\{c\})) = (\sum_{\{x,y\} \subseteq \Omega \setminus \{a,b\}} v^{\{x,y\}}, \sum_{z \in \Omega \setminus \{c\}} v^{\{c,z\}})$. If $c \in \{a,b\}$, then there are no points at which $v^{\overline{\{a,b\}}}$ and $v(\{c\})$ are commonly incident. If, on the other hand, $c \notin \{a,b\}$, then these two vectors are commonly incident at $n-3$ points. Hence, since n is odd, $(v^{\overline{\{a,b\}}}, v(\{c\})) = 0$ in each case. The linearity of the inner product implies that span $\{v(\{c\}) : \{c\} \in \Omega^{\{1\}}\} \subseteq C^{\perp}$. However, the set $\{v(\{c\}) : \{c\} \in \Omega^{\{1\}}\}$ is linearly dependent, since at each point $\{a,b\} \in \Omega^{\{2\}}$, only the vectors $v(\{a\})$ and $v(\{b\})$ are incident. Now each vector in $R = \{v(\{c\}) : \{c\} \in \Omega^{\{1\}}, c \neq 1\}$ is uniquely incident at the point $\{1,c\}$, and hence no non-trivial linear combination of vectors in R is zero. Neither does any linear combination of vectors in R equal the $\boldsymbol{j}$-vector. Since each incidence vector $v^{\overline{\{a,b\}}} \in C$ has weight $\binom{n-2}{2}$ which is even when $n \equiv 3 (\mathrm{mod}\ 4)$, but not when $n \equiv 1 (\mathrm{mod}\ 4)$, it follows that $R \cup \{\boldsymbol{j}\}$ is linearly independent in $C^{\perp}$ in the former case. □

In the above lemma potential basis vectors have been identified for $C^{\perp}$. In order to verify that these vectors are indeed basis vectors, the focus of the discussion shifts back to C, and the following notation is deemed helpful:

For any $\{a,b,c\} \in \Omega^{\{3\}}$, define a vector $v^{\overline{\{a,b,c\}}}$ by

$$v^{\overline{\{a,b,c\}}} = v^{\{a,b\}} + v^{\{a,c\}} + v^{\{b,c\}}. \tag{5.3}$$

Lemma 5.2.5. *If $n \equiv 1 (\mathrm{mod}\ 4)$, then the set U consisting of the $\binom{n-1}{2}$ vectors $\{v^{\overline{\{a,b,n\}}} : \{a,b\} \in \Omega^{\{2\}}, a,b \neq n\}$ is a basis for C. Consequently, R is a basis for $C^{\perp}$.*

Proof: In order to show that the set U is contained in C, consider the sum, $\sum_{\{x,y\} \subseteq \Omega \setminus \{a,b,n\}} v^{\overline{\{x,y\}}}$,

of incidence vectors. Now

$$\begin{aligned}\sum_{\{x,y\}\subseteq\Omega\setminus\{a,b,n\}} v^{\overline{\{x,y\}}} &= \tbinom{n-3}{2}v^{\{a,b\}} + \tbinom{n-3}{2}v^{\{a,n\}} + \tbinom{n-3}{2}v^{\{b,n\}} \\ &\quad + \tbinom{n-4}{2}\sum_{x\in\Omega\setminus\{a,b,n\}} v^{\{a,x\}} + \tbinom{n-4}{2}\sum_{y\in\Omega\setminus\{a,b,n\}} v^{\{b,y\}} \\ &\quad + \tbinom{n-4}{2}\sum_{z\in\Omega\setminus\{a,b,n\}} v^{\{z,n\}} + \tbinom{n-5}{2}\sum_{\{x',y'\}\subseteq\Omega\setminus\{a,b,n\}} v^{\{x',y'\}},\end{aligned}$$

and since $n \equiv 1(\text{mod } 4)$, this sum reduces to $v^{\{a,b\}} + v^{\{a,n\}} + v^{\{b,n\}}$ i.e. to $v^{\overline{\{a,b,n\}}}$. Next, to show that U spans C, it is sufficient to show that any incidence vector is a sum of vectors in U. Hence, consider the following sum of vectors in U:

$$\begin{aligned}\sum_{\{x,y\}\subseteq\Omega\setminus\{a,b,n\}} v^{\overline{\{x,y,n\}}} &= \sum_{\{x,y\}\subseteq\Omega\setminus\{a,b,n\}} v^{\{x,y\}} + \sum_{\{x,y\}\subseteq\Omega\setminus\{a,b,n\}} v^{\{x,n\}} + \sum_{\{x,y\}\subseteq\Omega\setminus\{a,b,n\}} v^{\{y,n\}} \\ &= \sum_{\{x,y\}\subseteq\Omega\setminus\{a,b,n\}} v^{\{x,y\}} + (n-4)\sum_{x'\in\Omega\setminus\{a,b,n\}} v^{\{x',n\}}\end{aligned}$$

Now since $n \equiv 1(\text{mod } 4)$, this sum reduces to $\sum_{\{x',y'\}\subseteq\Omega\setminus\{a,b\}} v^{\{x',y'\}}$ i.e. to the incidence vector $v^{\overline{\{a,b\}}}$. It remains to be shown that U is linearly independent, and to this end, the points of $\mathcal{P}$ are ordered as follows: the $\binom{n-1}{2}$ points

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

are followed by the remaining $n-1$ points

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

Then when the vectors of U are ordered according to lexicographic ordering, a matrix in standard form is obtained, the rank of which is easily seen to be $\binom{n-1}{2}$. Hence U is a basis for C, and $\dim(C) = \binom{n-1}{2}$. By Lemma 5.2.4, R is a linearly independent set in $C^{\perp}$, and $|R| = n-1 = \binom{n}{2} - \binom{n-1}{2}$. Hence R is a basis for $C^{\perp}$. □

Lemma 5.2.6. *If $n \equiv 1(\text{mod } 4)$, then the minimum weight of C is 3, and the set U together with the $\binom{n-1}{3}$ vectors $\{v^{\overline{\{a,b,c\}}} : \{a,b,c\} \in \Omega^{\{3\}}, a,b,c \neq n\}$ constitute the $\binom{n}{3}$ minimum words.*

Proof: Since each vector in U has weight 3, it is sufficient to show that C does not have vectors of smaller weight. Obviously, C does not have vectors of weight 1. So suppose that C has a vector w of weight 2. Then $w = v^{\{a,b\}} + v^{\{c,d\}}$, for some $\{a,b\}, \{c,d\} \in \Omega^{\{2\}}$. Now if $\{a,b\} \cap \{c,d\} = \emptyset$, then the inner product $(v^{\{a,b\}} + v^{\{c,d\}}, v(\{a\})) = 1$, contradicting the fact that $v(\{a\}) \in C^{\perp}$. On the other hand, if $\{a,b\} \cap \{c,d\} = \{a\}$, say, then $(v^{\{a,b\}} + v^{\{c,d\}}, v(\{b\})) = 1$, and since there are no other cases to consider, this implies that C has no vectors of weight 2. Hence the minimum weight of C is 3. Besides the vectors in U, vectors of weight 3 in C can be obtained from those in U as follows:

$$\begin{aligned}\sum_{\substack{\{x,y\}\subseteq\{a,b,c\}\\ a,b,c\neq n}} v^{\overline{\{x,y,n\}}} &= v^{\{a,b\}} + v^{\{a,c\}} + v^{\{b,c\}} + 2v^{\{a,n\}} + 2v^{\{b,n\}} + 2v^{\{c,n\}} \\ &= v^{\{a,b\}} + v^{\{a,c\}} + v^{\{b,c\}} \\ &= v^{\overline{\{a,b,c\}}}.\end{aligned}$$

$\binom{n-1}{3}$ vectors can be obtained in the above way, and it can easily be checked that besides these and those in U, there are no other vectors of weight 3 in C. Since there are $\binom{n-1}{2}$ vectors in U, C has a total of $\binom{n-1}{3} + \binom{n-1}{2} = \binom{n}{3}$ minimum words. □

In order to deduce analogous results in the case that $n \equiv 3(\text{mod } 4)$, the following notation is needed to facilitate the discussion:

For any $\{a,b,c,d\} \in \Omega^{\{4\}}$, define a vector $v[\{a,b\}|\{c,d\}]$ by

$$v[\{a,b\}|\{c,d\}] = v^{\{a,c\}} + v^{\{a,d\}} + v^{\{b,c\}} + v^{\{b,d\}}. \tag{5.4}$$

Lemma 5.2.7. *If $n \equiv 3(\text{mod } 4)$, then the set W consisting of the $\binom{n}{2} - n$ vectors $\{v[\{1,n\}|\{2,3\}]$, $v[\{1,n\}|\{3,4\}]$, $v[\{1,n\}|\{4,5\}]$, $\ldots$, $v[\{1,n\}|\{n-2,n-1\}]$, $v[\{1,n-2\}|\{n-1,n\}]$, $v[\{2,n\}|\{3,4\}]$, $\ldots$, $v[\{2,n\}|\{n-2,n-1\}]$, $v[\{2,n-2\}|\{n-1,n\}]$, $v[\{3,n\}|\{4,5\}]$, $\ldots$, $v[\{n-3,n-2\}|\{n-1,n\}]\}$ is a basis for C. Consequently, $R \cup \{\boldsymbol{j}\}$ is a basis for $C^{\perp}$.*

Proof: As in the case of the relevant previous lemmas, it will be shown that any vector

$v[\{a,b\}|\{c,d\}], \{a,b,c,d\} \in \Omega^{\{4\}}$ is in C, from which it will follow that the set W is in C. So consider the following sum of incidence vectors:

$$\begin{aligned}
& v^{\overline{\{a,c\}}} + v^{\overline{\{a,d\}}} + v^{\overline{\{b,c\}}} + v^{\overline{\{b,d\}}} \\
= & \sum_{\{x,y\}\subseteq\Omega\setminus\{a,c\}} v^{\{x,y\}} + \sum_{\{x',y'\}\subseteq\Omega\setminus\{a,d\}} v^{\{x',y'\}} + \sum_{\{x'',y''\}\subseteq\Omega\setminus\{b,c\}} v^{\{x'',y''\}} + \sum_{\{x''',y'''\}\subseteq\Omega\setminus\{b,d\}} v^{\{x''',y'''\}} \\
= & v^{\{a,c\}} + v^{\{a,d\}} + v^{\{b,c\}} + v^{\{b,d\}} + 2\sum_{x\in\Omega\setminus\{a,b,c,d\}} v^{\{a,x\}} + 2\sum_{y\in\Omega\setminus\{a,b,c,d\}} v^{\{b,y\}} \\
& +2\sum_{z\in\Omega\setminus\{a,b,c,d\}} v^{\{c,z\}} + 2\sum_{w\in\Omega\setminus\{a,b,c,d\}} v^{\{d,w\}} + 4\sum_{\{x',y'\}\subseteq\Omega\setminus\{a,b,c,d\}} v^{\{x',y'\}} \\
= & v^{\{a,c\}} + v^{\{a,d\}} + v^{\{b,c\}} + v^{\{b,d\}}.
\end{aligned}$$

In order to show that W is linearly independent, the points of $\mathcal{P}$ are ordered as follows: first the $\binom{n}{2} - n$ points

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

followed by the remaining n points

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

When the vectors in W are ordered as in the statement of the lemma, the result is an upper triangular matrix the rank of which is $\binom{n-2}{2}-1 = \binom{n}{2}-(n-1)-1 = \binom{n}{2}-n$. Hence $\dim(C) \geq \binom{n}{2}-n$. By Lemma 5.2.4, $\dim(C)^{\perp} \geq n$, and since C is linear, $\dim(C) \leq \binom{n}{2}-n$. Finally, since W is a linearly independent set in C and $|W| = \dim(C)$, it follows that W is a basis for C. By the same token, $R \cup \{\boldsymbol{j}\}$ is a basis for $C^{\perp}$. □

Recall that if $n \equiv 1(\text{mod } 4)$, the incidence vectors in C have odd weight and hence $\boldsymbol{j} \in C$. Subsequently, the minimum weight of C is odd. This differs from the case if $n \equiv 3(\text{mod } 4)$, and is elaborated below. Compare also, the configuration of the minimum words now that $\boldsymbol{j} \in C^{\perp}$.

Lemma 5.2.8. *If $n \equiv 3(\text{mod } 4)$, then the minimum weight of C is 4. The set of vectors $\{v[\{a,b\}|\{c,d\}], \{a,b,c,d\} \in \Omega^{\{4\}}\}$ constitute the $3.\binom{n}{4}$ minimum words in C.*

Proof: As remarked before, if $n \equiv 3(\text{mod } 4)$, then each incidence vector has even weight, and hence $\boldsymbol{j} \in C^{\perp}$. Subsequently, all vectors in C have even weight, and since each vector $v[\{a,b\}|\{c,d\}], \{a,b,c,d\} \in \Omega^{\{4\}}$ has weight 4, it remains to be shown that C has no vectors of weight 2. By the same argument as in Lemma 5.2.6, C has no vectors of weight 2. Hence the minimum weight of C is 4. In order to show that any vector w of weight 4 in C has the form $v[\{a,b\}|\{c,d\}], \{a,b,c,d\} \in \Omega^{\{4\}}$, suppose that w is incident at $\{a,c\}$ i.e. $w = v^{\{a,c\}} + v^X + v^Y + v^Z, X, Y, Z \in \Omega^{\{2\}}$. Now since w is orthogonal to $v(\{a\}),\ X = \{a,d\}$ say, and since w is then also orthogonal to $v(\{c\})$ and to $v(\{d\}),\ c,d \in Y \cup Z$. $Y \neq \{c,d\}$, otherwise any choice of $Z \in \Omega^{\{2\}}$ would result in w not being orthogonal to two of the vectors in $\{v(\{a\}) : \{a\} \in \Omega^{\{1\}}\}$. Hence $c \in Y$, and $d \in Z$, say. By the same reasoning, $Y = \{b,c\}$ and $Z = \{b,d\}$, say, and it follows that any vector in C of weight 4 is of the stated form. Finally, $|\{v[\{a,b\}|\{c,d\}], \{a,b,c,d\} \in \Omega^{\{4\}}\}|$ is equal to the number of ways of partitioning any 4-subset of Ω into 2-subsets, which in turn equals $\frac{1}{2} \cdot \binom{n}{4} \cdot \binom{4}{2} = 3\binom{n}{4}$. □

By Lemmas 5.2.6 and 5.2.8, C has a basis of minimum weight vectors when $n \equiv 1(\text{mod } 4)$ or $n \equiv 3(\text{mod } 4)$ - in fact, C always has a basis of minimum weight vectors when the trivial cases are also taken into account. However, the same is not true for $C^{\perp}$ as hinted at in Lemma 5.2.7. This will be shown by determining the minimum weight of $C^{\perp}$ by considering the weights of words formed by linear combinations of these basis elements.

Lemma 5.2.9. *If n is odd, then the minimum weight of $C^{\perp}$ is $n-1$. The set of vectors $\{v(\{a\}) : \{a\} \in \Omega^{\{1\}}\}$ constitute the n minimum words of $C^{\perp}$.*

Proof: Recall that $R = \{v(\{a\}) : \{a\} \in \Omega^{\{1\}}, a \neq 1\}$ is a basis for $C^{\perp}$ when $n \equiv 1(\text{mod } 4)$. Clearly, $v(\{a\}) = \sum_{x \in \Omega \setminus \{a\}} v^{\{a,x\}}$ has weight $n-1$, and any two vectors $v(\{a\})$ and $v(\{b\})$ are commonly incident only at $\{a,b\}$. Suppose then that a linear combination of k vectors in R yields a weight of less than $n-1$. Then

$$k(n-1) - 2\binom{k}{2} < n-1,$$

$$\text{i. e. } k < 1 \text{ or } k > n-1.$$

However, neither possibility for k is feasible - in the second instance there are a maximum of $n-1$ vectors in R from which a set of k has to be chosen. Adjoining the $\boldsymbol{j}$ vector to R in the case that $n \equiv 3(\text{mod } 4)$ does not affect the minimum weight. Equality in the expression for the weight of a linear combination of k basis vectors above implies that the minimum words are precisely $\{v(\{a\}) : \{a\} \in \Omega^{\{1\}}\}, v(\{1\})$ of course being included in this set. □

Lemmas 5.2.1 to 5.2.9 can be summed up in the following theorem:

Theorem 5.2.10. *The code obtained from the complements of the Triangular graph* $\overline{T(n)}$, *and the* $1-(\binom{n}{2}, \binom{n-2}{2}, \binom{n-2}{2})$ *design is*

(1) the full space $F_2^{\binom{n}{2}}$ *if* $n \equiv 0(\text{mod } 4)$,

(2) an $[\binom{n}{2}, \binom{n}{2} - n + 1, 3]$ *code if* $n \equiv 1(\text{mod } 4)$,

(3) an $[\binom{n}{2}, \binom{n}{2} - 1, 2]$ *code if* $n \equiv 2(\text{mod } 4)$,

(4) an $[\binom{n}{2}, \binom{n}{2} - n, 4]$ *code if* $n \equiv 3(\text{mod } 4)$.

By Lemmas 5.2.1 and 5.2.2, $C^\perp = \{0\}$ if $n \equiv 0(\text{mod } 4)$, and $C^\perp = \text{span } \{\boldsymbol{j}\}$ if $n \equiv 2(\text{mod } 4)$. The relationship between C and $C^\perp$ is examined next in the case that n is odd.

Lemma 5.2.11. *C is neither self-dual nor self-orthogonal for any value of n. If n is odd, then $C \oplus C^\perp = F_2^{\binom{n}{2}}$.*

Proof: The first statement is clear if n is even by Lemmas 5.2.1 and 5.2.2. If n is odd, then given that the vectors $\{v(\{a\}) : \{a\} \in \Omega^{\{1\}}\}$ are in $C^\perp$, consider the inner product $(v(\{a\}), v(\{b\})), a \neq b$. Since $v(\{a\})$ and $v(\{b\})$ are commonly incident only at $\{a, b\}, (v(\{a\}), v(\{b\})) = 1$, which implies that $v(\{a\}) \notin C$, and hence $C^\perp \not\subset C$. Neither is $C^\perp \subseteq C$, as is evident from the inner product $(v^{\overline{\{a,b\}}}, v^{\overline{\{c,d\}}})$ of any two incidence vectors

$v^{\overline{\{a,b\}}}, v^{\overline{\{c,d\}}} \in C$: if $|\{a,b\} \cap \{c,d\}| = 0$, then $(v^{\overline{\{a,b\}}}, v^{\overline{\{c,d\}}}) = \binom{n-4}{2}$, which is odd if $n \equiv 3(\text{mod } 4)$, and if $|\{a,b\} \cap \{c,d\}| = 1$, then $(v^{\overline{\{a,b\}}}, v^{\overline{\{c,d\}}}) = \binom{n-3}{2}$, which is odd if $n \equiv 1(\text{mod } 4)$. Alternatively, it can be argued that if $n \equiv 1(\text{mod } 4)$, C has vectors of weight 3 whereas $C^{\perp}$ does not since $n - 1 \geq 4$ if $n \geq 5$. The same can be said about vectors of weight 4 in the case that $n \equiv 3(\text{mod } 4)$. The last statement of the lemma follows from the observation that

$$v^{\overline{\{a,b\}}} = v(\{a\}) + v(\{b\}) + v^{\{a,b\}} + \boldsymbol{j}. \qquad \square$$

The Triangular graph $T(n)$ is a highly symmetrical graph, and this is reflected in the fact that its automorphism group is large. It is well-known that $\text{Aut}(T(n))$ is the symmetric group S_n, and since the automorphism group of any graph equals that of its complement, $\text{Aut}(\overline{T(n)})$ is also S_n. Now any automorphism of a graph induces an automorphism of the design $\mathcal{D}$ and the code C generated by the rows of the adjacency matrix of the graph. For example, if P and Q are adjacent in $\overline{T(n)}$ and $\sigma \in \text{Aut}(\overline{T(n)})$, then $\sigma(P)$ is adjacent to $\sigma(Q)$, and by defining

$$P' = \Omega \setminus \cup\{\sigma(Q) : P \text{ is adjacent to } Q\},$$

σ induces an automorphism of C which maps $v^{\overline{P}}$ to $v^{\overline{P'}}$ where the definition of $v^{\overline{P}}$ and $v^{\overline{P'}}$ is consistent with the use throughout this chapter. Hence S_n will be contained in $\text{Aut}(C)$. The following proposition establishes that $\text{Aut}(C)$ is in fact either S_n or $S_{\binom{n}{2}}$.

Proposition 5.2.12. *If n is even, then Aut(C) is $S_{\binom{n}{2}}$, and if n is odd, then Aut(C) is S_n. (It is assumed that $n \geq 5$.)*

Proof: The proposition is clear if n is even, since $C = F_2^{\binom{n}{2}}$ if $n \equiv 0(\text{mod}4)$, and $C^{\perp} = \text{span}\{\boldsymbol{j}\}$ if $n \equiv 2(\text{mod } 4)$. If n is odd, then the vectors $\{v(\{a\}) : \{a\} \in \Omega^{\{1\}}\}$ constitute the minimum words of C, and any $\sigma \in \text{Aut}(C)$ preserves these words, thereby inducing a permutation of the elements of Ω i.e. $\sigma \in S_n$. $\square$

5.3 Permutation Decoding sets for $C^{\perp}$

In general, the automorphism group of a t-error correcting code provides the base for membership of a permutation decoding 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. Since C has small minimum weights for all values of n, its error correcting potential is limited (in fact, non-existent if n is even), and hence permutation decoding sets will be sought for $C^{\perp}$ in the non-trivial cases.

Theorem 5.3.1. *Let $\mathcal{I}$ denote the points*

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

where $n \geq 5$. Then

(1) $\mathcal{S} = \{1_{S_n}\} \cup \{(i, n) : 1 \leq i \leq n-1\}$ is a PD-set of size n for $C^{\perp}$ with $\mathcal{I}$ as the information positions if $n \equiv 1 (\mathrm{mod}\ 4)$, and

(2) $\mathcal{S} = \{1_{S_n}\} \cup \{(i, n) : 1 \leq i \leq n-3\} \cup \{(j, n-1) : 1 \leq j \leq n-3\} \cup \{(i, n)(j, n-1) : 1 \leq i, j \leq n-3\}$ is a PD-set of size $n^2 - 5n + 7$ for $C^{\perp}$ with $\mathcal{I}$ including the point $\{n-2, n-1\}$ as the information positions if $n \equiv 3 (\mathrm{mod}\ 4)$.

Proof: (1) In Lemma 5.2.5 it is shown how an ordering of the points of $\mathcal{P}$ results in a generator matrix for C, and hence a check matrix for $C^{\perp}$ in standard form if $n \equiv 1 (\mathrm{mod}\ 4)$. By shifting the first $\binom{n}{2} - n + 1$ points to the end so that the ordering is

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

followed by the remaining points

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

a generator matrix for $C^{\perp}$ in standard form is obtained, thereby identifying the points P_1 to P_{n-1} as the information positions $\mathcal{I}$. Now since $C^{\perp}$ has minimum weight $n-1, C^{\perp}$ can correct $t = \dfrac{n-3}{2}$ errors. Suppose that $e \leq t$ errors occur at the points $\mathcal{E}$.

Case (i): $\mathcal{E} \subseteq \mathcal{P} \setminus \mathcal{I}$

The identity, 1_{S_n}, will leave $\mathcal{E}$ fixed.

Case (ii): $\mathcal{E} \subseteq \mathcal{I}$

Since $e \leq t = \dfrac{n-3}{2} \leq n-3$, there is an element $i \in \Omega, i \neq n$, such that $\{i, n\} \notin \mathcal{E}$. Hence the transposition (i, n) will map $\mathcal{E}$ into $\mathcal{P} \setminus \mathcal{I}$.

Case (iii): $\mathcal{E} \cap \mathcal{I} \neq \emptyset$ and $\mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I}) \neq \emptyset$

Suppose that $|\mathcal{E} \cap \mathcal{I}| = r$, and $|\mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I})| = m$. Then $|(\cup\mathcal{E}) \setminus \{n\}| \leq r + 2m$, and since $r + m \leq t = \dfrac{n-3}{2}$, it follows that $2r + 2m \leq n - 3$, and hence $r + 2m \leq n - 3$. Hence there is an element $i \in \Omega$ such that $\{i, k\} \notin \mathcal{E}$ for any $k \in \Omega$, and (i, n) will map $\mathcal{E} \cap \mathcal{I}$ into $\mathcal{P} \setminus \mathcal{I}$, while $\mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I})$ will remain fixed.

Hence $\mathcal{S} = \{1_{S_n}\} \cup \{(i, n) : 1 \leq i \leq n-1\}$ is a PD-set of size n for $C^{\perp}$ if $n \equiv 1 (\text{mod } 4)$.

(2) In Lemma 5.2.7 a specific ordering of the points results in a generator matrix for C in upper triangular form if $n \equiv 3 (\text{mod } 4)$. This matrix can of course be reduced to standard form, and by shifting the first $\binom{n}{2} - n$ points to the end so that the ordering is

$$P_1 = \{1, n\},\ P_2 = \{2, n\},\ \ldots,\ P_{n-3} = \{n-3, n\},\ P_{n-2} = \{n-2, n-1\},$$
$$P_{n-1} = \{n-2, n\},\ P_n = \{n-1, n\},$$

followed by

$$P_{n+1} = \{1, 2\},\ P_{n+2} = \{1, 3\},\ \ldots,\ P_{2n-1} = \{2, 3\},\ \ldots,\ P_{\binom{n}{2}} = \{n-3, n-1\},$$

a generator matrix in standard form can be obtained for $C^{\perp}$, and the set $\mathcal{I}$ consists of the points P_1 to P_n.

Case (i): $\mathcal{E} \subseteq \mathcal{P} \setminus \mathcal{I}$

As before, 1_{S_n}, will leave $\mathcal{E}$ fixed.

Case (ii): $\mathcal{E} \subseteq \mathcal{I}, \{n-2, n-1\} \notin \mathcal{E}$.

The following sub-cases have to be considered:

(a) $\{n-2,n\},\{n-1,n\} \in \mathcal{E}$,

(b) $\{n-2,n\} \in \mathcal{E}$, but $\{n-1,n\} \notin \mathcal{E}$, or $\{n-1,n\} \in \mathcal{E}$, but $\{n-2,n\} \notin \mathcal{E}$,

(c) $\{n-2,n\},\{n-1,n\} \notin \mathcal{E}$.

In each of the above sub-cases, $e \leq t = \dfrac{n-3}{2} \leq n-4$ if $n \geq 5$, and hence there is an element $i \in \Omega, i \neq n, n-1, n-2$, such that the transposition (i,n) will map $\mathcal{E}$ into $\mathcal{P} \setminus \mathcal{I}$.

Case (iii): $\mathcal{E} \cap \mathcal{I} \neq \emptyset,\ \mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I}) \neq \emptyset,\ \{n-2,n-1\} \notin \mathcal{E}$.
Sub-cases (a), (b) and (c) have to be considered again as in Case(ii). In each case, suppose that $|\mathcal{E} \cap \mathcal{I}| = r$ and $|\mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I})| = m$. Then since $r + m = e \leq \dfrac{n-3}{2}$, it follows that $2r + 2m \leq n-3$. Now $r \geq 1$ as well, and hence $|(\cup\mathcal{E}) \setminus \{n\}| \leq r + 2m \leq n-4$. Hence there is an element $i \in \Omega$, such that $\{i,k\} \notin \mathcal{E}$ for any $k \in \Omega$, and (i,n) will map $\mathcal{E} \cap \mathcal{I}$ into $\mathcal{P} \setminus \mathcal{I}$, while $\mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I})$ will remain fixed.

Case (iv): $\{n-2,n-1\} \in \mathcal{E},\ \mathcal{E} \setminus \{\{n-2,n-1\}\} \subseteq \mathcal{P} \setminus \mathcal{I}$.
Since $|\cup\mathcal{E}| \leq 2e \leq n-3$, and since $n-2, n-1 \in \cup\mathcal{E}$ there is an element $i \in \Omega,\ i \neq n, n-1, n-2$, such that $(i,n-1)$ will map $\{n-2,n-1\}$ into $\mathcal{P} \setminus \mathcal{I}$, but $\mathcal{E} \setminus \{\{n-2,n-1\}\}$ will remain in $\mathcal{P} \setminus \mathcal{I}$.

Case (v): $\{n-2,n-1\} \in \mathcal{E},\ \mathcal{E} \subseteq \mathcal{I}$.
In this case the sub-cases (a), (b) and (c) have to be considered again. In (a), (b) and (c), $|(\cup\mathcal{E}) \setminus \{n\}|$ equals $e-1, e$ and $e+1$ respectively. Now $e \leq \dfrac{n-3}{2} \leq n-5$ if $n \geq 7$. Hence in each sub-case there are elements $i,j \in \Omega, i,j \neq n, n-1, n-2$, such that $(i,n)(j,n-1)$ will map $\mathcal{E}$ into $\mathcal{P} \setminus \mathcal{I}$.

Case (vi): $\{n-2,n-1\} \in \mathcal{E},\ \mathcal{E} \cap \mathcal{I} \neq \Omega,\ \mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I}) \neq \emptyset$.
In the final case the sub-cases (a), (b) and (c) also arise. Then as in Case (iii), suppose that $|\mathcal{E} \cap \mathcal{I}| = r$ and $|\mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I})| = m$. In (a), (b) and (c), $|(\cup\mathcal{E}) \setminus \{n\}|$ equals $r+2m-1, r+2m$ and $r+2m+1$ respectively. By the same argument as in Case (iii), there are elements $i,j \in \Omega, i,j \neq n, n-1, n-2$, such that $(i,n)(j,n-1)$ will map $\mathcal{E} \cap \mathcal{I}$ into $\mathcal{P} \setminus \mathcal{I}$ but $\mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I})$ will remain in $\mathcal{P} \setminus \mathcal{I}$.

Hence $\mathcal{S} = \{1_{S_n}\} \cup \{(i,n) : 1 \leq i \leq n-3\} \cup \{(j,n-1) : 1 \leq j \leq n-3\} \cup \{(i,n)(j,n-1) : 1 \leq i,j \leq n-3\}$ is a PD-set of size $n^2 - 5n + 7$ for $C^{\perp}$ if $n \equiv 3 (\text{mod } 4)$. $\square$

It is easily observed that the Gordon bound for a PD-set for $C^{\perp}$ simplifies to $\frac{n-1}{2}$ if $n \equiv 1 (\text{mod } 4)$ or if $n \equiv 3 (\text{mod } 4)$. Using Magma [6], a table comparing the size of this bound to the size of the PD-sets constructed in Theorem 5.3.1 is given in Appendix B.

As a final comment on this chapter, it is noted that if $n \equiv 1 (\text{mod } 4)$, then the code of $\overline{T(n)}$ equals the dual of the code of $T(n)$ as given in [17]. This is not true in any of the other three cases, and the following questions come to mind: Are there any other graphs for which the code obtained from a graph equals the dual of the code obtained from its complement? If so, what are the defining properties of such graphs?

Chapter 6

Binary Codes and partial Permutation Decoding sets from the Odd graphs

In the previous chapter the codes generated by the adjacency matrix from the complements of the Triangular graph have been studied. While the focus remains on the class of Uniform Subset graphs in this chapter, the subclass of graphs, and consequently the code and dual code from it, are somewhat more complex. Recall that the **Odd graph**, denoted by $O(k)$, is the Uniform Subset graph $G(2k+1, k, 0)$ i.e. the graph of which the vertex-set is the set of all k-subsets of $\Omega = \{1, 2, \ldots, 2k+1\}$, and any two vertices u and v constitute an edge $[u, v]$ if and only if $u \cap v = \emptyset$. In this chapter it is shown that the code generated by the adjacency matrix of $O(k)$ is a $[\binom{2k+1}{k}, \binom{2k}{k}, k+1]$ code, and its dual a $[\binom{2k+1}{k}, \binom{2k}{k-1}, k+2]$ code. Moreover, the incidence vectors are shown to constitute the minimum words, and hence the code has a basis consisting of minimum weight vectors. The dual is also shown to have a minimum weight basis. Although these basis elements identify a set of $\binom{2k}{k}$ information positions for C, these are found to be unsuitable for the purpose of permutation decoding, and hence an alternative basis is sought.

The code described above is also the code of the $1-(\binom{2k+1}{k}, k+1, k+1)$ design $\mathcal{D}$ of which the point set $\mathcal{P}$ is the vertex-set of $O(k)$ and the block set $\mathcal{B}$ the supports of the set of 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 by a direct argument in Theorem 6.2.11 that the automorphism group of the code is also S_{2k+1}.

The code from $O(k)$ can also be viewed in the light of the primitive action of the alternating group A_{2k+1} on the k-subsets of $\Omega = \{1, 2, \ldots, 2k+1\}$. Now by Theorem 6.2.10 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

$$\overline{\{a_1, a_2, \ldots, a_k\}} = \{\{x_1, x_2, \ldots, x_k\} \in \Omega^{\{k\}} : \ \{x_1, x_2, \ldots, x_k\} \cap \{a_1, a_2, \ldots, a_k\} = \emptyset\},$$

i.e. the orbit of length $\binom{k}{0}\binom{k+1}{k}$. Then the points and blocks defined above form a $1-(\binom{2k+1}{k}, k+1, k+1)$ design which has the same binary code as $O(k)$.

As in the previous chapter, the point of departure is a brief discussion of some of the properties of $O(k)$.

6.1 Some basic properties of Odd graphs

$O(k)$ is regular, having $\binom{2k+1}{k}$ vertices and valency $\binom{k}{0}\binom{k+1}{k}$. It is not strongly regular, however, since the number of vertices to which two non-adjacent vertices are commonly adjacent is not constant: if $|u \cap v| = k-1$, then u and v are commonly adjacent to one vertex, but if $|u \cap v| < k-1$, then u and v are not commonly adjacent to any vertices. Besides being the complement of the Triangular graph $T(5)$, the Petersen graph is also the first non-trivial Odd graph ($O(2)$).

As expected, $O(k)$ is also distance-transitive, and there is a direct relationship between the distance between two vertices u and v and the size of their intersection as k-subsets.

This relationship is made explicit in the following lemma:

Lemma 6.1.1. [2, Lemma 3.5.2] *Suppose that u and v are vertices of $O(k)$. Then for $m \geq 0$,*

$$d(u,v) = \begin{cases} 2m & \text{if } |u \cap v| = k - m \\ 2m+1 & \text{if } |u \cap v| = m. \end{cases} \tag{6.1}$$

Note that the distance formula in Lemma 6.1.1 requires that $k > 2m$ for all m. A consequence of this condition is that there is a bound for the distance between two vertices in $O(k) : d(u,v) < k$ if it $(d(u,v))$ is even, and $d(u,v) < k+1$ if it is odd. The distance-transitivity of $O(k)$ then hinges on Lemma 6.1.1 in conjunction with the following facts:

(a) the automorphism group of $O(k)$ is known to be S_{2k+1}

(b) for any vertices u, v, s and t of $O(k)$ such that $|u \cap v| = |s \cap t|$, there is an automorphism $\sigma \in S_{2k+1}$ such that $\sigma(u) = s$ and $\sigma(v) = t$.

Now that the preliminaries have been dealt with, the discussion proceeds with a detailed investigation into the essence of this chapter.

6.2 Binary Codes from the Odd graphs

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 the set $\Omega = \{1, 2, \ldots, 2k+1\}$. $\mathcal{P}$ 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, and which is defined as follows:

$$\overline{\{a_1, a_2, \ldots, a_k\}} = \{\{x_1, x_2, \ldots, x_k\} : \{x_1, x_2, \ldots, x_k\} \subseteq \Omega \setminus \{a_1, a_2, \ldots, a_k\}\}.$$

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

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

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

$$v^{\overline{\{a_1,a_2,\ldots,a_k\}}} = \sum_{\{x_1,x_2,\ldots,x_k\}\subseteq\Omega\setminus\{a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_k\}} \tag{6.2}$$

where the less precise use of notation is justified as in the previous chapter.

Throughout this chapter it is assumed that $k \geq 2$. As in the previous chapter, C denotes the binary code of $O(k)$ and $C^{\perp}$ its dual.

The first task at hand is the identification of a natural basis for C.

Lemma 6.2.1. *The set S consisting of the $\binom{2k}{k}$ vectors $\{v^{\overline{\{a_1,a_2,\ldots,a_k\}}} : \{a_1, a_2, \ldots, a_k\} \subseteq \Omega \setminus \{1\}\}$ forms a basis for C.*

Proof: By equation 6.2,

$$\begin{aligned} v^{\overline{\{a_1,a_2,\ldots,a_k\}}} &= \sum_{\{x_1,x_2,\ldots,x_k\}\subseteq\Omega\setminus\{a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_k\}} \\ &= \sum_{\{x'_1,x'_2,\ldots,x'_{k-1}\}\subseteq\Omega\setminus\{1,a_1,a_2,\ldots,a_k\}} v^{\{1,x'_1,x'_2,\ldots,x'_{k-1}\}} + v^{\Omega\setminus\{1,a_1,a_2,\ldots,a_k\}} \end{aligned} \tag{6.3}$$

Since for each k-subset $\{a_1, a_2, \ldots, a_k\} \in \Omega \setminus \{1\}$, its complement $\Omega \setminus \{a_1, a_2, \ldots, a_k\}$ in $\Omega \setminus \{1\}$, and hence the incidence vector $v^{\Omega\setminus\{1,a_1,a_2,\ldots,a_k\}}$, is uniquely determined, it follows that no non-trivial linear combination of vectors in S is zero.

To show that S spans C, it is sufficient to show that each vector of the form $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-1}\}}}$ is in the span of S. Suppose then that $v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}} \in S$ and consider the sum $\sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1}\}} v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}}$. By equation 6.3,

$$\begin{aligned} &\sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1}\}} v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}} \\ &= \sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1}\}} \sum_{\{x'_1,x'_2,\ldots,x'_{k-1}\}\subseteq\Omega\setminus(1,a_1,a_2,\ldots,a_{k-1},x\}} v^{\{1,x'_1,x'_2,\ldots,x'_{k-1}\}} \\ &\quad + \sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1}\}} v^{\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1},x\}} \end{aligned}$$

Now each of the $k(k+1)$ vectors $v^{\{1,x'_1,x'_2,\ldots,x'_{k-1}\}}$ appearing in the above sum is a component of the incidence vectors $v^{\overline{\{a_1,a_2,\ldots,a_{k-1},\overline{x}\}}}$ and $v^{\overline{\{a_1,a_2,\ldots,a_{k-1},\tilde{x}\}}}$, where $\{1,x'_1,x'_2,\ldots,x'_{k-1}\} = \Omega \setminus \{a_1,a_2,\ldots,a_{k-1},\overline{x},\tilde{x}\}$, and of no other vectors appearing in the sum

$$\sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1}\}} v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}}.$$ Moreover, $\binom{k+1}{2}$ pairs of vectors $v^{\overline{\{a_1,a_2,\ldots,a_{k-1},\overline{x}\}}}$ and

$v^{\overline{\{a_1,a_2,\ldots,a_{k-1},\tilde{x}\}}}$, $\overline{x} \neq \tilde{x}$ and $\overline{x},\tilde{x} \in \Omega \setminus \{1,a_1,a_2,\ldots,a_{k-1}\}$ occur. Hence

$$\begin{aligned}\sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1}\}} v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}} &= 0 + \sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1}\}} v^{\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1},x\}} \\ &= \sum_{\{x_1,x_2,\ldots,x_k\}\subseteq\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-1}\}} v^{\{x_1,x_2,\ldots,x_k\}} \\ &= v^{\overline{\{1,a_1,a_2,\ldots,a_{k-1}\}}}.\end{aligned}$$

Clearly, $|S| = |\{v^{\overline{\{a_1,a_2,\ldots,a_k\}}} : \{a_1,a_2,\ldots,a_k\} \subseteq \Omega \setminus \{1\}\}| = \binom{2k}{k}$. □

Given that a basis for C has been identified, the minimum weight of C is easily determined by considering the weights of words formed by linear combinations of basis elements.

Lemma 6.2.2. *The minimum weight of C is $k+1$.*

Proof: Since there are $\binom{k+1}{k}$ k-subsets disjoint to any given k-subset $\{x_1,x_2,\ldots,x_k\}$, the vector $v^{\overline{\{x_1,x_2,\ldots,x_k\}}}$ has weight $k+1$. In particular, each basis vector $v^{\overline{\{a_1,a_2,\ldots,a_k\}}}$, $\{a_1,a_2,\ldots,a_k\} \subseteq \Omega \setminus \{1\}$, has weight $k+1$. Also, as pointed out in the proof of Lemma 6.2.1, two vectors $v^{\overline{\{x_1,x_2,\ldots,x_k\}}}$ and $v^{\overline{\{x'_1,x'_2,\ldots,x'_k\}}}$ are incident at a common point if and only if $\{x_1,x_2,\ldots,x_k\}$ and $\{x'_1,x'_2,\ldots,x'_k\}$ have $k-1$ elements in common. Hence the minimum weight vectors will be obtained by taking linear combinations of the basis vectors $\{v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}} : x \in \Omega \setminus \{1,a_1,a_2,\ldots,a_{k-1}\}\}$. Suppose then, that a linear combination of r such vectors yields a weight of less than $k+1$. Then

$$r(k+1) - 2\binom{r}{2} < k+1, \tag{6.4}$$

$$\text{i.e. } r < 1 \quad \text{or} \quad r > k+1.$$

Clearly, both possibilities for r are absurd since r is a positive number and
$r \leq |\{v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}} : x \in \Omega \setminus \{1, a_1, a_2, \ldots, a_{k-1}\}\}| = k+1.$ □

Equality in the expression for the weight of a linear combination of r basis vectors implies that any minimum weight vector is either a basis vector, or a linear combination of $k+1$ vectors from the set $\{v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}} : x \in \Omega \setminus \{1, a_1, a_2, \ldots, a_{k-1}\}\}$. Now it has been shown in Lemma 6.2.1 that such a linear combination results in the incidence vector $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-1}\}}}$, and since all the other incidence vectors which are not part of the basis can be obtained in a similar way, the following result can be deduced:

Lemma 6.2.3. *C has a basis of minimum weight vectors. These, in addition to the $\binom{2k}{k-1}$ vectors $\{v^{\overline{\{1,a_1,a_2,\ldots,a_{k-1}\}}} : \{a_1, a_2, \ldots, a_{k-1}\} \subseteq \Omega \setminus \{1\}\}$, constitute the $\binom{2k+1}{k}$ minimum words in C.*

The following notation, similar to that used in the previous chapter, is introduced to facilitate the investigation of 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

$$v(\{y_1, y_2, \ldots, y_{k-1}\}) = \sum_{y \in \Omega \setminus \{y_1,y_2,\ldots,y_{k-1}\}} v^{\{y_1,y_2,\ldots,y_{k-1},y\}} \tag{6.5}$$

As was the case for C, the identification of a basis for $C^{\perp}$ takes priority.

Lemma 6.2.4. *The set R consisting of the $\binom{2k}{k-1}$ vectors $\{v(\{b_1, b_2, \ldots, b_{k-1}\}) :$
$\{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{1\}\}$ forms a basis for $C^{\perp}$.*

Proof: Suppose that $v^{\overline{\{a_1,a_2,\ldots,a_k\}}} \in S, v(\{b_1, b_2, \ldots, b_{k-1}\}) \in R$, and consider the inner product

$$(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v(\{b_1, b_2, \ldots, b_{k-1}\}))$$

$$= \left(\sum_{\{x_1,x_2,\ldots,x_k\} \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_k\}}, \sum_{y \in \Omega \setminus \{b_1,b_2,\ldots,b_{k-1}\}} v^{\{b_1,b_2,\ldots,b_{k-1},y\}}\right).$$

If $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_{k-1}\} \neq \emptyset$, then there are no points at which both vectors $\sum_{\{x_1,x_2,\ldots,x_k\} \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_k\}}$ and $\sum_{y \in \Omega \setminus \{b_1,b_2,\ldots,b_{k-1}\}} v^{\{b_1,b_2,\ldots,b_{k-1},y\}}$ are commonly incident since $\{b_1, b_2, \ldots, b_{k-1}\} \not\subset \{x_1, x_2, \ldots, x_k\}$ for any $\{x_1, x_2, \ldots, x_k\} \subseteq \Omega \setminus \{a_1, a_2, \ldots, a_k\}$. On the other hand, if $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_{k-1}\} = \emptyset$, then these two vectors are commonly incident at the points $\{b_1, b_2, \ldots, b_{k-1}, \overline{y}\}$ and $\{b_1, b_2, \ldots, b_{k-1}, \tilde{y}\}$ where $\{\overline{y}, \tilde{y}\} = \Omega \setminus \{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_{k-1}\}$, and at no other points. Hence, in each case,

$$(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v(\{b_1, b_2, \ldots, b_{k-1}\})) = 0.$$

By the linearity of the inner product, it follows that any linear combination of vectors in R is orthogonal to every vector in C i.e. span $R \subseteq C^{\perp}$. Now by equation 6.5,

$$\begin{aligned} v(\{b_1, b_2, \ldots, b_{k-1}\}) &= \sum_{y \in \Omega \setminus \{b_1,b_2,\ldots,b_{k-1}\}} v^{\{b_1,b_2,\ldots,b_{k-1},y\}} \\ &= v^{\{1,b_1,b_2,\ldots,b_{k-1}\}} + \sum_{y' \in \Omega \setminus \{1,b_1,b_2,\ldots,b_{k-1}\}} v^{\{b_1,b_2,\ldots,b_{k-1},y'\}}. \end{aligned}$$

Since for each $(k-1)$-subset $\{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{1\}$, the k-subset $\{1, b_1, b_2, \ldots, b_{k-1}\}$ and hence the vector $v^{\{1,b_1,b_2,\ldots,b_{k-1}\}}$ is uniquely determined, it follows that no non-trivial linear combination of vectors in R is zero. Finally, since $|R| = |\{v(\{b_1, b_2, \ldots, b_{k-1}\}) : \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{1\}\}| = \binom{2k}{k-1}$, and since $\dim(C^{\perp}) = \binom{2k+1}{k} - \binom{2k}{k}$, it follows that R is a basis for $C^{\perp}$. □

The interaction between the basis vectors, for example, the conditions under which two basis vectors are incident at a common point, the maximum number of points at which two basis vectors can be incident, the maximum number of basis vectors of a certain form that can be incident at a common point, will now be explored further, the objective being the determination of the minimum weight of $C^{\perp}$.

Lemma 6.2.5. *The minimum weight of $C^{\perp}$ is $k + 2$.*

Proof: Clearly, by equation 6.5 each basis vector $v(\{b_1, b_2, \ldots, b_{k-1}\})$ and indeed each $v(\{y_1, y_2, \ldots, y_{k-1}\}), \{y_1, y_2, \ldots, y_{k-1}\} \subseteq \Omega$ has weight $k + 2$. Now consider the vectors

$v(\{y_1, y_2, \ldots, y_{k-1}\})$ and $v(\{y'_1, y'_2, \ldots, y'_{k-1}\})$. If $\{y_1, y_2, \ldots, y_{k-1}\}$ and $\{y'_1, y'_2, \ldots, y'_{k-1}\}$ have fewer than $k-2$ elements in common, then $v(\{y_1, y_2, \ldots, y_{k-1}\})$ and $v(\{y'_1, y'_2, \ldots, y'_{k-1}\})$ will not be incident at a common point: the vectors $v(\{b_1, b_2, \ldots, b_{k-2}, \overline{y}\})$ and $v(\{b_1, b_2, \ldots, b_{k-2}, \tilde{y}\})$ are both incident at $\{b_1, b_2, \ldots, b_{k-2}, \overline{y}, \tilde{y}\}$, and at no other point. Hence the minimum weight vectors will be obtained by taking linear combinations of the basis vectors $\{v(\{b_1, b_2, \ldots, b_{k-2}, y\}) : y \in \Omega \setminus \{1, b_1, b_2, \ldots, b_{k-2}\}\}$. Suppose that a vector of weight less than $k+2$ can be obtained by taking a linear combination of r such vectors. Then

$$r(k+2) - 2\binom{r}{2} < k+2, \tag{6.6}$$

$$\text{i.e. } r < 1 \quad \text{or} \quad r > k+2.$$

The restriction on r, namely that $1 \leq r \leq k+2$, renders both these possibilities invalid.

□

The above argument, in conjunction with Lemma 6.2.4, shows that the minimum words are either the basis vectors or the sum of the vectors in sets such as $\{v(\{b_1, b_2, \ldots, b_{k-2}, y\}) : y \in \Omega \setminus \{1, b_1, b_2, \ldots, b_{k-2}\}\}$. Hence, the following result is implied:

Lemma 6.2.6. *$C^\perp$ has a basis of minimum weight vectors. These, in addition to the $\binom{2k}{k-2}$ vectors $\{v(\{1, b_1, b_2, \ldots, b_{k-2}\}) : \{b_1, b_2, \ldots, b_{k-2}\} \subseteq \Omega \setminus \{1\}\}$, constitute the $\binom{2k+1}{k-1}$ minimum words in $C^\perp$.*

Lemmas 6.2.1 to 6.2.5 can be summarized as follows:

Theorem 6.2.7. *The code of the $1-(\binom{2k+1}{k}, k+1, k+1)$ design and the Odd graph $O(k)$, where $k \geq 2$, is a $[\binom{2k+1}{k}, \binom{2k}{k}, k+1]$ code, and its dual a $[\binom{2k+1}{k}, \binom{2k}{k-1}, k+2]$ code.*

Now the $\boldsymbol{j}$-vector plays a role in determining the relationship between C and $C^\perp$, and this is the focus of the next lemma.

Lemma 6.2.8. *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: By equation 6.3,

$$\begin{aligned}
&\sum_{\{a_1,a_2,\ldots,a_k\}\subseteq\Omega\setminus\{1\}} v^{\overline{\{a_1,a_2,\ldots,a_k\}}} \\
&= \sum_{\{a_1,a_2,\ldots,a_k\}\subseteq\Omega\setminus\{1\}} \sum_{\{x'_1,x'_2,\ldots,x'_{k-1}\}\subseteq\Omega\setminus\{1,a_1,a_2,\ldots,a_k\}} v^{\{1,x'_1,x'_2,\ldots,x'_{k-1}\}} \\
&\quad + \sum_{\{a_1,a_2,\ldots,a_k\}\subseteq\Omega\setminus\{1\}} v^{\Omega\setminus\{1,a_1,a_2,\ldots,a_k\}} \\
&= \binom{k+1}{k} \sum_{\{x_1,x_2,\ldots,x_{k-1}\}\subseteq\Omega\setminus\{1\}} v^{\{1,x_1,x_2,\ldots,x_{k-1}\}} \\
&\quad + \sum_{\{a_1,a_2,\ldots,a_k\}\subseteq\Omega\setminus\{1\}} v^{\Omega\setminus\{1,a_1,a_2,\ldots,a_k\}}. \qquad (6.7)
\end{aligned}$$

Similarly, by equation 6.5,

$$\begin{aligned}
&\sum_{\{b_1,b_2,\ldots,b_{k-1}\}\subseteq\Omega\setminus\{1\}} v(\{b_1,b_2,\ldots,b_{k-1}\}) \\
&= \sum_{\{b_1,b_2,\ldots,b_{k-1}\}\subseteq\Omega\setminus\{1\}} \sum_{y\in\Omega\setminus\{b_1,b_2,\ldots,b_{k-1}\}} v^{\{b_1,b_2,\ldots,b_{k-1},y\}} \\
&= \sum_{\{b_1,b_2,\ldots,b_{k-1}\}\subseteq\Omega\setminus\{1\}} v^{\{1,b_1,b_2,\ldots,b_{k-1}\}} + \sum_{\{b_1,b_2,\ldots,b_{k-1}\}\subseteq\Omega\setminus\{1\}} \sum_{y'\in\Omega\setminus\{1,b_1,b_2,\ldots,b_{k-1}\}} v^{\{b_1,b_2,\ldots,b_{k-1},y'\}} \\
&= \sum_{\{b_1,b_2,\ldots,b_{k-1}\}\subseteq\Omega\setminus\{1\}} v^{\{1,b_1,b_2,\ldots,b_{k-1}\}} + \binom{k}{k-1} \sum_{\{y_1,y_2,\ldots,y_k\}\subseteq\Omega\setminus\{1\}} v^{\{y_1,y_2,\ldots,y_k\}}. \qquad (6.8)
\end{aligned}$$

Now if k is even, then $k+1$ is odd, and by equation 6.7, $\boldsymbol{j} \in C$ and $\boldsymbol{j} \notin C^{\perp}$. On the other hand, if k is odd, then by equation 6.8, $\boldsymbol{j} \in C^{\perp}$. Alternatively it can be argued that, if k is even, then since each basis vector $v(\{b_1, b_2, \ldots, b_{k-1}\})$, $\{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{1\}$, in $C^{\perp}$ has even weight, $\boldsymbol{j}$ is orthogonal to each, and by linearity of the inner product, to each vector in $C^{\perp}$. Hence $\boldsymbol{j} \in C$. A similar argument shows that if k is odd, then $\boldsymbol{j} \in C^{\perp}$ and $\boldsymbol{j} \notin C$.

In order to determine whether $C \subseteq C^{\perp}$, consider the inner product $(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v^{\overline{\{a'_1,a'_2,\ldots,a'_k\}}})$ of any two incidence vectors $v^{\overline{\{a_1,a_2,\ldots,a_k\}}}$ and $v^{\overline{\{a'_1,a'_2,\ldots,a'_k\}}}$ in C. Now if $\{a_1,a_2,\ldots,a_k\}$ and $\{a'_1,a'_2,\ldots,a'_k\}$ have $k-1$ elements in common, then $v^{\overline{\{a_1,a_2,\ldots,a_k\}}}$ and $v^{\overline{\{a'_1,a'_2,\ldots,a'_k\}}}$ are commonly incident only at one point, and hence $(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v^{\overline{\{a'_1,a'_2,\ldots,a'_k\}}}) = 1$, and $C \not\subseteq C^{\perp}$. Neither is $C^{\perp} \subseteq C$, since the inner product $(v(\{b_1,b_2,\ldots,b_{k-1}\}), v(\{b'_1,b'_2,\ldots,b'_{k-1}\})) = 1$ if $\{b_1,b_2,\ldots,b_{k-1}\}$ and $\{b'_1,b'_2,\ldots,b'_{k-1}\}$ have $k-2$ elements in common. Alternatively, it could be argued that $C \not\subseteq C^{\perp}$ since C has vectors of weight $k+1$ whereas $C^{\perp}$ does not. It is also clear that $\boldsymbol{j} \notin C \cap C^{\perp}$, since it would imply that $\boldsymbol{j}$ is orthogonal to vectors of odd weight.

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

$$\sum_{i=0}^{k-2} \sum_{\substack{A_i \subseteq \{a_1,a_2,\ldots,a_k\} \\ |A_i|=i}} \sum_{\substack{Y_i \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\} \\ |Y_i|=k-1-i}} v(A_i \cup Y_i) + \sum_{\{x_1,x_2,\ldots,x_k\} \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\}} v^{\overline{\{x_1,x_2,\ldots,x_k\}}} + k\boldsymbol{j}. \tag{6.9}$$

Now for each $0 \leq i \leq k-2$ the vector sum $\displaystyle\sum_{\substack{A_i \subseteq \{a_1,a_2,\ldots,a_k\} \\ |A_i|=i}} \sum_{\substack{Y_i \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\} \\ |Y_i|=k-1-i}} v(A_i \cup Y_i)$

is the sum of all the unit 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, $\displaystyle\sum_{\{x_1,x_2,\ldots,x_k\} \subseteq \Omega \setminus \{a_1,a_2,\ldots,a_k\}} v^{\overline{\{x_2,x_2,\ldots,x_k\}}}$ is the sum of unit 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 unit 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 6.9 reduces to

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

$$= (2k+1)v^{\{a_1,a_2,\ldots,a_k\}},$$

and since $2k+1$ is always odd and the choice of $\{a_1, a_2, \ldots, a_k\} \subseteq \Omega$ was arbitrary, the result follows. $\square$

Note that in general, if the minimum words in C, respectively $C^{\perp}$, have even weight, then all the codewords in C, respectively $C^{\perp}$, have even weight, whereas if the minimum words in C, respectively $C^{\perp}$, have odd weight, then C, respectively $C^{\perp}$, has words of both even and odd weight. Note also, that the expression in 6.9 can be simplified to $v^{\overline{\{a_1,a_2\}}} + v(\{a_1\}) + v(\{a_2\}) + \boldsymbol{j}$ when $k = 2$, and to

$$\sum_{\{x_1,x_2,x_3\} \subseteq \Omega \setminus \{a_1,a_2,a_3\}} v^{\overline{\{x_1,x_2,x_3\}}} + \sum_{\{y_1,y_2,\} \subseteq \Omega \setminus \{a_1,a_2,a_3\}} v(\{y_1,y_2\}) + \boldsymbol{j} \text{ when } k = 3.$$

As a slight diversion from the main thrust of the discussion, the claim in the introductory remarks that the primitive action of the simple alternating group $A_{2k+1}, k \geq 2$, provides an alternative perspective on C will now be fully justified.

The stabilizer of the k-subset $\{a_1, a_2, \ldots, a_k\}$ in the action of a group H on $\Omega^{\{k\}}$, the k-subsets of Ω, 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 the factor group $H_{\{a_1,a_2,\ldots,a_k\}}/H_{(a_1,a_2,\ldots,a_k)}$ is isomorphic to a subgroup of S_k.

Now H is said to act k-transitively on Ω if and only if for any k-tuples $(a_1, a_2, \ldots, a_k)$ and $(a'_1, a'_2, \ldots, a'_k)$ each having distinct entries in Ω, there exists $\alpha \in H$ such that $\alpha(a_i) = a'_i$, for all $1 \leq i \leq k$. A concept which is weaker than k-transitivity is that of k-homogeneity. H is termed k-homogeneous if and only if it is transitive on $\Omega^{\{k\}}$. The following lemma establishes that the alternating group A_{2k+1}, where $k \geq 2$, is k-homogeneous.

Lemma 6.2.9. *The alternating group $A_{2k+1}, k \geq 2$, acts transitively on $\Omega^{\{k\}}$.*

Proof: Suppose that $\{a_1, a_2, \ldots, a_k\}, \{a'_1, a'_2, \ldots, a'_k\} \in \Omega^{\{k\}}$. If, on the one hand, $\{a_1, a_2, \ldots, a_k\}$ and $\{a'_1, a'_2, \ldots, a'_k\}$ are disjoint, then the permutations $(a_1, a'_1)(a_2, a'_2) \ldots (a_k, a'_k)$ or $(a_1, a'_1)(a_2, a'_2) \ldots (a_k, a'_k)(a_i, a_j)$ map them accordingly, and either is in A_{2k+1}, depending on whether k is even or odd. If, on the other hand, $\{a_1, a_2, \ldots, a_k\}$ and $\{a'_1, a'_2, \ldots, a'_k\}$ have r elements in common, let $\{a_{i_1}, a_{i_2}, \ldots, a_{i_{k-r}}\}$ and $\{a'_{j_1}, a'_{j_2}, \ldots, a'_{j_{k-r}}\}$ denote the relative complements of the intersection in $\{a_1, a_2, \ldots, a_k\}$ and $\{a'_1, a'_2, \ldots, a'_k\}$ respectively. Then the permutations $(a_{i_1}, a'_{j_1})(a_{i_2}, a'_{j_2}) \ldots (a_{i_{k-r}}, a'_{i_{k-r}})$ or $(a_{i_1}, a'_{j_1})(a_{i_2}, a'_{j_2}) \ldots (a_{i_{k-r}}, a'_{i_{k-r}})(x, y)$, where $x, y \in \Omega \setminus (\{a_1, a_2, \ldots, a_k\} \cup \{a'_1, a'_2, \ldots, a'_k\})$, are appropriate, and as before, either is even, depending on whether $k - r$ is even or odd. $\square$

The structure of the stabilizer of a k-subset $\{a_1, a_2, \ldots, a_k\}$ in A_{2k+1} will now be examined, and it will be shown that $(A_{2k+1})_{\{a_1, a_2, \ldots, a_k\}} \cong S_k \times A_{k+1}$. Since the action of any odd permutation in S_{2k+1} on a k-subset can be mimicked by a permutation in A_{2k+1}, the orbits of $(S_{2k+1})_{\{a_1, a_2, \ldots, a_k\}}$ and $(A_{2k+1})_{\{a_1, a_2, \ldots, a_k\}}$ are identical, and hence it is sufficient to consider the stabilizer in A_{2k+1}, rather than in the larger group. In order to continue the discussion, the following are worthwhile recalling: A block of $\Omega^{\{k\}}$ on which a group H acts transitively is a subset B of $\Omega^{\{k\}}$ such that, for each $\alpha \in H$, either $\alpha B = B$ or $\alpha B \cap B = \emptyset$. $B = \emptyset, B = \Omega^{\{k\}}$, and every one-element subset of $\Omega^{\{k\}}$ are called trivial blocks, and any other block is called non-trivial. $\Omega^{\{k\}}$ is primitive if and only if it contains no non-trivial blocks. The rank of $\Omega^{\{k\}}$ is the number of orbits of $H_{\{a_1, a_2, \ldots, a_k\}}$, for any $\{a_1, a_2, \ldots, a_k\} \in \Omega^{\{k\}}$.

Theorem 6.2.10. *The alternating group $A_{2k+1}, k \geq 2$, acts primitively as a rank $k + 1$ permutation group on $\Omega^{\{k\}}$.*

Proof: By Lemma 6.2.9, $A_{2k+1}, k \geq 2$ acts transitively on the $\binom{2k+1}{k}$ k-subsets of Ω. Hence, by the Orbit-Stabilizer theorem, it follows that

$$|(A_{2k+1})_{\{a_1, a_2, \ldots, a_k\}}| = \frac{\frac{(2k+1)!}{2}}{\binom{2k+1}{k}} = \frac{(2k+1)!}{2} \times \frac{k!(k+1)!}{(2k+1)!} = \frac{k!(k+1)!}{2}. \tag{6.10}$$

Observe that

$$\begin{aligned}(S_{2k+1})_{\{a_1,a_2,\ldots,a_k\}} &= \{\sigma\tau :\ \sigma \in S_{\{a_1,a_2,\ldots,a_l\}},\ \tau \in S_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}}\} \\ &\cong S_{\{a_1,a_2,\ldots,a_k\}} \times S_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}},\end{aligned}$$

and hence

$$(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}} \leq S_{\{a_1,a_2,\ldots,a_k\}} \times S_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}}.$$

Now suppose that

$$K = \{\alpha\beta : \alpha \in A_{\{a_1,a_2,\ldots,a_k\}}, \beta \in A_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}}\},$$

and

$$L = \{\gamma\delta : \gamma \in S_{\{a_1,a_2,\ldots,a_k\}} \setminus A_{\{a_1,a_2,\ldots,a_k\}},\ \delta \in S_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}} \setminus A_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}}\}.$$

Then $K \cup L \leq (A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}}$, and moreover,

$$|K \cup L| = |K| + |L| = 2|K| = 2\left(\frac{k!}{2} \cdot \frac{(k+1)!}{2}\right) = \frac{k!(k+1)!}{2} = |(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}}|$$

by 6.10. Hence $(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}} = K \cup L$, and it remains to be shown that $K \cup L \cong S_k \times A_{k+1}$. In this regard, define a function $f :\ K \cup L \to S_{\{a_1,a_2,\ldots,a_k\}} \times A_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}}$ by

$$f(\phi\lambda) = \begin{cases} (\phi, \lambda) & \text{if} \quad \phi\lambda \in K \\ (\phi, \overline{\lambda}) & \text{if} \quad \phi\lambda \in L, \quad \text{where} \quad \overline{\lambda} = \lambda(a_i, a_j) \quad \text{and} \quad 1 \leq i < j \leq k. \end{cases}$$

Clearly, f is one-one and onto. In order to show that f is a homomorphism, four cases have to be considered.

Case (i):

Suppose that $x, y \in K$. Then $x = \alpha\beta, y = \alpha'\beta'$, where $\alpha, \alpha' \in A_{\{a_1,a_2,\ldots,a_k\}}$ and $\beta, \beta' \in A_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}}$. Hence

$$f(xy) = f(\alpha\beta\alpha'\beta') = f(\alpha\alpha'\beta\beta') = (\alpha\alpha', \beta\beta') = (\alpha, \beta)(\alpha', \beta') = f(x)f(y).$$

Case (ii):

In this case, $x, y \in L$ and proceeds in a similar way to Case (i).

Case (iii):

Suppose that $x \in K,\ y \in L$. Then $x = \alpha\beta$, where $\alpha \in A_{\{a_1,a_2,\ldots,a_k\}}, \beta \in A_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}}$, and $y = \gamma\delta$, where $\gamma \in S_{\{a_1,a_2,\ldots,a_k\}} \setminus A_{\{a_1,a_2,\ldots,a_k\}}, \delta \in S_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}} \setminus A_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}}$, and hence

$$f(xy) = f(\alpha\beta\gamma\delta) = f(\alpha\gamma\beta\delta) = (\alpha\gamma, \overline{\beta\delta}) = (\alpha\gamma, \beta\overline{\delta}) = (\alpha, \beta)(\gamma, \overline{\delta}) = f(x)f(y).$$

Case (iv):

The final case in which $x \in L, y \in K$ is similar to Case (iii), bearing in mind that the transposition (a_i, a_j) where $1 \leq i < j \leq k$, is disjoint to any permutation in $S_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}}$, and thus commutes with it.

Hence

$$\begin{aligned}(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}} &= K \cup L \\ &\cong S_{\{a_1,a_2,\ldots,a_k\}} \times A_{\Omega\setminus\{a_1,a_2,\ldots,a_k\}} \\ &\cong S_k \times A_{k+1}.\end{aligned}$$

The stabilizer $(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}}$ has $k+1$ orbits, namely $\{A_i \cup B_i : A_i \subseteq \{a_1, a_2, \ldots, a_k\}$, $B_i \subseteq \Omega \setminus \{a_1, a_2, \ldots, a_k\}$, $|A_i| = i$, $|B_i| = k - i\}$, $0 \leq i \leq k-1$, and $\{\{a_1, a_2, \ldots, a_k\}\}$, having lengths $\binom{k}{i}\binom{k+1}{k-i}, 0 \leq i \leq k$, respectively. Now if any non-trivial block with respect to the action of A_{2k+1} on $\Omega^{\{k\}}$ contains the points $\{a_1, a_2, \ldots, a_k\}$ and $\{a'_1, a'_2, \ldots, a'_k\}$, then the orbit of $(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}}$ containing $\{a'_1, a'_2, \ldots, a'_k\}$ must also be contained in it, since $(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}} \leq A_{2k+1}$. In fact, such a block must contain every other orbit of $(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}}$, and hence A_{2k+1} acts primitively on $\Omega^{\{k\}}$. Finally, since $(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}}$ is the stabilizer of a point in the action of A_{2k+1} on $\Omega^{\{k\}}$, it follows that $(A_{2k+1})_{\{a_1,a_2,\ldots,a_k\}}$ is maximal. □

In general, the automorphism group of a structure provides deep insights into the constitution of that structure, and in the case of a graph, its automorphism group sheds light on its symmetries. Like $T(n), O(k)$ is a highly symmetrical graph. By resorting to the maximal independent subsets of $O(k)$ as the automorphism invariant, it is shown in [37,

Proposition 3.1.9] that the automorphism group of $O(k)$ is S_{2k+1}. Hence S_{2k+1} will be contained in $\mathrm{Aut}(C)$. In the following theorem it is shown that $\mathrm{Aut}(C)$ is indeed S_{2k+1}.

Theorem 6.2.11. *The automorphism group of the code generated by the adjacency matrix of the Odd graph $O(k), k \geq 2$, is S_{2k+1}.*

Proof: Suppose that $\sigma \in \mathrm{Aut}(C)$. Then certainly, σ permutes the k-subsets of Ω. To define an action of σ on Ω, the minimum words of $C^{\perp}$ are considered. By Lemma 6.2.6. the vectors

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

where $\{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega$, constitute the minimum words of $C^{\perp}$. Since σ preserves weight classes, σ induces a permutation of the $(k-1)$-subsets of Ω. Suppose then that

$$\sigma(v(\{b_1, b_2, \ldots, b_{k-1}\})) = v(\{b'_1, b'_2, \ldots, b'_{k-1}\}).$$

Then $\sigma(\{b_1, b_2, \ldots, b_{k-1}\}) = \{b'_1, b'_2, \ldots, b'_{k-1}\}$, and since σ preserves incidence of points of $\mathcal{D}$ on words of $C^{\perp}$, $\sigma(\{b_1, b_2, \ldots, b_{k-1}, y\})$, $y \in \Omega \backslash \{b_1, b_2, \ldots, b_{k-1}\}$, contains $\{b'_1, b'_2, \ldots, b'_{k-1}\}$, as well as an additional element, say y^*, i.e. $\sigma(\{b_1, b_2, \ldots, b_{k-1}, y\}) = \{b'_1 b'_2, \ldots, b'_{k-1}, y^*\}$. Now since $\sigma(\{b_1, b_2, \ldots, b_{k-1}\}) = \{b'_1, b'_2, \ldots, b'_{k-1}\}$, each of the $(k-1)$-subsets $\{b_{i_1}, b_{i_2}, \ldots, b_{i_{k-2}}, y\}$ has $k-1$ possible images under σ. Without loss of generality it can be assumed that for each such subset, $\sigma(\{b_{i_1}, b_{i_2}, \ldots, b_{i_{k-2}}, y\}) = \{b'_{i_1}, b'_{i_2}, \ldots, b'_{i_{k-2}}, y^*\}$. Consider $c_1, c_2, \ldots, c_{k-1} \in \Omega \backslash \{b_1, b_2, \ldots, b_{k-1}, y\}$. For each $1 \leq r \leq k-1$, $\sigma(\{b_{i_1}, b_{i_2}, \ldots, b_{i_{k-2}}, c_r, y\})$ $= \{b'_{i_1}, b'_{i_2}, \ldots, b'_{i_{k-2}}, c^*_r, y^*\}$ where $c^*_r \in \Omega \backslash \{b'_{i_1}, b'_{i_2}, \ldots, b'_{i_{k-2}}, y^*\}$. Since $\sigma(\{b_1, b_2, \ldots, b_{k-1}, y\})$ $= \{b'_1, b'_2, \ldots, b'_{k-1}, y^*\}$, each of the $(k-1)$-subsets $\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, c_r, y\}$ has $k-1$ possible images under the action of σ. Suppose that for some $j_1, j_2, \ldots, j_{k-3}$, $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, c_r,$ $y\}) \neq \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, c^*_r, y^*\}$. There are three cases resulting from this assumption that need to be examined.

Case (i):

Suppose that $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, c_r, y\}) = \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{q-1}}, b'_{j_{q+1}}, \ldots, b'_{j_{k-3}}, d_1, c^*_r, y^*\}$, where $d_1 \in \Omega \setminus \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{q-1}}, b'_{j_{q+1}}, \ldots, b'_{j_{k-3}}, c^*_r, y^*\}$ and $d_1 \neq b'_{j_q}$. Choose $b_m \in$

$\{b_1, b_2, \ldots, b_{k-1}\} \backslash \{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}\}$. Then $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, b_m, c_r, y\}$ contains $\{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, b'_m, d_1, c^*_r, y^*\}$, which contradicts the fact that σ permutes the k-subsets of Ω.

Case (ii):

Suppose that $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, c_r, y\}) = \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, d_2, y^*\}$, where $d_2 \in \Omega \setminus \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, y^*\}$ and $d_2 \neq c^*_r$. Choosing b_m as in the previous case implies that $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, b_m, c_r, y\}$ contains $\{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, b'_m, d_2, c^*_r, y^*\}$, which, as before, results in a contradiction.

Case (iii):

The same argument can be applied if $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, c_r, y\}) = \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, c^*_r, d_3\}$, where $d_3 \in \Omega \setminus \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, c^*_r\}$ and $d_3 \neq y^*$.

Hence $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, c_r, y\}) = \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, c^*_r, y^*\}$ for each $(k-3)$-subset $\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}\}$ of $\{b_1, b_2, \ldots, b_{k-1}\}$. This, in conjunction with the assumptions that $\sigma(\{b_{i_1}, b_{i_2}, \ldots, b_{i_{k-2}}, c_r, y\}) = \{b'_{i_1}, b'_{i_2}, \ldots, b'_{i_{k-2}}, c^*_r, y^*\}$ and $\sigma(\{b_{i_1}, b_{i_2}, \ldots, b_{i_{k-2}}, y\}) = \{b'_{i_1}, b'_{i_2}, \ldots, b'_{i_{k-2}}, y^*\}$, implies that $\sigma(\{b_{i_1}, b_{i_2}, \ldots, b_{i_{k-2}}, c_r\}) = \{b'_{i_1}, b'_{i_2}, \ldots, b'_{i_{k-2}}, c^*_r\}$ for each $(k-2)$-subset $\{b_{i_1}, b_{i_2}, \ldots, b_{i_{k-2}}\}$ of $\{b_1, b_2, \ldots, b_{k-1}\}$ and each $1 \leq r \leq k-1$. Then $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, c_1, c_2, y\}) = \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, c^*_1, c^*_2, y^*\}$, and each of the $(k-1)$-subsets $\{b_{l_1}, b_{l_2}, \ldots, b_{l_{k-4}}, c_1, c_2, y\}$ has $k-2$ possible images under σ. Suppose that for some $l_1, l_2, \ldots, l_{k-4}$, $\sigma(\{b_{l_1}, b_{l_2}, \ldots, b_{l_{k-4}}, c_1, c_2, y\}) \neq \{b'_{l_1}, b'_{l_2}, \ldots, b'_{l_{k-4}}, c^*_1, c^*_2, y^*\}$. Each of the resulting cases leads to the contradiction of the fact that σ permutes the k-subsets of Ω. Hence $\sigma(\{b_{l_1}, b_{l_2}, \ldots, b_{l_{k-4}}, c_1, c_2, y\}) = \{b'_{l_1}, b'_{l_2}, \ldots, b'_{l_{k-4}}, c^*_1, c^*_2, y^*\}$, and since for any $(k-3)$-subset $\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}\}$ of $\{b_1, b_2, \ldots, b_{k-1}\}$, and for any $1 \leq r \leq k-1$ $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, c_r, y\}) = \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, c^*_r, y^*\}$, it follows that $\sigma(\{b_{j_1}, b_{j_2}, \ldots, b_{j_{k-3}}, c_1, c_2\}) = \{b'_{j_1}, b'_{j_2}, \ldots, b'_{j_{k-3}}, c^*_1, c^*_2\}$. The argument can be continued in this way so that eventually $\sigma(\{b_{i_1}, c_1, c_2, \ldots, c_{k-2}\}) = \{b^*_{i_1}, c^*_1, c^*_2, \ldots, c^*_{k-2}\}$ and $\sigma(\{c_1, c_2, \ldots, c_{k-2}, y\}) = \{c^*_1, c^*_2, \ldots, c^*_{k-2}, y^*\}$. Then $\sigma(\{c_1, c_2, \ldots, c_{k-1}, y\}) = \{c^*_1, c^*_2, \ldots, c^*_{k-1}, y^*\}$. Finally, it can be deduced that $\sigma(\{c_1, c_2, \ldots, c_{k-1}\}) = \{c^*_1, c^*_2, \ldots, c^*_{k-1}\}$. Hence σ is defined in S_{2k+1}, and $\mathrm{Aut}(C) = S_{2k+1}$.

Alternatively, it can be argued as follows: Suppose that $\sigma \in \mathrm{Aut}(C)$. Then, as elaborated above, σ permutes both the k-subsets as well as the $(k-1)$-subsets of Ω. Moreover, since the vector $v^{\overline{\{a_1,a_2,\ldots,a_k\}}}$ is incident at the $k+1$ neighbours of $\{a_1, a_2, \ldots, a_k\}$, σ induces a map between the k-subsets of any two $(k+1)$-sets. In other words, σ maps the neighbours of $\{a_1, a_2, \ldots, a_k\}$ to the neighbours of some $\{w_1, w_2, \ldots, w_k\}$. Now suppose that $\sigma(\{a_1, a_2, \ldots, a_k\}) \neq \{w_1, w_2, \ldots, w_k\}$. Then there is a $v \in \sigma(\{a_1, a_2, \ldots, a_k\})$ such that v is an element of exactly k neighbours of $\{w_1, w_2, \ldots, w_k\}$. Let $N_v(\{w_1, w_2, \ldots, w_k\})$ denote these neighbours. Then $|\sigma(\{a_1, a_2, \ldots, a_k\}) \setminus \cap N_v(\{w_1, w_2, \ldots, w_k\})| = k-1$, but $|\sigma^{-1}(\sigma(\{a_1, a_2, \ldots, a_k\}) \setminus \cap N_v(\{w_1, w_2, \ldots, w_k\}))| = |\{a_1, a_2, \ldots, a_k\} \setminus \cap \sigma^{-1} N_v(\{w_1, w_2, \ldots, w_k\})| = k$, contradicting the fact that σ^{-1} also permutes the $(k-1)$-subsets of Ω. Hence $\sigma \in \mathrm{Aut}(O(k))$, and since it is known that $\mathrm{Aut}(O(k)) = S_{2k+1}$, $\mathrm{Aut}(C) = S_{2k+1}$. □

6.3 Permutation Decoding sets for C

The automorphism group of a code provides potential elements of a permutation decoding set which is such that any number of errors $e \leq t$, where t is the error-correcting capability of the code, can be corrected by such a set. In Lemma 6.2.1 the set $S = \{v^{\overline{\{a_1,a_2,\ldots,a_k\}}} : \{a_1, a_2, \ldots, a_k\} \subseteq \Omega \setminus \{1\}\}$ has been identified as a natural basis for C. However, for the purpose of error-correction, the information set yielded by S, namely $\{\{a_1, a_2, \ldots, a_k\} : \{a_1, a_2, \ldots, a_k\} \subseteq \Omega \setminus \{1\}\}$ proves to be inadequate since if errors occur at two information symbols of which the k-subsets are disjoint, then there is no automorphism of C which will map the errors into check positions. Thus, from a utility point of view, the identification of a new basis which circumvents this problem becomes imperative.

Lemma 6.3.1. *The set* $S^* = \{v^{\overline{\{a_1^*, a_2^* \ldots a_{k-2}^*, m, n\}}} : a_1^* < a_2^*, < \cdots < a_{k-2}^* < m < n \in \Omega,\ n \neq m+1\}$ *forms a basis for* C.

Proof: From the outset, observe that

$$\begin{aligned}
|S^*| &= |\{v^{\overline{\{a_1^*,a_2^*,\ldots,a_{k-2}^*,m,n\}}} : a_1^* < a_2^* < \cdots < a_{k-2}^* < m < n \in \Omega, n \neq m+1\}| \\
&= |\{v^{\overline{\{a_1,a_2,\ldots,a_k\}}} : \{a_1,a_2,\ldots,a_k\} \in \Omega^{\{k\}}\} \setminus \{v^{\overline{\{a_1',a_2',\ldots,a_{k-2}',m,m+1\}}} : \\
&\quad a_1' < a_2' < \cdots < a_{k-2}' < m \in \Omega\}| \\
&= \tbinom{2k+1}{k} - \tbinom{2k}{k-1} \\
&= \tbinom{2k}{k},
\end{aligned}$$

which concurs with the dimension of C. To show linear independence, it will be argued that the linear independence of the vectors in $S = \{v^{\overline{\{a_1,a_2,\ldots,a_k\}}} : \{a_1,a_2,\ldots,a_k\} \subseteq \Omega\backslash\{1\}\}$ imposes linear independence on the vectors in S^*. To this end, recall firstly that in Lemma 6.2.1 it is shown that every vector of the form $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-1}\}}}, \{a_1,a_2,\ldots,a_{k-1}\} \subseteq \Omega \setminus \{1\}$, can be written as a linear combination of vectors in S as follows:

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

Now suppose that

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

Each of the vectors in the sum above is either an element of S or a linear combination of elements in S. Hence the sum above reduces to a linear combination of elements of S. It remains to be shown that given the fact that the resulting coefficients of the elements of S are zero, each of the coefficients $\alpha_{\{a_1^*,a_2^*,\ldots,a_{k-2}^*,m,n\}}, a_1^* < a_2^* < \cdots < a_{k-2}^* < m < n, n \neq m+1$, in the sum above is zero. In this regard, the elements of S in the resulting sum are categorized as follows:

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

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

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

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

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 of those in S^*, occurs only in the linear combination for $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-3},m,m+2\}}}$. By the linear independence of the vectors in S, 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 $\alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,m+2\}}$, $1 < a_1 < a_2, < \cdots < a_{k-3} < m \in \Omega \setminus \{1\}$, 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, as was the case for $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,m+1,m+2\}}}$, is not in S^*. Nevertheless, $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,n,n+1\}}}$ 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 $\alpha_{\{1,a_1,a_2,\ldots,a_{k-3},m,p\}}$, $m < p, p \neq m+1$, 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 $k-1 \leq m \leq 2k-1, n \neq m+1$.

Thirdly, observe that the vector $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,m+1,n\}}}$ is in S^*, as well as in the linear combinations of the $k-2$ vectors in S^* of the form $v^{\overline{\{1,x_1,x_2,\ldots,x_{k-3},m+1,n\}}}$, $\{x_1,x_2,\ldots,x_{k-3}\} \subseteq \{a_1,a_2,\ldots,a_{k-3},m\}$, 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 $k-1 \leq m \leq 2k-1$. Finally, the vector $v^{\overline{\{a_1,a_2,\ldots,a_{k-3},m,n,q\}}} \in S_4$ is certainly in S^* as well as in the linear combinations for the k vectors in S^* of the form $v^{\overline{\{1,a_1,a_2,\ldots,a_{k-3},x,y\}}}$, $\{a_1,a_2,\ldots,a_{k-3},x,y\} \subseteq$

$\{a_1, a_2, \ldots, a_{k-3}, m, n, q\}$. 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 linear independence of the vectors in S implies that $\alpha_{\{a_1,a_2,\ldots,a_{k-3},m,n,q\}}$ is zero for all $k-2 \leq m \leq 2k-3, n \neq m+1, q \neq n+1$. Since all the vectors in S^* have been exhausted, it follows that S^* is linearly independent and is hence a basis for C. □

The identification of a basis for C, implies the identification of an information set for C, and hence the points $\{\{a_1, a_2, \ldots, a_{k-2}, m, n\} : a_1 < a_2 < \cdots < a_{k-2} < m < n,\ n \neq m+1\}$ are information positions for C. Given these information positions and the fact that C is able to correct $t = \lfloor \frac{k}{2} \rfloor$ errors, the whole automorphism group, S_{2k+1}, is a PD-set for C. The following theorem gives a 2-PD-set for C which is considerably smaller than S_{2k+1}, although the number of errors it is able to correct is limited.

Theorem 6.3.2. *Let $\mathcal{I}$ denote the points*

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

$P_{k+2} = \{1, 2, \ldots, k-2, k, k+2\}, \ldots,\ P_{2k+1} = \{1, 2, \ldots, k-2, k, 2k+1\}, \ldots,$

$P_{\binom{k+2}{2}} = \{1, 2, \ldots, k-2, 2k-1, 2k+1\},\ P_{\binom{k+2}{2}+1} = \{1, 2, \ldots, k-3, k-1, k, k+2\}, \ldots,$

$P_{\binom{k+3}{3}} = \{1, k+2, k+3, \ldots, 2k-1, 2k+1\}, \ldots,\ P_{\binom{2k}{k}} = \{k+1, k+2, \ldots, 2k-1, 2k+1\},$

where $k \geq 4$. Then

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

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

Case (i): $\mathcal{E} \subseteq \mathcal{P} \setminus \mathcal{I}$

The identity, $1_{S_{2k+1}} \in \mathcal{S}$, and will leave $\mathcal{E}$ fixed.

Case (ii): $\{e_1, e_2, \ldots, e_k\} \in \mathcal{P} \setminus \mathcal{I},\ \{e'_1, e'_2, \ldots, e'_k\} \in \mathcal{I}$.

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 (ii)(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 (ii)(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 (ii)(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 (iii)(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 (iii)(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 (iii)(f).

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

From the theorem above it is evident that, despite the fact that the 2-PD-set $\mathcal{S}$ does not exploit the full error-correcting capacity of C, the cases that need to be considered are many and varied. It may be entirely possible to find a smaller 2-PD-set by interchanging a check and an information position in the information set identified by the natural basis given in Lemma 6.2.1. However, the objective is the determination of a full PD-set for C, and to this end, the following is conjectured:

Conjecture 6.3.3. *Let $\mathcal{I}$ be the information positions as given in Theorem 6.3.2. Then for $k \ge 2$,*

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

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

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

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

($\lfloor \frac{k}{2} \rfloor - 1$ ceilings are determined in the expression above.)

It is easily observed that this bound is of the order of $2^{\lfloor \frac{k}{2} \rfloor + 1}$. In Appendix B the size of this bound is compared to the size of the 2-PD-set given in Theorem 6.3.2, and the order

of S_{2k+1}, which as stated previously, is a PD-set for C with the information positions as given in Theorem 6.3.2.

Recall that in the final comments in Chapter 5 the fact that the dual code obtained from the Triangular graph $T(n)$ is the code obtained from the complement of this graph when $n \equiv 1(\text{mod}4)$ was alluded to, and the possibility of finding other graphs for which the same is true was toyed with. Similar ideas are investigated below in the context of the Odd graphs.

6.4 The relationship between the dual code of $O(k)$ and the code of its complement $\overline{O(k)}$

The complement of the Odd graph, $\overline{O(k)}$, has as its vertex set $\mathcal{P}_c$, the set of k-subsets of $\Omega = \{1, 2, \ldots, 2k+1\}$, and two vertices u and v constitute an edge $[u, v]$ if and only if $u \cap v \neq \emptyset$. The code generated by the adjacency matrix of $\overline{O(k)}$ is also the code obtained from the $1-(\binom{2k+1}{k}, \binom{2k+1}{k}-k-2,\ \binom{2k+1}{k}-k-2)$ 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:

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

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

$$v_c^{\overline{\{a_1,a_2,\ldots,a_k\}}} = \sum_{\substack{\{x_1,x_2,\ldots,x_k\}\cap\{a_1,a_2,\ldots,a_k\}\neq\emptyset \\ \{x_1,x_2,\ldots,x_k\}\neq\{a_1,a_2,\ldots,a_k\}}} v^{\{x_1,x_2,\ldots,x_k\}} \tag{6.11}$$

Observe that

$$v_c^{\overline{\{a_1,a_2,\ldots,a_k\}}} = v^{\overline{\{a_1,a_2,\ldots,a_k\}}} + v^{\{a_1,a_2,\ldots,a_k\}} + \boldsymbol{j}. \tag{6.12}$$

where $v^{\overline{\{a_1,a_2,\ldots,a_k\}}}$ is as given in equation 6.2 and used throughout this chapter.

Let C and $C^\perp$ be as used throughout this chapter, and let $\overline{C}$ denote the code obtained from $\overline{O(k)}$.

In Lemma 6.2.4 the $\boldsymbol{j}$-vector provided insights into the relationship between C and $C^\perp$. The following lemma underlines the importance of the $\boldsymbol{j}$-vector in determining the relationship between $C^\perp$ and $\overline{C}$ as well.

Lemma 6.4.1. *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 the set $U = \{v(\{b_1, b_2, \ldots, b_{k-1}\}) + v(\{k+3, k+4, \ldots, 2k+1\} : \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{1\}, \{b_1, b_2, \ldots, b_{k-1}\} \neq \{k+3, k+4, \ldots, 2k+1\}\}$ is a basis for $C^\perp \cap \overline{C}$, and $dim(C^\perp \cap \overline{C}) = \binom{2k}{k-1} - 1$.*

Proof: In order to show that $C^\perp \subseteq \overline{C}$, it is sufficient to show that for each $\{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega$, $v(\{b_1, b_2, \ldots, b_{k-1}\}) \in \overline{C}$, since by Lemma 6.2.4, $\{v(\{b_1, b_2, \ldots, b_{k-1}\}) : \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{1\}\}$ is a basis for $C^\perp$. So consider the following sum in $\overline{C}$:

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

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 it can be shown by induction that $\binom{2k+1}{k}$ 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 once again, $v(\{b_1, b_2, \ldots, b_{k-1}\}) \in \overline{C}$. However, if k is odd and $k = 2^m - 1$, then it can be shown by induction that $\binom{2k+1}{k}$ is odd, and by a similar argument as above,

it follows that $\boldsymbol{j} \in \overline{C}^{\perp}$, and since its weight is odd, $\boldsymbol{j} \notin \overline{C}$. Of course, since k is odd, $\boldsymbol{j} \in C^{\perp}$ by Lemma 6.2.8. 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, $U = \{v(\{b_1, b_2, \ldots, b_{k-1}\}) + v(\{k+3, k+4, \ldots, 2k+1\} : \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{1\}, \{b_1, b_2, \ldots, b_{k-1}\} \neq \{k+3, k+4, \ldots, 2k+1\}\} \subseteq C^{\perp} \cap \overline{C}$, and its linear independence is a direct consequence of the linear independence of $\{v(\{b_1, b_2, \ldots, b_{k-1}\}) : \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{1\}\}$. Hence $\binom{2k}{k-1} = \dim(C^{\perp}) \geq \dim(C^{\perp} \cap \overline{C}) \geq \binom{2k}{k-1} - 1$. Now since $\boldsymbol{j} \in C^{\perp}$, and since no linear combination of vectors in U equals $\boldsymbol{j}$, it follows that $\dim(C^{\perp} \cap \overline{C}) = \binom{2k}{k-1} - 1$, and U is a basis for $C^{\perp} \cap \overline{C}$. □

From the above, it is evident that the Odd graphs provide a rich source of graphs for which the dual code from the graph is a subcode of the code from the graph of the complement. Again the questions that were raised in the context of the Triangular graphs, for which the dual code equals the code from the graph of the complement in certain instances, come to the fore: Are there any other graphs for which this is the case? If so, what are the discerning properties of such graphs?

Chapter 7

Binary Codes and partial Permutation Decoding sets from the Johnson graphs

The Odd graph $O(k)$ is the subclass of graphs of which the adjacency matrix generated a code which was described in the previous chapter. For any two vertices u and v of $O(k)$, if $d(u,v) = 1$, then by definition, $|u \cap v| = 0$, and if $d(u,v) = 2$, then it is easily seen that $|u \cap v| = k-1$. Hence the graph which has as its vertex-set the vertices of $O(k)$ and for which any two vertices u and v are adjacent if and only if $d(u,v) = 2$, is the Uniform Subset graph $G(2k+1, k, k-1)$. Now recall that the **Johnson graph** $J(n,k)$ is the graph $G(n,k,k-1)$ i.e. the graph of which the vertex-set is $\Omega^{\{k\}}$ where $\Omega = \{1,2,\ldots,n\}$, and any two vertices u and v constitute an edge $[u,v]$ if and only if $|u \cap v| = k-1$. Hence from any Odd graph a Johnson graph can be constructed, and can be viewed as a progression (the "distance-2 graphs") from the Odd graphs. In this chapter the codes and their duals generated by the adjacency matrix of $J(n,k)$ will be described. It will be shown that in each case, the code has a basis comprising minimum weight vectors. The same does not apply to the dual codes, however, for if both n and k are even, then the minimum weight vectors do not span the dual code. In [17] PD-sets were obtained for C if $k = 2$ and $n \geq 5$

is either even or odd. In Theorem 7.3.1 a 3-PD-set is obtained for C if $k \geq 4$ and $n \geq 8$ are even, and $n \geq 2k$, and in Theorem 7.3.2 one is obtained if $k \geq 6$ is even and $n > 2k$ is odd.

The codes from $J(n,k)$ are also the codes of the $1-(\binom{n}{k}, k(n-k), k(n-k))$ design $\mathcal{D}$ which has the vertices of $J(n,k)$ and the supports of the incidence vectors of its adjacency matrix as its point set $\mathcal{P}$ and its block set $\mathcal{B}$ respectively. The automorphism group of $J(n,k)$ is S_n (see [2, Chapter 3]), and hence is contained in the automorphism group of the codes. It is shown that the automorphism group of the code is also S_n for $k > 2$, except when k is odd and n is even, in which case it is $S_{\binom{n}{k}}$.

The Triangular graph $T(n)$ is the Johnson graph $J(n,2)$, and the codes derived from it as given in [17] are found to be a specific case of the codes derived from $J(n,k)$ when k is even. A similar statement applies to the codes from $J(n,3)$ as described in [35] in relation to the codes from $J(n,k)$ when k is odd. In fact, it is observed that the code from $J(n,k)$ equals the code from $O(k)$ when k is odd and $n = 2k+1$. Hence the notation used and results obtained in this chapter are closely linked to that in [17], [35] and the previous chapter, albeit at a greater level of generality and inclusivity.

Some of the basic graph-theoretical properties of $J(n,k)$ will now be reviewed.

7.1 Some basic properties of Johnson graphs

$J(n,k)$ is a regular graph with $\binom{n}{k}$ vertices. The valency is $\binom{k}{k-1}\binom{n-k}{1}$, since any vertex adjacent to a given vertex will consist of $k-1$ elements from the given vertex, and an additional element from the remaining $n-k$ vertices. In general, $J(n,k)$ is not strongly regular since two non-adjacent vertices u and v are not commonly adjacent to a constant number of vertices: if $|u \cap v| = k-2$, then u and v are commonly adjacent to four vertices, but if $|u \cap v| < k-2$, then there are no vertices to which they are commonly adjacent. The exception is $J(n,2)$, in which any two non-adjacent vertices are commonly

adjacent to four vertices - this can be traced back to the fact that in $J(n,2)$ the size of the intersection of any two non-adjacent vertices is constant, namely 0.

As is the case for all Uniform Subset graphs, $J(n,k)$ is distance-transitive. The following lemma makes explicit the fact that the distance between any two vertices u and v in $J(n,k)$ is directly linked to the size of their intersection as k-subsets.

Lemma 7.1.1. [2, Lemma 3.3.3] *Suppose that u and v are vertices of $J(n,k)$. Then for $m \geq 0$,*

$$d(u,v) = m \quad if \quad |u \cap v| = k - m. \tag{7.1}$$

In a similar vein as for $O(k)$, the distance-transitivity of $J(n,k)$ is a direct consequence of Lemma 7.1.1 and the following facts:

(a) the automorphism group of $J(n,k)$ is known to be S_n

(b) for any vertices u, v, s and t of $J(n,k)$ such that $|u \cap v| = |s \cap t|$, there is an automorphism $\sigma \in S_n$ such that $\sigma(u) = s$ and $\sigma(v) = t$.

The basic graph-theoretical properties of $J(n,k)$ are followed-up with the main area of focus in this chapter, namely a study of the codes generated by the adjacency matrix of $J(n,k)$.

7.2 Binary Codes from the Johnson graphs

Let k and $n \geq 2k$ be integers, and $J(n,k)$ the Johnson graph of which the point set $\mathcal{P}$ is the set consisting of the $\binom{n}{k}$ k-subsets of $\Omega = \{1, 2, \ldots, n\}$. Now the $1-(\binom{n}{k}, k(n-k), k(n-k))$ design $\mathcal{D}$ also has $\mathcal{P}$ as its point set, and for which each block denoted by $\overline{\{a_1, a_2, \ldots, a_k\}}$, where $\{a_1, a_2, \ldots, a_k\} \in \Omega^{\{k\}}$, is defined as follows:

$$\overline{\{a_1, a_2, \ldots, a_k\}} = \{\{x_1, x_2, \ldots, x_k\} : \ |\{x_1, x_2, \ldots, x_k\} \cap \{a_1, a_2, \ldots, a_k\}| = k-1\}.$$

As usual, the block set $\mathcal{B}$ is then given by

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

and the incidence vector associated with $\overline{\{a_1, a_2, \ldots, a_k\}}$ by

$$v^{\overline{\{a_1,a_2,\ldots,a_k\}}} = \sum_{\{x_1,x_2,\ldots,x_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_k\}} \quad \sum_{x\in\Omega\setminus\{a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_{k-1},x\}}. \tag{7.2}$$

Once again it should be borne in mind that since the points are in fact k-subsets, the unit vectors should in all correctness be written $v^{\{\{a_1,a_2,\ldots,a_k\}\}}$, but the less cumbersome notation $v^{\{a_1,a_2,\ldots,a_k\}}$ will again be resorted to.

In order to avoid trivial cases, it is assumed that $k \geq 2$ and that $n \geq 5$ - of course in the case of $J(n,k), n \geq 2k$. As usual, C denotes the binary code of $J(n,k)$ and $C^{\perp}$ its dual.

The various cases are considered in order of the algebraic simplicity of the codes which they yield.

The first result is a generalization of Lemma 9.2.1, (1)(c) and (2) in [35]:

Lemma 7.2.1. *If $k \geq 3$ is odd and $n \geq 6$ is even, then $C = F_2^{\binom{n}{k}}$, and consequently $Aut(C) = S_{\binom{n}{k}}$.*

Proof: It suffices to show that each unit vector $v^{\{a_1,a_2,\ldots,a_k\}}, \{a_1, a_2, \ldots, a_k\} \in \Omega^{\{k\}}$, is in C. To this end, consider the set of incidence vectors $\{v^{\overline{\{x_1,x_2,\ldots,x_k\}}} : \{x_1, x_2, \ldots, x_k\} \in \Omega^{\{k\}}, v^{\overline{\{x_1,x_2,\ldots,x_k\}}}$ is incident at $\{a_1, a_2, \ldots, a_k\}\}$, and in particular the sum,

$$\sum_{|\{x_1,x_2,\ldots,x_k\}\cap\{a_1,a_2,\ldots,a_k\}|=k-1} v^{\overline{\{x_1,x_2,\ldots,x_k\}}},$$ of such vectors. Clearly, by design, the vector

$v^{\{a_1,a_2,\ldots,a_k\}}$ occurs $\binom{k}{k-1}\binom{n-k}{1}$ times in the sum. Next, suppose that $\{a'_1, a'_2, \ldots, a'_k\} \in \Omega^{\{k\}}$ is such that $|\{a'_1, a'_2, \ldots, a'_k\} \cap \{a_1, a_2, \ldots, a_k\}| = k-1$, $a'_i = a_i$, $1 \leq i \leq k-1$ say. Then of the vectors in the above set, only the vectors $\{v^{\overline{\{a_1,a_2,\ldots,a_{k-1},x\}}} : x \in \Omega \setminus \{a_1, a_2, \ldots, a_{k-1}, a_k, a'_k\}\}$ and $\{v^{\overline{\{x_1,x_2,\ldots,x_{k-1},a'_k\}}} : \{x_1, x_2, \ldots, x_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\},$

$\{x_1, x_2, \ldots, x_{k-1}\} \neq \{a_1, a_2, \ldots, a_{k-1}\}\}$ are incident at $\{a'_1, a'_2, \ldots, a'_k\}$, and hence the vector $v^{\{a'_1, a'_2, \ldots, a'_k\}}$ occurs $n - k - 1 + (\binom{k}{k-1} - 1)$ times in the sum. If $|\{a'_1, a'_2, \ldots, a'_k\} \cap \{a_1, a_2, \ldots, a_k\}| = k - 2$, $a'_i = a_i, 1 \leq i \leq k-2$ say, then only the four vectors $\{v^{\overline{\{a_1, a_2, \ldots, a_{k-2}, x, \overline{x}\}}} : x \in \{a_{k-1}, a_k\}, \overline{x} \in \{a'_{k-1}, a'_k\}\}$ are incident at $\{a'_1, a'_2, \ldots, a'_k\}$. Finally, if $|\{a'_1, a'_2, \ldots, a'_k\} \cap \{a_1, a_2, \ldots, a_k\}| < k - 2$, then no vectors in the above set are incident at $\{a'_1, a'_2, \ldots, a'_k\}$. Hence the sum under consideration reduces to

$$\sum_{|\{x_1, x_2, \ldots, x_k\} \cap \{a_1, a_2, \ldots, a_k\}| = k-1} v^{\overline{\{x_1, x_2, \ldots, x_k\}}}$$

$$= k(n-k)v^{\{a_1, a_2, \ldots, a_k\}} + (n-2) \sum_{\{x_1, x_2, \ldots, x_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}} \sum_{x \in \Omega \setminus \{a_1, a_2, \ldots, a_k\}} v^{\{x_1, x_2, \ldots, x_{k-1}, x\}}$$

$$+ 4 \sum_{\{x_1, x_2, \ldots, x_{k-2}\} \subseteq \{a_1, a_2, \ldots, a_k\}} \sum_{\{x', x''\} \subseteq \Omega \setminus \{a_1, a_2, \ldots, a_k\}} v^{\{x_1, x_2, \ldots, x_{k-2}, x', x''\}},$$

and since k is odd and n is even, the result follows. Clearly then, $\mathrm{Aut}(C) = S_{\binom{n}{k}}$. $\square$

With k still being odd, but with n now odd as well, the following generalization of Proposition 9.2.2 in [35] is obtained:

Proposition 7.2.2. *If $k \geq 3$ and $n \geq 7$ are both odd, then C is an $[\binom{n}{k}, \binom{n-1}{k}, k+1]$ code, and $C^\perp$ an $[\binom{n}{k}, \binom{n-1}{k-1}, n-k+1]$ code. C has a basis of minimum weight vectors and these, in addition to another $\binom{n-1}{k+1}$ words, constitute the $\binom{n}{k+1}$ minimum words of C. $C^\perp$ also has a basis of minimum weight vectors and these, in addition to another $\binom{n-1}{k-2}$ words, constitute the $\binom{n}{k-1}$ minimum words of $C^\perp$. Furthermore, $C \oplus C^\perp = F_2^{\binom{n}{k}}$, and finally, Aut$(C) = S_n$.*

Proof: As a starting point for the discussion, for any $\{a_1, a_2, \ldots, a_{k+1}\} \in \Omega^{\{k+1\}}$ define the vector $w(\{a_1, a_2, \ldots, a_{k+1}\})$ by

$$w(\{a_1, a_2, \ldots, a_{k+1}\}) = \sum_{\{x_1, x_2, \ldots, x_k\} \subseteq \{a_1, a_2, \ldots, a_{k+1}\}} v^{\{x_1, x_2, \ldots, x_k\}}. \tag{7.3}$$

In order to explore the role that the above vectors play in C, they have of course to be shown to be in C. So consider the sum, $\sum_{\{x_1, x_2, \ldots, x_k\} \subseteq \{a_1, a_2, \ldots, a_{k+1}\}} v^{\overline{\{x_1, x_2, \ldots, x_k\}}}$, of incidence

vectors in C. Now only the vectors $\{v^{\overline{\{x'_1,x'_2,\ldots,x'_k\}}} : \{x'_1,x'_2,\ldots,x'_k\} \subseteq \{a_1,a_2,\ldots,a_{k+1}\}, \{x'_1,x'_2,\ldots,x'_k\} \neq \{x_1,x_2,\ldots,x_k\}\}$ in the above sum are incident at $\{x_1,x_2,\ldots,x_k\} \subseteq \{a_1,a_2,\ldots,a_{k+1}\}$, and hence the vector $v^{\{x_1,x_2,\ldots,x_k\}}$ occurs $\binom{k+1}{k} - 1$ times in the sum for each $\{x_1,x_2,\ldots,x_k\} \subseteq \{a_1,a_2,\ldots,a_{k+1}\}$. The only other points at which the vectors in the sum are incident are those of the form $\{x'_1,x'_2,\ldots,x'_{k-1},x'\}$, where $\{x'_1,x'_2,\ldots,x'_{k-1}\} \subseteq \{a_1,a_2,\ldots,a_{k+1}\}$ and $x' \in \Omega \setminus \{a_1,a_2,\ldots,a_{k+1}\}$ - the vectors $\{v^{\overline{\{x'_1,x'_2,\ldots,x'_{k-1},\overline{x}\}}} : \overline{x} \in \{a_1,a_2,\ldots,a_{k+1}\} \setminus \{x'_1,x'_2,\ldots,x'_{k-1}\}\}$ are incident at the point $\{x'_1,x'_2,\ldots,x'_{k-1},x'\}$. Hence the above sum reduces to

$$\begin{aligned}
&\sum_{\{x_1,x_2,\ldots,x_k\}\subseteq\{a_1,a_2,\ldots,a_{k+1}\}} v^{\overline{\{x_1,x_2,\ldots,x_k\}}} \\
= \; & k \sum_{\{x_1,x_2,\ldots,x_k\}\subseteq\{a_1,a_2,\ldots,a_{k+1}\}} v^{\{x_1,x_2,\ldots,x_k\}} \\
& + 2 \sum_{x'\in\Omega\setminus\{a_1,a_2,\ldots,a_{k+1}\}} \; \sum_{\{x'_1,x'_2,\ldots,x'_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_{k+1}\}} v^{\{x'_1,x'_2,\ldots,x'_{k-1},x'\}},
\end{aligned}$$

and finally to $w(\{a_1,a_2,\ldots,a_{k+1}\})$, since k is odd.

Now the vectors $\{w(\{a_1,a_2,\ldots,a_{k+1}\}) : \{a_1,a_2,\ldots,a_{k+1}\} \in \Omega^{\{k+1\}}\}$ also span C, as is evident from the following:

$$\begin{aligned}
&\sum_{x\in\Omega\setminus\{a_1,a_2,\ldots,a_k\}} w(\{a_1,a_2,\ldots,a_k,x\}) \\
= \; & \sum_{x\in\Omega\setminus\{a_1,a_2,\ldots,a_k\}} v^{\{a_1,a_2,\ldots,a_k\}} + \sum_{x\in\Omega\setminus\{a_1,a_2,\ldots,a_k\}} \; \sum_{\{x_1,x_2,\ldots,x_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_{k-1},x\}} \\
= \; & (n-k)v^{\{a_1,a_2,\ldots,a_k\}} + v^{\overline{\{a_1,a_2,\ldots,a_k\}}} \\
= \; & v^{\overline{\{a_1,a_2,\ldots,a_k\}}},
\end{aligned}$$

since n and k are both odd.

In fact, the set $S = \{w(\{a_1,a_2,\ldots,a_k,n\}) : \{a_1,a_2,\ldots,a_k\} \subseteq \Omega \setminus \{n\}\}$ spans C since in

addition to the above observation,

$$\sum_{\{x_1,x_2,\ldots,x_k\}\subseteq\{a_1,a_2,\ldots,a_{k+1}\}} w(\{x_1,x_2,\ldots,x_k,n\})$$

$$= \sum_{\{x_1,x_2,\ldots,x_k\}\subseteq\{a_1,a_2,\ldots,a_{k+1}\}} v^{\{x_1,x_2,\ldots,x_k\}} + 2 \sum_{\{x'_1,x'_2,\ldots,x'_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_{k+1}\}} v^{\{x'_1,x'_2,\ldots,x'_{k-1},n\}}$$

$$= w(\{a_1,a_2,\ldots,a_{k+1}\}). \tag{7.4}$$

Moreover, since

$$w(\{a_1,a_2,\ldots,a_k,n\}) = v^{\{a_1,a_2,\ldots,a_k\}} + \sum_{\{x_1,x_2,\ldots,x_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_{k-1},n\}},$$

and since $v^{\{a_1,a_2,\ldots,a_k\}}$ is uniquely determined for each $w(\{a_1,a_2,\ldots,a_k,n\})$, it follows that S is linearly independent. Hence S is a basis for C. Clearly, $|S| = \binom{n-1}{k}$.

The fact that S is a basis for C identifies the points

$\{1,2,\ldots,k\}$, $\{1,2,\ldots,k-1,k+1\},\ldots,$ $\{1,2,\ldots,k-1,n-1\}$, $\{1,2,\ldots,k,k+1\},\ldots,$ $\{1,n-k+1,n-k+2,\ldots,n-1\},\ldots,$ $\{n-k,n-k+1,\ldots,n-1\}$
as information positions, and the points

$\{1,2,\ldots k-1,n\}$, $\{1,2,\ldots,k-2,k,n\},\ldots,$ $\{1,2,\ldots,k-2,n-1,n\}$, $\{1,2,\ldots,k-3,k-1,k,n\},\ldots,$ $\{1,2,\ldots,k-3,n-2,n-1,n\},\ldots,$ $\{1,n-k+2,n-k+3,\ldots,n\},\ldots,$ $\{n-k+1,n-k+2,\ldots,n\}$
as check positions, since when the vectors in S are written in lexicographic order and the points in the order described, then a matrix of the form $[I_{\binom{n-1}{k}}|A]$ results.

The weight of each basis vector, and in general each vector $w(\{a_1,a_2,\ldots,a_{k+1}\})$, for $\{a_1,a_2,\ldots,a_{k+1}\} \in \Omega^{\{k+1\}}$, is $k+1$. To show that this is indeed the minimum weight, note that any two vectors in S are commonly incident at at most one point. Hence minimum weight vectors will be obtained by taking linear combinations of the basis vectors $\{w(\{x_1,x_2,\ldots,x_k,n\}) : \{x_1,x_2,\ldots,x_k\} \subseteq \{a_1,a_2,\ldots,a_{k+1}\}\}$ for any $\{a_1,a_2,\ldots,a_{k+1}\} \in \Omega^{\{k+1\}}$. Suppose a linear combination of m such vectors yields a weight of less than $k+1$.

Then

$$m(k+1) - 2.\tbinom{m}{2}.1 < k+1 \tag{7.5}$$

$$\text{i.e. } m < 1 \quad \text{or} \quad m > k+1.$$

Both solutions are clearly invalid, and hence the minimum weight of C is $k+1$. Equality in 7.5 implies that C has a basis of minimum weight vectors, and in conjunction with equation 7.4, further implies that C has an additional $\binom{n-1}{k+1}$ minimum words, and hence a total of $\binom{n-1}{k} + \binom{n-1}{k+1} = \binom{n}{k+1}$ minimum words.

To shift the focus of the discussion to $C^{\perp}$, for any $\{b_1, b_2, \ldots, b_{k-1}\} \in \Omega^{\{k-1\}}$, define the vector $v(\{b_1, b_2, \ldots, b_{k-1}\})$ by

$$v(\{b_1, b_2, \ldots, b_{k-1}\}) = \sum_{y \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-1}\}} v^{\{b_1, b_2, \ldots, b_{k-1}, y\}}. \tag{7.6}$$

In order to show that $v(\{b_1, b_2, \ldots, b_{k-1}\})$ is in $C^{\perp}$, consider the inner product $(\{v^{\overline{\{a_1, a_2, \ldots, a_k\}}}, v(\{b_1, b_2, \ldots, b_{k-1}\}))$. If $\{b_1, b_2, \ldots, b_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}$, then $v^{\overline{\{a_1, a_2, \ldots, a_k\}}}$ and $v(\{b_1, b_2, \ldots, b_{k-1}\})$ are commonly incident at $\{\{b_1, b_2, \ldots, b_{k-1}, y\} : y \in \Omega \setminus \{a_1, a_2, \ldots, a_k\}\}$ and hence the inner product is $n - k \equiv 0 (\text{mod } 2)$, since both k and n are odd. If $|\{b_1, b_2, \ldots, b_{k-1}\} \cap \{a_1, a_2, \ldots, a_k\}| = k - 2$, say $\{b_1, b_2, \ldots, b_{k-1}\} \cap \{a_1, a_2, \ldots, a_k\} = \{b_1, b_2, \ldots, b_{k-2}\}$, then $v^{\overline{\{a_1, a_2, \ldots, a_k\}}}$ and $v(\{b_1, b_2, \ldots, b_{k-1}\})$ are commonly incident at $\{\{b_1, b_2, \ldots, b_{k-1}, y\} : y \in \{a_1, a_2, \ldots, a_k\} \setminus \{b_1, b_2, \ldots, b_{k-2}\}\}$, and hence the inner product is $2 \equiv 0 (\text{mod } 2)$. Finally, if $|\{b_1, b_2, \ldots, b_{k-1}\} \cap \{a_1, a_2, \ldots, a_k\}| < k - 2$, then $v^{\overline{\{a_1, a_2, \ldots, a_k\}}}$ and $v(\{b_1, b_2, \ldots, b_{k-1}\})$ are not commonly incident at any point. Hence $v(\{b_1, b_2, \ldots, b_{k-1}\})$ is in $C^{\perp}$. The linearity of the inner product ensures that $\text{span}\{v(\{b_1, b_2, \ldots, b_{k-1}\}) : \{b_1, b_2, \ldots, b_{k-1}\} \in \Omega^{\{k-1\}}\} \subseteq C^{\perp}$. In order to identify a basis for $C^{\perp}$ from amongst these vectors, observe that for any $\{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{n\}$,

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

Given that $R = \{v(\{b_1, b_2, \ldots, b_{k-1}\}) : \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{n\}\}$, the above equation implies that R is linearly independent since $v^{\{b_1, b_2, \ldots, b_{k-1}, n\}}$ is unique for each $v(\{b_1, b_2, \ldots, b_{k-1}\})$ in R. Also, $|R| = \binom{n-1}{k-1} = \binom{n}{k} - \binom{n-1}{k}$, and since $\dim(C) = \binom{n-1}{k}$,

it follows that R is a basis for $C^{\perp}$. Note that when the vectors in R are written in lexicographic order and the points are ordered as described earlier for C, then a matrix of the form $[B|I_{\binom{n-1}{k-1}}]$ results, thereby identifying the last $\binom{n-1}{k-1}$ points as the information positions for $C^{\perp}$.

Clearly, each vector in R has weight $n-k+1$. Since any two vectors in R are commonly incident at at most one point, minimum weight vectors will be obtained by taking linear combinations of vectors in $\{v(\{b_1, b_2, \ldots, b_{k-2}, y\}) : y \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-2}, n\}\}$ for any $\{b_1, b_2, \ldots, b_{k-2}\} \subseteq \Omega \setminus \{n\}$. A similar argument to that used for $\{w(\{x_1, x_2, \ldots, x_k, n\}) : \{x_1, x_2, \ldots, x_k\} \subseteq \{a_1, a_2, \ldots, a_{k+1}\}\}$ in C can be used to show that the minimum weight of $C^{\perp}$ is $n-k+1$, and that $C^{\perp}$ has $\binom{n}{k-1}$ minimum words. Alternatively, it can be argued that any $v \in C^{\perp}$ which is incident at $\{b_1, b_2, \ldots, b_k\}$, is incident at at least an additional $n-k$ points since $(v, w(\{b_1, b_2, \ldots, b_k, y\})) = 0$ for each $y \in \Omega \setminus \{b_1, b_2, \ldots, b_k\}$, and any $w(\{b_1, b_2, \ldots, b_k, y\})$ and $w(\{b_1, b_2, \ldots, b_k, \overline{y}\})$ are commonly incident only at $\{b_1, b_2, \ldots, b_k\}$. Hence any $v \in C^{\perp}$ has weight at least $n-k+1$, and since $C^{\perp}$ has vectors of this weight, it follows that the minimum weight is $n-k+1$. On the other hand, any vector $v \in C^{\perp}$ of weight $n-k+1$ has this form: if v is incident at $\{b_1, b_2, \ldots, b_k\}$, then since $(v, w(\{b_1, b_2, \ldots, b_k, y\})) = 0$ for each $y \in \Omega \setminus \{b_1, b_2, \ldots, b_k\}$, v is incident at some other point $s_y \subseteq \{b_1, b_2, \ldots, b_k, y\}$ for each $y \in \Omega \setminus \{b_1, b_2, \ldots, b_k\}$. Now if $v \neq \sum_{y \in \Omega \setminus \{b'_1, b'_2, \ldots, b'_{k-1}\}} v^{\{b'_1, b'_2, \ldots, b'_{k-1}, y\}}$ for any $\{b'_1, b'_2, \ldots, b'_{k-1}\} \subseteq \{b_1, b_2, \ldots, b_k\}$, then for some $y', y'' \in \Omega \setminus \{b_1, b_2, \ldots, b_k\}$, $s_{y'} \cap \{b_1, b_2, \ldots, b_k\} \neq s_{y''} \cap \{b_1, b_2, \ldots, b_k\}$. But then $(v, w(s_{y'} \cup (s_{y''} \setminus \{b_1, b_2, \ldots, b_k\}))) \neq 0$, unless the weight of v is greater than $n-k+1$. In the case of C, if any $w \in C$ is incident at $\{a_1, a_2, \ldots, a_k\}$, then it is incident at at least an additional k points since $(w, v(\{x_1, x_2, \ldots, x_{k-1}\})) = 0$ for each $\{x_1, x_2, \ldots, x_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}$, and any $v(\{x_1, x_2, \ldots, x_{k-1}\})$ and $v(\{\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_{k-1}\})$ are commonly incident only at $\{a_1, a_2, \ldots, a_k\}$. Hence any $w \in C$ has weight at least $k+1$, and since C has vectors of this weight, it follows that the minimum weight is $k+1$. Also, any $w \in C$ of weight $k+1$ has this form: if w is incident at $\{a_1, a_2, \ldots, a_k\}$ then since $(w, v(\{x_1, x_2, \ldots, x_{k-1}\})) = 0$ for each $\{x_1, x_2, \ldots, x_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}$, it is inci-

dent at some other point $t_x \supseteq x$ for each $(k-1)$-subset $x \subseteq \{a_1, a_2, \ldots, a_k\}$. Now if $w \neq \sum_{\{x'_1, x'_2, \ldots, x'_k\} \subseteq \{a_1, a_2, \ldots, a_k, \overline{x}\}} v^{\{x'_1, x'_2, \ldots, x'_k\}}$, for any $\overline{x} \in \Omega \setminus \{a_1, a_2, \ldots, a_k\}$, then for some $x', x'' \subseteq \{a_1, a_2, \ldots, a_k\}$, $(w, v((t_{x'} \cap t_{x''}) \cup (t_{x'} \setminus x'))) \neq 0$, unless w has weight greater than $k+1$.

Now $C \not\subset C^\perp$, since if $|\{a_1, a_2, \ldots, a_k\} \cap \{a'_1, a'_2, \ldots, a'_k\}| = k-1$, then $(v^{\overline{\{a_1, a_2, \ldots, a_k\}}}, v^{\overline{\{a'_1, a'_2, \ldots, a'_k\}}}) = (n-k-1) + \binom{k-1}{k-2} \equiv 1 (\mathrm{mod}\ 2)$, since k and n are both odd. Neither is $C^\perp \not\subset C$, since if $|\{b_1, b_2, \ldots, b_{k-1}\} \cap \{b'_1, b'_2, \ldots, b'_{k-1}\}| = k-2$, then $(v(\{b_1, b_2, \ldots, b_{k-1}\}), v(\{b'_1, b'_2, \ldots, b'_{k-1}\})) = 1$. Furthermore, $\boldsymbol{j} \in C^\perp$, since the weight, $k(n-k)$, of each incidence vector is even. In order to show that $C \oplus C^\perp = F_2^{\binom{n}{k}}$, it is sufficient to show that any unit vector is in $C + C^\perp$. So consider the following sum:

$$
\begin{aligned}
& v^{\overline{\{a_1, a_2, \ldots, a_k\}}} + \sum_{\{y_1, y_2, \ldots, y_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}} v(\{y_1, y_2, \ldots, y_{k-1}\}) \\
= & \sum_{\{x_1, x_2, \ldots, x_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}} \; \sum_{x \in \Omega \setminus \{a_1, a_2, \ldots, a_k\}} v^{\{x_1, x_2, \ldots, x_{k-1}, x\}} \\
& + \sum_{\{y_1, y_2, \ldots, y_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}} \; \sum_{y \in \Omega \setminus \{y_1, y_2, \ldots, y_{k-1}\}} v^{\{y_1, y_2, \ldots, y_{k-1}, y\}} \\
= & \sum_{\{x_1, x_2, \ldots, x_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}} \; \sum_{x \in \Omega \setminus \{a_1, a_2, \ldots, a_k\}} v^{\{x_1, x_2, \ldots, x_{k-1}, x\}} \\
& + \sum_{\{y_1, y_2, \ldots, y_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}} v^{\{a_1, a_2, \ldots, a_k\}} \\
& + \sum_{\{y_1, y_2, \ldots, y_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}} \; \sum_{y \in \Omega \setminus \{a_1, a_2, \ldots, a_k\}} v^{\{y_1, y_2, \ldots, y_{k-1}, y\}} \\
= & \binom{k}{k-1} v^{\{a_1, a_2, \ldots, a_k\}},
\end{aligned}
$$

and since k is odd, the result follows.

Finally, to show that $\mathrm{Aut}(C) = S_n$, recall that the vectors $\{v(\{b_1, b_2, \ldots, b_{k-1}\}) : \{b_1, b_2, \ldots, b_{k-1}\} \in \Omega^{\{k-1\}}\}$ constitute the minimum words of $C^\perp$. Hence any $\sigma \in \mathrm{Aut}(C)$ induces a permutation on $\Omega^{\{k-1\}}$. σ certainly preserves incidence of points of $\mathcal{D}$ on words of $C^\perp$, and hence by precisely the same argument as in Theorem 6.2.11, it can be shown that $\mathrm{Aut}(C) = S_n$. □

With reference to the above proposition, note that the choice of n in the basis $\{w(\{a_1, a_2, \ldots, a_k, n\}) : \{a_1, a_2, \ldots, a_k\} \subseteq \Omega \setminus \{n\}\}$ is arbitrary, and hence $\{w(\{1, a_1, a_2, \ldots, a_k\}) : \{a_1, a_2, \ldots, a_k\} \subseteq \Omega \setminus \{1\}\}$ is also a basis for C. Then, if $n = 2k+1$,

$$\begin{aligned} w(\{1, a_1, a_2, \ldots, a_k\}) &= \sum_{\{x_1, x_2, \ldots, x_k\} \subseteq \{1, a_1, a_2, \ldots, a_k\}} v^{\{x_1, x_2, \ldots, x_k\}} \\ &= v^{\overline{\Omega \setminus \{1, a_1, a_2, \ldots, a_k\}}}, \end{aligned}$$

where $v^{\overline{\{\Omega \setminus \{1, a_1, a_2, \ldots, a_k\}}}}$ is a basis vector of the code from $O(k)$. Since this association is clearly bijective, the code from $J(n, k)$ equals the code from $O(k)$ if $n = 2k + 1$.

The following proposition, with n still odd but k now even, is a reversal of the situation in Proposition 7.2.2, and is a generalization of Lemmas 3.2 to 3.7 in [17] for n odd.

Proposition 7.2.3. *If $k \geq 2$ is even and $n \geq 5$ is odd, then C is an $[\binom{n}{k}, \binom{n-1}{k-1}, n-k+1]$ code, and $C^\perp$ an $[\binom{n}{k}, \binom{n-1}{k}, k+1]$ code. C has a basis of minimum weight vectors and these, in addition to another $\binom{n-1}{k-2}$ words, constitute the $\binom{n}{k-1}$ minimum words of C. $C^\perp$ also has a basis of minimum weight vectors and these, in addition to another $\binom{n-1}{k+1}$ words, constitute the $\binom{n}{k+1}$ minimum words of $C^\perp$. Furthermore, $C \oplus C^\perp = F_2^{\binom{n}{k}}$, and finally, $Aut(C) = S_n$.*

Proof: Fundamental to Proposition 7.2.3 is the observation that $v(\{b_1, b_2, \ldots, b_{k-1}\}) \in C$:

$$\begin{aligned}
&\sum_{y \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-1}\}} v^{\overline{\{b_1, b_2, \ldots, b_{k-1}, y\}}} \\
= &\sum_{y \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-1}\}} \quad \sum_{\overline{y} \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-1}, y\}} v^{\{b_1, b_2, \ldots, b_{k-1}, \overline{y}\}} \\
&+ \sum_{y \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-1}\}} \quad \sum_{\{y_1, y_2, \ldots, y_{k-2}\} \subseteq \{b_1, b_2, \ldots, b_{k-1}\}} \quad \sum_{\tilde{y} \in \Omega \setminus \{y_1, y_2, \ldots, y_{k-2}, y\}} v^{\{y_1, y_2, \ldots, y_{k-2}, y, \tilde{y}\}} \\
= &\ (n-k) \sum_{y \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-1}\}} v^{\{b_1, b_2, \ldots, b_{k-1}, y\}} \\
&+ 2 \sum_{\{y_1, y_2, \ldots, y_{k-2}\} \subseteq \{b_1, b_2, \ldots, b_{k-1}\}} \quad \sum_{\{y, \tilde{y}\} \subseteq \Omega \setminus \{b_1, b_2, \ldots, b_{k-1}\}} v^{\{y_1, y_2, \ldots, y_{k-2}, y, \tilde{y}\}},
\end{aligned}$$

and since k is even and n is odd, the above sum reduces to $v(\{b_1, b_2, \ldots, b_{k-1}\})$. Furthermore, the vectors $\{v(\{b_1, b_2, \ldots, b_{k-1}\}) : \{b_1, b_2, \ldots, b_{k-1}\} \in \Omega^{\{k-1\}}\}$ span C, since if k is even, then

$$\begin{aligned}
&\sum_{\{x_1, x_2, \ldots, x_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}} v(\{x_1, x_2, \ldots, x_{k-1}\}) \\
= &\ \tbinom{k}{k-1} v^{\{a_1, a_2, \ldots, a_k\}} + \sum_{\{x'_1, x'_2, \ldots, x'_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}} \quad \sum_{x' \in \Omega \setminus \{a_1, a_2, \ldots, a_k\}} v^{\{x'_1, x'_2, \ldots, x'_{k-1}, x'\}}, \\
= &\ v^{\overline{\{a_1, a_2, \ldots, a_k\}}}.
\end{aligned}$$

In fact, $\{v(\{b_1, b_2, \ldots, b_{k-1}\}) : \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega \setminus \{n\}\}$ spans C, since

$$\begin{aligned}
& \sum_{y \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-2}, n\}} v(\{b_1, b_2, \ldots, b_{k-2}, y\}) \\
= & \sum_{y \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-2}, n\}} \quad \sum_{\tilde{y} \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-2}, y\}} v^{\{b_1, b_2, \ldots, b_{k-2}, y, \tilde{y}\}} \\
= & \; 2 \sum_{\{y_1, y_2, \ldots, y_{k-2}\} \subseteq \{b_1, b_2, \ldots, b_{k-2}, n\}} \; \sum_{\{y, \overline{y}\} \subseteq \Omega \setminus \{b_1, b_2, \ldots, b_{k-2}, n\}} v^{\{y_1, y_2, \ldots, y_{k-2}, y, \overline{y}\}} \\
& + \sum_{y \in \Omega \setminus \{b_1, b_2, \ldots, b_{k-2}, n\}} v^{\{b_1, b_2 \ldots, b_{k-2}, y, n\}} \\
= & \; v(\{b_1, b_2, \ldots, b_{k-2}, n\}).
\end{aligned}$$

The dimension, the minimum weight and the minimum words of C can be deduced by exactly the same arguments as for $C^\perp$ in Proposition 7.2.2. With regard to $C^\perp$, it can be shown that $w(\{a_1, a_2, \ldots, a_{k+1}\})$ as defined in 7.3 is now in $C^\perp$: if $\{a'_1, a'_2, \ldots, a'_k\} \subseteq \{a_1, a_2, \ldots, a_{k+1}\}$, then $(v^{\overline{\{a'_1, a'_2, \ldots, a'_k\}}}, w(\{a_1, a_2, \ldots, a_{k+1}\})) = \binom{k}{k-1}.1 \equiv 0 (\text{mod } 2)$, since k is even, and if $|\{a'_1, a'_2, \ldots, a'_k\} \cap \{a_1, a_2, \ldots, a_{k+1}\}| = k-1$, then $(v^{\overline{\{a'_1, a'_2, \ldots, a'_k\}}}, w(\{a_1, a_2, \ldots, a_{k+1}\})) = 2 \equiv 0 (\text{mod } 2)$. Clearly, if $|\{a'_1, a'_2, \ldots, a'_k\} \cap \{a_1, a_2, \ldots, a_{k+1}\}| < k-1$, then $(v^{\overline{\{a'_1, a'_2, \ldots, a'_k\}}}, w(\{a_1, a_2, \ldots, a_{k+1}\})) = 0$. The linearity of the inner product implies that span $\{w(\{a_1, a_2, \ldots, a_{k+1}\}) : \{a_1, a_2, \ldots, a_{k+1}\} \in \Omega^{\{k+1\}}\} \subseteq C^\perp$. Again the identification of a basis, the dimension, the minimum weight and the minimum words of $C^\perp$ follow exactly as for C in the previous proposition.

Of course, $\boldsymbol{j} \in C^\perp$, and $C \not\subseteq C^\perp$ as in Proposition 7.2.2, and since $(\{w(\{a_1, a_2, \ldots, a_{k+1}\}), w(\{a'_1, a'_2, \ldots, a'_{k+1}\})) = 1$ if $|\{a_1, a_2, \ldots, a_{k+1}\} \cap \{a'_1, a'_2, \ldots, a'_{k+1}\}| = k$, $C^\perp \not\subset C$ either. In order to show that $C \oplus C^\perp = F_2^{\binom{n}{k}}$, consider the following sum:

$$\sum_{x\in\Omega\setminus\{a_1,a_2,\ldots,a_k\}} w(\{a_1,a_2,\ldots,a_k,x\})$$

$$= \sum_{x\in\Omega\setminus\{a_1,a_2,\ldots,a_k\}} v^{\{a_1,a_2,\ldots,a_k\}} + \sum_{x\in\Omega\setminus\{a_1,a_2,\ldots,a_k\}} \sum_{\{x_1,x_2,\ldots,x_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_{k-1},x\}}$$

$$= (n-k)v^{\{a_1,a_2,\ldots,a_k\}} + v^{\overline{\{a_1,a_2,\ldots,a_k\}}}.$$

Since k is even and n is odd, each unit vector is a sum of vectors in C and $C^\perp$, and the result follows.

It remains to be shown that $\mathrm{Aut}(C) = S_n$. Since any $\sigma \in \mathrm{Aut}(C)$ preserves the minimum words of C and incidence of points on words of C, σ induces a permutation of the $(k-1)$-subsets of Ω. By the same argument as in Proposition 7.2.2, it follows that $\mathrm{Aut}(C) = S_n$. □

The final case, when k and n are both even, is a generalization of Lemmas 3.2 to 3.7 in [17] for n even.

Proposition 7.2.4. *If $k \geq 2$ and $n \geq 6$ are both even, then C is an $[\binom{n}{k}, \binom{n-2}{k-1}, k(n-k)]$ code, and $C^\perp$ an $[\binom{n}{k}, \binom{n}{k} - \binom{n-2}{k-1}, k+1]$ code. C has a basis of minimum weight vectors but $C^\perp$, however, does not. $C \subseteq C^\perp$ and C is doubly-even. If $n > 2k$, then $Aut(C) = S_n$, except when $k = 2$ and $n = 6$, in which case $Aut(C) = PGL_4(2) \cong A_8$. If $n = 2k$, then $Aut(C) \cong S_n \times Z_2$.*

Proof: In order to identify a basis, observe the following relationship between the incidence vectors:

For $\{a_1, a_2, \ldots, a_k\} \subseteq \Omega \setminus \{1\}$,

$$\sum_{\{x_1,x_2,\ldots,x_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_k\}} v^{\overline{\{1,x_1,x_2,\ldots,x_{k-1}\}}}$$

$$= (k-1)\sum_{\{x_1,x_2,\ldots,x_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_k\}} v^{\{1,x_1,x_2,\ldots,x_{k-1}\}} + k\ v^{\{a_1,a_2,\ldots,a_k\}}$$

$$+ \sum_{\{x_1,x_2,\ldots,x_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_k\}}\ \sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_{k-1},x\}},$$

and since k is even, the above sum reduces to

$$\sum_{\{x_1,x_2,\ldots,x_{k-1}\}\subseteq\{a_1,a_2,\ldots,a_k\}}\ \sum_{x'\in\Omega\setminus\{a_1,a_2,\ldots,a_k\}} v^{\{x_1,x_2,\ldots,x_{k-1},x'\}} = v^{\overline{\{a_1,a_2,\ldots,a_k\}}}.$$

Furthermore,

$$\sum_{x\in\Omega\setminus\{1,a_1,\ldots,a_{k-2},n\}} v^{\overline{\{1,a_1,a_2,\ldots,a_{k-2},x\}}}$$

$$= (n-k-1)\sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-2},n\}} v^{\{1,a_1,a_2,\ldots,a_{k-2},x\}} + (n-k)\ v^{\{1,a_1,a_2,\ldots,a_{k-2},n\}}$$

$$+ \sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-2},n\}}\ \sum_{\{x_1,x_2,\ldots,x_{k-2}\}\subseteq\{1,a_1,a_2,\ldots,a_{k-2}\}} v^{\{x_1,x_2,\ldots,x_{k-2},x,n\}}$$

$$+ 2\sum_{\{x',x''\}\subseteq\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-2},n\}}\ \sum_{\{x_1,x_2,\ldots,x_{k-2}\}\subseteq\{1,a_1,a_2,\ldots,a_{k-2}\}} v^{\{x_1,x_2,\ldots,x_{k-2},x',x''\}}.$$

Since k and n are both even, this sum in turn reduces to

$$\sum_{x\in\Omega\setminus\{1,a_1,a_2,\ldots,a_{k-2},n\}}\ \sum_{\{x'_1,x'_2,\ldots,x'_{k-1}\}\subseteq\{1,a_1,a_2,\ldots,a_{k-2},n\}} v^{\{x'_1,x'_2,\ldots,x'_{k-1},x\}} = v^{\overline{\{1,a_1,a_2,\ldots,a_{k-2},n\}}}.$$

Hence $T = \{v^{\overline{\{1,a_1,a_2,\ldots,a_{k-1}\}}} : \{a_1,a_2,\ldots,a_{k-1}\}\subseteq\Omega\setminus\{1,n\}\}$ spans C. Now if the vectors in T are arranged in lexicographic order and the points as follows: first the points $\{2,3,\ldots,k,n\},\ \{2,3,\ldots,k-1,k+1,n\},\ldots,\ \{2,3,\ldots,k-1,n-1,n\},\ \{2,3,\ldots,k-2,k,k+1,n\},\ldots,\ \{2,3,\ldots,k-2,n-2,n-1,n\},\ldots,\ \{2,n-k+2,n-k+1,\ldots,n\}$, $\{3,4,\ldots,k+1,n\},\ldots,\ \{n-k+1,n-k+2,\ldots,n\}$,

followed by the points

$\{1,2,\ldots,k\}, \{1,2,\ldots,k-1,k+1\},\ldots,\{1,2,\ldots,k-1,n-1\},\{1,2,\ldots,k-2,k,k+1\},\ldots,$
$\{1,2,\ldots,k-2,k,n-1\},\ldots,\{1,n-k+1,n-k+2,\ldots,n-1\},$

and then

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

and finally

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

then a matrix of the form $[I_{\binom{n-2}{k-1}}|A]$ results. Hence T is a basis for C, and clearly, $|T| = \binom{n-2}{k-1}$.

With regard to the identification of a basis for $C^\perp$, consider the inner product $(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v^{\overline{\{a'_1,a'_2,\ldots,a'_k\}}})$ of any two incidence vectors. If $|\{a_1,a_2,\ldots,a_k\}\cap\{a'_1,a'_2,\ldots,a'_k\}|$ $= k-1$, then $(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v^{\overline{\{a'_1,a'_2,\ldots,a'_k\}}}) = n-k-1+\binom{k-1}{k-2} = n-2 \equiv 0(\text{mod } 2)$, since n is even. If on the other hand, $|\{a_1,a_2,\ldots,a_k\}\cap\{a'_1,a'_2,\ldots,a'_k\}| = k-2$, then $(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v^{\overline{\{a'_1,a'_2,\ldots,a'_k\}}}) = 4 \equiv 0(\text{mod } 2)$, and finally, if $|\{a_1,a_2,\ldots,a_k\}\cap\{a'_1,a'_2,\ldots,a'_k\}|$ $< k-2$, then clearly $(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v^{\overline{\{a'_1,a'_2,\ldots,a'_k\}}}) = 0$. Hence $C \subseteq C^\perp$. With $v(\{b_1,b_2,\ldots,b_{k-1}\})$ as defined in Proposition 7.2.2, consider also $(\{v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v(\{b_1,b_2,\ldots,b_{k-1}\}))$. As in Proposition 7.2.2 when k and n are both odd, $(v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, v(\{b_1,b_2,\ldots,b_{k-1}\})) = 0$ in all cases, and hence $v(\{b_1,b_2,\ldots,b_{k-1}\}) \in C^\perp$. Finally, with $w(\{a'_1,a'_2,\ldots,a'_{k+1}\})$ also as defined in Proposition 7.2.2, $(\{v^{\overline{\{a_1,a_2,\ldots,a_k\}}}, w(\{a'_1,a'_2,\ldots,a'_{k+1}\})) = 0$ in all cases as in Proposition 7.2.3 when k is even and n is odd. Hence $w(\{a'_1,a'_2,\ldots,a'_{k+1}\}) \in C^\perp$ as well. Let

$$\begin{aligned} U &= \{v^{\overline{\{a_1,a_2,\ldots,a_{k-1},n\}}} : \{a_1,a_2,\ldots,a_{k-1}\} \subseteq \Omega \setminus \{1,n\}\}, \\ V &= \{v(\{b_1,b_2,\ldots,b_{k-2},n\}) : \{b_1,b_2,\ldots,b_{k-2}\} \subseteq \Omega \setminus \{1,n\}\}, \\ W &= \{w(\{a'_1,a'_2,\ldots,a'_k,n\}) : \{a'_1,a'_2,\ldots,a'_k\} \subseteq \Omega \setminus \{1,n\}\}. \end{aligned}$$

Then certainly, span $(U \cup V \cup W) \subseteq C^{\perp}$. By arranging the vectors of U, followed by those in V, and finally by those in W all in lexicographic order, and the points as follows: first the last $\binom{n}{k} - \binom{n-2}{k-1}$ points and then the first $\binom{n-2}{k-1}$ points as ordered in the case of C above, an upper triangular matrix results, the rank of which is $\binom{n-2}{k-1} + \binom{n-2}{k-2} + \binom{n-2}{k}$. Since $\binom{n-2}{k-1} + \binom{n-2}{k-2} + \binom{n-2}{k} = \binom{n}{k} - \binom{n-2}{k-1} = \binom{n}{k} - \dim(C)$, it follows that $U \cup V \cup W$ is a basis for $C^{\perp}$.

In order to determine the minimum weight of $C^{\perp}$, suppose that $w \in C^{\perp}$ is incident at $\{a_1, a_2, \ldots, a_k\}$. For any $\{a'_1, a'_2, \ldots, a'_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}$, and any $x' \in \Omega \setminus \{a_1, a_2, \ldots, a_k\}$, consider the set of incidence vectors $\{v^{\overline{\{a'_1, a'_2, \ldots, a'_{k-1}, x\}}} : x \in \Omega \setminus \{a_1, a_2, \ldots, a_k, x'\}\}$. Then, since $(w, v^{\overline{\{a'_1, a'_2, \ldots, a'_{k-1}, x\}}}) = 0$ for each vector in the set, and since the vectors in the set are commonly incident only at $\{a_1, a_2, \ldots, a_k\}$ and at $\{a'_1, a'_2, \ldots, a'_{k-1}, x'\}$, w is incident at at least an additional point for each $\{a'_1, a'_2, \ldots, a'_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}$. Hence any $w \in C^{\perp}$ has weight at least $1 + \binom{k}{k-1}$. Now since the vectors in U, V and W have weights $k(n-k), n-k+1$ and $k+1$ respectively, and if $n \geq 2k$ as is true in the case of $J(n,k)$, then $k+1 \leq n-k+1 < k(n-k)$, it follows that the minimum weight is $k+1$. If $n > 2k$ and $J(n,k) \neq J(6,2)$, then any $w \in C^{\perp}$ of weight $k+1$ has this form: if w is incident at $\{a_1, a_2, \ldots, a_k\}$, then as explained above, w is incident at $\{a'_1, a'_2, \ldots, a'_{k-1}, x'\}$ and at $\{a''_1, a''_2, \ldots, a''_{k-1}, x''\}$, where $\{a'_1, a'_2, \ldots, a'_{k-1}\}, \{a''_1, a''_2, \ldots, a''_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}$, and $x', x'' \in \Omega \setminus \{a_1, a_2, \ldots, a_k\}$. If $x' \neq x''$, then for any $a \in \Omega \setminus \{a_1, a_2, \ldots, a_k, x', x''\}$, $(w, v^{\overline{(\{a'_1, a'_2, \ldots, a'_{k-1}\} \cap \{a''_1, a''_2, \ldots, a''_{k-1}\}) \cup \{x'\} \cup \{a\}}}) \neq 0$, unless the weight of w is greater than $k+1$. Note that W does not span the minimum words since for $\{a_1, a_2, \ldots, a_{k-1}\} \subseteq \Omega \setminus \{1, n\}$,

$$w(\{1, a_1, a_2, \ldots, a_{k-1}, n\}) = \sum_{x \in \Omega \setminus \{1, a_1, a_2, \ldots, a_{k-1}, n\}} w(\{a_1, a_2, \ldots, a_{k-1}, x, n\}) + v^{\overline{\{a_1, a_2, \ldots, a_{k-1}, n\}}},$$

and $v^{\overline{\{a_1, a_2, \ldots, a_{k-1}, n\}}}$ is not a linear combination of vectors in W. Neither do the minimum words span $C^{\perp}$ since $\dim(\{w(\{a_1, a_2, \ldots, a_{k+1}\}) : \{a_1, a_2, \ldots, a_{k+1}\} \subseteq \Omega\}) \leq \binom{n-1}{k} = \binom{n-2}{k} + \binom{n-2}{k-1} < \dim(C^{\perp})$. Hence $C^{\perp}$ does not have a basis of minimum weight vectors.

In [17] it is shown that in the case of $J(6,2), C^{\perp}$ has additional words of weight 3 of the form $v^{\{a,b\}} + v^{\{c,d\}} + v^{\{e,f\}}$. However, words of this form are not found in $C^{\perp}$ for any other

$n > 2k, k \geq 2$: if $n = k(k+1)$, then

$$u = v^{\{a_1,a_2,\ldots,a_k\}} + v^{\{a_{k+1},a_{k+2},\ldots,a_{2k}\}} + \cdots + v^{\{a_{n-k+1},a_{n-k+2},\ldots,a_n\}}$$

has weight $k+1$, but $(u, v^{\overline{\{a_1,a_2,\ldots,a_{k-1},a_{k+1}\}}}) = 1$, and hence $u \notin C^{\perp}$. If $n = 2k$, then for each $\{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega$, $v(\{b_1, b_2, \ldots, b_{k-1}\})$ also has weight $k+1$, and hence $C^{\perp}$ has $\binom{n}{k-1}$ additional minimum words.

With regard to the minimum weight of C, clearly the minimum weight will be obtained when combining the basis vectors of C in such a way that any pair of vectors is commonly incident at a maximum number of points. This is the case for the set $X = \{v^{\overline{\{1,a_1,a_2,\ldots,a_{k-2},x\}}} : x \in \Omega \backslash \{1, a_1, a_2, \ldots, a_{k-2}, n\}\}$, and the set $Y = \{v^{\overline{\{1,x_1,x_2,\ldots,x_{k-1}\}}} : \{x_1, x_2, \ldots, x_{k-1}\} \subseteq \{a_1, a_2, \ldots, a_k\}\}$ where $\{a_1, a_2, \ldots, a_k\} \subseteq \Omega \setminus \{1, n\}$. Firstly then, suppose that a linear combination of m vectors in X is formed.

Case (i): m is odd

It is easily checked that a vector resulting from such a linear combination will have weight

$$mk(n-k) - m(m-1) - (n-k+1-m)(m-1) - m(m-1)(k-1).$$

If this weight were less than $k(n-k)$, then

$$(m-k)(m(1-k) - (n-k)(1-k) + 1) < 0,$$

$$\text{i.e.} \quad m < 1 \text{ or } m > \frac{(n-k)(1-k)+1}{1-k} > n-k.$$

Both solutions are invalid - the second being invalid since $|X| = n-k$.

Case (ii): m is even

In this case the resulting vector will have weight

$$mk(n-k) - m(m-2) - m(n-k+1-m) - m(m-1)(k-1),$$

and if this weight were less than $k(n-k)$, then

$$(m(1-k)+k)(m-n+k) < 0,$$

$$\text{i.e. } m < \frac{k}{k-1} \text{ or } m > n-k.$$

Since $\frac{k}{k-1} \leq 2$ for $k \geq 2$, the first solution is invalid. The second solution is also invalid as before.

Next, suppose that a linear combination of m vectors in Y is formed.

Case (i): m is odd

Such a vector will have weight

$$mk(n-k) - (m-1)(k+1-m) - m(m-1) - m(m-1)(n-k-1).$$

If this weight were less than $k(n-k)$ then

$$(m-1)((n-k-1)(k-m)-1) < 0,$$

$$\text{i.e. } m < 1 \text{ or } m > \frac{k(n-k-1)-1}{n-k-1} > k-1.$$

The first solution is obviously invalid, and since $|Y| = k$, which is even, the second solution is also invalid.

Case (ii): m is even

This time such a vector will have weight

$$mk(n-k) - m(k+1-m) - m(m-2) - m(m-1)(n-k-1),$$

and if this weight were less than $k(n-k)$ then

$$(k-m)((m-1)(n-k)-m) < 0,$$

$$\text{i.e. } m < \frac{n-k}{n-k-1} \text{ or } m > k.$$

Since $\frac{n-k}{n-k-1} \leq 2$ for $n \geq 2k > k \geq 2$, the first solution is invalid. The second solution is invalid as before. Hence any vector in C has weight at least $k(n-k)$, and since each incidence vector has this weight, it follows that the minimum weight is $k(n-k)$. Since k and n are both even, C is doubly-even.

For $k = 4$ and $n = 8$, define a vector $v(\{a_1, a_1'\}|\{a_2, a_2'\}|\{a_3, a_3'\}|\{a_4, a_4'\})$ by

$$v(\{a_1, a_1'\}|\{a_2, a_2'\}|\{a_3, a_3'\}|\{a_4, a_4'\}) = \sum_{x_i \in \{a_i, a_i'\}} v^{\{x_1, x_2, x_3, x_4\}}. \tag{7.7}$$

Then it is easily established that $(v(\{a_1, a_1'\}|\{a_2, a_2'\}|\{a_3, a_3'\}|\{a_4, a_4'\}), u) = 0$ for each $u \in U \cup V \cup W$, and since $U \cup V \cup W$ is a basis for $C^\perp$, $v(\{a_1, a_1'\}|\{a_2, a_2'\}|\{a_3, a_3'\}|\{a_4, a_4'\}) \in C$. The weight of such a vector is $2^4 = 16$, and since the incidence vectors also have this weight, C has $\frac{\binom{8}{2}\binom{6}{2}\binom{4}{2}}{4!} = 105$ additional minimum words. With the exception of the trivial case when $k = 2$ and $n = 4$, for no other $n = 2k$ does such a partitioning result in a minimum word since $2^k = k^2$ only if $k = 2$ or 4.

Finally, the automorphism group of C needs to be considered. If $n > 2k$ and $J(n, k) \neq J(6, 2)$, then the minimum words of $C^\perp$ are of the form $w(\{a_1, a_2, \ldots, a_{k+1}\}), \{a_1, a_2, \ldots, a_{k+1}\} \subseteq \Omega$, and hence any $\sigma \in \mathrm{Aut}(C)$ induces a permutation on $\Omega^{\{k+1\}}$. Since σ also preserves incidence of points on words of $C^\perp$, a similar argument as used in Theorem 6.2.11 can be used to show that $\mathrm{Aut}(C) = S_n$.

In [17] it is shown that in the case of $J(6, 2), \mathrm{Aut}(C) = PGL_4(2) \cong A_8$. If $n = 2k$, then the minimum words are of the form $w(\{a_1, a_2, \ldots, a_{k+1}\}), \{a_1, a_2, \ldots, a_{k+1}\} \subseteq \Omega$, and $v(\{b_1, b_2, \ldots, b_{k-1}\}), \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega$. Hence any $\sigma \in \mathrm{Aut}(C)$ can either permute the elements of $\{v(\{b_1, b_2, \ldots, b_{k-1}\})\colon \{b_1, b_2, \ldots, b_{k-1}\} \subseteq \Omega\}$ which in turn induces a permutation on $\{w(\{a_1, a_2, \ldots, a_{k+1}\})\colon \{a_1, a_2, \ldots, a_{k+1}\}) \subseteq \Omega\}$, or it can map each $v(\{b_1, b_2, \ldots, b_{k-1}\})$ to $w(\Omega \setminus \{b_1, b_2, \ldots, b_{k-1}\})$, and then permute the elements of $\{w(\{a_1, a_2, \ldots, a_{k+1}\}) : \{a_1, a_2, \ldots, a_{k+1}\} \subseteq \Omega\}$. Hence if $n = 2k$, then $\mathrm{Aut}(C) = S_n \times Z_2$.

□

7.3 Permutation Decoding sets for C

While the automorphism group of C provides the base for membership of a PD-set for C, knowledge about the nature of the information positions and the subsequent action of the automorphism group determines this membership.

In Proposition 7.2.4 the points

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

have been identified as information points for C if $k \geq 2$ and $n \geq 6$ are both even. In this case C corrects $\dfrac{k(n-k)-2}{2}$ errors, and if $\dfrac{k(n-k)-2}{2} \geq 3$, then $k \geq 4$ and $n \geq 6$. Since in addition, $n \geq 2k$ for $J(n,k)$ if n is even, $n \geq 8$. Note that if $n = 2k$, then by Proposition 7.2.4, $\mathrm{Aut}(C) \cong S_{2k} \times Z_2$, but since S_{2k} is isomorphic to a subgroup of $S_{2k} \times Z_2$, the elements of S_{2k} are also potential elements of a PD-set for C. The following result is a simple, yet apt, demonstration of the fact that suitably chosen information positions greatly simplify the determination of a PD-set.

Theorem 7.3.1. *Let $\mathcal{I}$ denote the points*

$P_1 = \{2,3,\ldots,k,n\},\ P_2 = \{2,3,\ldots,k-1,k+1,n\},\ldots,\ P_{n-k} = \{2,3,\ldots,k-1,n-1,n\},$

$P_{n-k+1} = \{2,3,\ldots,k-2,k,k+1,n\},\ldots,\ P_{\binom{n-k+1}{2}} = \{2,3,\ldots,k-2,n-2,n-1,n\},\ldots,$

$P_{\binom{n-3}{k-2}} = \{2,n-k+2,n-k+3,\ldots,n\},\ P_{\binom{n-3}{k-2}+1} = \{3,4,\ldots,k+1,n\},\ldots,$

$P_{\binom{n-2}{k-1}-1} = \{n-k,n-k+2,n-k+3,\ldots,n\},\ P_{\binom{n-2}{k-1}} = \{n-k+1,n-k+2,\ldots,n\},$

where $k \geq 4, n \geq 8$ and $n \geq 2k$. Then

$$\mathcal{S} = \{(n,i)(j,1) :\ 1 \leq i \leq n,\ 1 \leq j \leq n-k+1\}$$

is a 3-PD-set for C with $\mathcal{I}$ as the information positions.

Proof: Let

$\mathcal{C}_1 = \{\{1,2,\ldots,k\},\ \{1,2,\ldots,k-1,k+1\},\ldots,\{1,2,\ldots,k-1,n-1\},\ \{1,2,\ldots,k-2,k,k+1\},\ldots,\{1,2,\ldots,k-2,k,n-1\},\ldots,\{1,n-k+1,n-k+2,\ldots,n-1\}\},$

$\mathcal{C}_2 = \{\{1,2,\ldots,k-1,n\},\ \{1,2,\ldots,k-2,k,n\},\ldots,\{1,2,\ldots,k-2,n-1,n\},\ \{1,2,\ldots,k-$

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

and

$\mathcal{C}_3 = \{\{2, 3, \ldots, k+1\},\ \{2, 3, \ldots, k, k+2\}, \ldots, \{2, 3, \ldots, k, n-1\},\ \{2, 3, \ldots, k-1, k+1, k+2\}, \ldots, \{2, 3, \ldots, k-1, n-2, n-1\}, \ldots, \{2, n-k+1, n-k+2, \ldots, n-1\},\ \{3, 4, \ldots, k+2\}, \ldots, \{3, n-k+1, n-k+2, \ldots, n-1\}, \ldots, \{n-k-1, n-k+1, \ldots, n-1\},\ \{n-k, n-k+1, \ldots, n-1\}\}.$

Furthermore, suppose that the 3 errors occur at $\mathcal{E}$.

Case(i): $\mathcal{E} \subseteq \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$

The identity, 1_{S_n}, will keep $\mathcal{E}$ fixed.

Case(ii): $\mathcal{E} \subseteq \mathcal{I}$

Then $(n, 1)$ will map $\mathcal{E}$ into $\mathcal{C}_1$.

Case(iii): $\mathcal{E} \subseteq \mathcal{I} \cup \mathcal{C}_2,\ \mathcal{E} \cap \mathcal{I} \neq \emptyset,\ \mathcal{E} \cap \mathcal{C}_2 \neq \emptyset$

Then $(n, 1)$ will map the points in $\mathcal{E} \cap \mathcal{I}$ into $\mathcal{C}_1$, and keep those in $\mathcal{E} \cap \mathcal{C}_2$ fixed.

Case(iv): $\mathcal{E} \subseteq \mathcal{I} \cup \mathcal{C}_3,\ \mathcal{E} \cap \mathcal{I} \neq \emptyset,\ \mathcal{E} \cap \mathcal{C}_3 \neq \emptyset$

Then $(n, 1)$ will act in a similar way as in Case (iii).

Case(v): $\mathcal{E} \subseteq \mathcal{I} \cup \mathcal{C}_1,\ \mathcal{E} \cap \mathcal{I} \neq \emptyset,\ \mathcal{E} \cap \mathcal{C}_1 \neq \emptyset$

If $\mathcal{E} \cap \mathcal{I} = \{\{e_1, e_2, \ldots, e_{k-1}, n\}\}$ where $e_1 < e_2 < \cdots < e_{k-1}$, then $(e_1, 1)$ will map $\{e_1, e_2, \ldots, e_{k-1}, n\}$ into $\mathcal{C}_2$, and the points in $\mathcal{E} \cap \mathcal{C}_1$ will either remain fixed or be mapped into $\mathcal{C}_3$. If, on the other hand, $\mathcal{E} \cap \mathcal{C}_1 = \{\{1, e'_1, e'_2, \ldots, e'_{k-1}\}\}$ where $e'_1 < e'_2 < \cdots < e'_{k-1}$, then $(n, 1)(e'_1, 1)$ will map $\{1, e'_1, e'_2, \ldots, e'_{k-1}\}$ into $\mathcal{C}_2$, and the points in $\mathcal{E} \cap \mathcal{I}$ will be mapped into $\mathcal{C}_1$ or $\mathcal{C}_3$.

Case(vi): $\mathcal{E} \subseteq \mathcal{I} \cup \mathcal{C}_2 \cup \mathcal{C}_3,\ \mathcal{E} \cap \mathcal{I} \neq \emptyset,\ \mathcal{E} \cap \mathcal{C}_2 \neq \emptyset,\ \mathcal{E} \cap \mathcal{C}_3 \neq \emptyset$

Then $(n, 1)$ will map the point in $\mathcal{E} \cap \mathcal{I}$ into $\mathcal{C}_1$, and keep those in $\mathcal{E} \cap (\mathcal{C}_2 \cup \mathcal{C}_3)$ fixed.

Case(vii): $\mathcal{E} \subseteq \mathcal{I} \cup \mathcal{C}_1 \cup \mathcal{C}_3,\ \mathcal{E} \cap \mathcal{I} \neq \emptyset,\ \mathcal{E} \cap \mathcal{C}_1 \neq \emptyset,\ \mathcal{E} \cap \mathcal{C}_3 \neq \emptyset$

If $\mathcal{E} \cap \mathcal{I} = \{\{e_1, e_2, \ldots, e_{k-1}n\}\}$ where $e_1 < e_2 < \cdots < e_{k-1}$, then $(e_1, 1)$ will map $\{e_1, e_2, \ldots, e_{k-1}, n\}$ into $\mathcal{C}_2$, the point in $\mathcal{E} \cap \mathcal{C}_1$ will either remain fixed or be mapped into $\mathcal{C}_3$, and the one in $\mathcal{E} \cap \mathcal{C}_3$ will either remain fixed or be mapped into $\mathcal{C}_1$.

Case(viii): $\mathcal{E} \subseteq \mathcal{I} \cup \mathcal{C}_1 \cup \mathcal{C}_2,\ \mathcal{E} \cap \mathcal{I} \neq \emptyset,\ \mathcal{E} \cap \mathcal{C}_1 \neq \emptyset,\ \mathcal{E} \cap \mathcal{C}_2 \neq \emptyset$

Now $|\cup(\mathcal{E} \cap (\mathcal{I} \cup \mathcal{C}_2))| \leq 2k - 1 \leq n - 1$, and hence there exists $a \in \Omega$ such that $a \notin \cup(\mathcal{E} \cap (\mathcal{I} \cup \mathcal{C}_2))$. Then (n, a) will map the point in $\mathcal{E} \cap \mathcal{I}$ into $\mathcal{C}_3$, the one in $\mathcal{E} \cap \mathcal{C}_2$ into $\mathcal{C}_1$, and the one in $\mathcal{E} \cap \mathcal{C}_1$ will either remain fixed or be mapped into $\mathcal{C}_2$.

Since $|\mathcal{E}| = 3$, there are no further cases to consider, and hence $\mathcal{S}$ is a 3-PD-set for C. $\square$

In Proposition 7.2.3 the points
$\{1, 2, \ldots, k-1, n\},\ \{1, 2, \ldots, k-2, k, n\}, \ldots, \{1, 2, \ldots, k-2, n-1, n\},\ \{1, 2, \ldots k-3, k-1, k, n\}, \ldots, \{1, 2, \ldots, k-3, n-2, n-1, n\}, \ldots, \{1, n-k+2, n-k+3, \ldots, n\}, \ldots, \{n-k+1, n-k+2, \ldots, n\}$
have been identified as information positions for C if $k \geq 2$ is even and $n \geq 5$ is odd. Note that C corrects $\dfrac{n-k-1}{2}$ errors, and if $3 \leq \dfrac{n-k-1}{2}$, then $n \geq k+7$. Also, $n > 2k$ for $J(n, k)$ if n is odd. Hence if C corrects 3 errors, then $n \geq \max\{k+7, 2k+1\}$ which implies that $n \geq k+7$ if $k = 2$ or 4, and $n > 2k$ otherwise. If $k = 2$, it is easily seen that $\{(n, i) :\ 1 \leq i \leq n\}$ is a 3-PD-set for C with the information positions as given above. Since the last basis element is $v(\{n-k+1, n-k+2, \ldots, n-1\})$, interchanging the points $\{n-k+1, n-k+2, \ldots, n\}$ and $\{n-k, n-k+1, \ldots, n-1\}$ leaves the generator matrix in standard form. Subsequently, the following result is obtained:

Theorem 7.3.2. *Let $\mathcal{I}$ denote the points*

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

$P_{n-k+2} = \{1, 2, \ldots, k-3, k-1, k, n\}, \ldots,\ P_{n-k+1+\binom{n-k+1}{2}} = \{1, 2, \ldots, k-3, n-2, n-1, n\}, \ldots, P_{\binom{n-k+2}{k-2}} = \{1, n-k+2, n-k+3, \ldots, n\}, \ldots, P_{\binom{n-1}{k-1}-1} = \{n-k, n-k+2, n-k+3, \ldots, n\},$

$P = P_{\binom{n-1}{k-1}} = \{n-k, n-k+1, \ldots, n-1\},$

where $k \geq 6$ is even and $n > 2k$ is odd. Then

$$\mathcal{S} = \{(n, i_1)(n-1, i_2)\ldots(n-k, i_{k+1}) :\ 1 \leq i_j \leq n-j+1,\ 1 \leq j \leq k+1\}$$

is a 3-PD-set for C with $\mathcal{I}$ as the information positions.

Proof: Let

$$Q = \{n-k+1, n-k+2, \ldots, n\}, \quad (Q \in \mathcal{P} \setminus \mathcal{I}),$$

and suppose that the $3 \leq \dfrac{n-k-1}{2}$ errors occur at $\mathcal{E}$.

Case(I): $\mathcal{E} \subseteq \mathcal{P} \setminus \mathcal{I}$

The identity, $1_{S_n} \in \mathcal{S}$, and will leave $\mathcal{E}$ fixed.

Case (II): $\mathcal{E} \subseteq \mathcal{I}$

(i) there exists $a \in \Omega$ such that $a \notin \cup\mathcal{E}$

(a) $P \notin \mathcal{E}$

If $a < n-k$, then (n, a) will map $\mathcal{E}$ into the check positions. The same applies if $a = n-k$, since $Q \notin \mathcal{I}$. Now if $n-k+1 \leq a \leq n-1$ and $\{e_1, e_2, \ldots, e_{k-1}, n\} \in \mathcal{E}$ where $\{e_1, e_2, \ldots, e_{k-1}\} = P \setminus \{a\}$, then $(n, a)(n-1, b)$ for some $b < n-k$, will do. Otherwise, if $n-k+1 \leq a \leq n-1$ and $\{e_1, e_2, \ldots, e_{k-1}, n\} \notin \mathcal{E}$ where $\{e_1, e_2, \ldots, e_{k-1}\} = P \setminus \{a\}$, then (n, a) will do.

(b) $P \in \mathcal{E}$

Then $a < n-k$, and hence $(n, a)(n-1, b)$ for some $b \neq a,\ b < n-k$, will map $\mathcal{E}$ into the check positions.

(ii) $\cup\mathcal{E} = \Omega$

(a) $P \notin \mathcal{E}$

Suppose that for each $a < n-k$, $a \in e, e'$ for some $e, e' \in \mathcal{E}$. Then the maximum number of elements of Ω that can still be accommodated in $\mathcal{E}$ is $3(k-1)-2(n-k-1)$. Now since $n > 2k$ for $J(n,k), n$ odd, $3(k-1)-2(n-k-1) < k-1$, and since $|P| = k, \cup\mathcal{E} \neq \Omega$. Hence there exists $a \in \Omega,\ a < n-k$, such that $a \in e$ for some $e \in \mathcal{E}$, but $a \notin e'$ for any other $e' \in \mathcal{E}$. If $e = \{e_1, e_2, \ldots, e_{k-1}, n\}$, where $e_1 < e_2 < \cdots < e_{k-1}$, then $(n,a)(n-1,e_{k-1})(n-2,e_{k-2})\ldots(n-k+1,e_1)$ will map $\mathcal{E}$ into the check positions.

(b) $P \in \mathcal{E}$

Since $|\cup(\mathcal{E} \setminus P)| \leq 2(k-1)+1 < n-1$, there exists $a \in \Omega$ such that $a \notin e$ for any $e \in \mathcal{E} \setminus P$. If $a < n-k$, then $(n,a)(n-1,b)$ for some $b < n-k$ will do. If $a = n-k$, then (n,a) will do. Finally, if $n-k+1 \leq a \leq n-1$ and $\{e_1, e_2, \ldots, e_{k-1}, n\} \in \mathcal{E}$ where $\{e_1, e_2, \ldots, e_{k-1}\} = P \setminus \{a\}$, then $\cup\mathcal{E} \neq \Omega$. Hence $(n,a)(n-1,e_{k-1})(n-2,e_{k-2})\ldots(n-k+1,e_1)$, where $(n,a)(P) = \{e_1, e_2, \ldots, e_{k-1}, n\}$ and $e_1 < e_2 < \cdots < e_{k-1}$, will do.

Case (III): $\mathcal{E} \cap \mathcal{I} \neq \emptyset,\ \mathcal{E} \cap \mathcal{P} \setminus \mathcal{I} \neq \emptyset$

(i) there exists $a \in \Omega$ such that $a \notin \cup\mathcal{E}$

(a) $P \notin \mathcal{E}, Q \notin \mathcal{E}$

If $a < n-k$, then (n,a) will map $\mathcal{E}$ into the check positions. Similarly for $a = n-k$, since $Q \notin \mathcal{I}$. Now if $n-k+1 \leq a \leq n-1$ and $\{e_1, e_2, \ldots, e_{k-1}, n\} \in \mathcal{E}$ where $\{e_1, e_2, \ldots, e_{k-1}\} = P \setminus \{a\}$, then $(n,a)(n-1,b)$ for some $b < n-k$, will do. Otherwise, if $n-k+1 \leq a \leq n-1$ and $\{e_1, e_2, \ldots, e_{k-1}, n\} \notin \mathcal{E}$, then (n,a) will do.

(b) $P \notin \mathcal{E}, Q \in \mathcal{E}$

Since $Q \in \mathcal{E},\ a < n-k+1$. If $a = n-k$, then $(n,a)(n-1,b)$ for some $b < n-k$ will do, and if $a < n-k$, then (n,a) will do.

(c) $P \in \mathcal{E}, Q \notin \mathcal{E}$

Since $P \in \mathcal{E},\ a = n$ or $a < n - k$. If $a = n$, then $(n-1, b)$ for some $b < n - k$ will do, and if $a < n - k$, then $(n, a)(n-1, b)$ for some $b \neq a,\ b < n - k$, will do.

(d) $P \in \mathcal{E}, Q \in \mathcal{E}$

Then $a < n - k$. If $\mathcal{E} \cap (\mathcal{I} \setminus P) \neq \emptyset$, then $(n, a)(n-1, b)$ for some $b < n - k$ will do. Otherwise, $(n - k, a)$ will do.

(ii) $\cup\mathcal{E} = \Omega$

(a) $P \notin \mathcal{E}, Q \notin \mathcal{E}$

If $|\mathcal{E} \cap \mathcal{I}| = 2$, then $|\cup(\mathcal{E} \cap \mathcal{I})| \leq 2(k-1)+1 < n-1$. Hence there exists $a \in \Omega$ such that $a \notin \cup(\mathcal{E} \cap \mathcal{I})$. Since $a \in \mathcal{E} \setminus \mathcal{I}$, $(n, a)(n-1, e_{k-1})(n-2, e_{k-2}) \ldots (n - k + 1, e_1)$, where $(n, a)(\mathcal{E} \setminus \mathcal{I}) = \{e_1, e_2, \ldots, e_{k-1}, n\}$ and $e_1 < e_2 \cdots < e_{k-1}$, will map $\mathcal{E}$ into the check positions. Otherwise, if $\mathcal{E} \cap \mathcal{I} = \{e'_1, e'_2, \ldots, e'_{k-1}, n\}$, where $e'_1 < e'_2 < \cdots < e'_{k-1}$, then $(n-1, e'_{k-1})(n-2, e'_{k-2}) \ldots (n-k+1, e'_1)$ will do.

(b) $P \notin \mathcal{E}, Q \in \mathcal{E}$

Then since $\cup\mathcal{E} = \Omega,\ |\mathcal{E} \cap \mathcal{I}| \neq 2$. Hence $|(\mathcal{E} \setminus \{Q\}) \cap (\mathcal{P} \setminus \mathcal{I})| = 1$. Now since any two points have a maximum of $2k < n$ elements, it follows that there exists $a \in \Omega$ such that $a \notin (\mathcal{E} \cap \mathcal{I}) \cup ((\mathcal{E} \setminus \{Q\}) \cap (\mathcal{P} \setminus \mathcal{I}))$. If $a < n - k$, then (n, a) will do. If $a = n - k$, then $(n, a)(n-1, b)$ for some $b < n - k$ will do. Otherwise, if $n - k + 1 \leq a \leq n - 1$ and $\{e_1, e_2, \ldots, e_{k-1}, n\} \in \mathcal{E}$, where $\{e_1, e_2, \ldots, e_{k-1}\} = P \setminus \{a\}$, then $(n, a)(n-1, b)$ for some $b < n - k$, will do. However, if $n-k+1 \leq a \leq n-1$ and $\{e_1, e_2, \ldots, e_{k-1}, n\} \notin \mathcal{E}$, then (n, a) will do.

(c) $P \in \mathcal{E}, Q \notin \mathcal{E}$

Then $(E \setminus \{P\}) \cap \mathcal{I} \neq \emptyset$ otherwise $n \notin \cup\mathcal{E}$. Hence $|E \cap (\mathcal{P} \setminus \mathcal{I})| = |(\mathcal{E} \setminus \{P\}) \cap \mathcal{I}| = 1$, and there exists $a \in \Omega$ such that $a \notin (\mathcal{E} \cap (\mathcal{P} \setminus \mathcal{I})) \cup ((\mathcal{E} \setminus \{P\}) \cap \mathcal{I})$. If $a \leq n-k$, then (n, a) will do. If $n-k+1 \leq a \leq n-1$ and $\{e_1, e_2, \ldots, e_{k-1}, n\} \in \mathcal{E}$ where $\{e_1, e_2, \ldots, e_{k-1}\} = P \setminus \{a\}$, then $(n, a)(n-1, b)$ for some $b < n - k$, will do.

Otherwise, if $n-k+1 \leq a \leq n-1$ and $\{e_1, e_2, \ldots, e_{k-1}, n\} \notin \mathcal{E}$, then (n, a) will do.

(d) $P \in \mathcal{E}, Q \in \mathcal{E}$

Then $(\mathcal{E} \setminus \{P\}) \cap \mathcal{I} = \emptyset$, otherwise $|\cup \mathcal{E}| \leq k-1+k+1 < n$. Hence $\mathcal{E} \cap \mathcal{I} = P$, and $(n-k, b)$ for some $b < n-k$, will map $\mathcal{E}$ into the check positions. $\square$

Note that if $k = 4, n \geq k+7$, and the information positions are as given in Theorem 7.3.1, then by similar reasoning as above, $\mathcal{S}$ is also a 3-PD-set for C.

The codes described in this chapter are the generalisations of the codes described in [17] and in [35]. However, PD-sets which exploit the full error-correcting capacity of the codes were not obtained - there has been a trade-off between generalising the size of the subset (k as opposed to 2 and 3), and consequently increasing the algebraic complexity of the code, and obtaining full PD-sets. However, the partial PD-sets may still be useful if the likelihood of more than three errors occurring during transmission is small.

Chapter 8

Binary Codes and Permutation Decoding sets from the graph products of Cycles

The class of graphs is a special class of relational structures, and as in the case of other classes of relational structures, the construction of products is permitted. However, Sabidussi [37] cautions that "simply to imitate what happens elsewhere would hardly be a justifiable motivation for defining graph products". Graph products were constructed in such a way that certain properties of the product are a consequence of the associated properties in the factors. These properties are varied and include the connectivity, the adjacency matrix and the automorphism group. The most important graph products appearing in the literature are the cartesian product, the categorical product, the lexicographic product and the strong product. All four products have as their vertex-set the cartesian product of the vertex-sets of the factors. In the case of the cartesian product the definition of adjacency is motivated by the need to minimize the distance between two vertices, whereas in the case of the categorical product the definition of adjacency ensures that the projections from the product to its factors are homomorphisms. The strong product is an amalgamation of the cartesian and the categorical product when there are

only two factors. The lexicographic product differs from the other three products in that it is not commutative, and hence an order has to be imposed on the set indexing the factors.

In this chapter the codes generated by the various graph products of the n-cycles C_n, will be discussed. The choice of the n-cycles was motivated by the fact that they are relatively straightforward graphs, the automorphism groups of which are equally straightforward and which it was thought would feature prominently in the automorphism groups of the various products. If $n = 2$, then the code generated by the categorical and the lexicographic product of m copies of C_n is the full space $F_2^{n^m}$. For the cartesian product, however, this is only the case when m is odd - when m is even then the code is an $[n^m, n^{m-1}, m]$ self-dual code. Furthermore, if n is odd, then the lexicographic product of m copies of C_n generate the dual code of the span of the $\boldsymbol{j}$-vector. With regard to the categorical product, m copies of C_n generate an $[n^m, (n-1)^m, 2^m]$ code of which the dual is an $[n^m, n^m - (n-1)^m, n]$ code if n is odd, and an $[n^m, (n-2)^m, 2^m]$ code of which the dual is an $[n^m, n^m - (n-2)^m, \frac{n}{2}]$ code if n is even. Finally, if $n = 2^k$ where $k \geq 2$, then it is conjectured that the cartesian product of m copies of C_n generate an $[n^m, (n-2).n^{m-1}, 2m]$ code which contains its dual.

With regard to permutation decoding, PD-sets were found for the codes generated by the categorical product of 2 and 3 copies of C_n both when n is odd and when it is even. PD-sets capable of correcting as many errors as there are copies of C_n were also found for this product both for when n is odd and when it is even. 2-PD-sets were also found for the code generated by the cartesian product of m copies of C_2 where m is even and $m \geq 4$.

The discussion is formally introduced by way of formal definitions and some graph-theoretical considerations of the various graph products as given in [37].

8.1 Graph products and their basic properties

Historically, the definition of the cartesian product preceded that of the other products. As mentioned earlier, the definition of adjacency was motivated by the need to minimize the distance between two vertices i.e. to have them as similar as possible.

Definition 8.1.1. *Let G_i, $i \in I$, be a non-empty family of graphs. The* **cartesian product***, denoted by $\Box_{i\in I}G_i$, is the graph which has as its vertex-set the cartesian product of the vertex-sets of G_i, $i \in I$, and any two vertices u and v constitute an edge $[u, v]$ if and only if there exists $j \in I$ such that the projections of u and v onto their jth coordinates, u_j and v_j respectively, constitute an edge $[u_j, v_j]$ of G_j, while their projections onto the remaining coordinates are respectively equal.*

The use of the symbol $\Box$ is derived from the observation that the cartesian product of two copies of C_2 is the square C_4. (This observation will prove useful in subsequent sections.)

The cartesian product is both associative and commutative, and has an identity element, namely the graph consisting of a singleton. Furthermore, if G and H are both regular, then $G\Box H$ is regular - in particular, if each vertex in G and H has degree r and s respectively, then the degree of each vertex in $G\Box H$ is $r + s$. Analogous statements apply to the connectedness of G and H. Examples of cartesian products are:

(a) the **hypercubes** $Q_d := \Box_{i=1}^{d} C_2$,

(b) the **tori** $T_{n_1,n_2,\ldots n_m} := C_{n_1}\Box C_{n_2} \ldots \Box C_{n_m}$, where $n_i \geq 3$ for each i, and $m \geq 2$,

(c) the **prisms** $C_n\Box C_2$, where $n \geq 3$.

Although details will not be provided here ([37] can be consulted), it may be the case that the projections from the cartesian product onto its factors are not homomorphisms - in fact, homomorphisms from the cartesian product onto its factors may not even exist. To circumvent this problem, an alternative definition of adjacency is required.

Definition 8.1.2. *Let $G_i, i \in I$, be a non-empty family of graphs. The* **categorical product**, *denoted by $\prod_{i\in I} G_i$, is the graph which has as its vertex-set the cartesian product of the vertex-sets of G_i, $i \in I$, and any two vertices u and v constitute an edge $[u, v]$ if and only if for all $i \in I$ the projections of u and v onto their ith coordinates, u_i and v_i respectively, constitute an edge $[u_i, v_i]$ of G_i.*

Evidently, adjacency as defined for the categorical product appears to be more natural than that as defined for the cartesian product. When limited to two factors, the union of these two products result in the strong product, the definition of which is as follows:

Definition 8.1.3. *Let $G_i \in i \in I$, be a non-empty family of graphs. The* **strong product**, *denoted by $\boxtimes_{i\in I} G_i$, is the graph which has as its vertex-set the cartesian product of the vertex-sets of $G_i, i \in I$, and any two vertices u and v constitute an edge $[u, v]$ if and only if there exists $J \subset I$, $J \neq \emptyset$, such that for all $j \in J$ the projections of u and v onto their jth coordinates, u_j and v_j respectively, constitute an edge $[u_j, v_j]$ of G_j, while their projections onto the remaining coordinates are respectively equal.*

The symbol $\boxtimes$ originates from the fact that the strong product of two copies of C_2 is the complete graph on four vertices. In general, the strong product of two complete graphs on r and s vertices is a complete graph on rs vertices. Hence, as the name suggests, strong products are "strongly" connected.

Unlike the preceding products, the following product is not commutative. In order to identify an order amongst the factors, the index set I has to be totally ordered.

Definition 8.1.4. *Let G_i, $i \in I$, be a family of graphs, where I is a non-empty set totally ordered by the relation $\leq$. The* **lexicographic product**, *denoted by $[\ \ ]_{i\in I} G_i$, is the graph which has as its vertex-set the cartesian product of the vertex-sets of $G_i, i \in I$, and any two vertices u and v constitute an edge $[u, v]$ if and only if there exists $j \in I$ such that the projections of u and v onto their jth coordinates, u_j and v_j respectively, constitute an edge $[u_j, v_j]$ of G_j, while their projections onto the preceding coordinates are respectively*

equal.

In the case of two factors, G and H, the lexicographic product $G[H]$ is obtained by replacing each vertex of G by a copy of H, and hence the notation underlines this notion of "composition" of graphs. As in the case of the cartesian product, $G[H]$ is regular if and only if both G and H are regular. However, the connectedness of $G[H]$ is determined only by $G - G[H]$ is connected if and only if G is connected. The lexicographic product of any family $G_i, i \in I$, also commutes with the operation of complementation i.e. $\overline{[\ ]_{i\in I} G_i} = [\ ]_{i\in I} \overline{G}_i$. As a final comment on the graph-theoretical properties of the lexicographic product, it is noteworthy that $[\ ]_{i\in I} G_i$ contains $\boxtimes_{i\in I} G_i$ as a spanning subgraph, which in turn contains both $\square_{i\in I} G_i$ and $\prod_{i\in I} G_i$ as spanning subgraphs. Now that a graph-theoretical foundation has been established for what follows in this chapter, the discussion shifts to the main area of focus.

8.2 Binary Codes from the graph products of n-Cycles

Let n be a positive integer. For the sake of clarity, an n-cycle denoted by C_n, is a graph of which the vertex-set is the set $\{0, 1, \ldots, n-1\}$, and any two vertices u and v constitute an edge $[u, v]$ if and only if $v = (u + 1) \bmod n$ or $v = (u - 1) \bmod n$. It is easily checked that the code generated by the adjacency matrix of C_n is an $[n, n-1, 2]$ code if n is odd, and an $[n, n-2, 2]$ code if n is even.

Now let m be a positive integer, and let $\square_{i=1}^{m} C_n, \prod_{i=1}^{m} C_n$ and $[\ ]_{i=1}^{m} C_n$ denote the cartesian, categorical and lexicographic products respectively of m copies of C_n which all have as their vertex-set the set $\mathcal{P}$, the n^m elements of $\{0, 1, \ldots, n-1\}^m$. $\mathcal{P}$ also forms the point set of the respective 1-designs where for each point $(a_1, a_2, \ldots, a_m) \in \mathcal{P}$, the corresponding blocks denoted by $\overline{(a_1, a_2, \ldots, a_m)_{\square}}$, $\overline{(a_1, a_2, \ldots, a_m)_{\Pi}}$ and $\overline{(a_1, a_2, \ldots, a_m)_{[\ ]}}$ are defined as follows:

$\overline{(a_1, a_2, \ldots, a_m)_{\square}} = \{(x_1, x_2, \ldots, x_m) :$ there exists $j \in \{1, 2, \ldots, m\}$ such that x_j is adjacent to a_j in C_n and $x_i = a_i,$ for all $i \in \{1, 2, \ldots, m\} \setminus \{j\}\}$,

$\overline{(a_1, a_2, \ldots, a_m)_{\Pi}} = \{(x_1, x_2, \ldots, x_m) : x_i$ is adjacent to a_i in $C_n,$ for all $i \in \{1, 2, \ldots, m\}\}$, and

$\overline{(a_1, a_2, \ldots, a_m)_{[\ ]}} = \{(x_1, x_2, \ldots, x_m) :$ there exists $j \in \{1, 2, \ldots, m\}$ such that x_j is adjacent to a_j in C_n and $x_i = a_i,$ for all $i < j\}$.

The incidence vectors corresponding to these blocks are then given by

$$v^{\overline{(a_1,a_2,\ldots,a_m)_{\square}}} = \sum_{x_1=(a_1\pm1) \bmod n} v^{(x_1,a_2,a_3,\ldots,a_m)} + \sum_{x_2=(a_2\pm1) \bmod n} v^{(a_1,x_2,a_3,a_4,\ldots,a_m)} + \cdots + \sum_{x_m=(a_m\pm1) \bmod n} v^{(a_1,a_2,\ldots,a_{m-1},x_m)}, \tag{8.1}$$

$$v^{\overline{(a_1,a_2,\ldots,a_m)_{\Pi}}} = \sum_{x_1=(a_1\pm1) \bmod n} \sum_{x_2=(a_2\pm1) \bmod n} \cdots \sum_{x_m=(a_m\pm1) \bmod n} v^{(x_1,x_2,\ldots,x_m)} \tag{8.2}$$

$$\begin{aligned} v^{\overline{(a_1,a_2,\ldots,a_m)_{[\ ]}}} = & \sum_{x_1=(a_1\pm1) \bmod n} \sum_{x_2\in\{0,1,\ldots,n-1\}} \cdots \sum_{x_m\in\{0,1,\ldots,n-1\}} v^{(x_1,x_2,\ldots,x_m)} \\ & + \sum_{x_2=(a_2\pm1) \bmod n} \sum_{x_3\in\{0,1,\ldots,n-1\}} \cdots \sum_{x_m\in\{0,1,\ldots,n-1\}} v^{(a_1,x_2,x_3,\ldots,x_m)} \\ & + \cdots + \sum_{x_m=(a_m\pm1) \bmod n} v^{(a_1,a_2,\ldots,a_{m-1},x_m)}. \end{aligned} \tag{8.3}$$

Attention is once again drawn to the fact that the use of the notation is somewhat sloppy, but is justified as in the previous chapters.

In all the results that follow it is assumed that $m, n \geq 2$. $C_{\square}, C_{\Pi}$ and $C_{[\ ]}$ will denote the binary code of $\square_{i=1}^{m} C_n$, $\prod_{i=1}^{m} C_n$ and $[\ ]_{i=1}^{m} C_n$ respectively, and $C_{\square}^{\perp}, C_{\Pi}^{\perp}$ and $C_{[\ ]}^{\perp}$ their respective duals.

The respective codes obtained when $n = 2$ is a natural point at which to start the investigation.

Lemma 8.2.1. *If $n = 2$, then $C_\Pi = F_2^{n^m}$.*

Proof: This is a direct consequence of the fact that for any point $(a_1, a_2, \ldots, a_m) \in \{0,1\}^m$,

$$v^{(a_1,a_2,\ldots,a_m)} = v^{\overline{(a_1',a_2',\ldots,a_m')_\Pi}},$$

where $a_i' = \{0,1\} \setminus \{a_i\}$, for all $i \in \{1, 2, \ldots, m\}$. □

Lemma 8.2.2. *If $n = 2$, then $C_{[\ ]} = F_2^{n^m}$.*

Proof: Suppose that $(a_1, a_2, \ldots, a_m) \in \{0,1\}^m$, and consider the sum

$$\sum_{\substack{(x_1,x_2,\ldots,x_m)\in\{0,1\}^m \\ (x_1,x_2,\ldots,x_m)\neq(a_1,a_2,\ldots,a_m)}} v^{\overline{(x_1,x_2,\ldots,x_m)_{[\ ]}}}$$ of the incidence vectors which are incident at

$(a_1, a_2, \ldots, a_m)$. Clearly, there are $2^m - 1$ vectors in this sum. Moreover, for each $(x_1, x_2, \ldots, x_m) \neq (a_1, a_2, \ldots, a_m)$ the vectors $v^{\overline{(x_1',x_2',\ldots,x_m')}}, (x_1', x_2', \ldots, x_m') \in \{0,1\}^m$, $(x_1', x_2', \ldots, x_m') \neq (x_1, x_2, \ldots, x_m)$, are each incident at $(x_1, x_2, \ldots, x_m)$. Hence the above sum reduces to

$$\sum_{\substack{(x_1,x_2,\ldots,x_m)\in\{0,1\}^m \\ (x_1,x_2,\ldots,x_m)\neq(a_1,a_2,\ldots,a_m)}} v^{\overline{(x_1,x_2,\ldots,x_m)_{[\ ]}}}$$

$$= (2^m - 2) \sum_{\substack{(x_1,x_2,\ldots,x_m)\in\{0,1\}^m \\ (x_1,x_2,\ldots,x_m)\neq(a_1,a_2,\ldots,a_m)}} v^{(x_1,x_2,\ldots,x_m)} + (2^m - 1)v^{(a_1,a_2,\ldots,a_m)},$$

and the result follows. □

Lemma 8.2.3. *If $n = 2$, then $C_\square = F_2^{n^m}$ if m is odd, and an $[n^m, n^{m-1}, m]$ self-dual code if m is even.*

Proof: Suppose firstly that m is odd, and that $(a_1, a_2, \ldots, a_m) \in \{0,1\}^m$. Similarly as in Lemmas 8.2.1 and 8.2.2, consider the sum

$$v^{\overline{(a_1', a_2, a_3, \ldots, a_m)\Box}} + v^{\overline{(a_1, a_2', a_3, \ldots, a_m)\Box}} + \cdots + v^{\overline{(a_1, a_2, \ldots, a_{m-1}, a_m')\Box}}, a_i' = \{0,1\} \backslash \{a_i\}, \text{ for all } i \in \{1, 2, \ldots, m\},$$

of the incidence vectors which are incident at $(a_1, a_2, \ldots, a_m)$. Clearly, there are m vectors in this sum. Now suppose that $(a_1'', a_2'', \ldots, a_m'') \in \{0,1\}^m, (a_1'', a_2'', \ldots, a_m'') \neq (a_1, a_2, \ldots, a_m)$. If $(a_1'', a_2'', \ldots, a_m'')$ and $(a_1, a_2, \ldots, a_m)$ differ in one coordinate position, say $(a_1'', a_2'', \ldots, a_m'') = (a_1', a_2, a_3, \ldots, a_m)$, then none of the vectors in the above sum are incident at $(a_1'', a_2'', \ldots, a_m'')$. However, if $(a_1'', a_2'', \ldots, a_m'')$ and $(a_1, a_2, \ldots, a_m)$ differ in two coordinate positions, say $(a_1'', a_2'', \ldots, a_m'') = (a_1', a_2', a_3, \ldots, a_m)$, then the vectors $v^{\overline{(a_1', a_2, a_3, \ldots, a_m)\Box}}$ and $v^{\overline{(a_1, a_2', a_3, \ldots, a_m)\Box}}$ are incident at $(a_1'', a_2'', \ldots, a_m'')$. Finally, if $(a_1'', a_2'', \ldots, a_m'')$ and $(a_1, a_2, \ldots, a_m)$ differ in three or more coordinate positions, then once again none of the vectors in the above sum are incident at $(a_1'', a_2'', \ldots, a_m'')$. Hence the above sum reduces to

$$v^{\overline{(a_1', a_2, a_3, \ldots, a_m)\Box}} + v^{\overline{(a_1, a_2', a_3, \ldots, a_m)\Box}} + \cdots + v^{\overline{(a_1, a_2, \ldots, a_{m-1}, a_m')\Box}} = m v^{(a_1, a_2, \ldots a_m)},$$

and since m is odd, the first part of the lemma follows.

For the second part of the lemma, suppose that m is even, and consider the set of vectors $R = \{v^{\overline{(0, a_1, a_2, \ldots, a_{m-1})\Box}} : a_i \in \{0,1\}, \text{ for all } i \in \{1, 2, \ldots, m-1\}\}$. Then R spans $C_\Box$, since for $a_i' = \{0,1\} \setminus \{a_i\}, \text{ for all } i \in \{1, 2, \ldots, m-1\}$,

$$\begin{aligned} & v^{\overline{(0, a_1', a_2, a_3, \ldots, a_{m-1})\Box}} + v^{\overline{(0, a_1, a_2', a_3, \ldots, a_{m-1})\Box}} + \cdots + v^{\overline{(0, a_1, a_2, \ldots, a_{m-2}, a_{m-1}')\Box}} \\ = \; & (m-1) v^{(0, a_1, a_2, \ldots, a_{m-1})} + v^{(1, a_1', a_2, \ldots, a_{m-1})} + v^{(1, a_1, a_2', a_3, \ldots, a_{m-1})} + \cdots + v^{(1, a_1, a_2, \ldots, a_{m-2}, a_{m-1}')} \\ = \; & v^{\overline{(1, a_1, a_2, \ldots, a_{m-1})\Box}}, \end{aligned}$$

since m is even. Furthermore, if the vectors in R as well as the points in $\Box_{i=1}^m C_2$ are arranged in lexicographic order, then a matrix of the form $[A|\ I_{2^{m-1}}]$ results, thereby identifying the points

$$(1,0,0,\ldots,0), (1,0,0,\ldots,0,1), (1,0,0,\ldots,0,1,0), \ldots, (1,1,1,\ldots,1)$$

as information positions. Hence R is a basis for $C_\Box$. Clearly, $|R| = 2^{m-1}$.

With regard to the minimum weight of $C_\square$, observe that any incidence vector has weight m. Hence the minimum weight is at most m. Also, two basis vectors $v^{\overline{(0,a_1,a_2,\ldots,a_{m-1})\square}}$ and $v^{\overline{(0,a'_1,a'_2,\ldots,a'_{m-1})\square}}$ are commonly incident at two points if and only if $(0,a_1,a_2,\ldots,a_{m-1})$ and $(0,a'_1,a'_2,\ldots,a'_{m-1})$ differ in two coordinate positions. Hence minimum weight vectors will be obtained by taking linear combinations of a set of basis vectors of which any two have this property. Suppose that a linear combination of k such vectors yields a vector of weight less than m. Then

$$km - 2\left\lfloor \frac{k}{2} \right\rfloor - 2\binom{k}{2} < m,$$

i.e. $k < 1$ or $k > m-1$ if k is odd, and $k < 2$ or $k \geq m$ if k is even.

Since the maximum number of vectors in a set such as the one described above is $m-1$ if k is odd, and $m-2$ if k is even, all the possibilities for k are invalid, and it follows that the minimum weight is m. Of course, $C_\square$ has a basis of minimum weight vectors.

In order to show that $C_\square$ is self-dual, it is necessary to show that any incidence vector $v^{\overline{(a_1,a_2,\ldots,a_m)\square}}$ is in $C_\square^\perp$. So consider the inner product $(v^{\overline{(a_1,a_2,\ldots,a_m)\square}}, v^{\overline{(a'_1,a'_2,\ldots,a'_m)\square}})$ of any two incidence vectors. If $(a_1,a_2,\ldots,a_m) = (a'_1,a'_2,\ldots,a'_m)$, then since each incidence vector has weight m which is even, $(v^{\overline{(a_1,a_2,\ldots,a_m)\square}}, v^{\overline{a'_1,a'_2,\ldots,a'_m)\square}}) \equiv 0 (\mathrm{mod}\, 2)$. If $(a_1,a_2,\ldots,a_m)$ and $(a'_1,a'_2,\ldots,a'_m)$ differ in one coordinate position, then $v^{\overline{(a_1,a_2,\ldots,a_m)\square}}$ and $v^{\overline{(a'_1,a'_2,\ldots,a'_m)\square}}$ are not commonly incident at any point, and hence $(v^{\overline{(a_1,a_2,\ldots,a_m)\square}}, v^{\overline{(a'_1,a'_2,\ldots,a'_m)\square}}) = 0$. However, if $(a_1,a_2,\ldots,a_m)$ and $(a'_1,a'_2,\ldots,a'_m)$ differ in two coordinate positions, then $v^{\overline{(a_1,a_2,\ldots,a_m)\square}}$ and $v^{\overline{(a'_1,a'_2,\ldots,a'_m)\square}}$ are commonly incident at two points, and hence $(v^{\overline{(a_1,a_2,\ldots,a_m)\square}}, v^{\overline{(a'_1,a'_2,\ldots,a'_m)\square}}) \equiv 0 (\mathrm{mod}\, 2)$. For the final consideration, if $(a_1,a_2,\ldots,a_m)$ and $(a'_1,a'_2,\ldots,a'_m)$ differ in more than two coordinate positions, then $v^{\overline{(a_1,a_2,\ldots,a_m)\square}}$ and $v^{\overline{(a'_1,a'_2,\ldots,a'_m)\square}}$ are clearly not commonly incident at any point, and hence $(v^{\overline{(a_1,a_2,\ldots,a_m)\square}}, v^{\overline{(a'_1,a'_2,\ldots,a'_m)\square}}) = 0$ once again. Hence $C_\square \subseteq C_\square^\perp$. Since in addition, $\dim(C_\square^\perp) = 2^m - 2^{m-1} = 2^{m-1} = \dim(C_\square)$, it follows that $C_\square = C_\square^\perp$. $\square$

As remarked upon in Section 8.1, $C_2 \,\square\, C_2 \cong C_4$. Hence the code generated by $\square_{i=1}^m C_4 \cong \square_{i=1}^{2m} C_2$ is a $[2^{2m}, 2^{2m-1}, 2m]$ self-dual code - this code will be encountered again in a later result.

Next, the codes generated by the lexicographic product $[\ ]_{i=1}^{m} C_n$ are investigated when n is odd.

Lemma 8.2.4. *If n is odd, then $C_{[\ ]}$ is an $[n^m, n^m - 1, 2]$ code i.e $C_{[\ ]}^{\perp} = \text{span}\{\boldsymbol{j}\}$.*

Proof: Observe that for any two points $(a_1, a_2, \ldots, a_m)$, $(a_1, a_2, \ldots, a_{m-1}, a'_m)$ $\in \{0, 1, \ldots, n-1\}^m$ where $a'_m = (a_m + 2) \mod n$,

$$\begin{aligned} & v^{\overline{(a_1,a_2,\ldots,a_m)_{[\ ]}}} + v^{\overline{(a_1,a_2,\ldots,a_{m-1},a'_m)_{[\ ]}}} \\ = \ & v^{(a_1,a_2,\ldots,a_{m-1},(a_m-1) \mod n)} + v^{(a_1,a_2,\ldots,a_{m-1},(a_m+3) \mod n)} \end{aligned}$$

Then, since n is odd, the set $S = \{v^{(a_1,a_2,\ldots,a_m)} + v^{(n-1,n-1,\ldots,n-1)} : (a_1, a_2, \ldots, a_m) \in \{0, 1, \ldots, n-1\}^m, (a_1, a_2, \ldots, a_m) \neq (n-1, n-1, \ldots, n-1)\}$ is in C. The weight of each incidence vector is $2n^{m-1} + 2n^{m-2} + \cdots + 2 = \frac{2(n^m-1)}{n-1}$ which is even, and hence S spans C. S is clearly a linearly independent set, and $|S| = n^m - 1$. Now $\boldsymbol{j} \notin C$ since it has weight n^m, which is odd since n is odd, and the result follows. □

Attention is next focused on the codes generated by the categorical product $\prod_{i=1}^{m} C_n$, when n is odd, and as usual, the identification of bases for C_Π and $C_\Pi^{\perp}$ takes precedence.

Lemma 8.2.5. *If n is odd, then the set $T = \{v^{\overline{(a_1,a_2,\ldots,a_m)_\Pi}} : (a_1, a_2, \ldots, a_m) \in \{0, 1, \ldots, n-2\}^m\}$ is a basis for C_Π.*

Proof: In order to show that T spans C_Π, it is sufficient to show that each incidence vector in the set $\{v^{\overline{(a_1,a_2,\ldots,a_m)_\Pi}} : \text{there exists } i \in \{1, 2, \ldots, m\} | a_i = n-1\}$ is a linear combination of vectors in T : it can easily be checked that for $(a_1, a_2, \ldots, a_m)$ where for some $1 \leq i \leq m,\ a_i = n-1$ but $a_j \neq n-1,$ for all $j \in \{1, 2, \ldots, m\} \setminus \{i\}$,

$$\sum_{x=0}^{n-2} v^{\overline{(a_1,a_2,\ldots,a_{i-1},x,a_{i+1},a_{i+2},\ldots,a_m)_\Pi}}$$

$$= 2 \sum_{x_1=(a_1\pm1)\bmod n} \sum_{x_2=(a_2\pm1)\bmod n} \cdots \sum_{x_{i-1}=(a_{i-1}\pm1)\bmod n} \sum_{x_i'\neq(a_i\pm1)\bmod n} \sum_{x_{i+1}=(a_i\pm1)\bmod n}$$

$$\sum_{x_{i+2}=(a_{i+2}\pm1)\bmod n} \cdots \sum_{x_m=(a_m\pm1)\bmod\ n} v^{(x_1,x_2,\ldots,x_m)}$$

$$+ \sum_{x_1'=(a_1\pm1)\bmod n} \sum_{x_2'=(a_2\pm1)\bmod n} \cdots \sum_{x_m'=(a_m'\pm1)\bmod n} v^{(x_1',x_2',\ldots,x_m')}$$

$$= v^{\overline{(a_1,a_2,\ldots,a_{i-1}n-1,a_{i+1},a_{i+2},\ldots,a_m)_\Pi}}.$$

Similarly, it can be shown that

$$\sum_{x_1=0}^{n-2}\sum_{x_2=0}^{n-2} v^{\overline{(a_1,a_2,\ldots,a_{i_1-1},x_1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2-1},x_2,a_{i_2+1},a_{i_2+2},\ldots,a_m)_\Pi}}$$

$$= v^{\overline{(a_1,a_2,\ldots,a_{i_1-1},n-1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2-1},n-1,a_{i_2+1},a_{i_2+2},\ldots,a_m)_\Pi}}$$

Continuing, in this way, it can finally be shown that

$$\sum_{x_1=0}^{n-2}\sum_{x_2=0}^{n-2}\cdots\sum_{x_m=0}^{n-2} v^{\overline{(x_1,x_2,\ldots,x_m)_\Pi}} = v^{\overline{(n-1,n-1,\ldots,n-1)_\Pi}}.$$

Hence T spans C_Π.

In order to show that T is a linearly independent set, suppose that

$$\sum_{a_1=0}^{n-2}\sum_{a_2=0}^{n-2}\cdots\sum_{a_m=0}^{n-2} \alpha_{(a_1,a_2,\ldots,a_m)} v^{\overline{(a_1,a_2,\ldots,a_m)_\Pi}} = 0, \tag{8.4}$$

and consider the coefficients of each of the n^m points $(a_1, a_2, \ldots, a_m) \in \{0, 1, \ldots, n-1\}^m$. Each coefficient is the sum of either $1, 2, 2^2, \ldots, 2^{m-1}$ or 2^m of the coefficients in the sum in 8.4. Any point of which the coefficient is $\alpha_{(a_1,a_2,\ldots,a_m)}$, has each of its coordinates equal to 0 or $n-2$. There are 2^m such points, and hence the 2^m coefficients which are immediately 0 are $\alpha_{(a_1,a_2,\ldots,a_m)}, a_i \in \{1, n-3\}$, for all $i \in \{1, 2, \ldots, m\}$. Then any point of which the

coefficient is $\alpha_{(a_1,a_2,\ldots,a_m)} + \alpha_{(a_1'',a_2'',\ldots,a_m'')}$, has $m-1$ of its coordinates equal to 0 or $n-2$, while the remaining coordinate is exclusive of $\{0, n-2, n-1\}$. There are $\binom{m}{1}2^{m-1}(n-3)$ such points, and as a result of the coefficients which were immediately 0, the coefficients $\alpha_{(a_1,a_2,\ldots,a_m)}$, where for some $i \in \{1,2,\ldots,m\}$, $a_i \in \{0,1,\ldots,n-2\} \setminus \{1, n-3\}$ and $a_j \in \{1, n-3\}$, for all $j \in \{1,2,\ldots,m\} \setminus \{i\}$, are all equal to 0. Furthermore, any point of which the coefficient is the sum of 2^2 coefficients in the sum in 8.4, has $m-2$ of its coordinates equal to 0 or $n-2$, while the remaining two coordinates are exclusive of $\{0, n-2, n-1\}$. There are $\binom{m}{2}2^{m-2}(n-3)^2$ such points, and as a result of the coefficients which were 0 by previous accounts, the coefficients $\alpha_{(a_1,a_2,\ldots,a_m)}$, where for some $i_1, i_2 \in \{1,2,\ldots,m\}$, $a_{i_1}, a_{i_2} \in \{0,1,\ldots,n-2\} \setminus \{1, n-3\}$ and $a_j \in \{1, n-3\}$, for all $j \in \{1,2,\ldots,m\} \setminus \{i_1, i_2\}$, are all equal to 0. Finally, by continuing the argument in this way, any point of which the coefficient is the sum of 2^m coefficients in the sum in 8.4, has 0, $n-1$ or $n-2$ in none of its coordinate positions. There are $(n-3)^m$ such points, and in conjunction with the coefficients that are already 0 at this stage, result in the coefficients $\alpha_{(a_1,a_2,\ldots,a_m)}$, where $a_i \in \{0,1,\ldots,n-2\} \setminus \{1, n-3\}$, for all $i \in \{1,2,\ldots,m\}$, all being equal to 0. Since these account for all the coefficients in the sum in 8.4, it follows that T is a linearly independent set. Hence T is a basis for C_Π. Clearly, $|T| = (n-1)^m$. $\square$

With regard to the above lemma, note that if $n = 3$ and the vectors in T are arranged in lexicographic order and the points as follows: first the points

$(0,0,\ldots,0)$, $(0,0,\ldots,0,1)$, $(0,0,\ldots,0,10)$, $(0,0,\ldots,0,1,1)$, $\ldots$, $(0,0,\ldots,0,1,1,1)$, $\ldots$, $(1,1,\ldots,1)$,

and then the points

$(0,0,\ldots,0,2)$, $(0,0,\ldots,0,1,2)$, $(0,0,\ldots,0,2,0)$, $\ldots$, $(0,0,\ldots,0,2,2)$, $(0,0,\ldots,1,0,2)$, $\ldots$, $(0,0,\ldots,0,1,2,2)$, $(0,0,\ldots,2,0,0)\ldots$, $(0,0,\ldots,0,2,2,2)$, $(0,0,\ldots,0,1,0,0,2)$, $\ldots$, $(0,0,\ldots,0,2,2,2,2)$, $\ldots$, $(2,2,\ldots,2)$,

a matrix of the form $\left[\begin{array}{ll} 0\ 0\ldots0\ 1 & | \\ 0\ldots0\ 1\ 0 & |\ A \\ \ldots\ldots & | \\ 1\ 0\ldots0 & | \end{array}\right]$ results. However, such an arrangement of vectors and points does not result in a matrix such as the one above if n is odd and

$n \neq 3$, since then, unlike in C_3, each point in C_n is not adjacent to every other point.

Lemma 8.2.6. *Let*

$$U_1 = \left\{ \sum_{x_1=0}^{n-1} v^{(a_1,a_2,\ldots,a_{i-1},x_1,a_{i+1},a_{i+2},\ldots,a_m)} : a_j \in \{0,1,\ldots,n-2), \textit{for all } j \in \{1,2,\ldots,m\} \setminus \{i\} \right\},$$

$$U_2 = \left\{ \sum_{x_1=0}^{n-1} \sum_{x_2=0}^{n-1} v^{(a_1,a_2,\ldots,a_{i_1-1},x_1,a_{i_1+1},a_{i_1+2}\ldots,a_{i_2-1},x_2,x_{i_2+2},\ldots,a_m)} : a_j \in \{0,1,\ldots,n-2\}, \right.$$

$$\left. \textit{for all } j \in \{1,2,\ldots,m\} \setminus \{i_1,i_2\} \right\}$$

$$\vdots$$

$$U_m = \left\{ \sum_{x_1=0}^{n-1} \sum_{x_2=0}^{n-1} \cdots \sum_{x_m=0}^{n-1} v^{(x_1,x_2,\ldots,x_m)} \right\} = \{\boldsymbol{j}\}.$$

Then if n is odd, then

$$U = \bigcup_{i=1}^{m} U_i$$

is a for basis $C_\Pi^\perp$.

Proof: Suppose that $w \in U$. Then $w \in U_i$ for some $1 \leq i \leq m$ i.e. w is incident at all the points for which for some $J \subset \{1,2,\ldots,m\}$, the coordinates a_j, for all $j \in J$, are fixed, while each of the remaining coordinates ranges over $\{0,1,\ldots,n-1\}$. Now for any incidence vector $v^{\overline{(a_1',a_2',\ldots,a_n')_\Pi}}$, consider the inner product $(w, v^{\overline{(a_1',a_2',\ldots,a_m')_\Pi}})$. Clearly, if there exists $j \in J$ such that $a_j' \neq (a_j \pm 1) \text{mod n}$, then $(w, v^{\overline{(a_1',a_2',\ldots,a_m')_\Pi}}) = 0$. Otherwise, if $a_j' = (a_j \pm 1) \text{mod}\, n$, for all $j \in J$, then $(w, v^{\overline{(a_1',a_2',\ldots,a_m')_\Pi}}) = 2^{m-|J|} \equiv 0 (\text{mod } 2)$. Hence $w \in C_\Pi^\perp$.

In order to show that U is a linearly independent set, the following notation is introduced:

For $i \in \{1,2,\ldots,m\}$ and $a_j \in \{0,1,\ldots,n-2\}$, for all $j \in \{1,2,\ldots,m\} \setminus \{i\}$, let

$$v[a_1,a_2,\ldots,a_{i-1},-,a_{i+1},a_{i+2},\ldots,a_m] = \sum_{x_1=0}^{n-1} v^{(a_1,a_2,\ldots,a_{i-1},x_1,a_{i+1},a_{i+2},\ldots,a_m)}, \tag{8.5}$$

and for $i_1, i_2 \in \{1, 2, \ldots, m\}$ and $a_j \in \{0, 1, \ldots, n-2\}$, for all $j \in \{1, 2, \ldots, m\} \setminus \{i_1, i_2\}$, let

$$v[a_1, a_2, \ldots, a_{i\_1}, -, a_{i_1+1}, a_{i_1+2}, \ldots, a_{i_2-1}, -, a_{i_2+1}, a_{i_2+2}, \ldots, a_m]$$

$$= \sum_{x_1=0}^{n-1} \sum_{x_2=0}^{n-1} v^{(a_1, a_2, \ldots, a_{i_1-1}, x_1, a_{i_1+1}, a_{i_1+2}, \ldots, a_{i_2-1}, x_2, a_{i_2+1}, a_{i_2+2}, \ldots, a_m)}. \tag{8.6}$$

Similar notation is used for the elements of $U_i, 3 \leq i \leq m$ - with this notation the $\boldsymbol{j}$-vector becomes $v[-, -, \ldots, -]$. By arranging the vectors in the order
$v[0, 0, \ldots, 0, -], v[0, 0, \ldots, 0, 1, -], \ldots, v[0, 0, \ldots, 0, n-2, -], v[0, 0, \ldots, 0, -, 0], v[0, 0, \ldots, 0, -, 1], \ldots, v[0, 0, \ldots, 0, -, -], v[0, 0, \ldots, 0, 1, 0, -], \ldots, v[0, 0, \ldots, 0, 1, n-2, -], v[0, 0, \ldots, 0, 1, -, 0], \ldots, v[0, 0, \ldots, 0, 1, -, n-2], v[0, 0, \ldots, 0, 1, -, -], v[0, 0, \ldots, 0, 2, 0, -], \ldots, v[0, 0, \ldots, 0, n-2, n-2, -], v[0, 0, \ldots, 0, n-2, -, -], v[0, 0, \ldots, 0, -, 0, 0], v[0, 0, \ldots, 0, -, 0, 1], \ldots, v[0, 0, \ldots, 0, -, -, -], v[0, 0, \ldots, 0, 1, 0, 0, -], \ldots, v[0, 0, \ldots, 0, 1, -, -, -], v[0, 0, \ldots, 0, 2, 0, 0, -], \ldots, v[0, 0, \ldots, 0, -, -, -, -], v[0, 0, \ldots, 0, 1, 0, 0, 0, -], \ldots, v[-, -, \ldots, -],$
and the points as follows: first the points
$(0, 0, \ldots, 0), (0, 0, \ldots, 0, 1), \ldots, (0, 0, \ldots, 0, n-2), (0, 0, \ldots, 0, 1, 0), \ldots, (0, 0, \ldots, 0, n-2, n-2), \ldots, (n-2, n-2, \ldots, n-2),$
and then the points
$(0, 0, \ldots, 0, n-1), (0, 0, \ldots, 0, 1, n-1), \ldots, (0, 0, \ldots, 0, n-2, n-1), (0, 0, \ldots, 0, n-1, 0), \ldots, (0, 0, \ldots, n-1, n-1), (0, 0, \ldots, 0, 1, 0, n-1), \ldots, (0, 0, \ldots, 0, 1, n-1, n-1), (0, 0, \ldots, 0, 2, 0, n-1), \ldots, (0, 0, \ldots, 0, n-1, n-1, n-1), (0, 0, \ldots, 0, 1, 0, 0, n-1), \ldots, (0, 0, \ldots, 0, n-1, n-1, n-1, n-1), \ldots, (n-1, n-1, \ldots, n-1),$
a lower triangular matrix results. Hence U is a linearly independent set. Now

$$\begin{aligned} |U| &= |U_1| + |U_2| + \cdots + |U_m| \\ &= \tbinom{m}{1}(n-1)^{m-1} + \tbinom{m}{2}(n-1)^{m-2} + \cdots + 1 \\ &= n^m - (n-1)^m \\ &= n^m - \dim C_\Pi, \end{aligned}$$

and it follows that U is a basis for $C_\Pi^\perp$. □

The definition of adjacency in $\prod_{i=1}^{m} C_n$ implies that the incidence vectors in C_Π have large weights. Moreover, the condition that any vector in C_Π be orthogonal to all the vectors in U implies that the minimum weight is large, as is evident from the following lemma.

Lemma 8.2.7. *If n is odd, then the minimum weight of C_Π is 2^m.*

Proof: Suppose that $w \in C_\Pi$, and that w is incident at $(a_1, a_2, \ldots, a_m)$. Now w is orthogonal to each vector in the set $\{v[-, a_2, a_3, \ldots, a_m],\ v[a_1, -, a_3, a_4, \ldots, a_m],\ \ldots,\ v[a_1, a_2, \ldots, a_{m-1}, -]\}$, and besides, these vectors are commonly incident only at $(a_1, a_2, \ldots, a_m)$. Hence w is incident at at least an additional $\binom{m}{1}$ points. Similarly, w is orthogonal to each of the vectors in the set $\{v[-, -, a_3, a_4, \ldots, a_m],\ v[-, a_2, -, a_4, a_5, \ldots, a_m],\ \ldots,\ v[a_1, a_2, \ldots, a_{m-2}, -, -,]\}$, and as before, these vectors are commonly incident only $(a_1, a_2, \ldots, a_m)$. Of the $\binom{m}{1}$ additional points at which w is incident, each of the vectors in the latter set are incident at only $\binom{2}{1}$ of these, and hence w is incident at at least an additional $\binom{m}{1} + \binom{m}{2}$ points in total. Furthermore, w is orthogonal to each vector in the set $\{v[-, -, -, a_4, a_5, \ldots, a_m],\ v[-, -, a_3, -, a_5, a_6, \ldots, a_m],\ \ldots,\ v[a_1, a_2, \ldots, a_{m-3}, -, -, -]\}$, and these are commonly incident only at $(a_1, a_2, \ldots, a_m)$. In this case, of the $\binom{m}{1} + \binom{m}{2}$ additional points at which w is incident, each vector in the last set is incident at only $\binom{3}{1} + \binom{3}{2}$ of these, and hence w is incident at at least an additional $\binom{m}{1} + \binom{m}{2} + \binom{m}{3}$ points in total. Continuing in this way, w is incident at at least an additional $\binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{m-1}$ points in total, and hence the weight of w is at least $1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{m-1} = 2^m - 1$. But if w has weight $2^m - 1$, then w is not orthogonal to $v[-, -, \ldots, -] = \boldsymbol{j}$, and hence the weight of w is at least 2^m. Hence any vector in C_Π has weight at least 2^m. Since the incidence vectors in C_Π have weight 2^m, it follows that the minimum weight is 2^m, and that C_Π has a basis of minimum weight vectors. □

Contrary to the situation in C_Π, the minimum weight of $C_\Pi^\perp$ is not of exponential order, as suggested by the weights of the vectors in U, which range over $n, n^2, \ldots, n^m$.

Lemma 8.2.8. *If n is odd, then the minimum weight of $C_\Pi^\perp$ is n.*

Proof: Suppose that $w \in C_\Pi^\perp$, and that w is incident at $(a_1, a_2, \ldots, a_m)$. Now w is orthogonal to $v^{\overline{(a_1+k) \mod n,(a_2+k) \mod n,\ldots,(a_m+k) \mod n)_\Pi}}$ for each k in the sequence $1, 3, \ldots, n-2, 0, 2, \ldots, n-1$, and since $v^{\overline{((a_1+k) \mod n,(a_2+k) \mod n,\ldots,(a_m+k) \mod n)_\Pi}}$ and $v^{\overline{((a_1+k+2) \mod n,(a_2+k+2) \mod n,\ldots,(a_m+k+2) \mod n)_\Pi}}$ are commonly incident only at $((a_1+k+1) \bmod n, (a_2+k+1) \bmod n, \ldots, (a_m+k+1) \mod n)$, it follows that w is incident at least an additional $n-1$ points. Hence any vector in $C_\Pi^\perp$ has weight at least n, and since the vectors in U_1 have weight n, it follows that the minimum weight is n. □

Similar parameters to those described in Lemmas 8.2.5 to 8.2.8 occur for C_Π if n is even and $n \geq 4$, and these are the focus of the following lemmas.

Lemma 8.2.9. *If $n \geq 4$ is even, then the set $V = \{v^{\overline{(a_1,a_2,\ldots,a_m)_\Pi}} : (a_1, a_2, \ldots, a_m) \in \{0, 1, \ldots, n-3\}^m\}$ is a basis for C_Π.*

Proof: In order to show that V spans C_Π in this case, it is sufficient to show that each incidence vector in the set $\{v^{\overline{(a_1,a_2,\ldots,a_m)_\Pi}} : \text{there exists } i \in \{1, 2, \ldots, m\} | a_i = n-2 \text{ or } a_i = n-1\}$ is in the span of V. So suppose that $(a_1, a_2, \ldots, a_m)$ is such that for some $1 \leq i \leq m$, $a_i = n-2$ but $a_j \neq n-2, n-1$, for all $j \in \{1, 2, \ldots, m\} \setminus \{i\}$. Then

$$\sum_{k=0}^{\frac{n-4}{2}} v^{\overline{(a_1,a_2,\ldots,a_{i-1},2k,a_{i+1},a_{i+2},\ldots,a_m)_\Pi}}$$

$$= 2 \sum_{x_1=(a_1\pm1) \bmod n} \sum_{x_2=(a_2\pm1) \bmod n} \cdots \sum_{x_{i-1}=(a_{i-1}\pm1) \bmod n} \sum_{x_i \neq (n-2\pm1) \bmod n} \sum_{x_{i+1}=(a_i\pm1) \bmod n}$$

$$\sum_{x_{i+2}=(a_{i+2}\pm1) \bmod n} \cdots \sum_{x_m=(a_m\pm1) \bmod n} v^{(x_1,x_2,\ldots,x_m)} + \sum_{x'_1=(a_1\pm1) \bmod n} \sum_{x'_2=(a_2\pm1) \bmod n} \cdots$$

$$\sum_{x'_{i-1}=(a_{i-1}\pm1) \bmod n} \sum_{x'_i=(n-2\pm1) \bmod n} \sum_{x'_{i+1}=(a_i\pm1) \bmod n} \sum_{x'_{i+2}=(a_{i+2}\pm1) \bmod n} \cdots \sum_{x'_m=(a_m\pm1) \bmod n} v^{(x'_1,x'_2,\ldots,x'_m)}$$

$$= v^{\overline{(a_1,a_2,\ldots,a_{i-1},n-2,a_{i+1},a_{i+2},\ldots,a_m)_\Pi}}.$$

In the same way it can be shown that

$$\sum_{k_1=0}^{\frac{n-4}{2}}\sum_{k_2=0}^{\frac{n-4}{2}} v^{\overline{(a_1,a_2,\ldots,a_{i_1}-1,2k_1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2}-1,2k_2,a_{i_2+1},a_{i_2+2},\ldots,a_m)_\Pi}}$$

$$= \quad v^{\overline{(a_1,a_2,\ldots,a_{i_1}-1,n-2,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2}-1,n-2,a_{i_2+1},a_{i_2+2},\ldots,a_m)_\Pi}}.$$

Continuing, in this way, it can finally be shown that

$$\sum_{k_1=0}^{\frac{n-4}{2}}\sum_{k_2=0}^{\frac{n-4}{2}}\cdots\sum_{k_m=0}^{\frac{n-4}{2}} v^{\overline{(2k_1,2k_2,\ldots,2k_m)_\Pi}} = v^{\overline{(n-2,n-2,\ldots,n-2)_\Pi}}.$$

If on the other hand, for some $1 \leq i \leq m,\ a_i = n-1$ but $a_j \neq n-2, n-1,$ for all $j \in \{1,2,\ldots,m\} \setminus \{i\}$, then

$$\sum_{k=0}^{\frac{n-4}{2}} v^{\overline{(a_1,a_2\ldots,a_{i-1},2k+1,a_{i+1},a_{i+2},\ldots,a_m)_\Pi}}$$

$$= \quad 2 \sum_{x_1=(a_1\pm1)\bmod\ \mathrm{n}} \sum_{x_2=(a_2\pm1)\bmod\ \mathrm{n}} \cdots \sum_{x_{i-1}=(a_{i-1}\pm1)\bmod\ \mathrm{n}} \sum_{x_i\neq(n-1\pm1)\bmod \mathrm{n}} \sum_{x_{i+1}=(a_i\pm1)\bmod\ \mathrm{n}}$$

$$\sum_{x_{i+2}=(a_{i+2}\pm1)\bmod\ \mathrm{n}} \cdots \sum_{x_m=(a_m\pm1)\bmod\ \mathrm{n}} v^{(x_1,x_2,\ldots,x_m)} + \sum_{x_1'=(a_1\pm1)\bmod\ \mathrm{n}} \sum_{x_2'=(a_2\pm1)\bmod\ \mathrm{n}} \cdots$$

$$\sum_{x_{i-1}'=(a_{i-1}\pm1)\bmod\ \mathrm{n}} \sum_{x_i'=(n-1\pm1)\bmod \mathrm{n}} \sum_{x_{i+1}'=(a_i\pm1)\bmod\ \mathrm{n}} \sum_{x_{i+2}'=(a_{i+2}\pm1)\bmod\ \mathrm{n}} \cdots$$

$$\cdots \sum_{x_m'=(a_m\pm1)\bmod\ \mathrm{n}} v^{(x_1',x_2',\ldots,x_m')}$$

$$= \quad v^{\overline{(a_1,a_2,\ldots,a_{i-1},n-1,a_{i+1},a_{i+2},\ldots,a_m)_\Pi}}.$$

Analogous formulae are valid for any incidence vector $v^{\overline{(a_1,a_2,\ldots,a_m)_\Pi}}$ for which there exists $J \subseteq \{1,2,\ldots,m\},\ |J| \geq 2,$ such that $a_j = n-1, \text{for all } j \in J$. Combining these formulae with the former set of formulae results in any incidence vector $v^{\overline{(a_1,a_2,\ldots,a_m)_\Pi}}$ for which there exists $J_1, J_2, \subseteq \{1,2,\ldots,m\}$ such that $a_j = n-1, \text{for all } j \in J_1,$ and $a_j = n-2, \text{for all } j \in J_2,$ being a linear combination of vectors in V. Hence V spans C_Π.

Furthermore, if the vectors in V are arranged in lexicographic order and the points as follows: first the points

$(1,1,\ldots,1)$, $(1,1,\ldots,1,2)$, $\ldots$, $(1,1,\ldots,1,n-2)$, $(1,1,\ldots,1,2,1)$, $\ldots$, $(1,1,\ldots,1,2,n-2)$, $\ldots$, $(1,1,\ldots,1,n-2,n-2)$, $\ldots$, $(n-2,n-2,\ldots,n-2)$,

and then the points

$(0,0,\ldots,0)$, $(0,0,\ldots,0,1)$, $\ldots$, $(0,0,\ldots,0,n-1)$, $(0,0,\ldots,0,1,0)$, $\ldots$, $(0,0,\ldots,0,n-1,n-1)$, $\ldots$, $(0,n-1,n-1,\ldots,n-1)$, $(1,0,0,\ldots,0)$, $\ldots$, $(1,1,\ldots,1,0)$, $(1,1,\ldots,1,n-1)$, $(1,1,\ldots,1,2,0)$, $(1,1,\ldots,1,2,n-1)$, $\ldots$, $(1,1,\ldots,1,n-1,n-1)$, $(1,1,\ldots,1,2,0,0)$, $\ldots$, $(1,1,\ldots,1,2,n-1,n-1)$, $\ldots$, $(1,1,\ldots,1,n-1,n-1,n-1)$, $\ldots$, $(n-1,n-1,\ldots,n-1)$,

a matrix having rank $|V|$ results. Hence V is a linearly independent set, and it follows that V is a basis for C_Π. Clearly, $|V| = (n-2)^m$. □

Lemma 8.2.10. *Let*

$$W_1(e_i) = \left\{ \sum_{k_1=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i-1},2k_1,a_{i+1},a_{i+2},\ldots,a_m)} : a_j \in \{0,1,\ldots,n-3),\ \textit{for all}\ j \in \{1,2,\ldots,m\}\setminus\{i\} \right\},$$

$$W_1(o_i) = \left\{ \sum_{k_1=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i-1},2k_1+1,a_{i+1},a_{i+2},\ldots,a_m)} : a_j \in \{0,1,\ldots,n-3),\ \textit{for all}\ j \in \{1,2,\ldots,m\}\setminus\{i\} \right\},$$

$$W_2(e_{i_1},e_{i_2}) = \left\{ \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i_1-1},2k_1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2-1},2k_2,a_{i_2+1},a_{i_2+2},\ldots,a_m)} : a_j \in \{0,1,\ldots,n-3\},\ \textit{for all}\ j \in \{1,2,\ldots,m\}\setminus\{i_1,i_2\} \right\},$$

$$W_2(e_{i_1}, o_{i_2}) = \left\{ \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i_1}-1,2k_1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2}-1,2k_2+1,a_{i_2+1},a_{i_2+2},\ldots,a_m)} : a_j \in \{0,1,\ldots, \right.$$

$$\left. n-2\},\ \textit{for all}\ j \in \{1,2,\ldots,m\} \setminus \{i_1, i_2\} \right\},$$

$$W_2(o_{i_1}, e_{i_2}) = \left\{ \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i_1}-1,2k_1+1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2}-1,2k_2,a_{i_2+1},a_{i_2+2},\ldots,a_m)} : a_j \in \{0,1,\ldots, \right.$$

$$\left. n-3\},\ \textit{for all}\ j \in \{1,2,\ldots,m\} \setminus \{i_1, i_2\} \right\},$$

$$W_2(o_{i_1}, o_{i_2}) = \left\{ \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i_1}-1,2k_1+1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2}-1,2k_2+1,a_{i_2+1},a_{i_2+2},\ldots,a_m)} : a_j \in \{0,1,\ldots, \right.$$

$$\left. n-3\},\ \textit{for all}\ j \in \{1,2,\ldots,m\} \setminus \{i_1, i_2,\} \right\},$$

$$\vdots$$

$$W_m(e_1, e_2, \ldots, e_m) = \left\{ \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} \cdots \sum_{k_m=0}^{\frac{n-2}{2}} v^{(2k_1,2k_2,\ldots,2k_m)} \right\}$$

$$\vdots$$

$$W_m(o_1, o_2, \ldots, o_m) = \left\{ \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} \cdots \sum_{k_m=0}^{\frac{n-2}{2}} v^{(2k_1+1,2k_2+1,\ldots,2k_m+1)} \right\},$$

and further, let

$$W_1 = \bigcup_{i\in\{1,2,\ldots,m\}} \bigcup_{x_i\in\{e_i,o_i\}} W_1(x_i),$$

$$W_2 = \bigcup_{\{i_1,i_2\}\subseteq\{1,2,\ldots,m\}} \bigcup_{x_{i_1}\in\{e_{i_1},o_{i_1}\}} \bigcup_{x_{i_2}\in\{e_{i_2},o_{i_2}\}} W_2(x_{i_1},x_{i_2}),$$

$$\vdots$$

$$W_m = \bigcup_{x_1\in\{e_1,o_1\}} \bigcup_{x_2\in\{e_2,o_2\}} \cdots \bigcup_{x_m\in\{e_m,o_m\}} W_m(x_1,x_2,\ldots,x_m).$$

Then if $n \geq 4$ is even, then

$$W = \bigcup_{i=1}^{m} W_i$$

is a for basis $C_\Pi^\perp$.

Proof: Suppose that $w \in W$. Then $w \in W_i$ for some $1 \leq i \leq m$ i.e. w is incident at all the points for which for some $J \subset \{1,2,\ldots,m\}$, the coordinates a_j, for all $j \in J$, are fixed, while each of the remaining coordinates ranges over either $\{0,2,4,\ldots,n-2\}$ or $\{1,3,5,\ldots,n-1\}$. Clearly, if for any incidence vector $v^{\overline{(a_1',a_2',\ldots,a_m')_\Pi}}$, there exists $j \in J$ such that $a_j' \neq (a_j \pm 1)\text{mod n}$, then $(w, v^{\overline{a_1',a_2',\ldots,a_m')_\Pi}}) = 0$. Otherwise, if $a_j' = (a_j \pm 1)\text{mod}\, n$, for all $j \in J$, then either $(w, v^{\overline{(a_1',a_2',\ldots,a_m')_\Pi}}) = 0$ or $(w, v^{\overline{(a_1',a_2',\ldots,a_m')_\Pi}}) = 2^{m-|J|} \equiv 0(\text{mod } 2)$. Hence $w \in C_\Pi^\perp$.

In order to show that W is a linearly independent set, the following notation is introduced:

For $i \in \{1,2,\ldots,m\}$ and $a_j \in \{0,1,\ldots,n-3\}$, for all $j \in \{1,2,\ldots,m\} \setminus \{i\}$, let

$$v[a_1,a_2,\ldots,a_{i-1},-,a_{i+1},a_{i+2},\ldots,a_m]_{e_i} = \sum_{k_1=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i-1},2k_1,a_{i+1},a_{i+2},\ldots,a_m)}, \tag{8.7}$$

$$v[a_1,a_2,\ldots,a_{i-1},-,a_{i+1},a_{i+2},\ldots,a_m]_{o_i} = \sum_{k_1=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i-1},2k_1+1,a_{i+1},a_{i+2},\ldots,a_m)}, \tag{8.8}$$

and for $i_1, i_2 \in \{1, 2, \ldots, m\}$ and $a_j \in \{0, 1, \ldots, n-3\}$, for all $j \in \{1, 2, \ldots, m\} \setminus \{i_1, i_2\}$, let

$$v[a_1, a_2, \ldots, a_{i_1-1}, -, a_{i_1+1}, a_{i_1+2}, \ldots, a_{i_2-1}, -, a_{i_2+1}, a_{i_2+2}, \ldots, a_m]_{e_{i_1}e_{i_2}}$$

$$= \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i_1-1},2k_1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2-1},2k_2,a_{i_2+1},a_{i_2+2},\ldots,a_m)}, \tag{8.9}$$

$$v[a_1, a_2, \ldots, a_{i_1-1}, -, a_{i_1+1}, a_{i_1+2}, \ldots, a_{i_2-1}, -, a_{i_2+1}, a_{i_2+2}, \ldots, a_m]_{e_{i_1}o_{i_2}}$$

$$= \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i_1-1},2k_1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2-1},2k_2+1,a_{i_2+1},a_{i_2+2},\ldots,a_m)}, \tag{8.10}$$

$$v[a_1, a_2, \ldots, a_{i_1-1}, -, a_{i_1+1}, a_{i_1+2}, \ldots, a_{i_2-1}, -, a_{i_2+1}, a_{i_2+2}, \ldots, a_m]_{o_{i_1}e_{i_2}}$$

$$= \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i_1-1},2k_1+1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2-1},2k_2,a_{i_2+1},a_{i_2+2},\ldots,a_m)}, \tag{8.11}$$

$$v[a_1, a_2, \ldots, a_{i_1-1}, -, a_{i_1+1}, a_{i_1+2}, \ldots, a_{i_2-1}, -, a_{i_2+1}, a_{i_2+2}, \ldots, a_m]_{o_{i_1}o_{i_2}}$$

$$= \sum_{k_1=0}^{\frac{n-2}{2}} \sum_{k_2=0}^{\frac{n-2}{2}} v^{(a_1,a_2,\ldots,a_{i_1-1},2k_1+1,a_{i_1+1},a_{i_1+2},\ldots,a_{i_2-1},2k_2+1,a_{i_2+1},a_{i_2+2},\ldots,a_m)}, \tag{8.12}$$

Similar notation is used for the elements of $W_i, 3 \leq i \leq m$. Using this notation,

$$\boldsymbol{j} = v[-, -, \ldots, -]_{e_1e_2\ldots,e_m} + v[-, -, \ldots, -]_{e_1e_2\ldots,e_{m-1}o_m} + \cdots + v[-, -, \ldots, -]_{o_1o_2\ldots,o_m}.$$

By arranging the vectors in the order

$v[0, 0, \ldots, 0, -]_{e_m}$, $v[0, 0, \ldots, 0, -]_{o_m}$, $v[0, 0, \ldots, 0, 1, -]_{e_m}$, $v[0, 0, \ldots, 0, 1, -]_{o_m}$, $v[0, 0, \ldots,$ $0, 2, -]_{e_m}$, $v[0, 0, \ldots, 0, 2, -]_{o_m}$, $\ldots$, $v[0, 0, \ldots, 0, n-3, -]_{o_m}$, $v[0, 0, \ldots, 0, -, o]_{e_{m-1}}$, $\ldots$, $v[0, 0, \ldots, 0, -, n-3]_{e_{m-1}}$, $v[0, 0, \ldots, 0, -, -]_{e_{m-1}e_m}$, $v[0, 0, \ldots, 0, -, -]_{e_{m-1}o_m}$, $v[0, 0, \ldots, 0,$ $-, 0]_{o_{m-1}}$, $\ldots$, $v[0, 0, \ldots, 0, -, -,]_{o_{m-1}o_m}$, $v[0, 0, \ldots, 0, 1, 0, -]_{e_m}$, $v[0, 0, \ldots, 0, 1, 0, -]_{o_m}$, $v[0,$ $0, \ldots, 0, 1, 1, -]_{e_m}$, $\ldots$, $v[0, 0, \ldots, 0, 1, -, -,]_{o_{m-1}o_m}$, $v[0, 0, \ldots, 0, 2, 0, -]_{e_m}$, $\ldots$, $v[0, 0, \ldots, 0,$ $-, -, -]_{o_{m-2}o_{m-1}o_m}$, $v[0, 0, \ldots, 0, 1, 0, 0, -]_{e_m}$, $\ldots$, $v[0, 0, \ldots, 0, -, -, -, -]_{o_{m-3}o_{m-2}o_{m-1}o_m}$,

$\ldots, v[0,-,-,\ldots,-]_{o_2o_3\ldots o_m}, \ldots, v[-,0,0,\ldots,0]_{e_1}, \ldots, v[-,-,\ldots,-]_{e_1o_2o_3\ldots,o_m}, v[-,0,0,\ldots,0]_{o_1}, \ldots, v[-,-,\ldots,-]_{o_1o_2\ldots o_m}$,

and the points as follows: first the points

$(0,0,\ldots,0), (0,0,\ldots,0,1), \ldots, (0,0,\ldots,0,n-3), (0,0,\ldots,0,1,0), \ldots, (0,0,\ldots,0,n-3,n-3), \ldots, (n-3,n-3,\ldots,n-3)$,

and then the points

$(0,0,\ldots,0,n-2), (0,0,\ldots,0,n-1), (0,0,\ldots,0,1,n-2), (0,0,\ldots,0,1,n-1), (0,0,\ldots,0,2,n-2), (0,0,\ldots,0,2,n-1), \ldots, (0,0,\ldots,n-3,n-1), (0,0,\ldots,n-2,0), \ldots, (0,0,\ldots,0,n-2,n-1), \ldots, (0,0,\ldots,0,n-1,n-1), (0,0,\ldots,0,1,0,n-2), (0,0,\ldots,0,1,0,n-1), (0,0,\ldots,0,1,1,n-2), (0,0,\ldots,0,1,1,n-1), \ldots, (0,0,\ldots,0,n-1,n-1,n-1), (0,0,\ldots,0,1,0,0,n-2), \ldots, (0,0,\ldots,0,n-1,n-1,n-1,n-1), \ldots, (n-1,n-1,\ldots n-1)$,

a lower triangular matrix results. Hence W is a linearly independent set. Finally,

$$\begin{aligned} |W| &= |W_1| + |W_2| + \cdots + |W_m| \\ &= \tbinom{m}{1}2(n-2)^{m-1} + \tbinom{m}{2}2^2(n-2)^{m-2} + \cdots + 2^m \\ &= n^m - (n-2)^m \\ &= n^m - \dim C_\Pi, \end{aligned}$$

and it follows that W is a basis for $C_\Pi^\perp$. □

The following two lemmas are the analogies of Lemmas 8.2.7 and 8.2.8

Lemma 8.2.11. *If n is even, then the minimum weight of C_Π is 2^m.*

Proof: Suppose that $w \in C_\Pi$, and that w is incident at $(a_1, a_2, \ldots, a_m)$. Without loss of generality, it can be assumed that a_i is even, for all $i \in \{1, 2, \ldots, m\}$. The proof follows exactly the same course as the proof in Lemma 8.2.7, except that $v[a_1, a_2, \ldots, a_{i-1}, -, a_{i+1}, a_{i+2}, \ldots, a_m]$ is replaced with $v[a_1, a_2, \ldots, a_{i-1}, -, a_{i+1}, a_{i+2}, \ldots, a_m]_{e_i}$, $v[a_1, a_2, \ldots, a_{i_1-1}, -, a_{i_1+1}, a_{i_1+2}, \ldots, a_{i_2-1}, -, a_{i_2+1}, a_{i_2+2}, \ldots, a_m]$ with $v[a_1, a_2, \ldots, a_{i_1-1}, -, a_{i_1+1}, a_{i_1+2}, \ldots, a_{i_2-1}, -, a_{i_2+2}, \ldots, a_m]_{e_{i_1}e_{i_2}}$, and so on. Also, the $\boldsymbol{j}$-vector is now no longer equal to $v[-,-,\ldots,-]$, but to $v[-,-,\ldots,-]_{e_1e_2\ldots e_m} + v[-,-,\ldots,-]_{e_1e_2\ldots,e_{m-1}o_m} + \cdots + v[-,-,\ldots,-]_{o_1o_2\ldots o_m}$, as indicated in Lemma 8.2.10. □

Lemma 8.2.12. *If $n \geq 4$ is even, then the minimum weight of $C_\Pi^\perp$ is $\frac{n}{2}$.*

Proof: Suppose that $w \in C_\Pi^\perp$, and that w is incident at $(a_1, a_2, \ldots, a_k)$. Now w is orthogonal to $v^{\overline{((a_1+k) \mod n,(a_2+k) \mod n,\ldots,(a_m+k) \mod n)_\Pi}}$ for each k in the sequence $1, 3, \ldots, n-1$, and since $v^{\overline{((a_1+k) \mod n,(a_2+k) \mod n,\ldots,(a_m+k) \mod n)_\Pi}}$ and $v^{\overline{((a_1+k+2) \mod n,(a_2+k+2) \mod n,\ldots,(a_m+k+2) \mod n)_\Pi}}$ are commonly incident only at $((a_1+k+1) \mod n, (a_2+k+1) \mod n, \ldots, (a_m+k+1) \mod n)$, it follows that w is incident at least and additional $\frac{n-2}{2}$ points. Hence any vector in $C_\Pi^\perp$ has weight at least $1 + \frac{n-2}{2} = \frac{n}{2}$, and since the vectors in W_1 have weight $\frac{n}{2}$, the minimum weight is $\frac{n}{2}$. □

Lemmas 8.2.5 to 8.2.12 can be summarised as follows:

Proposition 8.2.13. *Let $\prod_{i=1}^{m} C_n$ be the categorical product of m copies of the n-cycle C_n. Then the code generated by $\prod_{i=1}^{m} C_n$ is*

(a) an $[n^m, (n-2)^m, 2^m]$ code, and its dual an $[n^m, n^m - (n-2)^m, \frac{n}{2}]$ code if $n \geq 4$ is even, and

(b) an $[n^m, (n-1)^m, 2^m]$ code, and its dual an $[n^m, n^m - (n-1)^m, n]$ code if n is odd.

The code generated by the cartesian product $\square_{i=1}^{m} C_n$ is revisited next. Particular attention is paid to this code in the case that $n = 8$.

Lemma 8.2.14. *If $n = 8$, then the set $X = \{v^{\overline{(a_1,a_2,\ldots,a_m)_\square}} : a_1 \in \{1, 2, \ldots, 6\}, a_i \in \{0, 1, \ldots, 7\}, 2 \leq i \leq m\}$ is a linearly independent set in $C_\square$.*

Proof: The result is an immediate consequence of the fact that if the vectors in X as well as the points of $C_\square$, are arranged in lexicographic order, then an upper triangular matrix results. Clearly, $|X| = 6.8^{m-1}$, and hence $\dim(C_\square) \geq 6.8^{m-1}$. □

Lemma 8.2.15. *For* $\{(2,0,0,\ldots,0),(2,0,0,\ldots,0,1),\ \ldots,\ (2,0,0,\ldots,0,7),\ (2,0,0,\ldots,0,1,0),$ $\ldots,\ (2,7,7,\ldots,7),\ \ldots,\ (3,7,7,\ldots,7)\} \subset \{0,1,\ldots,7\}^m$*, let*

$$\begin{aligned}
w[(2,0,0,\ldots,0)] &= v^{\overline{(2,0,0,\ldots,0)_\square}} \\
&\quad + v^{\overline{(4,0,0,\ldots,0,2)_\square}} + v^{\overline{(4,0,0,\ldots,0,2,0)_\square}} + v^{\overline{(4,0,0,\ldots,0,2,0,0,)_\square}} + \cdots + v^{\overline{(4,2,0,0,\ldots,0)_\square}} \\
&\quad + v^{\overline{(4,0,0,\ldots,0,6)_\square}} + v^{\overline{(4,0,0,\ldots,0,6,0)_\square}} + v^{\overline{(4,0,0,\ldots,0,6,0,0)_\square}} + \cdots + v^{\overline{(4,6,0,0,\ldots,0)_\square}} \\
&\quad + v^{\overline{(6,0,0,\ldots,0)_\square}},
\end{aligned}$$

$$\begin{aligned}
w[(2,0,0,\ldots,0,1)] &= v^{\overline{(2,0,0,\ldots,1)_\square}} \\
&\quad + v^{\overline{(4,0,0,\ldots,0,3)_\square}} + v^{\overline{(4,0,0,\ldots,0,2,1)_\square}} + v^{\overline{(4,0,0,\ldots,0,2,0,1)_\square}} + \cdots + v^{\overline{(4,2,0,0,\ldots,0,1)_\square}} \\
&\quad + v^{\overline{(4,0,0,\ldots,0,7)_\square}} + v^{\overline{(4,0,0,\ldots,0,6,1)_\square}} + v^{\overline{(4,0,0,\ldots,0,6,0,1)_\square}} + \cdots + v^{\overline{(4,6,0,0,\ldots,0,1)_\square}} \\
&\quad + v^{\overline{(6,0,0,\ldots,0,1)_\square}},
\end{aligned}$$

$$\vdots$$

$$\begin{aligned}
w[(2,7,7,\ldots,7)] &= v^{\overline{(2,7,7,\ldots,7)_\square}} \\
&\quad + v^{\overline{(4,7,7,\ldots,7,1)_\square}} + v^{\overline{(4,7,7,\ldots,7,1,7)_\square}} + v^{\overline{(4,7,7,\ldots,7,1,7,7)_\square}} + \cdots + v^{\overline{(4,1,7,7,\ldots,7)_\square}} \\
&\quad + v^{\overline{(4,7,7,\ldots,7,5)_\square}} + v^{\overline{(4,7,7,\ldots,7,5,7)_\square}} + v^{\overline{(4,7,7,\ldots,7,5,7,7)_\square}} + \cdots + v^{\overline{(4,5,7,7,\ldots,7)_\square}} \\
&\quad + v^{\overline{(6,7,7,\ldots,7)_\square}},
\end{aligned}$$

$$\begin{aligned}
w[(3,0,0,\ldots,0)] &= v^{\overline{(3,0,0,\ldots,0)_\square}} \\
&\quad + v^{\overline{(5,0,0,\ldots,0,2)_\square}} + v^{\overline{(5,0,0,\ldots,0,2,0)_\square}} + v^{\overline{(5,0,0,\ldots,0,2,0,0,)_\square}} + \cdots + v^{\overline{(5,2,0,0,\ldots,0)_\square}} \\
&\quad + v^{\overline{(5,0,0,\ldots,0,6)_\square}} + v^{\overline{(5,0,0,\ldots,0,6,0)_\square}} + v^{\overline{(5,0,0,\ldots,0,6,0,0)_\square}} + \cdots + v^{\overline{(5,6,0,0,\ldots,0)_\square}} \\
&\quad + v^{\overline{(7,0,0,\ldots,0)_\square}},
\end{aligned}$$

$$\begin{aligned}
w[(3,7,7,\ldots,7)] &= v^{\overline{(3,7,7,\ldots,7)_\square}} \\
&\quad + v^{\overline{(5,7,7,\ldots,7,1)_\square}} + v^{\overline{(5,7,7,\ldots,7,1,7)_\square}} + v^{\overline{(5,7,7,\ldots,7,1,7,7)_\square}} + \cdots + v^{\overline{(5,1,7,7,\ldots,7)_\square}} \\
&\quad + v^{\overline{(5,7,7,\ldots,7,5)_\square}} + v^{\overline{(5,7,7,\ldots,7,5,7)_\square}} + v^{\overline{(5,7,7,\ldots,7,5,7,7)_\square}} + \cdots + v^{\overline{(5,5,7,7,\ldots,7)_\square}} \\
&\quad + v^{\overline{(7,7,\ldots,7)_\square}},
\end{aligned}$$

and let

$$Y = \{w[(2,0,0,0,\ldots,0)], w[(2,0,0,\ldots,0,1)],\ldots, w[(2,0,0,\ldots,0,7)], w[(2,0,0,\ldots,0,1,0)],$$
$$w[(2,7,7,\ldots,7)],\ \ldots,\ w[(3,7,7,\ldots,7)]\}.$$

Then Y is a linearly independent set in $C_{\Box}^{\perp}$. Consequently, X and Y are bases for $C_{\Box}$ and $C_{\Box}^{\perp}$ respectively.

Proof: Suppose that $(a_1', a_2', \ldots, a_m') \in \{0,1,\ldots,7\}^m$, and consider the inner product $(w[(2,a_2,a_3,\ldots,a_m)], v^{\overline{(a_1',a_2',\ldots,a_m')\Box}})$.

Case (i): $a_1' = 0$

If $a_i' = a_i$, for all $i \in \{2,3,\ldots,m\}$, then $(w[(2,a_2,a_3,\ldots,a_m)], v^{\overline{(a_1',a_2',\ldots,a_m')\Box}}) = 2 \equiv 0(\text{mod } 2)$. In all other cases when $a_1' = 0$, $(w[(2,a_2,a_3,\ldots,a_m)], v^{\overline{(a_1',a_2',\ldots,a_m')\Box}}) = 0$.

Case (ii): $a_1' = 2, 4$ or 6
The following sub-cases are distinguished:

(a) If $v^{\overline{(a_1',a_2',\ldots,a_m')\Box}}$ is one of the vectors in the sum $w[(2,a_2,a_3,\ldots,a_m)]$, then since $v^{\overline{(a_1',a_2',\ldots,a_m')\Box}}$ has weight $2m$, $(w[(2,a_2,a_3,\ldots,a_m)], v^{\overline{(a_1',a_2',\ldots,a_m')\Box}}) = 2m \equiv 0(\text{mod } 2)$.

(b) If there exist $i_1, i_2 \in \{2,3,\ldots,m\}$ such that $a_{i_1}' = (a_{i_1} \pm 1)\text{mod n}$ and $a_{i_2}' = (a_{i_2} \pm 1)\text{mod n}$, then $(w[(2,a_2,a_3,\ldots,a_m)], v^{\overline{(a_1',a_2',\ldots,a_m')\Box}}) = 2 \equiv 0(\text{mod } 2)$.

(c) If there exists $j \in \{2,3,\ldots,m\}$ such that $a_j' = (a_j \pm 2)\text{mod n}$ and $a_i' = a_i$, for all $i \in \{2,3,\ldots,m\} \setminus \{j\}$, then $(w[(2,a_2,a_3,\ldots,a_m)], v^{\overline{(a_1',a_2',\ldots,a_m')\Box}}) = 2 \equiv 0(\text{mod } 2)$.

In all other cases when $a_1' = 2, 4$ or $6, (w[2,a_2,a_3,\ldots,a_m)], v^{\overline{(a_1',a_2',\ldots,a_m')\Box}}) = 0$.

Case (iii): $a_1' = 1, 3, 5$ or 7

If there exists $i \in \{2,3,\ldots,m\}$ such that then $a_i' = (a_i \pm 1)\text{mod n}$ and $a_j' = a_j$, for all $j \in \{2,3,\ldots,m\} \setminus \{i\}$, then $(w[(2,a_2,a_3,\ldots,a_m)], v^{\overline{(a_1',a_2',\ldots,a_m')\Box}}) = 0$.

In all other cases when $a'_1 = 1, 3, 5$ or 7, $(w[(2, a_2, a_3, \ldots, a_m)], v^{\overline{(a'_1, a'_2, \ldots, a'_m)\Box}}) = 0$.

Analogous cases are valid if $(w[(3, a_2, a_3, \ldots, a_m)], v^{\overline{(a'_1, a'_2, \ldots, a'_m)\Box}})$ is considered. Hence $Y \subset C_\Box^\perp$.

Now if the elements of Y are arranged in lexicographic order and the points as follows:
first the points
$(1,0,0,\ldots,0), (1,0,0,\ldots,0,1), \ldots, (1,0,0,\ldots,0,7), (1,0,0,\ldots,0,1,0), \ldots, (1,0,0,\ldots,0,$
$7,7), \ldots, (1,7,7,\ldots,7), (2,0,0,\ldots,0), \ldots, (2,7,7,\ldots,7),$
and then the points
$(0,0,\ldots,0), (0,0,\ldots,0,1), \ldots, (0,0,\ldots,0,7), (0,0,\ldots,0,1,0), \ldots, (0,0,\ldots,0,7,7), \ldots,$
$(0,7,7,\ldots,7), (3,0,0,\ldots,0,), (3,0,0,\ldots,0,1), \ldots, (3,7,7,\ldots,7), \ldots, (7,7,\ldots,7),$
an upper triangular matrix results. Hence Y is a linearly independent set in $C_\Box^\perp$. Clearly, $|Y| = 2.8^{m-1}$, and hence $\dim(C_\Box^\perp) \geq 2.8^{m-1}$, and since $C_\Box$ is linear, $\dim(C_\Box) \leq 8^m - 2.8^{m-1} = 6.8^{m-1}$. By the previous lemma, $\dim(C_\Box) \geq 6.8^{m-1}$. Hence $\dim(C_\Box) = 6.8^{m-1}$, and it follows that X and Y are bases for $C_\Box$ and $C_\Box^\perp$ respectively. Note that $Y \subset C_\Box$, and hence $C_\Box^\perp \subset C_\Box$. □

Lemma 8.2.16. *If $n = 8$, then the minimum weight of $C_\Box$ is $2m$.*

Proof: Suppose that $v \in C_\Box$, and that v is incident at $(a_1, a_2, \ldots, a_m)$.

Case (i): $a_1 = 4$ or 5
Suppose that $a_1 = 4$, and consider the set of incidence vectors

$$\begin{aligned} E \;=\; \{ & v^{\overline{(4,(a_2-1) \mod 8, a_3, a_4, \ldots, a_m)\Box}}, \\ & v^{\overline{(4,a_2,(a_3-1) \mod 8, a_4, a_5, \ldots, a_m)\Box}}, \ldots, v^{\overline{(4,a_2,a_3,\ldots,a_{m-1},(a_m-1) \mod 8)\Box}}, v^{\overline{(4,(a_2+1) \mod 8, a_3, a_4, \ldots, a_m)\Box}}, \\ & v^{\overline{(4,a_2,(a_3+1) \mod 8, a_4, a_5, \ldots, a_m)\Box}}, \ldots, v^{\overline{(4,a_2,a_3,\ldots,a_{m-1},(a_m+1) \mod 8)\Box}}, v^{\overline{(5,a_2,a_3,\ldots,a_m)\Box}} \}. \end{aligned}$$

Now $v^{\overline{(4,a'_2,a'_3,\ldots,a'_m)\Box}} \in E$ is included in each vector in the set
$Y_{(4,a'_2,a'_3,\ldots,a'_m)} = \{w[(2, (a'_2-2) \mod 8, a'_3, a'_4, \ldots, a'_m)], w[(2, a'_2, (a'_3-2) \mod 8, a'_4, a'_5, \ldots, a'_m)],$
$\ldots, w[(2, a'_2, a'_3, \ldots, a'_{m-1}, (a'_m-2) \mod 8)], w[(2, (a'_2+2) \mod 8, a'_3, a'_4, \ldots, a'_m)], w[(2, a'_2, (a'_3+$

$2)\bmod 8, a'_4, \ldots, a'_m)], \ \ldots, \ w[(2, a'_2, a'_3, \ldots, \ a'_{m-1}, (a'_m + 2)\bmod 8)]\}$, and the vectors in $Y_{(4,a'_2,a'_3,\ldots,a'_m)}$ are commonly incident only at the points at which $v^{\overline{(4,a'_2,a'_3,\ldots,a'_m)\Box}}$ are incident at.

Similarly, $v^{\overline{(5,a_2,a_3,\ldots,a_m)\Box}} \in E$ is included in each vector in the set $Y_{(5,a_2,a_3,\ldots,a_m)} = \{w[(3, (a_2 - 2)\bmod 8, a_3, a_4, \ldots, a_m)], \ w[(3, a_2, (a_3 - 2)\bmod 8, a_4, a_5, \ \ldots, \ a_m)], \ \ldots, \ w[(3, a_2, a_3, \ \ldots, \ a_{m-1}, (a_m - 2)\bmod 8)], \ w[(3, (a_2 + 2)\bmod 8, a_3, a_4, \ldots, a_m)], \ w[(3, a_2, (a_3 + 2)\bmod 8, a_4, a_5, \ \ldots, \ a_m)], \ \ldots, \ w[(3, a_2, a_3, \ldots, a_{m-1}, (a_m + 2)\bmod 8)]\}$, and the vectors in $Y_{(5,a_2,a_3,\ldots,a_m)}$ are commonly incident only at the points at which $v^{\overline{(5,a_2,a_3,\ldots,a_m)\Box}}$ are incident at.

Moreover, the vectors in E are commonly incident only at $(4, a_2, a_3, \ldots, a_m)$.
Now let

$$\overline{Y} = \bigcup_{v^{\overline{(x_1,x_2,\ldots,x_m)\Box}} \in E} Y_{(x_1,x_2,\ldots,x_m)}.$$

Since $(v, w) = 0,$ for all $w \in \overline{Y}$, and for any $(x'_1, x'_2, \ldots, x'_m) \neq (x''_1, x''_2, \ldots, x''_m)$, and any $w' \in Y_{(x'_1,x'_2,\ldots,x'_m)}, w'' \in Y_{(x''_1,x''_2,\ldots,x''_m)}, w'$ and w'' are commonly incident only at $(4, a_2, a_3, \ldots, a_m)$, it follows that for each vector in E, v is incident at at least an additional point i.e. v is incident at at least an additional $2(m-1)+1$ points. Hence v has weight at least $2(m-1)+1+1 = 2m$. A similar argument is valid if $a_1 = 5$.

Case (ii): $a_1 = 2, 3, 6$ or 7

Suppose that $a_1 = 2$, and consider the set

$$\begin{aligned} Y_{(2,a_2,a_3,\ldots,a_m)} \ = \ & \{w[(2, (a_2 - 1)\bmod 8, a_3, a_4, \ldots, a_m)], w[(2, a_2, (a_3 - 1)\bmod 8, a_4, a_5, \ldots, a_m)], \\ & \ldots, w[(2, a_2, a_3, \ldots, a_{m-1}, (a_m - 1)\bmod 8)], w[(2, (a_2 + 1)\bmod 8, a_3, a_4, \\ & \ldots, a_m)], w[(2, a_2, (a_3 + 1)\bmod 8, a_4, a_5, \ldots, a_m)], \ldots, w[(2, a_2, a_3, \ldots, a_{m-1}, \\ & (a_m + 1)\bmod 8)], w[(3, a_2, a_3, \ldots, a_m)]\}. \end{aligned}$$

Since $(v, w) = 0,$ for all $w \in Y_{(2,a_2,a_3,\ldots,a_m)}$, and since the vectors in $Y_{(2,a_2,a_3,\ldots,a_m)}$ are commonly incident at points other than $(2, a_2, a_3, \ldots, a_m)$, it follows that v is incident at at least an additional point P. Now either $P = (4, a_2, a_3, \ldots, a_m)$, or $P = (6, a_2, a_3, \ldots, a_m)$,

or P is of the form $(4, a'_2, a'_3, \ldots, a'_m)$, where for some $j \in \{2, 3, \ldots, m\}, a'_j = (a_j \pm 2) \bmod 8$, and $a'_i = a_i,$ for all $i \in \{2, 3, \ldots, m\} \setminus \{j\}$. These sub-cases are considered below:

(a) If $P = (4, a_2, a_3, \ldots, a_m)$, then by the same argument as in Case(i) but with

$$E = \{v^{\overline{(4,(a_2-1) \mod 8, a_3, a_4, \ldots, a_m)\sqcup}}, v^{\overline{(4,a_2,(a_3-1) \mod 8, a_4, a_4, \ldots, \ldots, a_m)\square}}, \ldots,$$
$$v^{\overline{(4,a_2,a_3,\ldots,a_{m-1},(a_m-1) \mod 8)\square}}, v^{\overline{(4,(a_2+1) \mod 8, a_3, a_4, \ldots, a_m)\square}}, v^{\overline{(4,a_2,(a_3+1) \mod 8, a_4, a_5, \ldots, a_m)\square}},$$
$$\ldots, v^{\overline{(4,a_2,a_3,\ldots,a_{m-1},(a_m+1) \mod 8)\square}}\},$$

v is incident at at least an additional $2(m-1)+1$ points in total. Hence v has weight at least $2(m-1)+1+1 = 2m$.

(b) Suppose that $P = (6, a_2, a_3, \ldots, a_m)$.
Now the incidence vector $v^{\overline{(5,a_2,a_3,\ldots,a_m)\square}}$ is included in each vector in the set $\{w[(3, (a_2 - 2) \bmod 8, a_3, a_4, \ldots, a_m)], w[(3, a_2, (a_3 - 2) \bmod 8, a_4, a_5, \ldots, a_m)], \ldots, w[(3, a_2, a_3, \ldots, a_{m-1}, (a_m - 2) \bmod 8)], w[(3, (a_2 + 2) \bmod 8, a_3, a_4, \ldots, a_m)], w[(3, a_2, (a_3 + 2) \bmod 8, a_4, a_5, \ldots, a_m)], \ldots, w[(3, a_2, a_3, \ldots, a_{m-1}, (a_m + 2) \bmod 8)]\}$, and since these vectors are commonly incident only at the points at which $v^{\overline{(5,a_2,a_3,\ldots,a_m)\square}}$ is incident at, v is incident at at least an additional point P' at which $v^{\overline{(5,a_2,a_3,\ldots,a_m)\square}}$ is incident at. W. l. o. g. it can be assumed that $P' = (5, a_2, a_3, \ldots, (a_m + 1) \bmod 8)$. Then by the same argument as in Case (i) but with

$$E = \{v^{\overline{(5,(a_2-1) \mod 8, a_3, a_4, \ldots, (a_m+1) \mod 8)\square}}, v^{\overline{(5,a_2,(a_3-1) \mod 8, a_4, a_5, \ldots, (a_m+1) \mod 8)\square}},$$
$$\ldots, v^{\overline{(5,a_2,a_3,\ldots,a_{m-1},a_m)\square}}, v^{\overline{(5,(a_2+1) \mod 8, a_3, a_4, \ldots, (a_m+1) \mod 8)\square}},$$
$$v^{\overline{(5,a_2,(a_3+1) \mod 8, a_4, a_5, \ldots (a_m+1) \mod 8)\square}}, \ldots, v^{\overline{(5,a_2,a_3,\ldots,a_{m-1},(a_m+2) \mod 8)\square}},$$
$$v^{\overline{(4,a_2,a_3,\ldots,(a_m+1) \mod 8)\square}}\}$$

v is incident at at least an additional $(2(m-1)+1)+1 = 2m$ points in total. Hence v has weight at least $2m+1$.

(c) The argument in the case of P being of the form $(4, a'_2, a'_3, \ldots, a'_m)$ where for some $j \in \{2, 3, \ldots, m\}, a'_j = (a_j \pm 2) \bmod 8$, and $a'_i = a_i,$ for all $i \in \{2, 3, \ldots, m\} \setminus \{j\}$, follows a similar course as the argument in (b) above.

Hence if $a_1 = 2$, then v has weight at least $2m$. Similar arguments are valid if $a_1 = 3, 6$ or 7.

Case (iii): $a_1 = 0$ or 1

Suppose that $a_1 = 0$. Then since $w[(3, a_2, a_3, \ldots, a_m)]$ is incident at $(0, a_2, a_3, \ldots, a_m)$ and $(v, w[(3, a_2, a_3, \ldots, a_m)]) = 0, v$ is incident at at least an additional point P at which some incidence vector included in $w[(3, a_2, a_3, \ldots, a_m)]$ is incident. There are three sub-cases which need to be considered:

(a) P is a point at which $v^{\overline{(7,a_2,a_3,\ldots,a_m)_\Box}}$ is incident:

The argument is similar to the argument in Case (ii)(a), and hence v has weight at least $2m$.

(b) P is a point at which $v^{\overline{(3,a_2,a_3,\ldots,a_m)_\Box}}$ is incident:

In this case the argument is similar to the argument in Case (ii)(b), and hence v has weight at least $2m + 1$.

(c) P is a point at which some vector in the set

$$\{v^{\overline{(5,(a_2-2) \mod 8,a_3,a_3,\ldots,a_m)_\Box}}, v^{\overline{(5,a_2,(a_3-2) \mod 8,a_4,a_5,\ldots,a_m)_\Box}}, \ldots, v^{\overline{(5,a_2,a_3,\ldots,a_{m-1},(a_m-2) \mod 8)_\Box}},$$

$$v^{\overline{(5,(a_2+2) \mod 8,a_3,a_4,\ldots,a_m)_\Box}}, v^{\overline{(5,a_2,(a_3+2) \mod 8,a_4,a_5,\ldots,a_m)_\Box}}, \ldots, v^{\overline{(5,a_2,a_3,\ldots,a_{m-1},(a_m+2) \mod 8)_\Box}}\}$$

is incident:

In the final case, the argument is similar to the argument in Case (ii)(c), and again, v has weight at least $2m + 1$.

Hence if $a_1 = 0$, then v has weight at least $2m$. A similar argument holds if $a_1 = 1$.

Since each incidence vector has weight $2m$, and for each $(a_1, a_2, \ldots, a_m) \in \{0, 1, 2, \ldots, 7\}^m$, there is an incidence vector which is incident at it, it follows that the minimum weight is $2m$. □

Note that if $n = 8$, then since $C_\Box^\perp \subset C_\Box$, the minimum weight of $C_\Box^\perp$ is at least $2m$. In addition, since the vectors in $Y \subset C_\Box^\perp$ each have weight $(1 + 2(m - 1) + 1).2m = 4m^2$,

the minimum weight is at most $4m^2$.

Lemmas 8.2.14 to 8.2.16 can be summarised by the following proposition:

Proposition 8.2.17. *Let $\square_{i=1}^{m} C_8$ be the cartesian product of m copies of the 8-cycle C_8. Then the code generated by $\square_{i=1}^{m} C_8$ is an $[8^m, 6.8^{m-1}, 2m]$ code which contains its dual.*

Now recall that as a consequence of Lemma 8.2.3 and the fact that $C_2 \square C_2 \cong C_4$, it was noted that if $n = 4$, then $C_\square$ is a $[2^{2m}, 2^{2m-1}, 2m]$ i.e. a $[4^m, 2.4^{m-1}, 2m]$ self-dual code. In conjunction with Proposition 8.2.17, the following is conjectured:

Conjecture 8.2.18. *Let $\square_{i=1}^{m} C_n$ be the cartesian product of m copies of the n-cycle C_n. If $n = 2^k$, where $k \geq 2$, then the code generated by $\square_{i=1}^{m} C_n$ is an $[n^m, (n-2)n^{m-1}, 2m]$ code which contains its dual. Furthermore, if $n = 4$, then the code is self-dual.*

A few ideas about the automorphisms and partial PD-sets for the codes generated by the various cycle products will be discussed next. It should be emphasised that these ideas merely skim the surface of the topic, and much more could be done in this area.

8.3 Automorphism groups and PD-sets for the Codes from Cycle Products

Recall from the introduction that the original motivation for focusing on the graph products of C_n in particular was that it was conjectured that the automorphism groups of the various products, and hence the candidates for PD-sets would be easily identifiable, and would be a product of some sort of the Dihedral group D_{2n}. Results concerning the automorphism groups of graph products in general do not abound in the literature. Some of the most important results can be found in [37]. With regard to the automorphism groups of the codes generated by these various cycle products, the main objective was

the identification of PD-sets. Hence the identification of a set of automorphisms for the various graph products, and not the entire automorphism group as such took priority, since such a set is obviously contained in the automorphism group of the code.

In some of the cases that were studied, the wreath product of D_{2n} by S_m provided the key to determining PD-sets. The wreath product $H = K \wr S_m$ of K and S_m is the semi-direct product $H = L \rtimes S_m$ where $L = K \times K \times \cdots \times K$ to m factors. In particular, if $K = D_{2n}$, then for $((\sigma_1, \sigma_2, \ldots, \sigma_m), \alpha) \in H$, and $(a_1, a_2, \ldots, a_m) \in \{0, 1, \ldots, n-1\}^m$,

$$\begin{aligned} ((\sigma_1, \sigma_2, \ldots, \sigma_m), \alpha)(a_1, a_2, \ldots, a_m) &= ((\sigma_1(a_1), \sigma_2(a_2), \ldots, \sigma_m(a_m)), \alpha) \\ &= (\sigma_{\alpha(1)}(a_{\alpha(1)}), \sigma_{\alpha(2)}(a_{\alpha(2)}), \ldots, \sigma_{\alpha(m)}(a_{\alpha(m)})). \end{aligned}$$

By Proposition 8.2.13, if n is odd, then the code C_Π generated by the categorical product $\prod_{i=1}^{m} C_n$ of m copies of C_n is an $[n^m, (n-1)^m, 2^m]$ code having the points

$(0, 0, \ldots, 0)$, $(0, 0, \ldots, 0, 1)$, $\ldots$, $(0, 0, \ldots, 0, n-2)$, $(0, 0, \ldots, 0, 1, 0)$, $\ldots$, $(0, 0, \ldots, 0, n-2, n-2)$, $\ldots$, $(n-2, n-2, \ldots, n-2)$,

as information positions. In addition, C_Π corrects $2^{m-1} - 1$ errors. Clearly, if $\sigma = ((\sigma_1, \sigma_2, \ldots, \sigma_m), \alpha) \in D_{2n} \wr S_m$, then σ preserves adjacency of points of $\prod_{i=1}^{m} C_n$, and hence $\sigma \in \text{Aut}\left(\prod_{i=1}^{m} C_n\right)$. Firstly, observe that if $m = 2$, then C_Π corrects one error, and syndrome decoding could be used to correct the error. Secondly, if $m = 3$, then C_Π corrects three errors, and

$$\mathcal{S} = \{((\sigma_1, \sigma_2, \sigma_3), 1_{S_3}) : \ \sigma_1, \sigma_2, \sigma_3 \text{ are rotations in } \ D_{2n}\}$$

is a PD-set of size n^3 for C_Π with the information positions as given above. In general, observe the following:

Proposition 8.3.1. *Let $\mathcal{I}$ denote the points*
$P_1 = (0, 0, 0, \ldots, 0)$, $P_2 = (0, 0, \ldots, 0, 1)$,$\ldots$, $P_{n-1} = (0, 0, \ldots, 0, n-2)$, $P_n = (0, 0, \ldots, 0, 1, 0)$, $\ldots$, $P_{(n-1)^2} = (0, 0, \ldots, 0, n-2, n-2)$, $\ldots$, $P_{(n-1)^m} = (n-2, n-2, \ldots, n-2)$.

Then if n is odd and $m \geq 4$,

$$\mathcal{S} = \{((\sigma_1, \sigma_2, \ldots, \sigma_m), 1_{S_m}) : \ \sigma_i \ \textit{is a rotation in } D_{2n}, \ \textit{for all } i \in \{1, 2, \ldots, m\}\}$$

is an m-PD-set of size n^m for C_Π with $\mathcal{I}$ as information positions.

Proof: Suppose that the $m < 2^{m-1} - 1$ errors occur at $\mathcal{E} = \{(e_{11}, e_{12}, \ldots, e_{1m}), (e_{21}, e_{22}, \ldots, e_{2m}), \ldots, (e_{m1}, e_{m2}, \ldots, e_{mm})\}$. Clearly, in all cases, $((\sigma_1, \sigma_2, \ldots, \sigma_m), 1_{S_m})$ where $\sigma_i(e_{ii}) = n - 1$, for all $i \in \{1, 2, \ldots, m\}$, will map $\mathcal{E}$ into $\mathcal{P} \setminus \mathcal{I}$. □

The situation is somewhat different if n is even, as is evident from the next observation.

Lemma 8.3.2. *If n is even, then $\prod_{i=1}^{m} C_n$ is not connected.*

Proof: This follows directly from the fact that, since n is even, each point $(a_1, a_2, \ldots, a_m) \in \{0, 1, \ldots, n-1\}^m$ is connected only to points of the form $(a'_1, a'_2, \ldots, a'_m)$, where for all $i \in \{1, 2, \ldots, m\}$, $(a_i + a'_i) \bmod 2$ is constant. □

A consequence of the above lemma is that no two points in the set $T = \{(0, a_2, a_3, \ldots, a_m) : a_i \in \{0, 1\}, \text{for all } i \in \{2, 3, \ldots, m\}\}$ are connected. Hence each is in a different component of $\prod_{i=1}^{m} C_n$, and thus $\prod_{i=1}^{m} C_n$ has at least 2^{m-1} components. Since each point $(a'_1, a'_2, \ldots, a'_m) \in \{0, 1, \ldots, n-1\}^m$ is connected to exactly one point in T, it follows that $\prod_{i=1}^{m} C_n$ has precisely 2^{m-1} components each having $\frac{n^m}{2^{m-1}} = 2.(\frac{n}{2})^m$ points.

Let $\mathcal{P}$ denote the points of $\prod_{i=1}^{m} C_n$, and for $t \in T$, let $\mathcal{P}_t$ denote the points of the component of $\prod_{i=1}^{m} C_n$ which contains t.

For $(k_1, k_2, \ldots, k_m) \in \{0, 2, \ldots, n-2\}^m$, $(a_1, a_2, \ldots, a_m) \in \mathcal{P}$, and $t \in \mathcal{P}_t$, let

$\lambda_t^{(k_1,k_2,\ldots,k_m)} : \mathcal{P} \to \mathcal{P}$ be defined by

$$\lambda_t^{(k_1,k_2,\ldots,k_m)}(a_1,a_2,\ldots,a_m) = \begin{cases} (a_1,a_2,\ldots,a_m) \text{ if } (a_1,a_2,\ldots,a_m) \in \mathcal{P} \setminus \mathcal{P}_t \\ \\ ((a_1+k_1) \bmod n, (a_2+k_2) \bmod n, \ldots, (a_m+k_m) \bmod n) \\ \text{if } (a_1,a_2,\ldots,a_m) \in \mathcal{P}_t. \end{cases}$$

Lemma 8.3.3. *If n is even, then for $t \in \mathcal{P}_t$, $(k_1,k_2,\ldots,k_m) \in \{0,2,\ldots,n-2\}^m$, $\lambda_t^{(k_1,k_2,\ldots,k_m)}$ is an automorphism of $\prod_{i=1}^{m} C_n$.*

Proof: The result is immediate from the observation that for $t \in \mathcal{P}_t, (k_1,k_2,\ldots,k_m) \in \{0,2,\ldots,n-2\}^m$, $\lambda_t^{(k_1,k_2,\ldots,k_m)}$ preserves adjacency of points of $\prod_{i=1}^{m} C_n$. □

Recall that by Proposition 8.2.13, if $n \geq 4$ is even, then C_Π is an $[n^m, (n-2)^m, 2^m]$ code with the points
$(1,1,\ldots,1)$, $(1,1,\ldots,1,2)$, $\ldots$, $(1,1,\ldots,1,n-2)$, $(1,1,\ldots,1,2,1)$, $\ldots$, $(1,1,\ldots,1,2,n-2)$, $\ldots$, $(1,1,\ldots,1,n-2,n-2)$, $\ldots$, $(n-2,n-2,\ldots,n-2)$,
as information positions. As in the case when n is odd, C_Π corrects $2^{m-1}-1$ errors. Observe that if $m=2$, then C_Π corrects one error, and syndrome decoding could be used to correct the error. Next, observe that if $m=3$, then C_Π corrects three errors, and

$$\mathcal{S} = \{\lambda_{t_1}^{(k_1,0,0)} \circ \lambda_{t_2}^{(0,k_2,0)} \circ \lambda_{t_3}^{(0,0,k_3)} : t_1,t_2,t_3 \in \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\}, k_1,k_2,k_3 \in \{0,2,\ldots,n-2\}\}$$

is a PD-set of size $4^3(\frac{n}{2})^3$ for C_Π with the information positions as given above. The following is the analogy to Proposition 8.3.1:

Proposition 8.3.4. *Let $\mathcal{I}$ denote the points*

$P_1 = (1,1,1,\ldots,1)$, $P_2 = (1,1,\ldots,1,2)$, $\ldots$, $P_{n-2} = (1,1,\ldots,1,n-2)$, $P_{n-1} = (1,1,\ldots,1,2,1)$, $\ldots$, $P_{(n-2)^2} = (1,1,\ldots,1,n-2,n-2)$, $\ldots$, $P_{(n-2)^m} = (n-2,n-2,\ldots,n-2)$.
Then if $n \geq 4$ is even and $m \geq 4$,

$$\mathcal{S} = \{\lambda_{t_1}^{(k_1,0,0,\ldots,0)} \circ \lambda_{t_2}^{(0,k_2,0,0,\ldots,0)} \ldots \circ \lambda_{t_m}^{(0,0,\ldots,0,k_m)} : \ t_i \in \{(0,0,\ldots,0),(0,0,\ldots,0,1),$$

$$\ldots, (0,1,1,\ldots,1)\},\ k_i \in \{0,2,\ldots,n-2\},\ \textit{for all}\ i \in \{1,2,\ldots,m\}\}$$

is an m-PD-set of size $(2^{m-1})^m(\frac{n}{2})^m$ *for* C_Π *with* $\mathcal{I}$ *as information positions.*

Proof: Suppose that the $m < 2^{m-1} - 1$ errors occur at $\mathcal{E} = \{(e_{11}, e_{12}, \ldots, e_{1m}), (e_{21}, e_{22}, \ldots, e_{2m}), \ldots, (e_{m1}, e_{m2}, \ldots, e_{mm})\}$. For each $i \in \{1,2,\ldots,m\}$, let $t_i \in \{(0,0,\ldots,0), (0,0,\ldots,0,1), \ldots, (0,1,1,\ldots,1)\}$ be such that $(e_{i1}, e_{i2}, \ldots, e_{im}) \in \mathcal{P}_{t_i}$. Then in all cases, $\lambda_{t_1}^{(k_1,0,0,\ldots,0)} \circ \lambda_{t_2}^{(0,k_2,0,0,\ldots,0)} \ldots \circ \lambda_{t_m}^{(0,0,\ldots,0,k_m)}$, where $\lambda_{t_i}^{(0,\ldots,0,k_i,0,\ldots,0)}(e_{i1}, e_{i2}, \ldots, e_{im}) = (a_{i1}, a_{i2}, \ldots, a_{im})$ and $a_{ii} \in \{0, n-1\}$, for all $i \in \{1,2,\ldots,m\}$, will map $\mathcal{E}$ into $\mathcal{P} \setminus \mathcal{I}$. □

The final observations relate to the code generated by the cartesian product $\square_{i=1}^m C_n$. If $n = 2$ and m is even, then by Lemma 8.2.3, $C_\square$ is a $[2^m, 2^{m-1}, m]$ code and the points $(1,0,0,\ldots,0)$, $(1,0,0,\ldots,0,1)$, $(1,0,0,\ldots,0,1,0)$, $\ldots$, $(1,1,\ldots,1)$ are information positions for $C_\square$. In addition, $C_\square$ corrects $\dfrac{m-2}{2}$ errors. It is well documented that the automorphism group of $\square_{i=1}^m C_2$ is $S_2 \wr S_m$ which has order $2^m.m!$. Also, since $C_4 \cong C_2 \square C_2$, the automorphism group of $\square_{i=1}^m C_4 \cong \square_{i=1}^{2m} C_2$ is $S_2 \wr S_{2m}$.

The following observations relate to the code generated by $\square_{i=1}^m C_2$:
Observe that if $m = 4$, then $C_\square$ corrects one error, and syndrome decoding could be used to correct the error. The following proposition is next observed:

Proposition 8.3.5. *Let* $\mathcal{I}$ *denote the points*

$P_1 = (1,0,0,\ldots,0)$, $P_2 = (1,0,0,\ldots,0,1)$, $P_3 = (1,0,0,\ldots,0,1,0)$, $\ldots$,

$P_{2^{m-1}-1} = (1,1,\ldots,1,0)$, $P = P_{2^{m-1}} = (0,1,1,\ldots,1,0)$.

Then if $n = 2$ *and* $m \geq 6$ *is even ,*

$$\mathcal{S} = \{((\sigma_1, \sigma_2, \ldots, \sigma_m), \alpha) : \sigma_i \in S_2, \text{ for all } i \in \{1,2,\ldots,m\}, \alpha \in \{1_{S_m}, (m, m-1)\}\}$$

is a 2-PD-set of size 2^{m+1} *for* $C_\square$ *with* $\mathcal{I}$ *as information positions.*

Proof: Let

$$Q = (1, 1, \ldots, 1),\ Q \in \mathcal{P} \setminus \mathcal{I},$$

and suppose that the $2 \leq \dfrac{m-2}{2}$ errors occur at $\mathcal{E}$.

Case (i): $\mathcal{E} \subseteq \mathcal{P} \setminus \mathcal{I}$

Then $((1_{S_2}, 1_{S_2}, \ldots, 1_{S_2}), 1_{S_m})$ will keep $\mathcal{E}$ fixed.

Case (ii): $\mathcal{E} \subseteq \mathcal{I}$

(a) $P \notin \mathcal{E}$

Then since $Q \notin \mathcal{E}, (((0,1), 1_{S_2}, 1_{S_2}, \ldots, 1_{S_2}, (0,1)), 1_{S_m})$ will map $\mathcal{E}$ into $\mathcal{P} \setminus \mathcal{I}$.

(b) $P \in \mathcal{E}$

Then $(((0,1), 1_{S_2}, 1_{S_2}, \ldots, 1_{S_2}, (0,1)), 1_{S_m})$ will map P to Q and $\mathcal{E} \setminus \{P\}$ into $\mathcal{P} \setminus \mathcal{I}$.

Case (iii): $\mathcal{E} \cap I \neq \emptyset, \mathcal{E} \cap \mathcal{P} \setminus \mathcal{I} \neq \emptyset$

(a) $P \in \mathcal{E}, Q \in \mathcal{E}$

Then $((1_{S_2}, 1_{S_2}, \ldots, 1_{S_2}), (m, m-1))$ will map $\mathcal{E}$ into $\mathcal{P} \setminus \mathcal{I}$.

(b) $P \in \mathcal{E}, Q \notin \mathcal{E}$

Suppose that $\mathcal{E} \cap \mathcal{P} \setminus \mathcal{I} = \{(0, a_2, a_3, \ldots, a_m)\}$. If there exists $i \in \{2, 3, \ldots, m\}$ such that a_i is equal to the ith coordinate of P, then $((\sigma_1, \sigma_2, \ldots, \sigma_m), 1_{S_m})$ where $\sigma_i = (0,1)$ and $\sigma_j = 1_{S_2}$, for all $j \in \{1, 2, \ldots, m\} \setminus \{i\}$ will do. Otherwise, $((1_{S_2}, 1_{S_2}, 1_{S_2}, \ldots, 1_{S_2}), (m, m-1))$ will do.

(c) $P \notin \mathcal{E}, Q \in \mathcal{E}$

Suppose that $\mathcal{E} \cap \mathcal{I} = \{(1, a_2, a_3, \ldots, a_m)\}$. Then $(((0,1), (0,1), \ldots, (0,1)), \alpha)$, where $\alpha = (m, m-1)$ if $((0,1), (0,1), \ldots, (0,1))((1, a_2, a_3, \ldots, a_m)) = P$ and $\alpha = 1_{S_m}$ otherwise, will map P into $\mathcal{P} \setminus \mathcal{I}$ and Q to $(0, 0, \ldots, 0)$.

(d) $P \notin \mathcal{E}, Q \notin \mathcal{E}$

Suppose that $\mathcal{E} \cap \mathcal{I} = \{(1, a_2, a_3, \ldots, a_m)\}$, and $\mathcal{E} \cap \mathcal{P} \backslash \mathcal{I} = \{(0, a'_2, a'_3, \ldots, a'_m)\}$. Since $\mathcal{E} \cap \mathcal{I} \neq \{Q\}$, there exist $i_1, i_2, \ldots, i_k \in \{2, 3, \ldots, m\}$ such that $a_{i_j} = 0$, for all $j \in \{1, 2, \ldots, k\}$. Then $((1_{S_2}, \sigma_2, \sigma_3, \ldots, \sigma_m), \alpha)$, where $\sigma_i = (0, 1)$ if $i \in \{i_1, i_2, \ldots, i_k\}$, $\sigma_i = 1_{S_2}$, for all $i \in \{2, 3, \ldots, m\} \setminus \{i_1, i_2, \ldots, i_k\}$, and $\alpha = (m, m-1)$ if $(1_{S_2}, \sigma_2, \sigma_3, \ldots, \sigma_m)((0, a'_2, a'_3, \ldots, a'_m)) = P$, and $\alpha = 1_{S_m}$ otherwise, will map $\mathcal{E}$ into $\mathcal{P} \setminus \mathcal{I}$. Hence $\mathcal{S}$ is a 2-PD-set for $C_\square$. □

Note that the partial PD-set in the above proposition is unable to correct three or more errors. In [21] Key and Seneviratne have found 3-PD-sets of size $m.2^m$ for $\square_{i=1}^m C_2$ where $m \geq 6$ is even. However, for correcting two errors, the 2-PD-set given in Proposition 8.3.5 is the better option.

In conclusion, it should be iterated that the work in this chapter merely skims the surface of this vast area of knowledge that needs to be uncovered. Not only do the codes generated by the various products of other graphs need to be investigated, but deeper questions relating to which properties of the code from the original graph are reflected in the codes from the various products of the graph need to be investigated. For example, it has been shown that the code generated by the Petersen graph is a $[\binom{5}{2}, \binom{4}{2}, 3]$ code. Will the code generated by the categorical product of m copies of the Petersen graph be a $[\binom{5}{2}^m, \binom{4}{2}^m, 3^m]$ code? Will the code generated by the cartesian product be a $[\binom{5}{2}^m, \binom{4}{2}\binom{5}{2}^{m-1}, 3m]$ code? What will the parameters of the code generated by the lexicographic product be?

Appendix A
Constructing codes from Uniform Subset graphs

The following series of functions was written to construct binary codes from the Uniform Subset graphs $G(n, r, k)$ in much the same, albeit more general way, than has been the case in Appendix G in [33]. It has been implemented to obtain the codes from the complements of the Triangular graphs, the codes from the Odd graphs, and the codes from the Johnson graphs. The function `next_vert` appears as `next_set` in [19].

```
>next_vert:=function(a,n,r);
function> b:=a;
function> for i:=0 to r-1 do
function|for> if a[r-i] lt n-i then
function|for|if> for j:=0 to i do
function|for|if|for> b[r-i+j]:=a[r-i]+1+j;
function|for|if|for> end for;
function|for|if> break i;
function|for|if> else
function|for|if> end if;
function|for> end for;
```

```
function> return b;
function> end function;


>gen_verts:=function(n,r);
function> a:=[1..r];
function> verts:=[a];
function> while a[1] ne n-r+1 do
function|while> a:=next_vert(a,n,r);
function|while> verts:=Append(verts,a);
function|while> end while;
function> return verts;
function> end function;


> count_verts:=function(n,r);
function> verts:=gen_verts(n,r);
function> v:=#(gen_verts(n,r));
function> return v;
function> end function;


> make_des:=function(n,r,k);
function> verts:=gen_verts(n,r);
function> v:=count_verts(n,r);
function> blox:=[ ];
function> for i:=1 to v do
function|for> blok:= ;
function|for> a:=Seqset(verts[i]);
function|for> for j:=1 to v do
function|for|for> b:=Seqset(verts[j]);
```

```
function|for|for> if #(a meet b) eq k then
function|for|for|if> blok:=blok join j;
function|for|for|if> end if;
function|for|for> end for;
function|for|for> blox:=Append(blox,blok);
function|for|for> end for;
function> des:=Design<1,v|blox>;
function> return des;
function> end function;


> give_code:=function(n,r,k);
function> des:=make_des(n,r,k);
function> code:=LinearCode(des,GF(2));
function> return code;
function> end function;
```

Appendix B

B 1: The Gordon Bound for $\overline{T(n)}$

The following tables are comparisons between the Gordon bound for the size of the PD-sets of the dual code obtained from the complement of the Triangular graph if $n \equiv 1 (\text{mod } 4)$, and if $n \equiv 3 (\text{mod } 4)$. The first column gives the value of n, the second the length of the code, the third the number of errors corrected, the fourth the Gordon bound, and the last column gives the size of the PD-set constructed. Magma [6] was used to obtain the values in the tables.

n	length	t	bound	PD-set
5	10	1	2	5
9	36	3	4	9
13	78	5	6	13
17	136	7	8	17
21	210	9	10	21
25	300	11	12	25
29	406	13	14	29
33	528	15	16	33
37	666	17	18	37

n	length	t	bound	PD-set
7	21	2	3	21
11	55	4	5	73
15	105	6	7	157
19	171	8	9	273
23	253	10	11	421
27	351	12	13	601
31	465	14	15	813
35	595	16	17	1057
39	741	18	19	1333

B2 : The Gordon Bound for $O(k)$

The following table compares the values of the Gordon bound for PD-sets obtained from the Odd graph $O(k)$ where $k \geq 2$, the size of the 2-PD-set obtained in Theorem 6.3.2, and the order of the automorphism group, S_{2k+1}, which is a full PD-set with the information positions as given in the above-mentioned theorem. The first column gives the size of k, the second the length of the code, the third the number of errors corrected, the fourth the Gordon bound, the fifth the size of the 2-PD-set, and the sixth the order of S_{2k+1}.

k	$\binom{2k+1}{k}$	$\lfloor \frac{k}{2} \rfloor$	Gordon bound	2-PD-set	$\lvert S_{2k+1} \rvert$
2	10	1	3	100	120
3	35	1	3	225	5040
4	126	2	7	441	362880
5	462	2	7	784	3991680
6	1716	3	16	1296	6227020800
7	6435	3	15	2025	1307674368000
8	24310	4	32	3025	355687428100000
9	92378	4	32	4356	121645100400000000
10	352716	5	68	6084	$\approx 5.2 \times 10^{19}$
11	1352078	5	67	8281	$\approx 2.6 \times 10^{20}$
12	5200300	6	140	11025	$\approx 1.6 \times 10^{25}$
13	20058300	6	140	14400	$\approx 1.1 \times 10^{28}$
14	77558760	7	288	18496	$\approx 8.8 \times 10^{30}$
15	300540195	7	288	23409	$\approx 8.2 \times 10^{33}$

Appendix C

A PD-set of size 36 for $O(4)$

The following PD-set was calculated for the codes generated by the adjacency matrix of the Odd graph, $O(4)$, with the information positions as given in Theorem 6.3.2. The automorphism group of the code from the general Odd graph, $O(k)$, has been shown to be S_{2k+1}, and hence the elements of the PD-set are elements of S_9, and written below in cycle notation. The calculations were done using the Magma programmes given in [19].

$(1,4,9,3,2)(5,7,8)$;
$(2,3)(4,6,9)$;
$(1,8,5,3,9,6,2,7)$;
$(1,9,7,4,2,8,5)(3,6)$;
$(3,4,8,9)(5,6)$;
$(1,4,5,7,8,9,2)$;
$(1,3,2,4,7,5,8,9)$;
$(1,5)(2,8,9,7,4,3,6)$;
$(1,5,8,2,4,7,9)$;
$(1,5)(2,7,4,3,6)(8,9)$;
$(1,7,3,6,5,2,9,8)$;
$(1,7,2,6,4)(3,8,9,5)$;
$(1,8,4,9,7)(2,6,3,5)$;

$(1,8,9,7)(2,6,3,5)$;

$(4,9)(5,6)$;

$(2,3)(4,7,6,9)$;

$(2,9,4,5,7,6,3)$;

$(1,4,5,6,7,8,3,9,2)$;

$(2,3)(4,5,6,9)$;

$(3,9)(4,8)$;

$(1,6)(2,5,4)(3,7)(8,9)$;

$(1,6,7,3,5,2,9,8)$;

$(1,9,2)(4,6,5,7,8)$.

Appendix D
Constructing codes from the Cartesian product of n-cycles

The following series of functions was written to construct binary codes from the cartesian product of n-cycles in a similar way as had been the case in Appendix A. The function `make_proddes` can be adapted to obtain the $1-(v,k,k)$ design from the categorical product, the lexicographic product, or the strong product of n-cycles.

```
> next_prodvert:=function(a,n,r);
function> b:=a;
function> if a[r] lt n then
function|if> b[r]:=a[r]+1;
function|if> else
function|if> if exists(m)i:i in [1..r]|forallj:j in [i..r]|a[j] eq n and a[i-1]
ne n then
function|if|if> b[m-1]:=a[m-1]+1;
function|if|if> for k:=m to r do
function|if|if|for> b[k]:=0;
function|if|if|for> end for;
function|if|if> end if;
```

```
function|if> end if;
function> return b;
function> end function;

> gen_prodverts:=function(n,r);
function> a:=[ ];
function> for i:=1 to r do
function|for> a:=Append(a,0);
function|for> end for;
function> prodverts:=[a];
function> while existsj:j in[1..r]|a[j] ne n do
function|while> a:=next_prodvert(a,n,r);
function|while> prodverts:=Append(prodverts,a);
function|while> end while;
function> return prodverts;
function> end function;

> count_prodverts:=function(n,r);
function> verts:=gen_prodverts(n,r);
function> v:=#(gen_prodverts(n,r));
function> return v;
function> end function;

> make_proddes:=function(n,r);
function> verts:=gen_prodverts(n,r);
function> v:=count_prodverts(n,r);
function> blox:=[ ];
function> for i:=1 to v do
function|for> blok:=;
function|for> for j:=1 to v do
```

```
function|for|for> if existsk:k in [1..r]|(verts[i][k] eq (verts[j][k]+1) mod
(n+1) and foralll:l in [1..k-1] cat [k+1..r]|verts[i][l] eq verts[j][l]) or
(verts[i][k] eq (verts[j][k]-1) mod (n+1) and foralll:l in [1..k-1] cat [k+1..r]|vert
eq verts[j][l]) then
function|for|for|if> blok:=blok join j;
function|for|for|if> end if;
function|for|for> end for;
function|for> blox:=Append(blox,blok);
function|for> end for;
function> des:=Design<1,v|blox>;
function> return des;
function> end function;

> give_prodcode:=function(n,r);
function> des:=make_proddes(n,r);
function> code:=LinearCode(des,GF(2));
function> return code;
function> end function;
```

References

[1] E. F. Assmus Jr. and J. D. Key, *Designs and their Codes*, Cambridge Tracts in Mathematics vol.103, Cambridge University Press, Cambridge,1992.

[2] R. F. Bailey, *Distance-Transitive Graphs*, project submitted for the module MATH4081, University of Leeds, 2002.

[3] A. T. Balaban, *Chemical graphs, part XII: Combinatorial patterns*, Rev. Roumaine Math. Pures Appl. **17** (1972), 3 - 16.

[4] N. L. Biggs, *An edge-colouring problem*, Amer. Math. Monthly **79** (1972), 1018 - 1020.

[5] N. L. Biggs, *Some odd graph theory*, Second International Conference on Combinatorial Mathematics, Annals of the New York Academy of Sciences vol. 319 (1979), 71 - 85.

[6] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, November 1994.

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

[8] P. J. Cameron, *Automorphism groups of graphs*, Selected Topics in Graph Theory 2, Academic Press, London, 1983.

[9] B-L Chen and K-W Lih, *Hamiltonian Uniform Subset Graphs*, J. Combin. Theory B 42 (1987), 257 - 263.

[10] R. T. Curtis and T. R. Morris, *Codes, Graph Connections*, Oxford Lecture Ser. Math. Appl. vol. 5, Oxford University Press, New York, 1997, 116 - 127.

[11] M. Giudici and C. E. Praeger, *Completely Transitive Codes in Hamming Graphs*, European J. Combin. **20** (1999), 647 - 662.

[12] C. D. Godsil, *More odd graph theory*, Discrete Math. **32** (1980), 205 - 207.

[13] W. H. Haemers, R. Peeters and J. M. van Rijckenvorsel, *Binary codes of strongly regular graphs*, Des. Codes Cryptogr. **17** (1999), 187 - 207.

[14] D. G. Hoffman, D. A. Leonard, C. C. Lidner and K. T.Phelps, *Coding Theory - The Essentials*, Marcel Dekker Inc., New York, 1991.

[15] W. C. Huffman, *Codes and Groups*, in V. S Pless, W. C. Huffman (Eds.), Handbook of Coding Theory vol. 2, Elsevier, Amsterdam, 1345 - 1440.

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

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

[18] J. D. Key and P. Seneviratne, *Codes from the line graphs of complete multipartite graphs and PD-sets*, Discrete Math. (2007), doi:10.1016/j. disc. 2006.11.008.

[19] J. D. Key, *Permutation decoding through codes from designs*, http:www.ces.clemson.edu/∼keyj/Key/PMB05.pdf, unpublished article.

[20] J. D. Key and J. Moori, *Designs, Codes and graphs from the Janko groups J_1 and J_2*, J. Combin. Math. and Combin. Comput. **40** (2002), 143 - 159.

[21] J. D. Key and P. Seneviratne, *Permutation decoding for binary self-dual codes from the graph Q_n where n is even*, in T. Shaska, W. C. Huffman, D. Joyner, V. Ustimenko (Eds.), Advances in Coding Theory and Cryptology, Series on Coding Theory and Cryptology **2**, World Scientific Publishing Co. Ltd., Hackensack, NJ, 2007. To appear.

[22] S. Klavžar et al., *An almost complete description of perfect codes in direct products of cycles*, Advances in Appl. Math. (2003), doi:10.1016/j.aaam.2005.10.002.

[23] M. Kneser, Aufgabe 300, Jber. Deutsch. Math. - Verein **58** (1955).

[24] H. J. Kroll and R. Vincenti, *PD-sets related to the codes of some classical varieties*, Discrete Math., **301**, (2005), 89 - 105.

[25] L. Lovász, *Kneser's conjecture, Chromatic Number and Homotopy*, J. Combin. Theory Ser. A **25** (1978), 319 - 324.

[26] L. Lovász, *Combinatorial Problems and Exercises*, North-Holland, Amsterdam, 1970.

[27] F. J. MacWilliams, *Permutation decoding of systematic codes*, Bell System Tech. J. **43** (1964), 485 - 505.

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

[29] M. Mather, *The rugby footballers of Croam*, J. Combin. Theory Ser. B **20** (1976), 62 - 63.

[30] G. H. J. Meredith and E. K. Lloyd, *The footballers of Croam*, J. Combin.Theory Ser. B **15** (1973), 161 - 166.

[31] G. H. J. Meredith and E. K. Lloyd, *The Hamiltonian graphs O_4 to O_7*, Combinatorics, Institute of Mathematics and its Applications, Southend-on-Sea, 1972.

[32] A. Moon, *The Graphs $G(n, k)$ of the Johnson Schemes are Unique for $n \geq 20$*, J. Combin. Theory Ser. B **37** (1984), 173 - 188.

[33] E. Mwambene, *On vertex-transitive graphs as subgraphs of uniform subset graphs*, unpublished article.

[34] O. Pretzel, *Error-Correcting Codes and Finite Fields*, Oxford University Press, Oxford, 1992.

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

[36] S. Roman, *Coding and Information Theory*, Springer-Verlag, New York, 1992.

[37] G. Sabidussi, *Mappings in Graph Theory - An Introduction*, preprint.

[38] G. Sabidussi, *Vertex-transitive graphs*, Monatshefte fr Math. **68** (1964), 426 - 438.

[39] J. Schönheim, *On coverings*, Pacific J. Math. **14** (1964), 1405 - 1411.

[40] V. D. Tonchev, *Combinatorial Configurations : Designs, Codes, Graphs*, Pitman Monographs and Surveys in Pure and Applied Mathematics 40, Longman, New York, 1988, Translated from the Bulgarian by Robert A. Melter.

[41] L. R. Vermani, *Elements of Algebraic Coding Theory*, Chapman and Hall, London, 1996.

[42] D. B. West, *Introduction to Graph Theory*, Prentice-Hall Inc., New Jersey, 2001.

[43] H. Whitney, *Congruent graphs and the connectivity of graphs*, Amer. J. Math. **54** (1932), 154 - 168.

[44] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice-Hall Inc., New Jersey, 1995.

Index