SELF-DUAL CODES AND GRAPHS

by

Haluk Oral

B. Sc., Istanbul University, 1978

M. Sc., Bosphorus University, 1981

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in the Department

of

Mathematics and Statistics

© Haluk Oral 1989

SIMON FRASER UNIVERSITY

August 1989

All rights reserved. This work may not be

reproduced in whole or in part, by photocopy

or other means, without the permission of the author.

APPROVAL

Name: Haluk Oral

Degree: Ph.D. (Mathematics)

Title of Thesis: Self-Dual Codes and Graphs

Examining Committee:

Chairman: Dr. A. Lachlan

Dr. C. Godsil
Professor
Senior Supervisor

Dr. T. C. Brown
Professor

Dr. K. Heinrich
Professor

Dr. B. Alspach
Professor

Dr. S. A. Vanstone
External Examiner
Professor
Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario

Date Approved: August 14, 1989

PARTIAL COPYRIGHT LICENSE

I hereby grant to Simon Fraser University the right to lend my thesis, project or extended essay (the title of which is shown below) to users of the Simon Fraser University Library, and to make partial or single copies only for such users or in response to a request from the library of any other university, or other educational institution, on its own behalf or for one of its users. I further agree that permission for multiple copying of this work for scholarly purposes may be granted by me or the Dean of Graduate Studies. It is understood that copying or publication of this work for financial gain shall not be allowed without my written permission.

Title of Thesis/Project/Extended Essay

SELF-DUAL CODES AND GRAPHS

Author: _____
(signature)

HALUK ORAL
(name)

Aug 17 89
(date)

ABSTRACT

In this thesis we investigate binary self-dual codes. We give a new method to construct self-dual and self-orthogonal codes. We prove that almost every self-dual code must be indecomposable. We also investigate the automorphism groups of self-orthogonal codes. We prove that a self-orthogonal code with minimum distance four cannot have trivial automorphism group and we give an example of a self-orthogonal code with trivial automorphism group. In the last chapter we make some observations on the Barnette conjecture.

To the memory of my father.

Derviş Yunus bu sözü eğri bügrü söyleme
Seni sigaya çeken bir Molla Kasım gelir.

YUNUS EMRE

Acknowledgements

I would like to express my appreciation for the useful discussions I had with Louis Goddyn and Gordon F. Royle, and for the friendship and support of everybody at the University of Waterloo Combinatorics and Optimization Department during the last year of my Ph.D. studies. I also thank Steve White and Rob Ballantyne for their help in the printing of this thesis.

Finally, I would like to thank my adviser Dr. Chris Godsil for his patience and guidance.

CONTENTS

FIGURES

CHAPTER 1

INTRODUCTION

In this thesis we investigate self-dual codes. Self-dual codes constitute one of the most interesting families of codes. Many celebrated codes are self-dual, e.g., the extended binary Hamming code, the extended Golay code, and certain quadratic residue codes.

In Chapter 2 we present some known methods of constructing self-dual codes. There are only a few of these. If we restrict ourselves to the binary codes, these make use of designs or Hadamard matrices. We present a theorem of Asmuss et al. which gives constructions of self-orthogonal and self-dual codes obtained from symmetric designs. Then we consider Hadamard matrices and present two different approaches to constructing self-dual codes from them. One method is to consider the row space of a Hadamard matrix whose order is divisible by a prime p but not by p^2. Since the order of a Hadamard matrix must be divisible by four this method is not useful for constructing binary self-dual codes. The second method is due to Ozeki. In this method Hadamard matrices of order n are used to construct binary self-dual codes, provided n is not divisible by eight. Also, certain quadratic residue codes are self-dual codes. We state a theorem about such codes. Finally using the Kronecker product of generator matrices of self-dual codes we give a way of combining two self-dual codes to obtain another self-dual code.

In Chapter 3 we present a new method to construct binary self-dual codes. We prove that the row space of the face-vertex incidence matrix of a cubic planar bipartite graph is a binary self-dual code. This depends on a characterization of the minimal dependent subsets of the set of faces of these graphs. These sets are obtained as the union of pairwise colour classes of the proper 3-face colouring of the graph. An interesting result is that there is a relation between connectivity of the graph and the decomposability of the code obtained from the graph: the code obtained from the graph is indecomposable if and only if the graph is 3-connected. With our method we can construct all self-dual codes up to length 20. In Appendix B we give the list of the graphs corresponding to these codes.

We also give a lower bound for the rank of the face-vertex incidence matrix of a cubic planar graph. Since a cubic planar graph on n vertices has $\frac{n}{2}+2$ faces, the rank of the face-vertex incidence matrix of cubic planar graphs is less than or equal to $\frac{n}{2}+2$. We prove that the rank is greater than or equal to $\frac{n}{2}$. The embedding of cubic graphs on surfaces other than the plane can also be used for constructing self-orthogonal and self-dual codes. At the end of the chapter we give two examples of such constructions.

In Chapter 4 we give an enumeration theorem for self-dual codes. Then we prove that the ratio of the number of indecomposable self-dual codes of length n to the number of all self-dual codes of length n goes to zero as n goes to infinity. In other words almost all self-dual codes are indecomposable. We then prove that a self-orthogonal code of minimum distance four cannot have trivial automorphism group. Since the self-orthogonal codes of minimum distance two cannot have trivial automorphism group, the smallest possible minimum distance for a self-orthogonal code with identity automorphism group is six. Then we construct a self-orthogonal code of minimum distance six which has trivial automorphism group. For this construction we use the face-vertex incidence matrix of a planar cubic graph which has trivial automorphism group.

In Chapter 5 we give some early results about the Barnette conjecture. This conjecture states that every 3-connected cubic planar bipartite graph is

Hamiltonian. We present a different approach to this conjecture, which uses the fact that any cubic planar bipartite graph is 3-face colourable. The proper 3-face colouring of a cubic planar bipartite graph corresponds to a proper 3-vertex colouring of its dual. A *bicoloured subgraph* of G^* is a subgraph of G^* which contains vertices coloured by two of the three colours. We prove that an induced bicoloured tree in the dual graph G^* corresponds to a cycle in the graph G which passes through all vertices of G that lie on faces of G corresponding to the vertices of the tree. With this result we present a conjecture that implies the Barnette conjecture. As an application of the above result we prove that every vertex-transitive cubic planar bipartite 3-connected graph is Hamiltonian. (The classification of these graphs has been done in [8].)

CHAPTER 2

CONSTRUCTIONS

In this chapter we will give some methods to construct self-dual codes (see Appendix A for definitions). These methods make use of Design Theory and Hadamard matrices. In certain cases quadratic residue codes are also examples of self-dual codes. We will concentrate on binary codes.

2.1 Codes from designs

Let P be a set of v objects. A *2-(v,k,λ) design* based on P is a collection of k-subsets of P with the property that for any two elements x and y of P the subset $\{x,y\}$ is contained in λ of the k-subsets and each object belongs to r of the k-sets. The elements of P are called the *points* of the design and k-subsets in the collection are called the *blocks* of the design. If the number of blocks of a 2-design is equal to the number of points then it is called a *symmetric design.* Symmetric designs with certain parameters can be used to construct self-dual codes. We will need the following definition from linear algebra. Two matrices D and M are called *elementarily equivalent* if there exists matrices P and Q with determinant equal to 1 such that $PMQ = D$.

2.1.1 Lemma. *Let M be an $n \times n$ matrix. There exists a diagonal matrix $D = diag\ \{d_1, d_2, \cdots, d_n\}$ such that d_i divides d_{i+1} for all i in $\{1, 2, \cdots, n-1\}$ and which is elementarily equivalent to M.*

We start with the following theorem.

2.1.2 Theorem. *(Assmus et al. [3].) Let p be a prime and D be a (v,k,λ) symmetric design with incidence matrix M.*

(1) If $k \equiv \lambda \equiv 0 \pmod{p}$, then the row space of M over $GF(p)$ is a self-orthogonal code.

(2) If $p|(k-\lambda)$, and $p \not| k$, then let G be the $v \times (v+1)$ matrix defined as

$$G := \begin{pmatrix} \sqrt{-k} & & \\ \sqrt{-k} & & \\ . & & M \\ . & & \\ \sqrt{-k} & & \end{pmatrix}.$$

If $-k$ is a quadratic residue with respect to p, then the row space of G is a self-orthogonal code over $GF(p)$. If $-k$ is not a quadratic residue with respect to p, then the row space of G is a self-orthogonal code C over $GF(p^2)$. Moreover, if $p^2 \not| (k-\lambda)$, then it is a self-dual code.

(3) If $p|\lambda$ and $k \equiv -1 \pmod{p}$, let G be the $v \times 2v$ matrix defined as

$$G := (I \quad M)$$

Then the row space of G over $GF(p)$ is a $[2v, v]$ self-dual code.

(4) *If $p = 2$, λ is odd, and k is even, let G be the $(v+1) \times (2v+2)$ matrix defined by*

$$G := \begin{pmatrix} & & 0 & 1 & 1 & . & . & 1 \\ & & 1 & & & & & \\ & I & . & & & M & & \\ & & . & & & & & \\ & & 1 & & & & & \end{pmatrix}.$$

Then the row space of G over $GF(2)$ is a $[2v+2, v+1]$ self-dual code.

Proof. We will give the proof of (2). Others are just routine calculations. The first assertion is clearly true. Since C is self-orthogonal, $rank_F(G) \leq \frac{v+1}{2}$, where F is $GF(p^2)$. Now we will prove that $det(M) = k(k-\lambda)^{\frac{v-1}{2}}$. For this first observe that

$$M^T M = \begin{pmatrix} k & \lambda & \lambda & . & . & \lambda \\ \lambda & k & \lambda & . & . & \lambda \\ \lambda & \lambda & k & . & . & \lambda \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \lambda & \lambda & \lambda & . & . & k \end{pmatrix}$$

We calculate the determinant of $M^T M$ as follows, subtract the first column of $M^T M$ from every other column. We get

$$\begin{pmatrix} k & \lambda - k & \lambda - k & . & . & \lambda - k \\ \lambda & k - \lambda & 0 & . & . & 0 \\ \lambda & 0 & k - \lambda & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \lambda & 0 & 0 & . & . & k - \lambda \end{pmatrix}.$$

Then adding all rows to the first row we get

$$\begin{pmatrix} k + (v-1)\lambda & 0 & 0 & . & . & 0 \\ \lambda & k - \lambda & 0 & . & . & 0 \\ \lambda & 0 & k - \lambda & . & . & 0 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ \lambda & 0 & 0 & . & . & k - \lambda \end{pmatrix}.$$

The determinant of $M^T M$ is equal to the determinant of the above matrix, and hence

$$det(M^T M) = [k + (v-1)\lambda](k-\lambda)^{v-1}.$$

Since $\lambda(v-1) = k(k-1)$ and

$$det(M^T M) = det(M^T)\, det(M) = det(M)^2$$

we get

$$det(M) = \sqrt{k^2(k-\lambda)^{v-1}} = k(k-\lambda)^{\frac{v-1}{2}}.$$

Now let D be the diagonal matrix $D = diag\,\{d_1, d_2, \cdots, d_v\}$ elementarily equivalent to M. Then

$$rank_F(G) = rank_F(M) = rank_F(D) \geq v - \frac{v-1}{2} = \frac{v+1}{2},$$

when $p^2 \not| (k-\lambda)$. Hence $rank_F(G) = \frac{v+1}{2}$ and C is self-dual in this case. ∎

For non-trivial examples of *(1)* with $p = 2$ we can take any of the three $(16, 6, 2)$ designs. For the second method we can take any projective plane of order divisible by the prime p. Or we can take the unique $(11, 5, 2)$ design with $p = 3$ and produce the ternary $[12, 6]$ *Golay Code*. In *(3)* we can take any $(v, k, 2)$ design with k odd, e.g, if we take all 3-subsets of a 4-set we obtain the $[8, 4]$ *Hamming Code*. For a non-trivial example of *(4)* we can take the symmetric $(11, 6, 3)$ design to obtain the $[24, 12]$ *binary Golay Code*. (The designs referred to can be found, for example, in Husain [15].)

2.2 Hadamard matrices

A Hadamard matrix H of order n is an $n \times n$ matrix with each element either 1 or -1, which satisfies

$$HH^T = nI.$$

A class of self-dual codes can be obtained by considering the row space of an $n \times n$ Hadamard matrix over $GF(p)$, for some prime p dividing n such that p^2 does not divide n. Another construction is given in Ozeki [20].

2.2.1 Theorem. *Let H be a Hadamard matrix of order n and and let p be a prime such that $p|n$ and p^2 does not divide n. Then the row space of H over $GF(p)$ is a self-dual code over $GF(p)$.*

Proof. Let D be the diagonal matrix $D = diag\ \{d_1, d_2, \cdots, d_n\}$ elementarily equivalent to H. So we have $det(H) = det(D)$. Now we will find the determinant of H. Since H is a Hadamard matrix we have $HH^T = nI$ hence $det(H)det(H^T) = n^n$. Suppose $n = pq$. Since p^2 does not divide n, it follows that p and q must be relatively prime. So we have

$$det(D) = det(H) = n^{n/2} = p^{n/2}q^{n/2}.$$

Since d_i divides d_{i+1}, at most $n/2$ of the diagonal terms are divisible by p. So the rank of H over $GF(p)$ is at least $n/2$. But $HH^T = pqI = 0$ in $GF(p)$. So the rank of H over $GF(p)$ is at most $n/2$. Hence

$$rank_{GF(p)}H = n/2$$

and the row space of H is a $[n, n/2]$ self-dual code over $GF(p)$. ∎

2.2.2 Definition. Two Hadamard matrices $H^{(1)}$ and $H^{(2)}$ of the same order n are said to be *equivalent* if $H^{(2)}$ is obtained from $H^{(1)}$ by a sequence of operations of exchanging two rows (or columns) of $H^{(1)}$ or multiplying some rows (or columns) of $H^{(1)}$ by -1. It is easy to see that any Hadamard matrix is equivalent to a matrix of the form

$$\begin{pmatrix} -1 & 1 & 1 & . & . & . & 1 \\ 1 & & & & & & \\ 1 & & & & & & \\ . & & & * & & & \\ . & & & & & & \\ . & & & & & & \\ 1 & & & & & & \end{pmatrix}.$$

We will call a Hadamard matrix of this form as *standardized Hadamard matrix.* The following theorem is due to Ozeki. By J_n we denote the $n \times n$ matrix whose all entries are 1.

2.2.3 Theorem. *(Ozeki [20].) Let H_n be a standardized Hadamard matrix of order n, let $K_n = 1/2(H_n + J_n)$ and $C_n = (I_n : K_n)$. If $n \equiv 4 \pmod 8$, then C_n generates a doubly even self-dual code of length $2n$. Moreover, equivalent Hadamard matrices give equivalent codes.*

2.3 Other constructions

Now we will consider the *quadratic residue* codes. Quadratic residue codes are cyclic codes of a prime length p over a field $GF(l)$, where l is a prime which is a quadratic residue modulo p. If we consider the binary case, i.e., $l = 2$, this means that p has to be a prime of the form $8m \pm 1$ (for a proof see, e.g., Apostol [2: p. 181]). Some of the best known codes are examples of quadratic residue codes, e.g., the binary $[7, 4, 3]$ Hamming code, the binary $[23, 12, 7]$ and ternary $[11, 6, 5]$ Golay codes.

Let p be a prime, let Q denote the set of quadratic residues modulo p and N the set of nonresidues. Let α be a p^{th} root of unity. Define $q(x)$ and $n(x)$ as

$$q(x) = \prod_{r \in Q} (x - \alpha^r) \text{ and } n(x) = \prod_{n \in N} (x - \alpha^n)$$

Then the *quadratic residue* codes $Q, \bar{Q}, N, \bar{N}$ are cyclic codes with the generator polynomials $q(x)$, $q(x)(x-1)$, $n(x)$ and $n(x)(x-1)$ respectively.

2.3.1 Theorem. *If $p \equiv -1 \pmod 4$ then the extensions of the quadratic residue codes Q and N by a parity check digit are self-dual.*

For a proof see MacWilliams and Sloane [17: p. 490].

Now we will see that, using the Kronecker product of the generating matrices of self-dual codes, we can construct new self-dual codes. The Kronecker product of two matrices $A_{n \times m} := [a_{ij}]$ and B is defined as

$$A \otimes B := \begin{pmatrix} a_{11}B & a_{12}B & . & . & . & a_{1m}B \\ a_{21}B & a_{22}B & . & . & . & a_{2m}B \\ & & . & . & . & \\ & & . & . & . & \\ a_{n1}B & a_{n2}B & . & . & . & a_{nm}B \end{pmatrix}$$

2.3.2 Theorem. *If* $[I_k : A_1]$ *and* $[I_l : A_2]$ *are generator matrices for self-dual codes, so is* $[I_{kl} : A_1 \otimes A_2]$

Proof. We should prove that $A_1 \otimes A_2$ is also a self-orthogonal matrix. We have

$$(A_1 \otimes A_2)(A_1 \otimes A_2)^T = (A_1 \otimes A_2)(A_1^T \otimes A_2^T) = A_1 A_1^T \otimes A_2 A_2^T = I_k \otimes I_l = I_{kl},$$

so $[I_{kl} : A_1 \otimes A_2]$ is a generator matrix for a self-dual code of length $2kl$. ∎

CHAPTER 3

A NEW CONSTRUCTION

In this chapter we will give a new construction method for self-dual codes. This method uses cubic planar bipartite graphs. We will give some examples of this construction. We will also give a lower bound for the rank of the face-vertex incidence matrix of any cubic planar graph.

3.1 Self-dual codes from cubic planar bipartite graphs

Let G be a connected cubic planar bipartite graph with vertex set $\{1, 2, \cdots, n\}$. We define the face-vertex incidence matrix $D = (d_{ij})$ of G as the matrix with columns indexed by the vertices $1, 2, \cdots, n$ of G, rows indexed by the faces $f_1, f_2, \cdots, f_s$ of G with d_{ij} defined by

$$d_{ij} := \begin{cases} 1, & \text{if } j \text{ is incident with } f_i; \\ 0, & \text{otherwise.} \end{cases}$$

For a face f of G the corresponding row of D will also be denoted by f. We thus identify subsets of faces of G with corresponding subsets of the rows of D. The *support* of a face f which is denoted by supp(f) is the set of vertices incident with the face. The *degree* of a face is the number of elements of its support. Our main result is that the row space of D over $GF(2)$ is a binary self-dual code of length n.

We will begin by characterizing the minimal linearly dependent subsets of the the row space of D over $GF(2)$. We need the following lemma.

3.1.1 Lemma. *A connected cubic bipartite graph has no cut-edge.*

Proof. Assume that L is a connected cubic bipartite graph with a cut-edge e. Consider a component H of $L-e$. The graph H has one vertex of degree two and all other vertices of degree three. But H is a bipartite graph say with partition (X,Y). Without loss of generality assume that the vertex in H of degree two is in X. Then the sum of the degrees of the vertices in X is congruent to 2 (modulo 3), but the sum of the degrees of vertices in Y is equal to 0 (modulo 3). This is impossible. ∎

So any edge of a cubic planar bipartite graph must be incident with two faces; otherwise it would be a cut-edge. Two faces of a planar graph are said to be *adjacent* if they share an edge.

We also need the following lemma.

3.1.2 Lemma. *A cubic planar graph is 3-face colourable if and only if it is bipartite.*

For a proof see, e.g, Wilson [30: p. 91].

3.1.3 Lemma. *Let G be a cubic planar bipartite graph with vertex set $\{1,2,\cdots,n\}$ and with its faces properly coloured with three colours. The only minimal dependent subsets of the faces of G are pairwise unions of two colour classes.*

Proof. Let M be a minimal dependent set of faces. First observe that since the sum of the elements of M is zero, every vertex of G is incident with an even number of faces in M. Since G is a cubic graph, we have only two choices for these even numbers — 0 and 2. We will prove two claims that will imply that M is a union of two colour classes.

(a) Every vertex of the graph is incident with exactly two elements of M.

Let X be the set of vertices incident with two elements of M. If $X \neq V(G)$ then $V(G) - X \neq \phi$. Since G is connected there exists some y in $V(G) - X$ which is adjacent to some x in X. The two face adjacent to the edge xy are not in M implying the third face incident with x is not in M which contradicts

$x \in X$. Hence $X = V(G)$. So if M is a nonempty minimal dependent subset of M, every vertex of G must be incident with exactly two elements of M.

(b) Suppose the faces of G are coloured by the colours a, b, c. If M contains a face coloured by a then it contains all faces coloured by a.

Let $f \in M$ and suppose that f is coloured by a. Every face adjacent to f must have colour b or c. Also the sum of the elements of M is zero. A vertex x of f is incident with at least one element of M, namely f, so there must be exactly one more face in M which is incident with x. Therefore of the faces adjacent to f, the minimal dependent set M must contain all those coloured by b or all those coloured by c. Assume M contains those faces adjacent to f which are coloured by b. Now let f' be a face of G coloured by b and adjacent to f. By the same reasoning we conclude that all faces of G that are adjacent to f' and that are coloured by a, must be in M.

Hence to conclude that all faces of colour a are in M, we have to prove that between any face of colour a and f, there is a chain of adjacent faces of colours a and b. To prove this we will consider the dual graph G^* of G. In this case G^* is a connected triangulation with its vertices 3-coloured by $\{a, b, c\}$. The required chain of adjacent faces of G, corresponds to a walk in G^* whose vertices are coloured by a and b. So the result will follow if we can show that any two vertices coloured by a are joined by a walk using only vertices with colours a and b. Let x, y be any two distinct vertices of G^* with colour a. Since G^* is connected, there is a walk joining x and y. If this walk contains a vertex z coloured by c, consider the set $N(z)$ of vertices of G^* which are adjacent to z. The subgraph of G^* induced by $N(z)$ is a cycle whose vertices are coloured by a and b. Using the appropriate part of this cycle we can find a walk joining x and y which does not contain z, and hence we can get the required 2-coloured walk. This implies that any face coloured by a or b must be in M.

Together (a) and (b) imply that M is union of two colour classes: by the second claim all faces coloured by a and b are in M and by the first claim any vertex is incident with exactly two element of M. Hence M cannot contain any face coloured by c as otherwise the vertices of this face would be incident with

three elements of M. ∎

Now we will prove that the row space of the face-vertex incidence matrix of a connected cubic planar bipartite graph is a self-dual code of length n.

3.1.4 Theorem. *Let G be a connected cubic planar bipartite graph with vertex set $\{1, 2, \cdots, n\}$ and face-vertex incidence matrix D. Let f_1, f_2 be any two faces of G of different colours in a 3-face colouring of G. If we delete the rows corresponding to f_1 and f_2 from D, the resulting matrix is a generator matrix for a self-dual code of length n. Moreover, this code is independent of the choice of faces f_1, f_2.*

Proof. Let S be the matrix obtained by deleting the rows corresponding to f_1 and f_2 from D. We will prove that the rows of S form a basis for the row space of D and then we will prove that S is a generator matrix of a self-dual code. Since the set of rows of S does not contain the union of any two colour classes, from Lemma 3.1.3 we see that it is linearly independent.

We will now prove that the row space of S is equal to the row space of D. Since every row of D other than f_1 and f_2 is also a row of S, to prove this equality it is enough to prove that there are two minimal dependent subsets M_1 and M_2 of the set of faces of G such that:

(a) $f_1 \in M_1$ and $f_2 \notin M_1$,
(b) $f_1 \notin M_2$ and $f_2 \in M_2$.

For if (a) holds then f_1 is a linear combination of the rows of D that correspond to the elements of $M_1 - \{f_1\}$. The set $M_1 - \{f_1\}$ is a subset of the rows of S, therefore f_1 is in the row space of S. Similarly (b) will imply that f_2 is a linear combination of the elements of $M_2 - \{f_2\}$.

We can choose M_1 to be the union of two colour classes that do not contain f_2 and M_2 to be the union of two colour classes that do not contain f_1. This implies that f_1 and f_2 are in the row space of S and hence that the row space of S is equal to the row space of D. It also proves that the row space of S is independent of the choice of faces f_1, f_2.

To prove that S is a generator matrix of a self-orthogonal code, we have to

prove that the rows of S are orthogonal to each other. Since G is bipartite, every row of S has even weight and hence each row of S is orthogonal to itself. Since G is cubic, two faces of G cannot have an odd number of vertices in common: if two faces have a vertex x in common, then they share an edge incident with x. Again, since G is cubic, they cannot share two adjacent edges. Hence any two adjacent faces of a cubic planar graph share some edges which are not adjacent to each other. So these two faces must have an even number of vertices (the endpoints of the shared edges) in common. So, any two rows of S must be orthogonal and hence the row space of S is a self-orthogonal code.

A self-orthogonal code is self-dual if and only if its dimension is equal to half of its length. To complete our proof now we will prove that the dimension of the row space of S is equal to half of its length. The graph G has n vertices so the length of the row space of S is n. Let us denote the set of edges of G by E and the set of faces of G by F. We have $|E| = 3n/2$. By Euler's formula

$$n - \frac{3n}{2} + |F| = 2.$$

Hence

$$|F| = \frac{n}{2} + 2.$$

So S has $n/2$ rows. We conclude that S is a generator matrix for a self-dual code of length n, and this code is independent of the faces deleted provided they are coloured differently in the 3-face colouring. ∎

3.2. Remarks

In this section we will mention some relations between the graph and the code obtained from the graph. We will also give some examples. By $F(G)$ we denote the set of faces of the graph G and by $V(f)$ we denote the set vertices incident with the face f.

The self-dual code C obtained from a cubic planar bipartite graph must have minimum distance two or four. We prove this in the following form.

3.2.1 Lemma. *A cubic planar bipartite graph G, must have at least six faces of degree four.*

Proof. To see this we will prove the following.

$$\sum_{f \in F(G)} (|V(f)| - 6) = -12. \tag{1}$$

This will imply the lemma because the only faces that contribute negative numbers to the summation are faces of degree four, and each such face contributes -2.

Counting the pairs consisting of a vertex and an incident face in two different ways, we obtain $\sum_{f \in F(G)} |V(f)| = 3|V(G)|$. By Euler's formula we have $|F(G)| = \frac{|V(G)|}{2} + 2$. It follows that

$$\sum_{f \in F(G)} (|V(f)| - 6) = \sum_{f \in F(G)} |V(f)| - 6|F(G)|$$

and therefore

$$3|V(G)| - 6(\frac{|V(G)|}{2} + 2) = -12.$$

The proof is completed. ∎

The fact that the minimum distance is less than or equal to four can also be proven as follows. Let S be the generator matrix of C obtained by deleting two suitable rows of the face-vertex incidence matrix D of the graph. Since D has exactly three 1's in each column, S has at most three 1's in each column and strictly less than three 1's in some columns (because of the deleted faces). If we denote the minimum distance of C by d then by counting the nonzero entries

of S in two different ways, we get $3n > (n/2)d$, where $n = |V(G)|$, which that implies $d < 6$. We deduce $d = 4$ or $d = 2$. We also remark that if the graph has multiple edges, our theorem is still valid.

If the graph has connectivity two, it yields a decomposable code. So if the code obtained from the graph G is indecomposable then G is 3-connected. It is quite interesting to see that there is a relation between the connectivity of the graph and indecomposability of the code. For the converse we give the following lemma.

3.2.2 Lemma. *Let G be a 3-connected cubic planar bipartite graph with vertex set $\{1, 2, \cdots, n\}$. The self-dual code C obtained from G is indecomposable.*

Proof. First we claim that any two faces of G share one or no edge. Assume by way of contradiction that e_1 and e_2 are two edges shared by two faces f_1 and f_2 of G and consider the graph $G - \{e_1, e_2\}$. Let $F(G)$ be the set of faces of the graph G. We define f' to be the face of $G - \{e_1, e_2\}$ whose edge set is $E(f_1) \cup E(f_2) - \{e_1, e_2\}$. The set of faces of $G - \{e_1, e_2\}$ is

$$F(G - \{e_1, e_2\}) = (F(G) - \{f_1, f_2\}) \cup \{f'\}.$$

From this we see that the graph $G - \{e_1, e_2\}$ has one less face than G. Now G has n vertices, $\frac{3n}{2}$ edges and $\frac{n}{2} + 2$ faces. So $G - \{e_1, e_2\}$ has n vertices, $\frac{3n}{2} - 2$ edges and $\frac{n}{2} + 1$ faces. If $G - \{e_1, e_2\}$ were connected, applying Euler's formula to this graph we would get

$$n - (\frac{3n}{2} - 2) + \frac{n}{2} + 1 = 2$$

which would imply 1 is equal to 0, a contradiction. Hence $G - \{e_1, e_2\}$ is not connected and so if G is 3-connected, any two faces can share at most one edge.

Now let f be a face of G and let S be a proper subset of $supp(f)$. We prove that S cannot be the support of any codeword. For suppose that S is the support of a codeword u. Choose a vertex x of f which is not in S. Let y be a vertex of f adjacent to x and let f' be the face which shares the edge xy with f. Since C is a self-dual code $supp(f')$ and $supp(u)$ must have an even number of common points. Now $supp(u)$ is a subset of $supp(f)$ so this intersection must be

a subset of $\{x, y\}$. We have chosen x outside of the support of u hence the only possibility we are left with is that the intersection of $supp(u)$ with $supp(f')$ is empty. So y is not an element of the support of u which is S. Now if we choose x as vertex of f which is adjacent to an element of S we get a contradiction. Hence a proper nonempty subset of $supp(f)$ cannot be a codeword.

If C is decomposable then we can partition $V(G)$ into sets V_1 and V_2. We can find sets of codewords

$$U = \{u_1, u_2, \cdots, u_t\}$$

and

$$W = \{w_1, w_2, \cdots, w_s\}$$

such that $supp(u_i) \subseteq V_1$, where $1 \leq i \leq t$, and $supp(w_j) \subseteq V_2$, where $1 \leq j \leq t$, and $U \cup W$ is a basis. Let $f \in F(G)$. Then

$$f = (\sum_{i=1}^{t} \lambda_i u_i) + (\sum_{j=1}^{s} \mu_j u_j).$$

Now, $u = \sum_{i=1}^{t} \lambda_i u_i$ is a codeword with $supp(u) \subseteq V_1$. Since $supp(u) \subseteq supp(f)$ we conclude that $u = 0$ or $f = \sum_{i=1}^{t} \lambda_i u_i$. Thus, every face of G has all of its vertices in one of V_1 or V_2. This implies that there is no edge from any vertex in V_1 to any vertex in V_2. If both V_1 and V_2 are not empty we conclude that G is disconnected. Since this is contrary to the hypothesis, $C(G)$ has only one component and is indecomposable. ∎

Since a self-dual code of minimum distance two is decomposable 3-connected cubic planar bipartite graphs yield self-dual codes of minimum distance four. If G is a connected cubic planar bipartite graph then $C(G)$ will denote the self-dual code generated by the face-vertex incidence matrix of G. We will prove that if self-dual codes C_1 and C_2 are obtained from cubic planar bipartite graphs then their composition $C_1 \oplus C_2$ can also be obtained from a cubic planar bipartite graph. First we give the following definition. Let G_1 and G_2 be connected cubic planar bipartite graphs and let x_1y_1 be an edge of the outside face of G_1 and x_2y_2 be an edge of outside face of G_2. We define a graph $G_1 \oplus G_2$ as follows:

$$V(G_1 \oplus G_2) = V(G_1) \cup V(G_2)$$

$$E(G_1 \oplus G_2) = [E(G_1) \cup E(G_2) - \{x_1y_1, x_2y_2\}] \cup \{x_1x_2, y_1y_2\}.$$

(Graphs $G_1 \oplus G_2$ is dependent of the edges we use. But they yields the same code.) We will give an example.

3.2.3 Example. Consider the following two cubic planar bipartite graphs G_1 and G_2, where $x_1 = 9$, $y_1 = 19$, $x_2 = 1$, $y_2 = 7$.

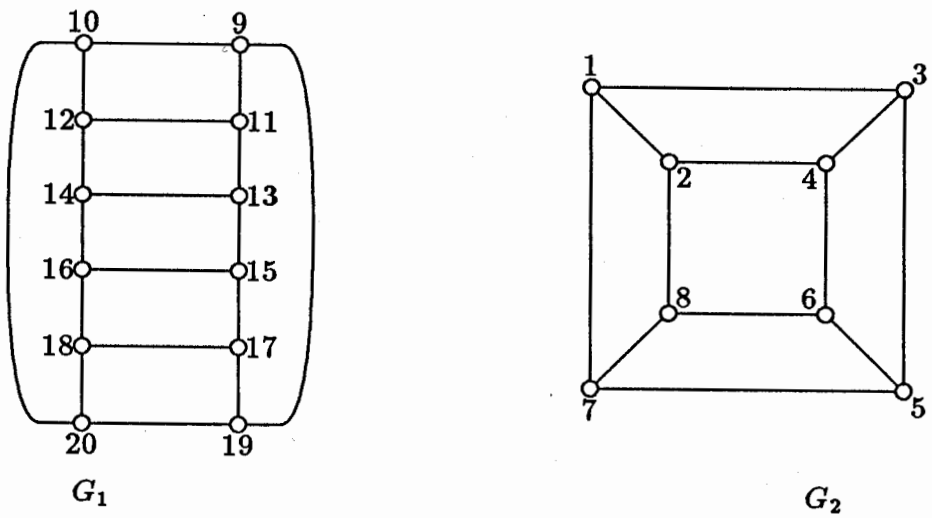

Figure 1. G_1 and G_2.

Now $G_1 \oplus G_2$ is the following graph shown in Figure 2.

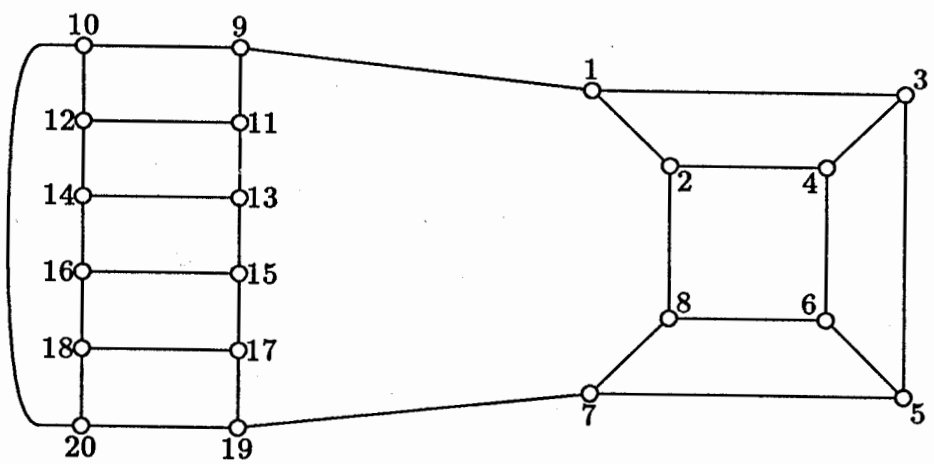

Figure 2. $G_1 \oplus G_2$

3.2.4 Lemma. *Let G_1 and G_2 be two cubic planar graphs. The graph $G_1 \oplus G_2$ is also a cubic planar bipartite graph and*

$$C(G_1 \oplus G_2) = C(G_1) \oplus C(G_2).$$

Proof. Obviously $G_1 \oplus G_2$ is cubic and planar. To show that it is bipartite all we have to prove is that all faces of $G_1 \oplus G_2$ have an even number of edges. Let f_1 be the outside face of G_1 and f_1' be the face of G_1 that shares the edge x_1y_1 with f_1. Also, let f_2 be the outside face of G_2 and f_2' be the face of G_2 that shares the edge x_2y_2 with f_2. Now we describe the set of faces of the graph $G_1 \oplus G_2$ which are not faces of the graphs G_1 or G_2, by their edge sets. The outside face f_3 of $G_1 \oplus G_2$ has edge set

$$E(f_3) = [E(f_1) \cup E(f_2) - \{x_1y_1, x_2y_2\}] \cup \{x_1x_2, y_1y_2\}.$$

The other face f_3' is the one with edge set

$$E(f_3') = ([E(f_1) - \{x_1y_1\}] \cup [E(f_2) - \{x_2y_2\}]) \cup \{x_1x_2, y_1y_2\}.$$

The set of faces of the graph $G_1 \oplus G_2$ is

$$F(G_1 \oplus G_2) = ((F(G_1) \cup F(G_2)) - \{f_1, f_1', f_2, f_2'\}) \cup \{f_3, f_3'\}.$$

Now since $|E(f_1)|$ and $|E(f_2)|$ are even, so are $|E(f_3)|$ and $|E(f_3')|$. Hence the graph $G_1 \oplus G_2$ is bipartite.

We claim that for any choice of edges x_1y_1 and x_2y_2 we have,

$$C(G_1 \oplus G_2) = C(G_1) \oplus C(G_2).$$

To show this it is enough to make the following observation. Let A be the generator matrix of $C(G_1)$ obtained from the face-vertex matrix of G_1 by deleting the rows corresponding to f_1 and f_1'. Also let B be the generator matrix of $C(G_2)$ obtained from a face-vertex matrix of G_2 by deleting the rows corresponding f_2 and f_2'. Consider the matrix

$$D := \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

The rows of D are elements of $C(G_1 \oplus G_2)$ and they are linearly independent. Hence D is a generator matrix for $C(G_1 \oplus G_2)$. This completes the proof. ∎

We will illustrate this with an example.

3.2.5 Example. Let G_1 and G_2 be the graphs in Figure 1. Then a generator matrix of the code $C(G_1)$ is

$$A := \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ & & 1 & 1 & 1 & 1 & & & & & & \\ & & & & 1 & 1 & 1 & 1 & & & & \\ & & & & & & 1 & 1 & 1 & 1 & & \\ & & & & & & & & 1 & 1 & 1 & 1 \\ & 1 & & 1 & & 1 & & 1 & & 1 & & 1 \end{pmatrix}$$

(the blank spaces contain zero, the rows corresponding to the outside face and to the face with the support $\{9, 11, 13, 15, 17, 19\}$ are deleted from the face-vertex incidence matrix of G_1). A generator matrix of $C(G_2)$ is

$$B := \begin{pmatrix} 1 & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 1 & 1 & & \\ & & & & 1 & 1 & 1 & 1 \\ & 1 & & 1 & & 1 & & 1 \end{pmatrix}$$

(the rows corresponding to the outside face and to the face with the support $\{1, 2, 7, 8\}$ are deleted from the face-vertex incidence matrix of G_2). A generator matrix for $C(G_1 \oplus G_2)$ is

$$D := \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & & & & & \\ & & 1 & 1 & 1 & 1 & & & & & & & & & & \\ & & & & 1 & 1 & 1 & 1 & & & & & & & & \\ & 1 & & 1 & & 1 & & 1 & & & & & & & & \\ & & & & & & & & 1 & 1 & 1 & 1 & & & & \\ & & & & & & & & & & 1 & 1 & 1 & 1 & & \\ & & & & & & & & & & & & 1 & 1 & 1 & 1 \\ & & & & & & & & 1 & & 1 & & 1 & & 1 & \end{pmatrix}$$

(the rows corresponding to the outside face and to the face with the support $\{1, 2, 7, 8, 9, 11, 13, 15, 17, 19\}$ are deleted from the face-vertex incidence matrix of $G_1 \oplus G_2$). Now D is of the form

$$D := \begin{pmatrix} B & 0 \\ 0 & A \end{pmatrix}$$

Hence $C(G_1 \oplus G_2) = C(G_1) \oplus C(G_2)$.

Non-isomorphic graphs may yield the same code. The graphs S_{20} and S' are examples (see Appendix B Figure 18 and Figure 19.) It can be seen that

every face of the graph S_{20} is orthogonal to every face of the graph S', and hence they generate the same code, altough they are not isomorphic. (Two non-isomorphic 3-connected cubic planar bipartite graphs with less than 20 vertices yield different codes.)

In Appendix B we list the cubic planar bipartite graphs which yield all self-dual codes up to length 20.

3.3 Self-orthogonal codes from cubic planar graphs

We can use any cubic planar graph (not necessarily bipartite) to construct self-orthogonal codes. From Euler's formula, we know that a cubic planar graph on n vertices must have $n/2+2$ faces. We will prove that the rank of the face-vertex incidence matrix of such a graph is greater than or equal to $n/2$. For this we first give the following lemma.

3.3.1 Lemma. *Let G be a planar 2-edge connected graph on n vertices such that G has maximum valency 3 and has some vertex u of degree 2. Let $F(G)$ be the set of faces of G. If f is a face incident with u then $F(G)-f$ is an independent subset of $[GF(2)]^n$.*

Proof. The proof is by induction on the number of faces. If the graph is a cycle the claim is obviously correct. Now assume that the graph has more than two faces. Say u is incident with the faces f' and f. Now consider the graph G' which we obtain from G by deleting all vertices of f' which are only incident with faces f and f'. We see that

$$F(G') = F(G) - \{f, f'\} \cup \{f''\}$$

where f'' is the face of the graph G' whose edge set is the symmetric difference of the edge sets of f and f'. The vertices of G' which are adjacent to the deleted vertices of G have degree 2 in G' (becouse maximum valency is 3 and G is 2-edge connected) and these vertices are incident with the face f''. So G' satisfies the induction hypothesis and $|F(G')| < |F(G)|$. Hence by induction $F(G') - \{f''\} = F(G) - \{f, f'\}$ is independent.

Now we will prove that the minimal dependent subsets of $F(G) - \{f, f'\}$ are the minimal dependent subsets of $F(G) - f$. (This will imply that $F(G) - f$

is also linearly independent.) Again consider the vertex u. Since u is incident with only one face in $F(G)-f$, namely f', it follows that f' cannot be in any minimal dependent subset of $F(G)-f$. (If f' were in some minimal dependent subset M, then M should contain another face from $F(G)-f$ which is incident with u.) Therefore the set of minimal dependent subsets of $F(G)-f$ is equal to the set of minimal dependent subsets of $F(G)-\{f,f'\}$. ∎

3.3.2 Corollary. *Let G be a connected cubic planar graph on n vertices and let D be its face-vertex incidence matrix. Then the rank of D is at least $n/2$.*

Proof. Let e be an edge of G. Consider the graph $G-e$. Let f be the face of $G-e$ which is not a face of G, i.e., f is the face whose edge set is the symmetric difference of the edge sets of the faces incident with e. Then by the above lemma, $F(G-e)-f$ is linearly independent. This set is a subset of $F(G)$ hence,

$$rank(D) \geq |F(G-e)-f| = n/2. \blacksquare$$

Let G be a planar graph with t faces of odd degree. Let D be the face-vertex incidence matrix of G which has the faces of odd degree in its first t rows. We define the matrix D^* as

$$D^* := \left(\begin{array}{c|c} & I_t \\ D & \hline \\ & 0 \end{array}\right).$$

It is easy to see that any two rows of D^* are orthogonal to each other so we have the following theorem.

3.3.3 Theorem. *Let G be a cubic planar graph. Then the row space of D^* is a self-orthogonal code.*

3.4 Some applications of the face-vertex incidence matrix

We also can use the face-vertex incidence matrix of a graph which is embedded on a surface other than the plane. We will give two examples.

In [21], Pless has classified all self-dual codes of length less than or equal to 20. The self-dual code of minimum distance 4 which is called M_{20} in [21], has only five codewords of weight 4, while it is known that a connected cubic planar bipartite graph must have at least six faces of degree 4 (see Lemma 3.2.1). So the self-dual code M_{20} cannot be obtained from a cubic planar bipartite graph. Now we will obtain this code from a non-planar graph.

3.4.1 Example. Consider the graph of Figure 3, embedded on the Möbius strip (which is same as embedding on the projective plane).

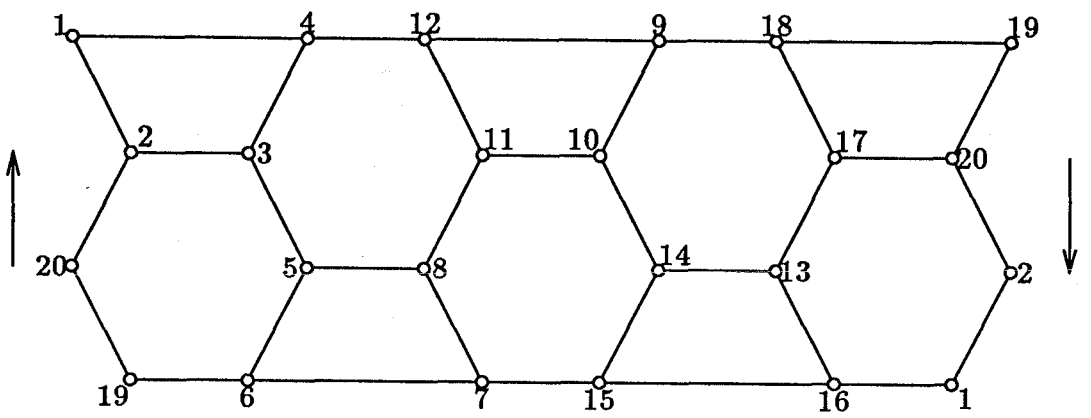

Figure 3. M_{20}

Let M be the matrix that we obtain from a face-vertex incidence matrix of the embedding by deleting the row corresponding to the face which is not of degree four or six. Thus

$$M = \begin{pmatrix}
1 & 1 & 1 & 1 & & & & & & & & & & & & & & & & \\
 & & & & 1 & 1 & 1 & 1 & & & & & & & & & & & & \\
 & & & & & & & & 1 & 1 & 1 & 1 & & & & & & & & \\
 & & & & & & & & & & & & 1 & 1 & 1 & 1 & & & & \\
 & & & & & & & & & & & & & & & & 1 & 1 & 1 & 1 \\
 & & & & & & & & 1 & 1 & & & 1 & 1 & & & 1 & 1 & & \\
1 & 1 & & & & & & & & & & & 1 & & & 1 & 1 & & & 1 \\
 & 1 & 1 & & 1 & 1 & & & & & & & & & & & & & 1 & 1 \\
 & & 1 & 1 & 1 & & & 1 & & & 1 & 1 & & & & & & & & \\
 & & & & & & 1 & 1 & & 1 & 1 & & & 1 & 1 & & & & & \\
\end{pmatrix}.$$

We will show that M is a generator matrix of the self-dual code M_{20}. In her paper a generator matrix of M_{20} is given as

$$A = \begin{pmatrix}
1 & 1 & 1 & 1 & & & & & & & & & & & & & & & & \\
 & & & & 1 & 1 & 1 & 1 & & & & & & & & & & & & \\
 & & & & & & & & 1 & 1 & 1 & 1 & & & & & & & & \\
 & & & & & & & & & & & & 1 & 1 & 1 & 1 & & & & \\
 & & & & & & & & & & & & & & & & 1 & 1 & 1 & 1 \\
 & & & & & & & & 1 & 1 & & & 1 & 1 & & & 1 & 1 & & \\
1 & 1 & & & & & & & & & & & & 1 & 1 & & & 1 & 1 & \\
 & 1 & 1 & & 1 & 1 & & & & & & & & & & & & & 1 & 1 \\
 & & 1 & 1 & & 1 & 1 & & & & 1 & 1 & & & & & & & & \\
 & & & & & & 1 & 1 & & 1 & 1 & & 1 & & & 1 & & & & \\
\end{pmatrix}.$$

The 7^{th} row of M is the sum of the 4^{th}, 5^{th} and 7^{th} rows of A, the 9^{th} row of M is the sum of the 9^{th} and 2^{nd} rows of A, 10^{th} row of M is the sum of the 10^{th} and 4^{th} rows of A. All other rows of M and A are same. Hence the row spaces of M and A are same. So M is a generator matrix for M_{20}.

3.4.2 Example. We can also consider face-vertex incidence matrices of cubic graphs embedded on the projective plane. As an example, we will give the embedding of the Petersen graph on the projective plane.

Consider the following embedding of the Petersen graph on the projective plane.

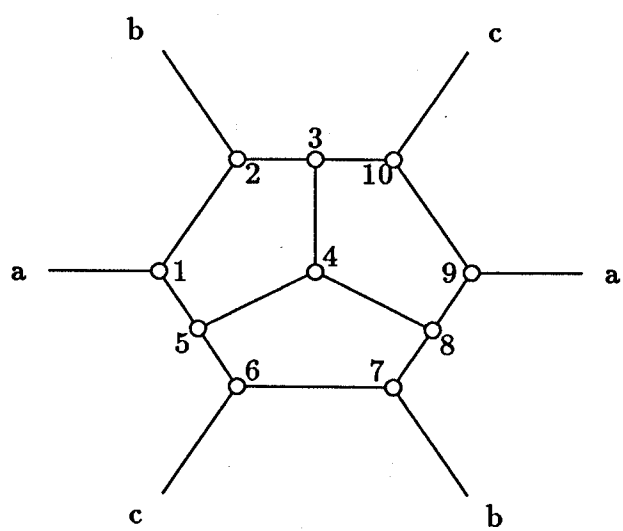

Figure 4. The Petersen graph on the projective plane.

Let F be the following face-vertex incidence matrix of this embedding.

$$F = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

As we can also see from the graph, any two faces of the embedding share two vertices and hence any two distinct rows of F are orthogonal to each other. Now we define the matrix A as $A := [F : I_6]$. Then the code C generated by G is a self-orthogonal $[16, 6]$ code. We have found the weight distribution of this code to be

$$A_0 = A_{16} = 1, \qquad A_6 = A_{10} = 16, \qquad A_8 = 30.$$

The codewords of weight six are the blocks of a symmetric $(16, 6, 2)$ design. The codewords of weight ten are the blocks of the complementary design. So using the face-vertex incidence matrix of certain graphs, we can also construct symmetric designs.

The codewords of weight eight are the blocks of a 2-$(16, 8, 7)$ design. Each codeword of weight eight is the sum of two or four distinct rows of A.

CHAPTER 4

THE ENUMERATION AND AUTOMORPHISMS OF SELF-DUAL CODES

In this chapter we first will give an enumeration theorem for self-dual codes. We will prove that almost all self-dual codes are indecomposable. Then we will mention the work done by Huffman, Yorgov and Pless under the assumption of the existence of an automorphism of odd order. In Section 4.3 we will prove that a self-orthogonal code with minimum distance four cannot have trivial automorphism group. In Section 4.4 we will construct a self-orthogonal code with trivial automorphism group.

4.1 Enumeration and related results

This section presents theorems on the enumeration of binary self-dual codes.

4.1.1 Theorem. *(MacWilliams et al. [18].) Let n be even and suppose C is a binary $[n,k]$ self-orthogonal code containing the all-one vector, with $k \geq 1$. Then the number of binary self-dual codes containing C is*

$$\prod_{i=1}^{\frac{n}{2}-k} (2^i + 1)$$

Proof. Let $\sigma_{n,m}$, for $k \leq m < n/2$, be the number of $[n,m]$ self-orthogonal codes which contain C. We establish a recursion formula for $\sigma_{n,m}$. Let D be an $[n,m]$ self-orthogonal code containing the C. First we count the number of ways D can be extended to an $[n,m+1]$ self-orthogonal code containing the all-one vector. Now D can be extended by adjoining an element of $D^{\perp}$ not already in D. Since dim $D = m$, we have dim $D^{\perp} = n - m$. Consider the cosets of D in $D^{\perp}$. There are $|D^{\perp}|/|D| = 2^{n-m}/2^m = 2^{n-2m}$ cosets. Say

$$D^{\perp} = D \cup (h_1 + D) \cup (h_2 + D) \cup \cdots \cup (h_l + D),$$

where $l = 2^{n-2m} - 1$. Clearly any two extensions of D obtained by adjoining u and v are different if and only if u and v belong to different cosets. Hence we have exactly $2^{n-2m} - 1$ extensions, namely

$$D \cup (h_j + D) \ \ for \ \ j = 1, 2, ..., l.$$

Now all we have to do is to find the number of $[n,m]$ subcodes containing C in an extension. Since an extension $D \cup (h_j + D)$ is of dimension $m+1$ then

$$|D \cup (h_j + D)|/|C| = 2^{m+1}/2^k = 2^{m+1-k}$$

so there are $2^{m+1-k} - 1$ subcodes of $D \cup (h_j + D)$ properly containing C. Thus for $k \leq m < n/2$,

$$\sigma_{n,m+1} = \sigma_{n,m} \cdot \frac{2^{n-2m} - 1}{2^{m+1-k} - 1}.$$

Starting from $\sigma_{n,k} = 1$ gives the result. ∎

4.1.2 Corollary. *The number of binary self-dual codes of length n is*

$$\prod_{i=1}^{\frac{n}{2}-1}(2^i+1).$$

Proof. In the above theorem, take C to be the self-orthogonal code of length n which consists of the all-one vector and the zero vector. ∎

If a self-dual code is decomposable, then each component must be self-dual. Indeed, let C be a decomposable self-dual code. Without loss of generality we can assume that C has a generator matrix of the form

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

To prove the claim it is enough to prove that the submatrix A generates a self-dual code. Let C_1 be the code generated by A and C_2 be the code generated by B. Let k be the length of C_1. So the length of C_2 is $n-k$. Since C is a self-dual code, C_1 and C_2 must be self-orthogonal codes. So we have

$$dim(C_1) \leq \frac{k}{2} \tag{1}$$

and

$$dim(C_2) \leq \frac{n-k}{2}. \tag{2}$$

We have

$$dim(C_1) + dim(C_2) = dim(C) = \frac{n}{2}$$

So the equalities must hold in (1) and (2). Hence C_1 is a self-orthogonal code of length k and dimension $\frac{k}{2}$. This implies that C_1 is a self-dual code.

Using this and a counting argument we can prove the following theorem.

4.1.3 Theorem. *Almost all self-dual codes are indecomposable.*

Proof. Let G_n be the number of self-dual codes of length n and C_n be the number of indecomposable self-dual codes of length n. We define G_0 to be 1. By counting the self-dual codes of length n with a distinguished coordinate place in two different ways we will show that

$$nG_n = \sum_{k=1}^{n/2} \binom{n}{2k} 2k\, C_{2k} G_{n-2k}. \tag{3}$$

Indeed, we can choose any of n coordinate places as the distinguished coordinate place so we have nG_n self-dual codes of length n with a distinguished coordinate place. On the other hand, the distinguished coordinate place must occur in a component of length $2k$, where $k \in \{1, 2, 3, \cdots, \frac{n}{2}\}$. The binomial coefficient $\binom{n}{2k}$ is the number of ways to select $2k$ coordinate places for the coordinate places of the component containing the distinguished coordinate place. Since any one of $2k$ coordinate places may be the distinguished one, we have

$$\binom{n}{2k} 2k\, C_{2k}$$

choices for the component that contains the distinguished coordinate place. The remaining $n-2k$ coordinate places determine a self-dual code of length $n-2k$. So any of G_{n-2k} self-dual codes may occur in the remaining $n-2k$ coordinate places. Thus the sum

$$\sum_{k=1}^{n/2} \binom{n}{2k} 2k\, C_{2k} G_{n-2k},$$

also counts the self-dual codes of length n with a distinguished coordinate place. This proves the equality.

Dividing both sides of (3) by nG_n, we obtain

$$\begin{aligned} 1 &= \sum_{k=1}^{n/2} \binom{n}{2k} \frac{2k}{n} C_{2k} \frac{G_{n-2k}}{G_n} \\ &= \sum_{k=1}^{n/2} \binom{n-1}{2k-1} \frac{C_{2k}}{G_{2k}} \frac{G_{n-2k} G_{2k}}{G_n} \\ &= \frac{C_n}{G_n} + \sum_{k=1}^{(n/2)-1} \binom{n-1}{2k-1} \frac{C_{2k}}{G_{2k}} \frac{G_{n-2k} G_{2k}}{G_n}. \end{aligned}$$

Set

$$F_n = \sum_{k=1}^{(n/2)-1} \binom{n-1}{2k-1} \frac{C_{2k}}{G_{2k}} \frac{G_{n-2k} G_{2k}}{G_n}.$$

So we have

$$F_n \leq \sum_{k=1}^{(n/2)-1} \binom{n-1}{2k-1} \frac{G_{n-2k} G_{2k}}{G_n}.$$

Now since

$$\frac{G_{n-2(\frac{n}{2}-k)} G_{2(\frac{n}{2}-k)}}{G_n} = \frac{G_{n-2k} G_{2k}}{G_n},$$

unless $k = n/4$ the term $\frac{G_{n-2k}G_{2k}}{G_n}$ will occur twice in the summation

$$\sum_{k=1}^{(n/2)-1} \binom{n-1}{2k-1} \frac{G_{n-2k}G_{2k}}{G_n}.$$

The coefficients of these occurences are $\binom{n-1}{2k-1}$ and $\binom{n-1}{n-2k-1}$. So if n is not divisible by four we have

$$\begin{aligned}
\sum_{k=1}^{(n/2)-1} \binom{n-1}{2k-1} \frac{G_{n-2k}G_{2k}}{G_n} &= \sum_{k=1}^{\lfloor n/4 \rfloor} \left(\binom{n-1}{2k-1} + \binom{n-1}{n-2k-1} \right) \frac{G_{n-2k}G_{2k}}{G_n} \\
&= \sum_{k=1}^{\lfloor n/4 \rfloor} \left(\binom{n-1}{2k-1} + \binom{n-1}{2k} \right) \frac{G_{n-2k}G_{2k}}{G_n} \\
&= \sum_{k=1}^{\lfloor n/4 \rfloor} \binom{n}{2k} \frac{G_{n-2k}G_{2k}}{G_n}.
\end{aligned}$$

If n is divisible by four, similarly we see that

$$\sum_{k=1}^{(n/2)-1} \binom{n-1}{2k-1} \frac{G_{n-2k}G_{2k}}{G_n} = \binom{n-1}{\frac{n}{2}-1} \frac{G_{\frac{n}{2}}G_{\frac{n}{2}}}{G_n} + \sum_{k=1}^{\lfloor n/4 \rfloor - 1} \binom{n}{2k} \frac{G_{n-2k}G_{2k}}{G_n}.$$

Since

$$\binom{n-1}{\frac{n}{2}-1} = \binom{n-1}{\frac{n}{2}} < \binom{n}{\frac{n}{2}},$$

in both cases we have

$$\sum_{k=1}^{(n/2)-1} \binom{n-1}{2k-1} \frac{G_{n-2k}G_{2k}}{G_n} \leq \sum_{k=1}^{\lfloor n/4 \rfloor} \binom{n}{2k} \frac{G_{n-2k}G_{2k}}{G_n}.$$

So for any n we have

$$F_n \leq \sum_{k=1}^{\lfloor n/4 \rfloor} \binom{n}{2k} \frac{G_{n-2k}G_{2k}}{G_n}.$$

Also

$$\begin{aligned}
\frac{G_{n-2k}G_{2k}}{G_n} &= \frac{G_{2k}}{G_n/G_{n-2k}} \\
&= \frac{\prod_{i=1}^{k-1}(2^i+1)}{\prod_{i=\frac{n-2k}{2}}^{\frac{n}{2}-1}(2^i+1)} \\
&< \frac{\prod_{i=1}^{k-1} 2^{i+1}}{\prod_{i=\frac{n-2k}{2}}^{\frac{n}{2}-1} 2^i} \\
&= \frac{2^k}{2 \cdot 2^{\frac{(n-2k)k}{2}}}.
\end{aligned}$$

Since $k \leq \frac{n}{4}$, we have $\frac{n-2k}{2} \geq \frac{n}{4}$ and thus

$$\frac{2^k}{2 \cdot 2^{\frac{n-2k}{2}k}} \leq \frac{2^k}{2 \cdot 2^{\frac{n}{4}k}} = \frac{1}{2}(\frac{1}{2^{\frac{n}{4}-1}})^k.$$

We also have $\binom{n}{2k} \leq n^{2k}$. Hence we get

$$F_n \leq \frac{1}{2} \sum_{k=1}^{\lfloor n/4 \rfloor} n^{2k}(\frac{1}{2^{\frac{n}{4}-1}})^k < \sum_{k=1}^{\lfloor n/4 \rfloor} (\frac{n^2}{2^{\frac{n}{4}-1}})^k.$$

Since $lim_{n\to\infty}(\frac{n^2}{2^{\frac{n}{4}-1}}) = 0$ we can choose n so large that $(\frac{n^2}{2^{\frac{n}{4}-1}}) < 1$. Hence for sufficiently large n we have

$$F_n \leq \sum_{k=1}^{\lfloor n/4 \rfloor} (\frac{n^2}{2^{\frac{n}{4}-1}})^k < \sum_{j=1}^{\infty} (\frac{n^2}{2^{\frac{n}{4}-1}})^j = \frac{n^2}{2^{\frac{n}{4}-1}} \cdot \frac{1}{1 - \frac{n^2}{2^{\frac{n}{4}-1}}}.$$

If $n \geq 64$ and n large enough that $\frac{n^2}{2^{n/4-1}} < 1$, then $\frac{1}{1-\frac{n^2}{2^{\frac{n}{4}-1}}} < 2$, and hence for such n we have

$$F_n \leq 2 \cdot (\frac{n^2}{2^{\frac{n}{4}-1}}).$$

By taking the limit of both sides, we see that

$$\lim_{n\to\infty} F_n = 0.$$

Using the equality $1 = \frac{C_n}{G_n} + F_n$ and the above result, we conclude that

$$\lim_{n\to\infty} \frac{C_n}{G_n} = 1. \blacksquare$$

4.2 A Search for codes using their automorphism groups

Self-dual codes through length 30 and doubly even self-dual codes of length 32 have been completely enumerated in Pless [21], Pless and Conway [5], and Pless and Sloane [23]. This seems infeasible for any greater length because of the large number of such codes; there are at least

$$\frac{\prod_{i=1}^{\frac{n}{2}-1}(2^i+1)}{n!}$$

inequivalent codes of length n. For example, we would have at least 17,000 inequivalent codes of length 40. However, those of largest minimum distance, called *extremal codes*, seem relatively rare among these codes. (We should remind the reader that some authors define extremal codes to be the self-dual codes whose minimum distances realizes the bound given by the Gleason theorem. See Appendix A.) In particular, there are one extremal self-dual doubly even code of length 8, two of length 16, one of length 24, and five of length 32. Only one is known of length 48 and it is the extended quadratic residue code. An interesting observation is that each of these codes possesses a nontrivial automorphism of odd order.

The existence of an odd automorphism leads to a decomposition of the doubly even codes into shorter self-dual codes and therefore the classification problem reduces to a simpler case. To show this we need the following definitions. Let C be a self-dual code of length n and let σ be an automorphism of C of prime order p. Suppose in the cycle decomposition of σ there are c cycles of length p and f fixed points. Denote the cycles by $\Omega_1, \Omega_2, \cdots, \Omega_c$ and the fixed points by $\Omega_{c+1}, \Omega_{c+2}, \cdots, \Omega_{c+f}$. The subspace $E_\sigma(C)$ is defined to be the set of codewords v such that $|supp(v) \cap \Omega_i|$ is even for $1 \leq i \leq c+f$. We define $F_\sigma(C)$ to be the set of codewords which are fixed by σ. If $v \in F_\sigma(C)$, then the entries of v are constant on each cycle Ω_i. We define π as follows

$$\pi : F_\sigma(C) \to (GF(2))^{c+f}$$

$$(\pi(v))_i = v_j$$

for $j \in \Omega_i$, $i = 1, 2, \cdots, c+f$. The following was proved in Huffman [13]. We present it in a different form.

4.2.1 Lemma. *If C is a self-dual code, then the subspaces $F_\sigma(C)$ and $E_\sigma(C)$ have no common element other than zero, and span C. The code $\pi(F_\sigma(C))$ is a self-dual code of length $c+f$.*

In Huffman [13] it is proven that an extremal doubly even code of length 48 with a nontrivial automorphism of odd order is equivalent to the extended quadratic residue code. In Pless and Conway [6], Huffman and Yorgov [14], Pless [22] and Pless and Thompson [24] the assumption of the existence of an automorphism of odd order has been used to search for a $[72, 36, 16]$ doubly even code. The use of the assumption is, if the code C has an automorphism of odd order then it is spanned by two subcodes. One of these subcodes, namely $F_\sigma(C)$, can be determined from $\pi(F_\sigma(C))$ which is a self-dual code of a shorter length. So the problem reduces to the existence of a shorter self-dual code. In [1] Anstee, Hall and Thompson have used the same idea to search for the projective plane of order 10. In Yorgov [28] all extremal even self-dual codes of length 40 which have an automorphism of order a prime greater than 5 are obtained. The same author [29] has also classified all extremal doubly even self-dual codes of length 56 with an automorphism of order 13. (There are sixteen such inequivalent codes.)

4.3 Self-orthogonal codes with distance four

In this section we will prove that a self-orthogonal code of minimum distance four cannot have trivial automorphism group. For this we will make use of the classification of the self-orthogonal codes generated by codewords of weight four. All indecomposable, self-orthogonal codes which are generated by codewords of weight four are described in Pless and Sloane [23] using the following notation.

For $n = 4, 6, 8, \cdots$, we define d_n to be the self-orthogonal $[n, \frac{1}{2}n-1]$ code with a generator matrix

$$d_n := \begin{pmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ & & 1 & 1 & 1 & 1 & & & & & & \\ & & & & \cdot & \cdot & \cdot & \cdot & & & & \\ & & & & & & \cdot & \cdot & \cdot & \cdot & & \\ & & & & & & & & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The self-orthogonal $[7, 3]$ code e_7 has the following generator matrix

$$e_7 := \begin{pmatrix} 1 & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 1 & 1 & & \\ 1 & & 1 & & 1 & & 1 & \end{pmatrix}.$$

Finally, E_8 has the generator matrix

$$E_8 := \begin{pmatrix} 1 & 1 & 1 & 1 & & & & \\ & & 1 & 1 & 1 & 1 & & \\ & & & & 1 & 1 & 1 & 1 \\ & 1 & & 1 & & 1 & & 1 \end{pmatrix}.$$

(It is the self-dual $[8,4]$ Hamming code.)

We define Z_n as the group of integers modulo n and define S_n as the symmetric group on n elements. The automorphism group of d_n is

$$Aut(d_4) = S_4$$

and if n is greater than four, then $Aut(d_n)$ is the wreath product of Z_2 by $S_{n/2}$. (See Pless and Sloane [23].)

The automorphism group of e_7 is $PSL_2(7)$ which has 168 elements [22]. It is also known that E_8 has an automorphism group of order 1344, namely $GL_3(2)$.

Now we will define some vectors of length n and using them describe the duals of the above codes. For even n greater than four,

$$a_n := 1010\cdots 10$$

$$b_n := 1100\cdots 00$$

$$a_n' := a_n + b_n = 0110101\cdots 10$$

and

$$c_7 := 1111111.$$

We know that

$$d_n^{\perp} = d_n \cup (a_n + d_n) \cup (b_n + d_n) \cup (a_n' + d_n)$$

$$e_7^{\perp} = e_7 \cup (c_7 + e_7).$$

Since E_8 is self-dual we have:

4.3.1 Lemma. *(Pless and Sloane [23].) If C is a self-orthogonal code containing E_8 as a subcode, then C is decomposable.*

Proof. Without loss of generality we can assume that C has a generator matrix of the form

$$A = \left(\begin{array}{c|c} E_8 & 0 \\ \hline R & M \end{array}\right).$$

Since C is self-orthogonal each row of R must be in the dual of E_8. But E_8 is self-dual, hence each row of R is in E_8. Therefore any row of R can be written as a linear combination of the rows of E_8. So if in the matrix A we replace the submatrix R with the zero matrix, we still have a generator matrix of C. From this we conclude that C is decomposable. ∎

Now we can state the theorem characterizing indecomposable self-orthogonal codes generated by codewords of weight four.

4.3.2 Theorem. *(Pless and Sloane [23].) An indecomposable self-orthogonal code C of length n which is generated by codewords of weight four is either d_n $(n = 4, 6, 8, \cdots)$, e_7 or E_8.*

So if we have a self-orthogonal code C of minimum distance four, the subcode generated by codewords of weight four must be of the form

$$d_{r_1} \oplus d_{r_2} \oplus \cdots \oplus d_{r_l} \oplus e_7 \oplus e_7 \oplus \cdots \oplus e_7 \oplus E_8 \oplus E_8 \oplus \cdots \oplus E_8$$

for some integers $r_1, r_2, \cdots, r_l$. In the above direct sum e_7 occurs m times and E_8 occurs k times (say).

Let C be an indecomposable self-orthogonal code of minimum distance four and let C' be its subcode generated by codewords of weight four. From Theorem 4.3.2 and Lemma 4.3.1 we know that C' must be a direct sum of the form

$$C' = d_{r_1} \oplus \cdots \oplus d_{r_l} \oplus e_7 \oplus \cdots \oplus e_7.$$

Then C has a generator matrix A of the form

$$\left(\begin{array}{c|c|c|c|c|c|c|c|c} d_{r_1} & & & & & & & & \\ -- & -- & & & & & & & \\ & d_{r_2} & & & 0 & & & & \\ & -- & . & & & & & & \\ & & . & & & & & & \\ & & & -- & & & & & \\ & & & d_{r_l} & & & & & 0 \\ & & & -- & -- & & & & \\ & 0 & & & e_7 & & & & \\ & & & & -- & & & & \\ & & & & & & & -- & \\ & & & & & & & e_7 & \\ -- & -- & -- & -- & -- & -- & -- & -- & -- \\ R_1 & R_2 & .. & R_l & M_1 & .. & M_m & Q & \end{array}\right). \quad (1)$$

Note that any row of R_i must be in $d_{r_i}^{\perp}$ for $i \in \{1, 2, \cdots, l\}$, and any row of M_j must be in $e_7^{\perp}$ for $j \in \{1, 2, \cdots, m\}$. Now we are ready for the following lemma.

4.3.3 Lemma. *Let C be an indecomposable self-orthogonal code of minimum distance four and A be a generator matrix of C in the above form. Let π be a permutation of the first r_1 columns of A such that,*

(a) $\pi \in Aut(d_{r_1})$, *and*

(b) for any row u of R_1, the image $\pi(u)$ belongs to the same coset of d_{r_1} in $d_{r_1}^{\perp}$ as u.

Then π is an automorphism of C.

Proof. Observe that if any row v of R_1 is replaced by some element in the coset $v + d_{r_1}$ in $d_{r_1}^{\perp}$, we still have a generator matrix for C. ∎

Now all we have to do is to find a nontrivial automorphism of d_{r_1} which satisfies the hypothesis of Lemma 4.3.3.

4.3.4 Theorem. *A self-orthogonal code with minimum distance four cannot have trivial automorphism group.*

Proof. Let C be an indecomposable self-orthogonal code of minimum distance four and A be its generator matrix of the form given in (1). We can assume

that the rows of the matrix R_1 are all in the set $\{0, a_{r_1}, b_{r_1}, a'_{r_1}\}$. Now we can easily prove that the permutation $\pi = (13)(24)$ is an automorphism of d_{r_1} for any value of r_1. Moreover we can also see that it satisfies the second requirement of Lemma 4.3.3:

$$\pi(a_{r_1}) = \pi(1010\cdots10) = a_{r_1}$$
$$\pi(b_{r_1}) = \pi(1100\cdots00) = 0011\cdots00 = b_{r_1} + 111100\cdots00 \in b_{r_1} + d_{r_1}$$
$$\pi(a'_{r_1}) = \pi(0110\cdots10) = 1001\cdots10 = a'_{r_1} + 111100\cdots00 \in a'_{r_1} + d_{r_1}$$
$$\pi(0) = 0$$

So by Lemma 4.3.3 $\pi \in A(C)$. If e_7 occurs in the matrix A, then the automorphism group of C contains a copy of $PSL_2(7)$, since we can assume that the rows of the matrix M_1 are elements of the set $\{0000000, 1111111\}$ and any automorphism of e_7 fixes these two vectors. Hence the automorphism group of C is nontrivial. ∎

If a self-orthogonal code has minimum weight two, the two columns that correspond to the support of a codeword of weight two must be the same. So the transposition interchanging these two columns must be an automorphism of the code. Hence a self-orthogonal code with minimum distance two cannot have trivial automorphism group. Therefore a self-orthogonal code with identity automorphism group must have minimum distance at least six.

4.4 A self-orthogonal code with trivial automorphism group

From the last section we know that a self-orthogonal code of minimum distance less than or equal to four cannot have trivial automorphism group. In this section we will construct a self-orthogonal code with trivial automorphism group. For this we will use a cubic planar graph with trivial automorphism group.

The following graph G has trivial automorphism group (Faulkner [7]):

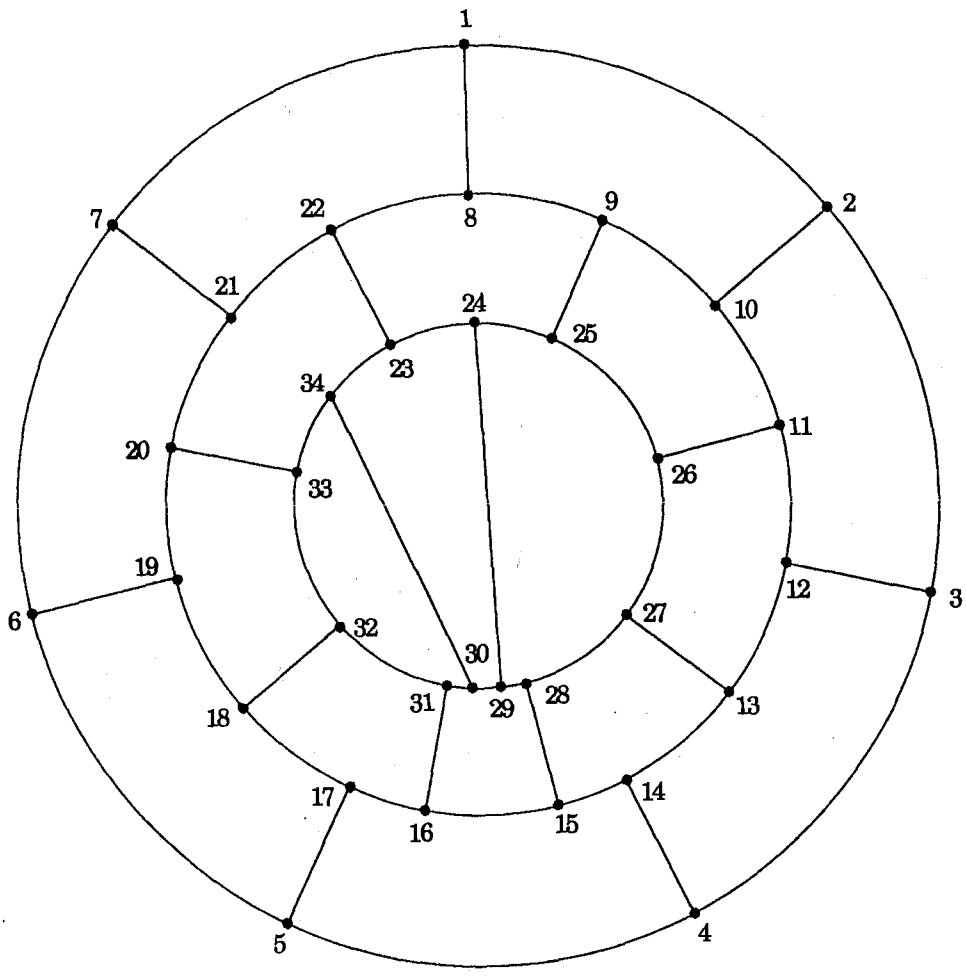

Figure 5. A graph with trivial automorphism group.

This graph has 34 vertices and 19 faces. Let F be the following face-vertex incidence matrix of G.

$$\begin{pmatrix}
1&1&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&1&0&0&0&1\\
1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

In the matrix F the first thirteen rows correspond to the faces of degree five and the fourteenth to the face of degree seven. We define the matrix $A_{19\times 48}$ as

$$A := \left(\begin{array}{c|c} & I_{14} \\ F & \\ \hline & \\ & 0 \end{array}\right)$$

4.4.1 Theorem. *A is a generator matrix for a $[48, 19]$ self-orthogonal code with trivial automorphism group.*

Proof. We first prove that the rows of A are linearly independent. The proof is by contradiction. Let S be a subset of the set of rows of A. If S is a minimal dependent subset then $\sum_{u\in S} u = 0$. For $1 \le i \le 14$, the i^{th} row is the only row which has 1 in the $(34+i)^{th}$ column, so none of the first fourteen rows can be in S. Hence S must be a subset of the last five rows. But in the support of any one of the last five rows, there is a coordinate place which does not belong to

the support of the other four. So there is no subset of the last five rows whose sum is equal to zero. Hence the last five rows are linearly independent and A is of rank 19.

To prove that the row space C of A is self-orthogonal all we need to observe is that any two rows of A are orthogonal to each other. This follows as any two faces of G share two or zero vertices. Each row of A has even weight, so any row is orthogonal to itself. This proves that C is a self-orthogonal code.

Now we will prove that C has trivial automorphism group. Using the computer we have determined the weight distribution of C as $A_0 = 1$, $A_6 = 18$, $A_8 = 45$, $A_{10} = 136$, $A_{12} = 572$, $A_{14} = 2154$, $A_{16} = 7915$, $A_{18} = 25310$, $A_{20} = 60740$, $A_{22} = 103454$, $A_{24} = 123598$ (since all-one vector is in C we have $A_i = A_{48-i}$ for $i = 0, 2, \cdots, 24$). So the only codewords of weight six are the eighteen rows of A of weight six, i.e., all rows except the fourteenth row. We conclude that any automorphism of C must permute these eighteen rows. There are 45 codewords of weight eight. Observe that the sum of any two rows of weight six that correspond to two adjacent faces of G is a codeword of weight eight. The number of such pairs is just the number of edges not on the boundary face. So we have

$$|E(G)| - 7 = 44$$

pairs of adjacent faces whose sums give codewords of weight eight. With the row corresponding to the outside face, we have 45 codewords of weight eight. So we see that a codeword of weight eight is either the row corresponding to the outside face or the sum of two rows that correspond to adjacent faces of degree five or six. From this it follows that the fourteenth row is the only codeword of weight eight that covers the last coordinate place. There are no codewords of weight six which cover the last coordinate place and the last column is the only coordinate place which is not covered by codewords of weight six. So the last column must be fixed under every automorphism of C. Thus the fourteenth row must be fixed under any automorphism of C. We conclude that any automorphism of C must result in a permutation of the rows of A.

We partition the coordinate places into two parts X and Y by defining

X to be the set of the first 34 coordinate places and Y the set of remaining coordinate places. We first prove that the parts X and Y are fixed under any automorphism of C. We have already proven that the last coordinate place must be fixed under any automorphism of C. Any $i \in X$ is covered by at least two codewords of weight six, while if $j \in Y$ and $j \neq 48$ then it is covered by exactly one codeword of weight six. So no automorphism of C can interchange any element of X with any element of Y. Hence X and Y are fixed under any automorphism of C. Now let π be an automorphism of C. We will consider three cases.

(1) Assume π fixes every element of X.

If π is not the trivial automorphism, then it must move some elements of Y. Say $\pi(35) = j$. So the support of the image of the first row under π is $\{1, 2, 8, 9, 10, j\}$. But there is no codeword with this support in C unless $j = 35$. So we conclude that in this case π must be the trivial automorphism.

(2) Assume π fixes every element of Y.

We already know that π must permute the rows of A. So in this case π must permute the rows of the submatrix F. This means π must be an automorphism of the graph G. Since G has trivial automorphism group we conclude that π must be the trivial automorphism.

(3) Assume π moves points of both of X and Y.

Then again π must permute the rows of F and we already know that the partition (X,Y) is fixed under any automorphism of the code. So the restriction of π to first 34 coordinate places must be an automorphism of the graph G. Since G has trivial automorphism group this restriction must be the trivial automorphism. But this shows that the action of π on Y is trivial too because $supp(r_i) \cap \{1, 2, \cdots, 34\}$ determines the support of r_i and since each row of F is fixed then each row of A is also fixed. ∎

CHAPTER 5

THE BARNETTE CONJECTURE

In this chapter we will make some observations about cubic planar bipartite graphs. We will survey some approaches to the Barnette conjecture and give a new conjecture which implies it. We will also give an infinite family of Hamiltonian cubic planar bipartite graphs.

5.1 The Barnette conjecture and early results

Problem 5 in Tutte [25: p. 343] states what has become known as the *Barnette conjecture*. The conjecture states that every cubic 3-connected bipartite planar graph is Hamiltonian. A famous result of Tutte [27] shows that the 4-connected planar graphs are Hamiltonian. In [26] Tutte also showed that some 3-connected planar graphs are non-Hamiltonian. That the same is true for bipartite cubic 3-connected graphs is shown by a graph of Horton, see Bondy and Murty [4: p. 240]. Recent work has been expended on trying to determine the order of the smallest non-Hamiltonian cubic 3-connected planar graph. Lederberg, Bosák and Barnette (see Grunbaum [10]) have constructed a non-Hamiltonian cubic 3-connected planar graph of order 38. Okamura [19] has shown that the smallest non-Hamiltonian cubic 3-connected planar graph has order at least 34. In [12] Holton and McKay have shown that the conjecture is true for graphs of order up to and including 64.

A different approach to the Barnette conjecture can be found in Hakimi and Schmeichel [11]. The *vertex arboricity* of a graph G is defined as the minimum number of subsets into which $V(G)$ can be partitioned so that each subset induces an acyclic graph. In [11] the planar graphs with vertex arboricity two are characterized in terms of their dual graphs.

5.1.1 Theorem. *(Hakimi and Schmeichel [11].) Let G be a planar graph. Then the vertex arboricity of G is equal to two if and only if the dual of G contains a connected Eulerian spanning subgraph.*

Proof. Suppose that the vertex arboricity of G is equal to two. Let $\{V_1, V_2\}$ be an acyclic partition of G (i.e., the graphs induced by V_1 and V_2 are acyclic). Let $E(V_1, V_2)$ denote the edges in G joining a vertex in V_1 to one in V_2, and consider the corresponding set of edges E' in G^*. Let H denote the subgraph of G^* induced by E'; we will show that H is a connected Eulerian spanning subgraph of G^*.

Since $E(V_1, V_2)$ is an edge cut in G, the graph H is Eulerian. Since every cycle of G contains an edge of $E(V_1, V_2)$, every face of G contains one or more edges of $E(V_1, V_2)$, and hence H is spanning in G^*. If H were disconnected, then G^* would contain an edge cut E_1' containing none of the edges of E'. But then the corresponding set of edges E_1 in G would induce an Eulerian subgraph G_1 in G containing none of the edges in $E(V_1, V_2)$, contradicting the assumption that $\{V_1, V_2\}$ is an acyclic partition in G.

Conversely, suppose G^* contains a connected Eulerian spanning subgraph H'. Let H denote the subgraph induced by the corresponding set of edges in G. Since H' is Eulerian, the edges of H form an edge cut $E(V_1, V_2)$ in G. Since every edge cut in G^* contains at least one edge of H', every cycle in G contains one or more edges of $E(V_1, V_2)$. Thus the graph induced by V_i is acyclic for $i = 1, 2$, and so the vertex arboricity of G is equal to two. ∎

Since a connected Eulerian spanning subgraph in a cubic graph is a Hamiltonian cycle, using the above theorem Barnette's conjecture can be reformulated as, "Every Eulerian planar triangulation has vertex arboricity equal to two".

5.2 Another approach to the Barnette conjecture

In Chapter 3 we have shown that the minimal dependent subsets of the faces of a cubic planar bipartite graph are the pairwise unions of the colour classes of the faces (see Lemma 3.1.3). In this section we will use these sets again. Let G be a 3-connected cubic planar bipartite graph whose faces are properly coloured by the colours 1, 2 and 3. This colouring gives a proper vertex colouring of the dual graph G^*. We define G_i^* to be the subgraph of G^* induced by the vertices coloured j and k where $\{i,j,k\} = \{1,2,3\}$. Clearly G_1^*, G_2^* and G_3^* are bipartite subgraphs of G^*. We will call these graphs the *minimal dependent graphs* of G. The *symmetric difference* of a collection of sets $\{A_i : i = 1,2,\cdots,n\}$ is defined as the set of elements x such that x belongs to exactly one A_i, where $i = 1,2,\cdots,n$.

5.2.1 Lemma. *Let G be a 3-connected cubic planar bipartite graph and let G_i^* be a minimal dependent graph of G. Let T^* be an induced subgraph of G_i^* which is a tree. Define the subgraph C of G by its edge set $E(C)$ as the symmetric difference of the set $\{E(f) : f \in V(T^*)\}$. Then C is a cycle in the graph G which passes through all vertices of the graph G which lie on faces of G corresponding to the vertices of T^*.*

Proof. The proof is by induction on the number of edges of T^*. If $|E(T^*)| = 1$ then T^* corresponds to two adjacent faces f_1, f_2 of G. In this case

$$E(C) = E(f_1) \cup E(f_2) - [E(f_1) \cap E(f_2)]$$

is a cycle and the lemma holds. Now assume T^* is an induced subgraph of G_i^* which is a tree with $k+1$ edges. Let x be a vertex of T^* of degree one and e^* be the unique edge of T^* which is adjacent to x. Let e be the edge of G corresponding to the edge e^*. Now consider the subgraph T_x^* of G_i^* which is induced by the vertex set $V(T^*) - x$. The tree T_x^* is an induced subgraph of G_i^* with k edges. So by the induction hypothesis the set of edges that are in the symmetric difference of the set $\{E(f) : f \in V(T_x^*)\}$ is a cycle C' in G that passes through all vertices of the graph G which lie on faces corresponding to the vertices of T_x^*. Now $e \in E(C')$ and since T^* is an induced subgraph of G_i^*,

the vertex x of T^* is adjacent to exactly one vertex of T_x^*. So the symmetric difference of the set $\{E(f) : f \in V(T^*)\}$ is equal to

$$E(C) = \Big(E(C') - \{e\}\Big) \cup (E(f) - \{e\}).$$

Obviously C is a cycle in G passing through all vertices of the graph G which lie on faces of G corresponding to the vertices of T^*. This completes our proof. ∎

Since G is a cubic graph, every vertex must be incident with a face of each colour in the proper face colouring of G. So if G^* has an induced subgraph T^* which is a bicoloured tree and $V(T^*)$ contains a colour class, then G is Hamiltonian.

Now we will give two lemmas about minimal dependent graphs.

5.2.2 Lemma. *A minimal dependent graph of a 3-connected cubic planar bipartite graph is a 2-edge connected planar bipartite graph.*

Proof. Let H^* be a minimal dependent graph of a 3-connected cubic planar bipartite graph G. We already know that H^* is connected (by the proof of Lemma 3.1.3). Now we will prove that any edge of H^* is shared by two distinct faces of H^*, i.e., H^* has no cut edge. The vertices of H^* correspond to the union of two colour classes of the proper 3-face colouring of G. Say the faces of G are coloured by the colours a, b and c and $V(H^*)$ is the union of colour classes a and b. Let e^* be an edge of H^* between vertices x and y. Now x and y are two faces of G that are coloured (distinctly) by a and b (as G is 3-connected). Let $e = (v_1, v_2)$ be the edge of G corresponding to e^*. The vertex v_1 is incident with the faces x and y. Let f be the third face of G which is incident with v_1. The face f must be coloured by c. Also the vertex v_2 is incident with the faces x and y. Let f' be the third face of G which is incident with v_2. The face f' must be coloured by c too (the faces f and f' must be different because G is 3-connected). Let $N(f)$ be the set of faces adjacent to f. In the dual graph G^*, the subgraphs induced by $N(f)$ and $N(f')$ give the two faces of H^* that share e^*. Hence e^* cannot be a cut-edge. So the proof is completed. ∎

On the other hand we have the following lemma.

5.2.3 Lemma. *If H^* is a 2-edge connected planar bipartite graph, then it is a minimal dependent graph of some 3-connected cubic planar bipartite graph G on $2|E(H^*)|$ vertices.*

Proof. We define the graph G^* with its vertex and edge sets as follows,

$$V(G^*) = V(H^*) \cup F(H^*)$$

and

$$E(G^*) = E(H^*) \cup \{(x,f) : x \in V(f) \text{ and } f \in F(H^*)\}.$$

Then the dual G of G^* is a 3-connected cubic planar bipartite graph and one of its minimal dependent graphs is H^*. ∎

From the construction in Lemma 5.2.3 we can see that if the bipartite graph H^* with the bipartition (X,Y) is a minimal dependent graph of G, then the other two minimal dependent graphs H_1^* and H_2^* of G are given as

$$V(H_1^*) = X \cup F(H^*)$$

$$E(H_1^*) = \{(x,f) : f \in F(H^*) \text{ and } x \in (X \cap V(f))\}$$

and

$$V(H_2^*) = Y \cup F(H^*)$$

$$E(H_2^*) = \{(y,f) : f \in F(H^*) \text{ and } y \in (Y \cap V(f))\}.$$

Now we can state the following conjecture which would imply the Barnette conjecture.

5.2.4 Conjecture. *Let H^* be a 2-connected planar bipartite graph with the bipartition (X,Y). Let H_1^* and H_2^* be defined as above. Then one of the bipartite graphs H^*, H_1^*, H_2^* has an induced subtree containing one of X and Y in its vertex set.*

As an application of Lemma 5.2.1 we will prove the following lemma. We already know that a cubic planar bipartite graph must have some faces of degree four.

5.2.5 Lemma. *Let G be a 3-connected cubic planar bipartite graph. If every vertex of G is incident with exactly one face of degree four, then G is Hamiltonian.*

Proof. Let G be such a graph. First we will prove that in the proper 3-colouring of the faces of G, all faces of degree four must have the same colour. Consider the set S of all faces of degree other than four. Exactly two elements of S are incident with each vertex of the graph. Hence S is a minimal dependent subset of faces and is the union of two colour classes (the minimal dependent subsets of faces are characterized in Lemma 3.1.3). This proves our claim.

Now by X let us denote the colour class of all faces of degree four and let Y be another colour class of G. Consider the subgraph H^* of G^* induced by $X \cup Y$, i.e., H^* is a minimal dependent graph of G. Now H^* is a 2-connected planar bipartite graph with the partition (X, Y) and all vertices in X have degree two. Let f be the boundary of the infinite face of H^*. If H^* has no cycle other than f, then, by deleting a vertex of f which belongs to X, we obtain an induced tree containing all vertices in Y. If H^* has some cycle C other than f, then delete a vertex $x \in C \cap X$. Clearly $H^* - x$ is a connected graph which has fewer cycles than H^* has. If $H^* - x$ is a tree we are done, if not by repeating this we will get a tree which contains all vertices in Y. So G^* has an induced subgraph which is a tree and contains all vertices in one colour class. This implies by Lemma 5.2.1 that G is hamiltonian. ∎

All connected simple planar vertex-transitive graphs are determined by Fleischner and Imrich [8]. Without using this classification, as a consequence of Lemma 5.2.1 and Lemma 5.2.5 we can prove the following.

5.2.6 Theorem. *Every vertex-transitive cubic planar bipartite 3-connected graph is Hamiltonian.*

Proof. Let G be such a graph. We know that G has some faces of degree four. Since G is vertex transitive, every vertex is adjacent to the same number of faces of degree four. If this number is one the result follows from Lemma 5.2.5. So we have two cases remaining:

(a) Each vertex is incident with three faces of degree four.

This implies that all faces of the graph are of degree four. Then the equality (see Lemma 3.2.1)

$$\sum_{f \in F(G)} (V(f) - 6) = -12$$

implies that the graph G has six faces and therefore has eight vertices. The only cubic planar bipartite 3-connected graph on eight vertices is the cube and it is Hamiltonian.

(b) Each vertex is incident with two faces of degree four.

First we count the number of faces of degree four. Each vertex is incident with two faces of degree four, and each face of degree four is incident with four vertices. By counting the pairs (f,v), $f \in F(G)$ and f is of degree 4 and $v \in V(f)$ in two different ways, we find that number of faces of degree four is equal to $\frac{|V(G)|}{2}$. The graph G has $\frac{|V(G)|}{2} + 2$ faces. So it has two faces which are not of degree four. These two faces cannot be adjacent, because otherwise any vertex that these two faces share would be incident with two faces which are not of degree four. Since each vertex is incident with exactly two faces of degree four, the set of faces of degree four is a union of two colour classes of the graph G (Lemma 3.1.3). Now consider the subgraph C of G^* which is induced by the vertices corresponding to the faces of G of degree four. We know that C is 2-edge connected (Lemma 5.2.2) and every vertex of C is of degree 2. So C must be a cycle. Let x be any vertex of this cycle. The graph $C - \{x\}$ is an induced subgraph of G^* which is a tree and it covers one of the colour classes of G. Hence by Lemma 5.2.1, G is Hamiltonian. ∎

APPENDIX A

A REVIEW OF CODING THEORY

A linear binary code of length n and dimension k is a k-dimensional subspace of $[GF(2)]^n$ and is called a binary $[n,k]$ code. The elements of the code are called *codewords*. The *distance* between two codewords is the number of coordinate places in which they differ. The *weight* $w(u)$ of a codeword u is the distance between u and 0. Observe that for a linear code C, the smallest nonzero weight is the smallest nonzero distance that occurs between codewords. The *support* of a codeword is the set of non-zero coordinate places. Let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x. The following theorem emphasizes the importance of the minimum distance of a code.

1. Theorem. *If d is the minimum distance of a code C, then C can correct $\lfloor (d-1)/2 \rfloor$ or fewer errors, and conversely.*

The *dual* $C^\perp$ of a code C is defined as

$$C^\perp := \{ v \in [GF(2)]^n \ : \ u \cdot v = 0 \quad \text{for all } u \in C \ \},$$

where the multiplication is the ordinary dot product, modulo 2. If $C \subseteq C^\perp$, C is called a *self-orthogonal* code and if $C = C^\perp$, C is called a *self-dual* code. If C is a linear code of length n then

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

So if C is a self-dual code, the dimension $dim(C)$ of C must be half of its length. Hence the length of a self-dual code must be even and every codeword must have even weight. A matrix which has a basis of the code C as its rows is called a *generator matrix* of the code C. Since any element of a code is a linear combination of the rows of a generating matrix of the code we have the following theorem.

2. Theorem. *If the rows of a generator matrix G for a binary $[n,k]$ code C have even weight and are orthogonal to each other, then C is self-orthogonal, and conversely.*

A binary self-dual code C is called *doubly even*, or just *even* if the weight of every codewords is divisible by 4. We state the following theorem from Gleason [9].

3. Theorem. *A doubly even code of length n exists if and only if n is divisible by 8.*

4. Lemma. *The largest minimum distance d a self-dual code of length n can have is as follows.*

(a) A self-dual code over $GF(2)$; $d = 2\lfloor n/8 \rfloor + 2$.

(b) A doubly even code over $GF(2)$; $d = 4\lfloor n/24 \rfloor + 4$.

(c) A self-dual code over $GF(3)$; $d = 3\lfloor n/12 \rfloor + 3$.

We call a self-dual code that has the largest possible minimum weight an *extremal code.* At the time this thesis is written 72 is the smallest number divisible by 24 for which it is not known whether or not an extremal, doubly even $[72, 36]$ code of minimum distance 16 exists. A code C of length n and dimension k is said to be the *direct sum* of two codes C_1 and C_2 and denoted by $C_1 \oplus C_2$, if it has a generator matrix of the form

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix},$$

where A_1 and A_2 are generator matrices for C_1 and C_2 respectively. The codes C_1 and C_2 are *components* of C. If a code cannot be written as a direct sum of subcodes, it is called *indecomposable*, and otherwise *decomposable.*

The *weight distribution* of a code is the number of codewords of any weight in the code. This is often described by the list of numbers A_i, where A_i is the number of codewords of weight i in the code. Another way to view the weight distribution is as polynomials called weight enumerators. Let C be a code of length n with A_i again the number of vectors of weight i. A polynomial in x and y is *homogeneous* of degree n if the powers of x and y in each term add up to n. Define the *weight enumerator* of C to be the following homogeneous polynomial.

$$W_C(x,y) = A_0x^n + A_1x^{n-1}y + A_2x^{n-2}y^2 + \cdots + A_ny^n.$$

In [16] MacWilliams has proven that

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

or, if we denote the number of codewords of weight i in $C^\perp$ by B_i,

$$\sum_{i=0}^{n} B_i x^{n-i}y^i = \frac{1}{|C|}\sum_{j=0}^{n} A_j(x+y)^{n-j}(x-y)^j.$$

Hence MacWilliams equation establishes a very interesting relationship between the weight distribution of a code C and the weight distribution of the dual code $C^\perp$.

A binary *cyclic code* of length n is an ideal of the ring

$$(GF(2))[x]/(x^n - 1).$$

The generator of this ideal is called the *generator polynomial* of the cyclic code.

An *automorphism* of a code C is a permutation of the columns of a generator matrix of C which gives another, or the same, generator matrix of C. It is easy to see that the set $Aut(C)$ of all automorphisms of C, is a subgroup of the symmetric group S_n, where n is the length of C. The group $Aut(C)$ is called the *automorphism group* of C. The two codes C_1 and C_2 are said to be *equivalent* if we can get a generator matrix of C_2 by permuting the columns of a generator matrix of C_1. If C_1 and C_2 are equivalent then $Aut(C_1)$ and $Aut(C_2)$ are conjugate in S_n, i.e., there is an element π of S_n such that

$$Aut(C_1) = \pi^{-1} \cdot Aut(C_2) \cdot \pi$$

If H and K are groups we write $H \times K$ for their *direct product*, H^k for $H \times H \times \cdots \times H$ (k factors), and $H \cdot K$ for a *semidirect product*. The following two lemma are in Sloane and Pless [23].

5. Lemma. *If $C = C_1 \oplus C_2 \oplus \cdots \oplus C_k$ where C_i are indecomposable and equivalent, then*

$$Aut(C) = Aut(C_i)^k \cdot S_k.$$

6. Lemma. *Let $C = D_1 \oplus D_2 \oplus \cdots \oplus D_l$ where each D_i is a direct sum of equivalent codes, and for $i \neq j$ no summand of D_i is equivalent to a summand of D_j. Then*

$$Aut(C) = \prod_{i=1}^{l} Aut(D_i).$$

APPENDIX B

CLASSIFICATION

In [20], Pless has classified all self-dual codes of length less than or equal to 20. With one exception, we can construct all these codes from the face-vertex incidence matrices of cubic planar bipartite graphs. (The exception, denoted M_{20} in [20] was constructed from a cubic bipartite graph embedded on the Möbius strip, as Example 3.4.1.) We now give the list of graphs generating all self-dual codes of length less than or equal to twenty, other than M_{20}. It is enough to give the graphs corresponding to the indecomposable self-dual codes (see Lemma 3.2.4).

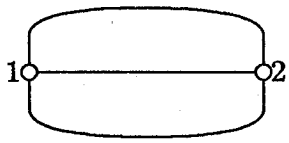

Figure 6. C_2

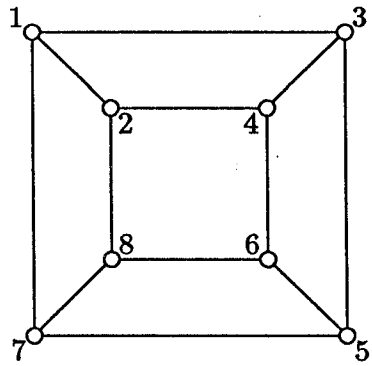

Figure 7. A_8

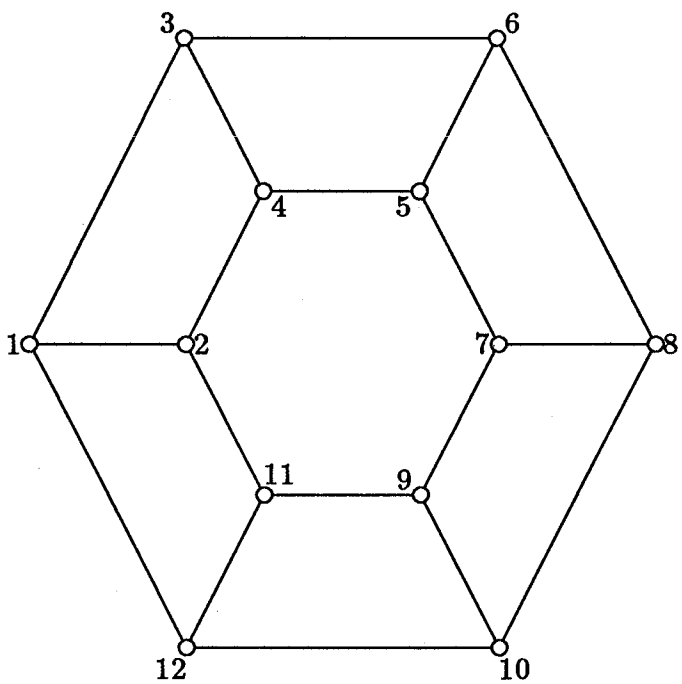

Figure 8. B_{12}

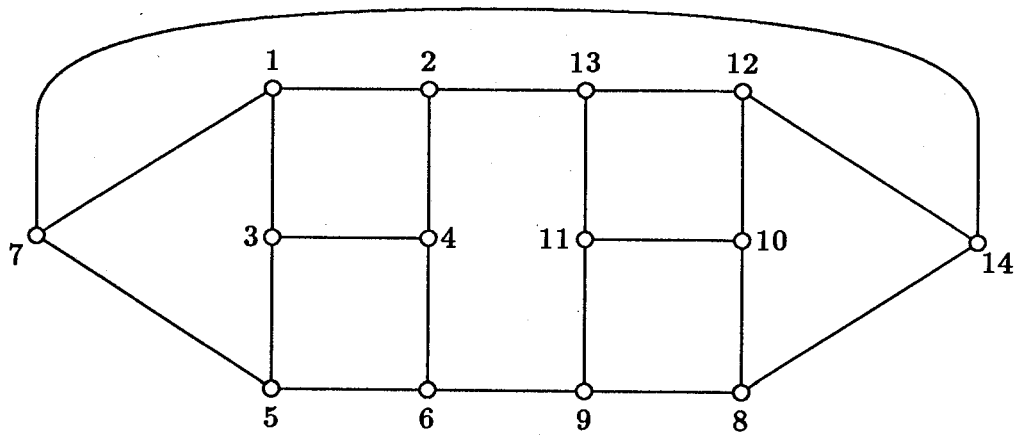

Figure 9. D_{14}

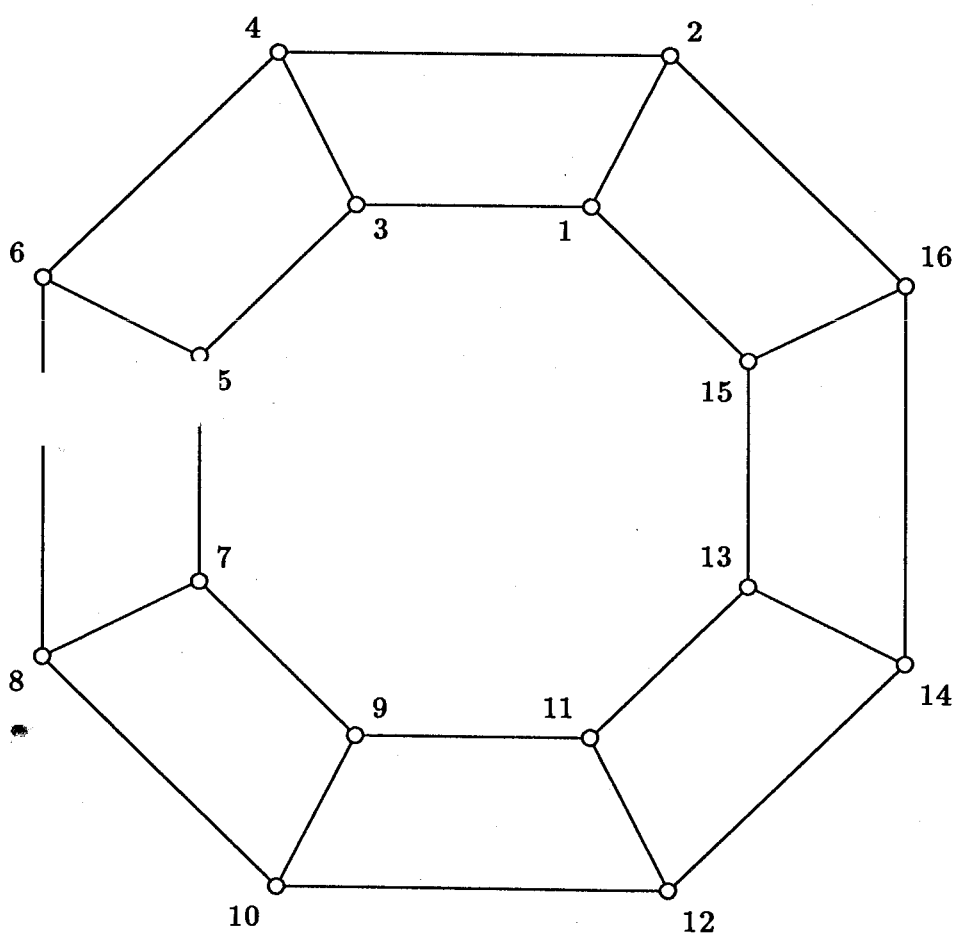

Figure 10. E_{16}

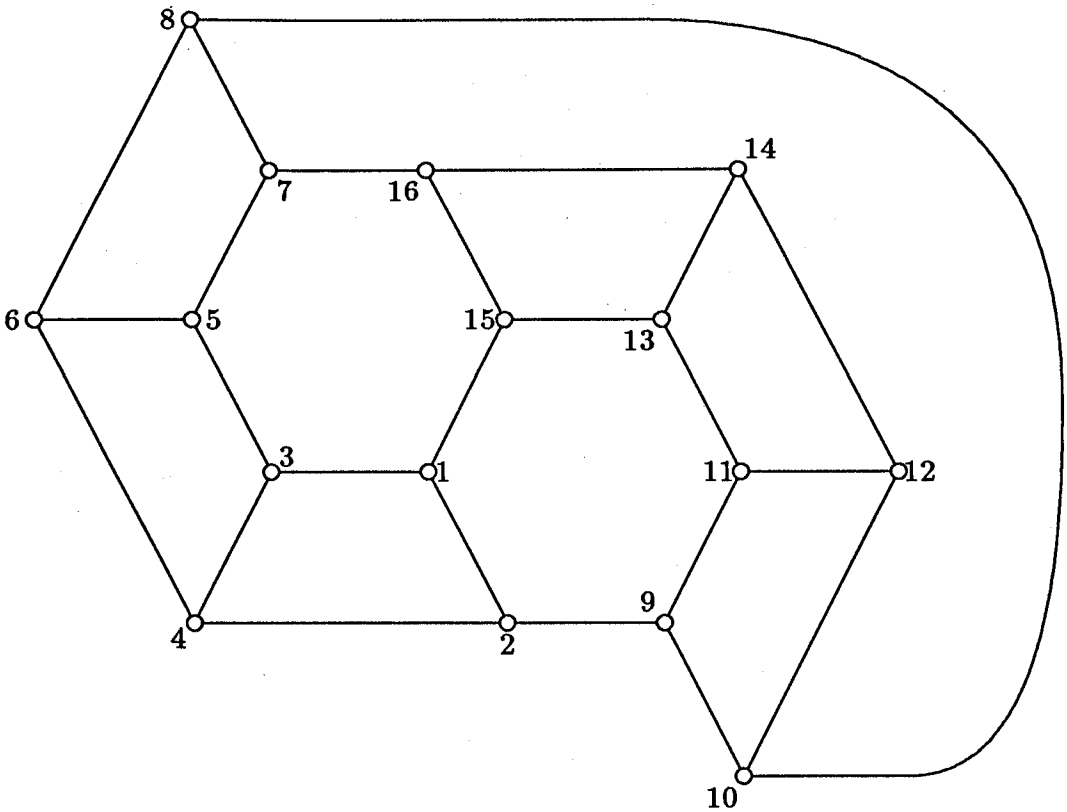

Figure 11. F_{16}

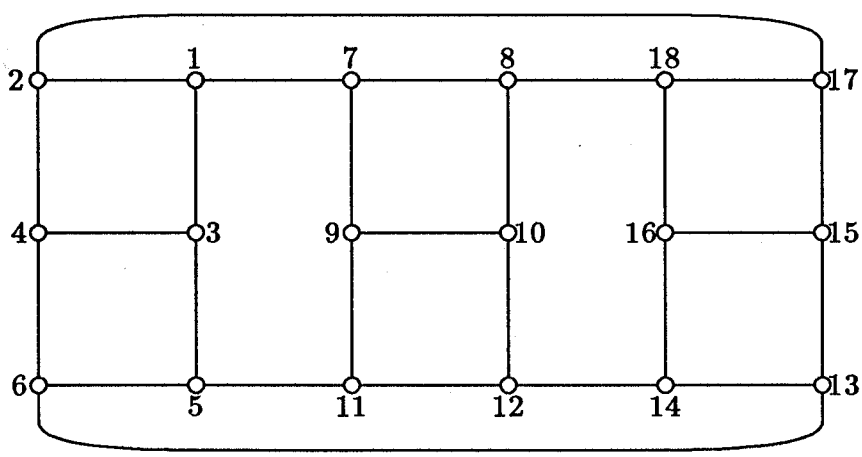

Figure 12. H_{18}

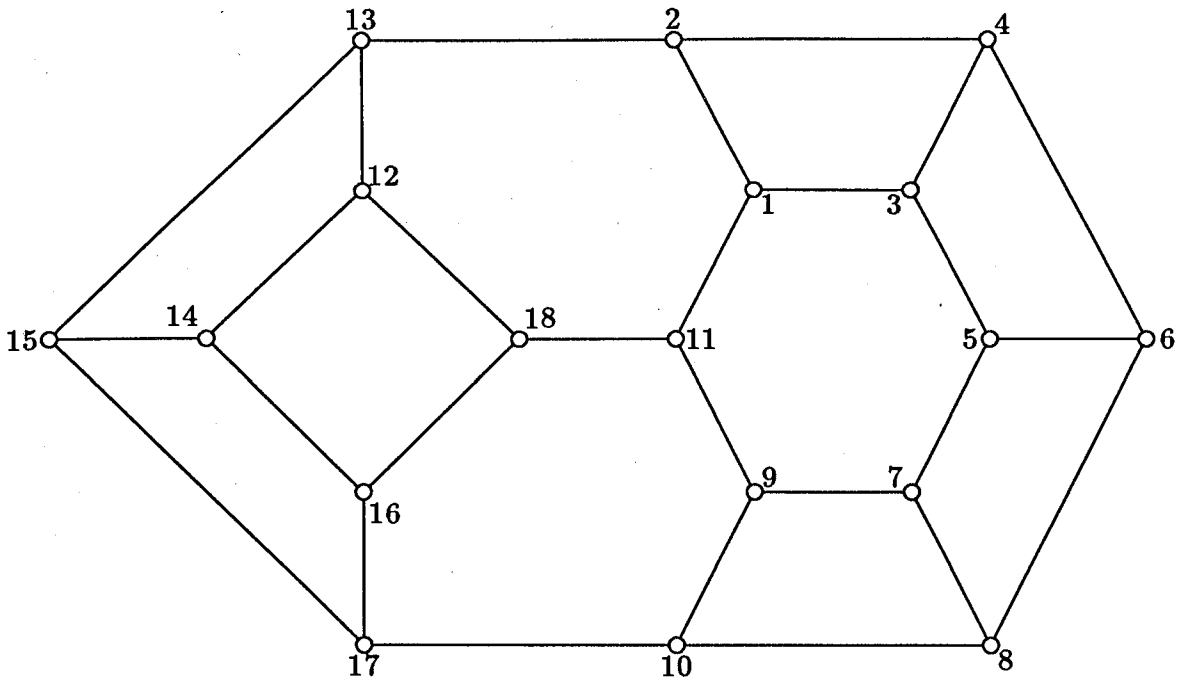

Figure 13. I_{18}

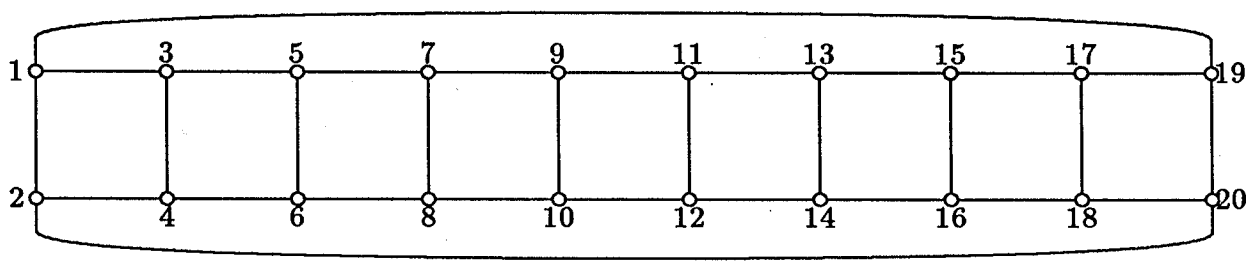

Figure 14. J_{20}

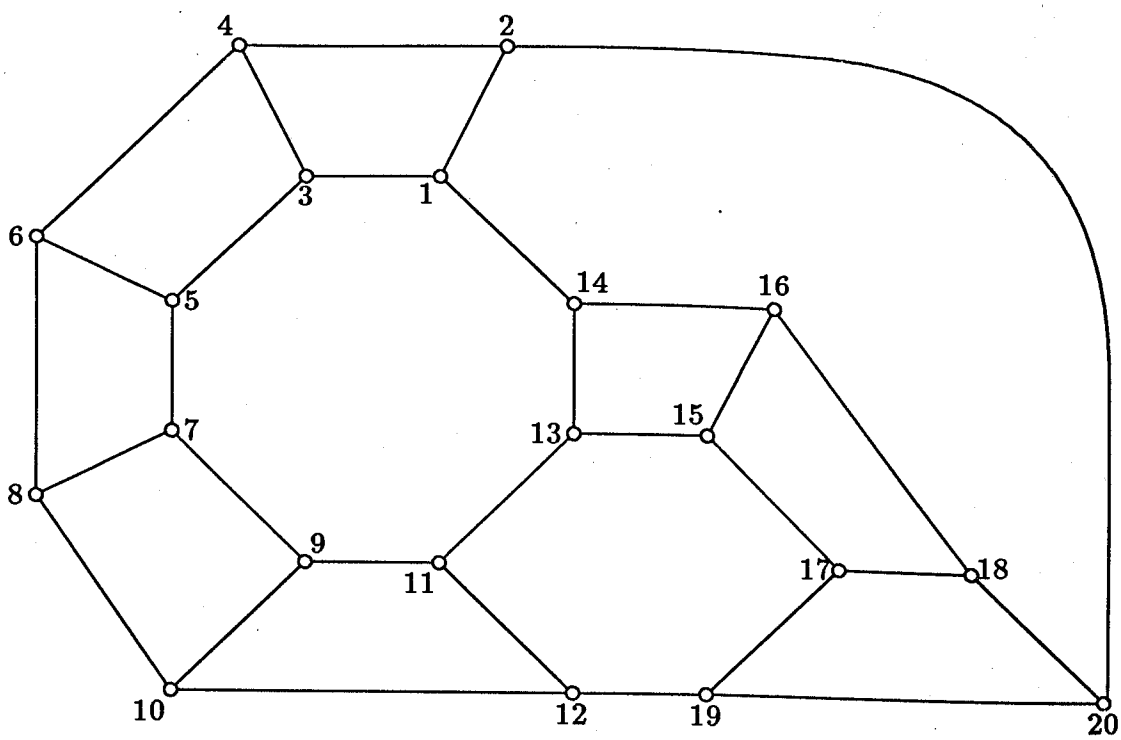

Figure 15. K_{20}

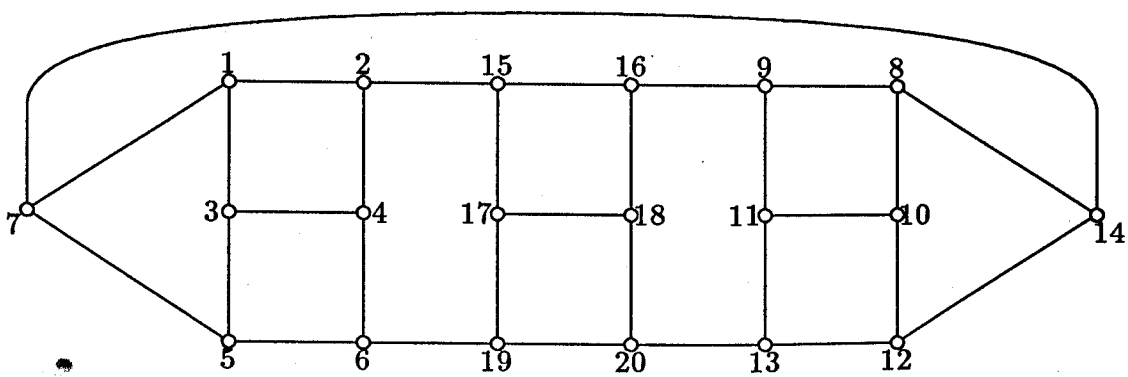

Figure 16. L_{20}

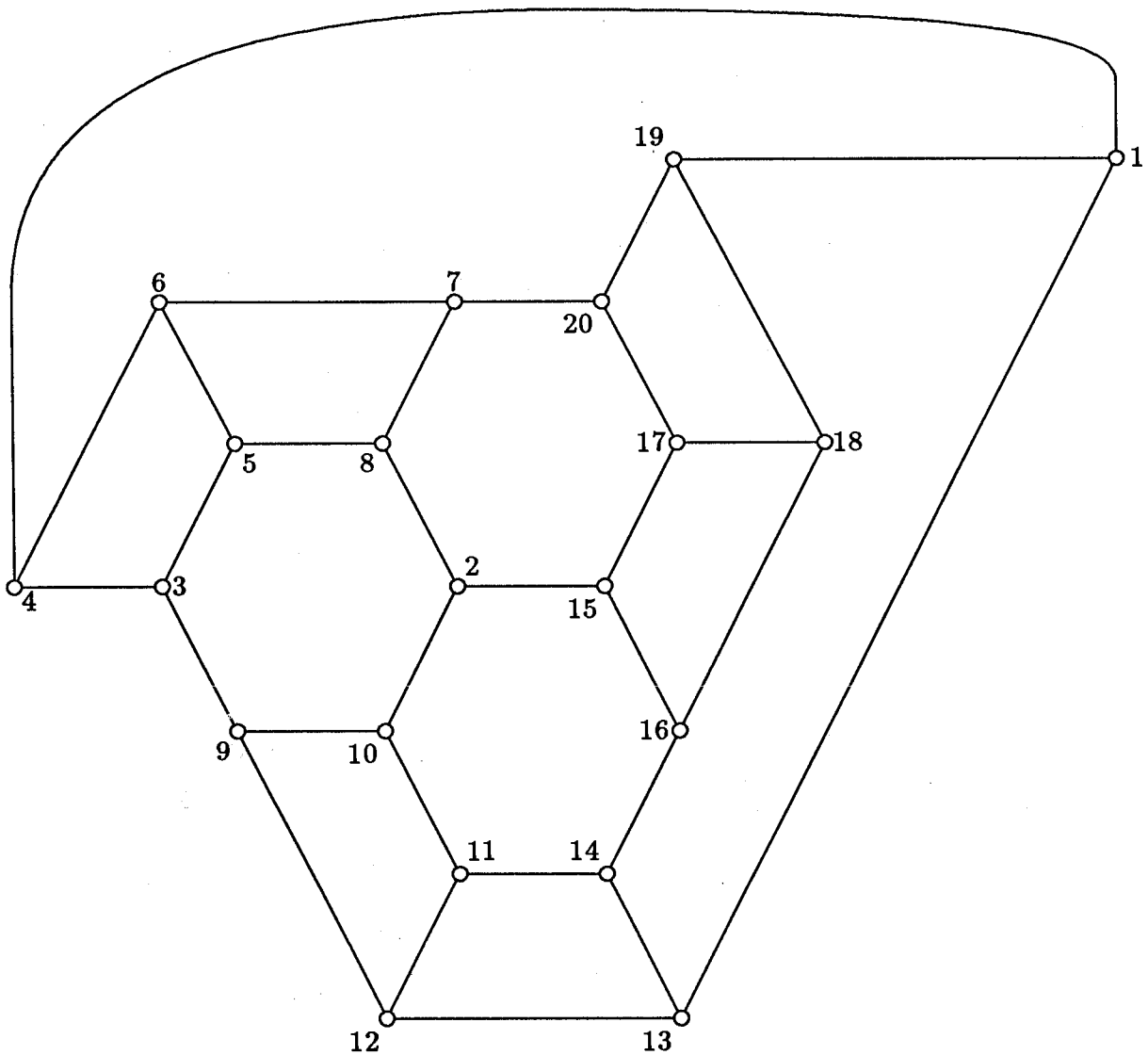

Figure 17. R_{20}

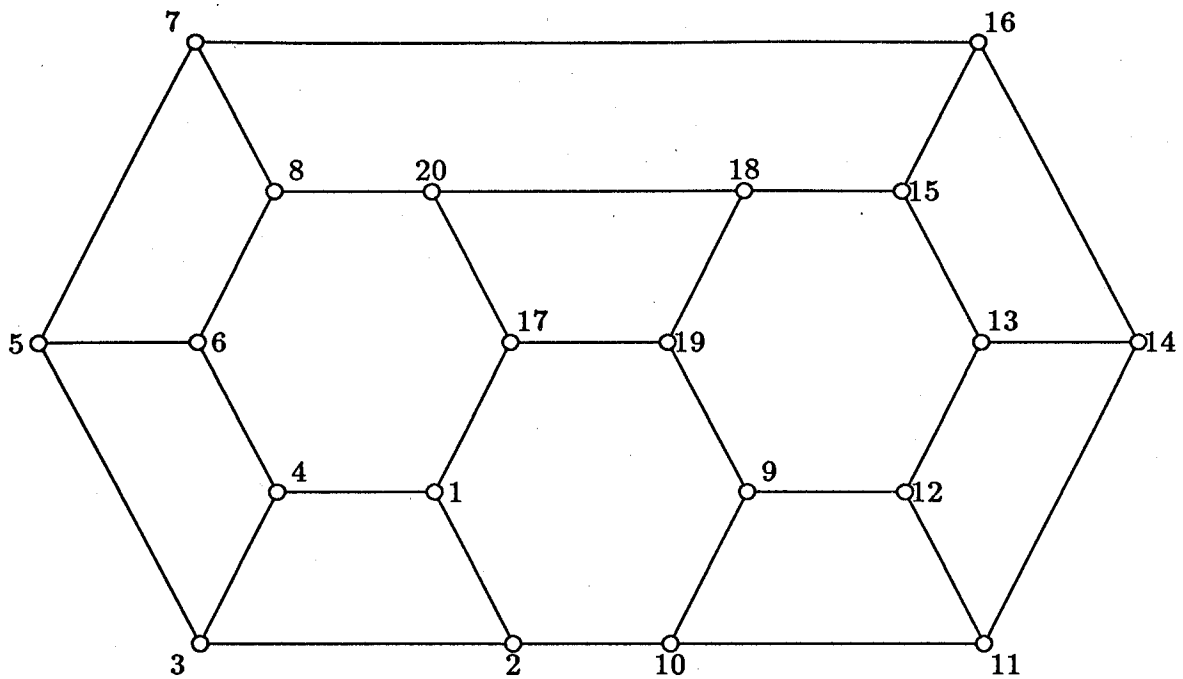

Figure 18. S_{20}

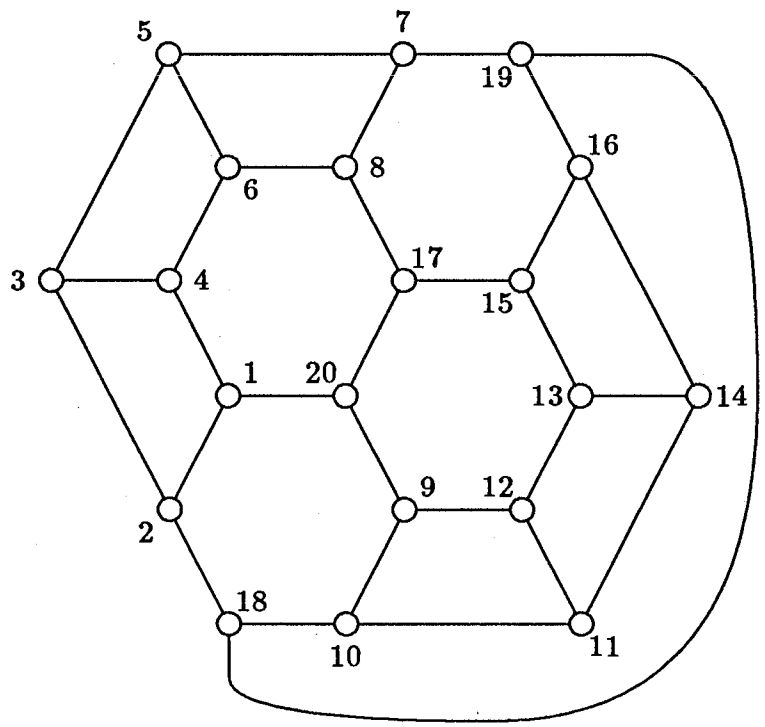

Figure 19. S'

BIBLIOGRAPHY

[1] R. P. Anstee, M. Hall, Jr., and J. G. Thompson, Planes of order 10 do not have a collineation of order 5, *J. Combin. Theory A*, **29** (1980), 39–58.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[3] E. F. Assmus, Jr., J. A. Mezzaroba, and C. J. Salwach, Planes and biplanes, *Proceedings of the 1976 Berlin Combinatorics Conference*, Vance-Reidle (1977), 205–212.

[4] J. A. Bondy, U. S. R. Murty, *Graph Theory with Applications*, North-Holland, Amsterdam, 1976.

[5] J. H. Conway, V. Pless, On the enumeration of self-dual codes, *J. Combin. Theory A*, **28** (1980), 26–53.

[6] J. H. Conway, V. Pless, On primes dividing the group order of a doubly even $(72, 36, 16)$ code and and the group of a quaternary $(24, 12, 10)$ code, *Discrete Math.*, **38** (1982), 143–156.

[7] G. B. Faulkner, *Recursive generation of cyclically k-connected cubic planar graphs*, Ph. D. thesis, Univ. of Waterloo, (Aug. 1971).

[8] H. Fleischner, W. Imrich, Transitive planar graphs, *Mathematica Slovaca*, **29** (1979), 97–105.

[9] A. M. Gleason, Weight polynomials of self-dual codes and the Mac- Williams identities, *Actes Congres Internl. de Mathematique*, **3** 1970 Gauthier - Villars, Paris, (1971), 211–215.

[10] B. Grünbaum, *Convex Polytopes*, Wiley, New York, 1967.

[11] S. L. Hakimi, E. F. Schmeichel, A Note on the Vertex Arboricity of a Graph,

SIAM J. Disc. Math., **2** (1989), 64–67.

[12] D. A. Holton, B. Manvel, and B. D. McKay, Hamiltonian Cycles in Cubic 3-Connected Bipartite Planar Graphs, *J. Combin. Theory B*, **38** (1985), 279–297.

[13] W. C. Huffman, Automorphism of codes with applications to extremal doubly-even codes of length 48, *IEEE Trans. Inform. Theory.*, **IT-28** (1982), 511–521.

[14] W. C. Huffman, V. Y. Yorgov, A $(72, 36, 16)$ doubly even code does not have an automorphism of order 11, *IEEE Trans. Inform. Theory.*, **IT-33** (1987), 749–752.

[15] Q. M. Husain, On the totality of the solutions for the symmetrical incomplete block designs: $\lambda = 2$, $k = 5$ or 6, *Sankhya*, **7** (1945-46), 204–208.

[16] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.*, **42** (1963), 79–94.

[17] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[18] F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson, Good self-dual codes exist, *Discrete Math.*, **3** (1972), 153–162.

[19] H. Okamura, Every simple 3-polytope of order 32 or less is Hamiltonian, *J. Graph. Theory* , **6** (1982), 185–196.

[20] M. Ozeki, Hadamard matrices and doubly even self-dual error correcting codes, *J. Combin. Theory A*, **44** (1987), 274–287.

[21] V. Pless, A classification of self-dual codes over $GF(2)$, *Discrete Math.*, **3** (1972), 209–246.

[22] V. Pless, 23 does not divide the order of the group of a $(72, 36, 16)$ doubly even code, *IEEE Trans. Inform. Theory.*, **IT-28** (1982), 113–117.

[23] V. Pless, N. J. A. Sloane, On the classification and enumeration of self-dual codes, *J. Combin. Theory A*, **18** (1975), 313–335.

[24] V. Pless, J. G. Thompson, 17 does not divide the order of the group of a $(72, 36, 16)$ doubly even code, *IEEE Trans. Inform. Theory.*, **IT-28** (1982), 537–541.

[25] W. T. Tutte (Ed.), *Recent Progess in Combinatorics*, Academic Press, New York, (1969).

[26] W. T. Tutte, On Hamilton circuits, *J. London Math. Soc.*, **21** (1946), 98–101.

[27] W. T. Tutte, A theorem on planar graphs, *Trans. Amer. Math. Soc.*, **82** (1956), 99–116.

[28] V. V. Yorgov, Binary self-dual codes with automorphism of odd order, *Probl. Inform. Transmission.*, **XIX** (1983), 11–24.

[29] V. V. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Inform. Theory.*, **IT-33** (1987), 77–82.

[30] R. J. Wilson, *Introduction to Graph Theory*, Longman, Hong Kong 1972.