

University of South Wales



2059568

AN INVESTIGATION OF RELATIONSHIPS  
BETWEEN GRAPH THEORY AND CODING THEORY

Peter Hammond

A thesis submitted for the degree of Doctor of Philosophy

October 1975

Department of Mathematics  
and Computer Science,  
Glamorgan Polytechnic.

## Abstract

The problem of the existence of perfect and nearly perfect codes over finite alphabets is generalised in two directions. This thesis is concerned with the existence and combinatorial properties of completely regular codes in distance-regular graphs. One of the main tools is the generalisation of Lloyd's Theorem.

There are connections with designs, orthogonal latin squares and finite projective planes and various existence and non-existence results are derived for completely regular codes in three infinite families of distance-regular graphs.

## Acknowledgements

I should like to express my sincere thanks to Derek Smith for his advice and guidance during the period this research was undertaken. I appreciate the generous amount of time he has given to discussion of the work, and subsequently his help in the preparation of the thesis.

I am also indebted to Norman Biggs for his encouragement and interest throughout and for stimulating discussion of coding and graph theory.

Finally I should also like to thank Barbara Miles for her efficient and accurate typing of the manuscript.

## CONTENTS

1.	INTRODUCTION	
1.1	Perfect code problem	1
1.2	Codes in other settings	2
1.3	Summary	2
2.	PERFECT AND NEARLY PERFECT CODES	
2.1	Distance-regular graphs	9
2.2	e-codes in distance-regular graphs	12
2.3	Nearly perfect and perfect codes	15
2.4	The weight vector of a nearly perfect code	22
2.5	Constructing perfect codes from nearly perfect codes	25
3.	COMPLETELY REGULAR CODES	
3.1	Definitions	29
3.2	An analogue of Lloyd's theorem for completely regular codes	30
3.3	Antipodal distance-regular graphs	34
3.4	Locally regular e-codes of external distance e	38
3.5	Locally regular e-codes of external distance e+1	39
3.6	Generalised uniformly packed codes	41
4.	CODES IN THE GRAPHS $\Gamma(m,q)$	
4.1	Introduction	42
4.2	The eigenvector sequence for $\Gamma(m,q)$	42
4.3	Nearly perfect codes in $\Gamma(m,q)$	44
4.4	Completely regular codes in $\Gamma(m,q)$	50

5.	CODES IN THE GRAPHS $O_k$	
5.1	Definitions of the graphs and eigenvalues	56
5.2	Construction of codes in $O_k$	57
5.3	The eigenvector sequence for $O_k$	59
5.4	Perfect codes in $O_k$	63
5.5	Nearly perfect codes in $O_k$	74
6.	CODES IN THE GRAPHS $J(a,b)$	
6.1	Introduction	77
6.2	Eigenvalues of $J(a,b)$	77
6.3	Nearly perfect 1-codes in $J(a,b)$	80
6.4	Completely regular codes and designs	81
6.5	$J(2b,b)$	84
6.6	Equidistant codes and finite projective planes	86

## 1. Introduction

### 1.1 Perfect code problem

Coding theory began as a study of the possibilities of correcting errors in certain communications systems (Shannon [33]). Much of the research in this field is still concerned with the theoretical study and construction of such codes (Sloane [34]).

The algebraic and combinatorial properties of codes have undergone closer scrutiny more recently and an area of coding theory which has provoked particular interest has been the investigation of the existence of perfect codes. From a combinatorial point of view perfect codes are interesting because of the connection with the existence of certain designs ([27]).

The perfect code problem for finite field alphabets was finally resolved in 1973 when Tietäväinen [38] proved that the only non-trivial perfect codes are those already known. There are many known examples of perfect 1-codes (including the Hamming perfect 1-codes); there is the ternary Golay perfect 2-code of length 11 and the binary Golay perfect 3-code of length 23 (van Lint [27]).

A result which has proved useful in many of the non-existence results for perfect codes is Lloyd's theorem [28]. The theorem states that if a perfect  $e$ -code of length  $m$  over a  $q$ -ary alphabet exists then the polynomial (usually referred to as the Lloyd polynomial)

$$\psi_e(x) = \sum_{i=0}^e (-1)^i \binom{m-x}{e-i} \binom{x-1}{i} (q-1)^{e-i} \quad (1.1.1)$$

has  $e$  distinct zeros in the set  $\{1, 2, \dots, m\}$ .

## 1.2 Codes in other settings

Biggs in [5] and Delsarte in [9] generalised the idea of a perfect code to distance-transitive graphs and to metric association schemes respectively, and both authors have proved an analogous result to Lloyd's theorem. Delsarte paid particular attention to the Hamming schemes which correspond to the original setting and also to the Johnson schemes. Both Biggs [6] and Delsarte have also established connections between codes in the Johnson schemes (or correspondingly the graphs  $J(a,b)$ ) and the existence of certain Steiner systems.

In [14] Goethals and Snover defined the class of nearly perfect codes over a binary field and showed that they have similar properties to perfect codes which include an analogue of Lloyd's theorem and the construction of designs.

The aim of this thesis is to generalise the problem in two directions. Firstly we wish to change the setting to distance-regular graphs (a class of graphs which contains the class of distance-transitive graphs). Secondly we define a general class of codes (which contains perfect and nearly perfect codes) called completely-regular codes.

## 1.3 Summary

In Chapter 2 we begin with a description of the main properties of a distance-regular graph  $\Gamma$  with diameter  $d$  and valency  $k$ . We define the adjacency algebra  $\mathcal{A}(\Gamma)$  of dimension  $d+1$  in terms of the adjacency matrix  $A$  of  $\Gamma$ . The adjacency matrices  $A_0 = I, A_1 = A, \dots, A_d$  form a basis for  $\mathcal{A}(\Gamma)$ . If we represent  $\mathcal{A}(\Gamma)$  as an algebra of  $(d+1) \times (d+1)$  matrices representing left multiplication we generate an algebra  $\hat{\mathcal{A}}(\Gamma)$  which is isomorphic to  $\mathcal{A}(\Gamma)$ .  $\hat{\mathcal{A}}(\Gamma)$  has as a basis the intersection matrices  $B_0 = I, B_1, \dots, B_d$ ; the intersection matrix  $B = B_1$

is tri-diagonal and its main diagonals form the intersection array of  $\Gamma$ .

We define the eigenvector sequence of polynomials  $v_0(\lambda), v_1(\lambda), \dots, v_d(\lambda)$  in terms of the intersection array and the partial sum  $v_0(\lambda) + v_1(\lambda) + \dots + v_i(\lambda)$  is denoted by  $x_i(\lambda)$ . The polynomial  $x_d(\lambda)$  is a rational multiple of the characteristic polynomial of  $B$  and has zeros  $\lambda_1, \dots, \lambda_d$  where  $k, \lambda_1, \dots, \lambda_d$  are the distinct eigenvalues of  $B$  (or of  $\Gamma$  as we shall sometimes write).

In §2.2 we define an e-code  $C$  as a subset of the vertex set  $V\Gamma$  of  $\Gamma$  with mutual minimum distance  $2e+1$ . We also define the weight vector  $[p_{0i}(C, u), p_{1i}(C, u), \dots, p_{di}(C, u)]^t$  of  $C$  with respect to the vertex  $u$  at minimum distance  $i$  from the elements of  $C$ . These definitions are followed by a generalisation of an upper bound for  $|C|$  obtained by Goethals and Snover [14] who used their bound to define nearly perfect binary codes. In §2.3 we define a nearly perfect code in  $\Gamma$  as a code satisfying our generalised bound with equality.

A perfect e-code is also defined in §2.3 and we note that the class of perfect codes is a subclass of the class of nearly perfect codes. The remainder of §2.3 is devoted to a comparison of the properties of perfect codes and nearly perfect codes which are not perfect. We follow the method of Biggs [5] to obtain a result analogous to Lloyd's theorem for nearly perfect codes and obtain the generalisation of Goethals and Snover as a corollary.

In §2.4 we confine our attention to a more detailed study of the weight vector of a nearly perfect code  $C$  and we obtain explicit expressions connecting the related weight vectors of  $C$ . We prove that the weight vectors of a nearly perfect code are independent of the vertex with respect to which they are calculated. We also state

corresponding results for perfect codes.

We end Chapter 2 by considering the possibility of constructing perfect codes from nearly perfect codes. We find that it is possible, under certain circumstances, to construct perfect 1-codes from nearly perfect 2-codes. This particular construction is shown not to hold for other values of  $e$ .

An important consequence of Chapter 2 is that vertices of the graph are at distance at most  $e$  (respectively  $e+1$ ) from code vertices of a perfect (respectively nearly perfect)  $e$ -code. In Chapter 3 we examine  $e$ -codes which have the property that vertices of the graph are at distance at most  $e+m$  from vertices of the code, that is, codes which have external distance  $e+m$ . We pose two important questions which are the essential problems of this thesis:

- (i) If  $C$  is an  $e$ -code with external distance  $e+m$ , what conditions must  $C$  satisfy in order that we can prove a result which is analogous to Lloyd's theorem?
- (ii) What properties would a code satisfying such conditions have in common with nearly perfect codes?

In §3.1 we begin to answer the first of these conditions by defining locally regular and completely regular codes in terms of components of the related weight vectors. We also indicate the difference between Delsarte's and our definition of external distance.

We show in §3.2 that very little extra work is needed in order to establish an analogue of Lloyd's theorem for completely regular codes. This generalised condition (usually referred to as the polynomial condition) establishes that the zeros of a certain polynomial are eigenvalues of the graph. These results also enable us to prove

the equivalence of completely regular and locally regular codes. The last theorem of §3.2 is a generalisation of a result due to O. Heden[21].

We introduce, in §3.3, the idea and some of the properties of antipodal distance-regular graphs and we illustrate how we can derive another distance-regular graph from such a graph. The aim of this section is to show that under certain circumstances the derived graph also contains a completely regular code which is constructed from the code in the antipodal graph. In fact when this is the case we apply our polynomial condition to the derived graph and obtain an improved polynomial condition.

In §3.4 and §3.5 we discuss briefly locally regular e-codes of external distance  $e$  and  $e+1$  respectively. In particular in §3.5 we determine the extra parameter which arises in the improved polynomial condition for antipodal graphs. We find an explicit form for this parameter for the classes of nearly perfect and uniformly packed codes. Finally in §3.6 we define  $m^{\text{th}}$  order generalised uniformly packed codes [52]. Although these codes are not necessarily completely regular we are still able to prove an analogue of Lloyd's theorem.

The remaining three chapters are devoted to examples and non-existence results of locally regular e-codes. The setting for each chapter is one of three infinite families of distance-regular graphs.

In Chapter 4 we restrict our attention to the graph  $\Gamma(m, q)$  which corresponds to the Hamming schemes of Delsarte. §4.1 contains a short account of recent work on the existence of perfect codes in  $\Gamma(m, q)$  for  $q$  a non-prime power.

We begin §4.2 with a statement of the intersection array of  $\Gamma(m, q)$ . The graph  $\Gamma(m, 2)$  is antipodal and with a view to applying our improved polynomial condition we state the eigenvalues of the derived graph  $\Gamma(m, 2)/2$ .

The existence of nearly perfect codes is investigated in §4.3. We consider first the binary case and obtain a non-existence result for odd  $e$  with  $5 \leq e \leq 17$  (the case  $e=3$  has been dealt with by van Lint [26]). Although this result should easily extend to further odd values of  $e$  it is obviously overshadowed by the complete non-existence result recently proved by K. Lindstrom [23]. However, Lindstrom's proof is very complicated [41, page 14] and involves a computer search for the values  $e \leq 100$  and  $m \leq 10,000$  so it might be useful to illustrate another approach.

Also in §4.3 we prove that the only nearly perfect 1-codes and 2-codes in  $\Gamma(m, q)$  are the binary codes already obtained by Goethals and Snover [14]. Binary nearly perfect 1-codes (other than perfect 1-codes) are obtained by dropping the same component from each of the code vertices of a perfect 1-code [14, page 83]. Preparata 2-codes [30] are examples of nearly perfect 2-codes which are not perfect.

Finally in §4.4 we give two examples of parameter sets for completely regular 1-codes in  $\Gamma(m, q)$ . The first and most interesting is connected closely with mutually orthogonal latin squares. The second is still an open case but we discuss a possible method of construction using a result of Goethals and van Tilborg [15].

The existence of interesting codes in the infinite family of  $O_k$  graphs is demonstrated in Chapter 5. §5.2 includes a description of a method of constructing codes in  $O_k$  from antipodal codes in  $\Gamma(2k-1, 2)$ . We illustrate how the perfect 1-code in  $O_4$  can be obtained from the perfect Hamming 1-code in  $\Gamma(7, 2)$ .

In §5.3 we use the eigenvector sequence for  $O_k$  to obtain results connecting the roots of  $x_e(\lambda)$ . Expressions of the sum and products of the roots of these and related polynomials have been used

successfully in non-existence proofs for both perfect and nearly perfect codes in  $\Gamma(m, q)$  ([33] and [25]).

In §5.4 we obtain a lower bound on  $k$  as a necessary condition for the existence of a perfect  $e$ -code in  $O_k$ . The most interesting result of §5.4 is the characterisation of perfect 1-codes in  $O_k$  as the Steiner systems  $S(2k-1, k-1, k-2)$ . The first two codes in this series are in  $O_4$  and  $O_6$  and correspond to the well known Steiner systems  $S(7, 3, 2)$  and  $S(11, 5, 4)$  respectively. It does not seem likely that other perfect 1-codes exist in  $O_k$  because we would require the existence of  $t$ -designs with  $t$  greater than 5. However we do prove that the components of the weight enumerator for these codes are integers so we have yet to rule out the possibility of perfect 1-codes in  $O_k$ . For the rest of §5.4 we use the weight enumerator and sphere packing condition to obtain lower bounds on  $k$  as necessary conditions for the existence of perfect  $e$ -codes in  $O_k$  with  $e=2, 3$  and 4.

We follow the method of proof of Theorem 4.3.4 to prove in §5.5 that there are no nearly perfect  $e$ -codes in  $O_k$  with  $e$  odd and  $3 \leq e \leq 14$ . Once again this result should easily be extended to further odd values of  $e$ . For the particular case  $e=2$  we are able to apply Theorem 2.5.1 and from the existence of a nearly perfect 2-code in  $O_6$  we obtain the perfect 1-code in  $O_6$ .

The final chapter deals with the family of distance-regular graphs  $J(a, b)$  which correspond to the Johnson schemes of Delsarte [9]. In §6.2 we state the intersection array and calculate the eigenvalues of  $J(a, b)$ . We show also how the eigenvector sequence of  $J(a, b)$  is related to the Eberlein polynomials [37].

The only complete non-existence result we have obtained is for nearly perfect 1-codes in  $J(a,b)$  and this is contained in §6.3.

In §6.4 we derive a number of interesting results connecting the existence of completely regular codes in  $J(a,b)$  and certain Steiner systems.

The graph  $J(2b,b)$  is the setting for §6.5. Since the graph is antipodal we have the possibility of applying the results of §3.3. The interpretation of the results of §6.4 in the case of  $J(2b,b)$  is particularly interesting. A great deal of research has already been carried out on the related Steiner systems; in particular by Alltop[1], Hermoso and Assmus [3].

The final section of Chapter 6 illustrates the relationship between equidistant codes in  $J(a,b)$  and finite projective planes.

## 2. Perfect and Nearly Perfect Codes

We begin with a brief description of the main properties of distance-regular graphs. The reader should refer to Biggs[7] for further details and proofs.

### 2.1 Distance-regular graphs

A distance-regular graph, with distance function  $\partial$ , diameter  $d$  and vertex set  $V\Gamma$  is a simple regular connected graph  $\Gamma$  of valency  $k$  with the following property. If  $z \in V\Gamma$  and  $\Gamma_i(z) = \{u \in V\Gamma \mid \partial(u, z) = i\}$  then there are natural numbers  $b_0 = k, b_1, \dots, b_{d-1}, a_1, \dots, a_d, c_2, \dots, c_d$  such that for each pair  $(u, v)$  of vertices satisfying  $\partial(u, v) = j$  we have

- (i) The number of vertices of  $\Gamma_{j-1}(v)$  adjacent to  $u$  is  $c_j$  ( $0 < j \leq d$ ).
- (ii) The number of vertices of  $\Gamma_j(v)$  adjacent to  $u$  is  $a_j$  ( $0 < j \leq d$ ).
- (iii) The number of vertices of  $\Gamma_{j+1}(v)$  adjacent to  $u$  is  $b_j$  ( $0 \leq j < d$ ).

We infer from (i), (ii), (iii) that  $k = a_i + b_i + c_i$  ( $0 \leq i < d$ ) and  $c_d + a_d = k$  with  $a_0 = 0$  and  $c_1 = 1$ .

Let  $n = |V\Gamma|$ . We define  $d+1$  matrices  $A_0, A_1, \dots, A_d$  each having  $n$  rows and columns indexed by the vertices of  $\Gamma$  as follows:

$$(A_h)_{uv} = \begin{cases} 1 & \text{if } \partial(u, v) = h; \\ 0 & \text{otherwise.} \end{cases} \quad (2.1.1)$$

Then  $A_0 = I$  and  $A_1 = A$  is the usual adjacency matrix of  $\Gamma$ .

The commutative adjacency algebra,  $\mathcal{A}(\Gamma)$ , is the algebra of polynomials in  $A$  (over  $\mathbb{C}$ ); in [7, Theorem 20.7] it is shown that  $\mathcal{A}(\Gamma)$  has dimension  $d+1$  and possesses a basis  $\{A_0, A_1, \dots, A_d\}$ . The multiplication of basis elements is given by

$$A_h A_i = \sum_{j=0}^d s_{hij} A_j \quad (h, i \in \{0, 1, \dots, d\}) \quad (2.1.2)$$

where the numbers  $s_{hij}$  are called the intersection numbers of  $\Gamma$ ; these numbers have the following combinatorial interpretation: for  $\partial(u, v) = j$

$$s_{hij} = |\{w \in V\Gamma \mid \partial(u, w) = h \text{ and } \partial(w, v) = i\}| \quad (2.1.3)$$

Since  $\mathcal{A}(\Gamma)$  has dimension  $d+1$  it can be represented as an algebra of  $(d+1) \times (d+1)$  matrices. This representation assigns to each  $X$  in  $\mathcal{A}(\Gamma)$  the  $(d+1) \times (d+1)$  matrix  $\hat{X}$ , which represents left multiplication by  $X$  in  $\mathcal{A}(\Gamma)$  with respect to the basis  $\{A_0, A_1, \dots, A_d\}$ . The matrix  $B_h = \hat{A}_h$  has entries  $(B_h)_{ij} = s_{hij}$  and the matrices  $\hat{X}$ , for each  $X$  in  $\mathcal{A}(\Gamma)$ , form an algebra  $\hat{\mathcal{A}}(\Gamma)$ .  $\hat{\mathcal{A}}(\Gamma)$  is isomorphic to  $\mathcal{A}(\Gamma)$  and has a basis  $\{B_0, B_1, \dots, B_d\}$  [7, Proposition 21.1].

In particular we see from the triangle inequality that the intersection numbers  $s_{lij}$  are non-zero only when  $|i-j| \leq 1$  and hence  $B = B_1$  is tri-diagonal; the diagonals of  $B$  are the rows of the intersection array of  $\Gamma$

$$\left\{ \begin{array}{cccccc} * & 1 & c_2 & \cdots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \cdots & a_{d-1} & a_d \\ k & b_1 & b_2 & \cdots & b_{d-1} & * \end{array} \right\}$$

and  $B$  is called the intersection matrix of  $\Gamma$ .

From (2.1.2) we infer that for  $1 \leq i \leq d-1$

$$AA_i = c_{i+1}A_{i+1} + a_iA_i + b_{i-1}A_{i-1} \quad (2.1.4)$$

and by the isomorphism between  $\mathcal{A}(\Gamma)$  and  $\hat{\mathcal{A}}(\Gamma)$

$$BB_i = c_{i+1}B_{i+1} + a_iB_i + b_{i-1}B_{i-1} \quad (2.1.5)$$

Let  $\mathbb{Q}[\lambda]$  denote the ring of polynomials in  $\lambda$  with rational coefficients, and let  $v_0(\lambda), v_1(\lambda), \dots, v_d(\lambda)$  be elements of  $\mathbb{Q}[\lambda]$  defined as follows:

$$\begin{aligned} v_0(\lambda) &= 1, & v_1(\lambda) &= \lambda & \text{and for } 1 \leq i < d \\ \lambda v_i(\lambda) &= c_{i+1}v_{i+1}(\lambda) + a_iv_i(\lambda) + b_{i-1}v_{i-1}(\lambda) \end{aligned} \quad (2.1.6)$$

For  $i \in \{0, 1, \dots, d\}$   $v_i(\lambda)$  is a polynomial of degree  $i$  in  $\lambda$  and from (2.1.4), (2.1.5) and (2.1.6) we have

$$v_i(B) = B_i, \quad v_i(A) = A_i, \quad v_i(k) = k_i \quad (2.1.7)$$

where  $k_i = |\Gamma_i(u)|$ . We note also that (2.1.6) arises when we consider the eigenvector equation for  $\underline{v}(\lambda) = [v_0(\lambda), v_1(\lambda), \dots, v_d(\lambda)]^t$

$$B\underline{v}(\lambda) = \lambda\underline{v}(\lambda) \quad (2.1.8)$$

For this reason  $\{v_i(\lambda)\}$  is called the eigenvector sequence of  $\Gamma[5]$ .

Using the eigenvector sequence we are able to find each  $v_i(\lambda)$  from  $B$  and then define for  $0 \leq i \leq d$

$$x_i(\lambda) = \sum_{j=0}^i v_j(\lambda) \quad (2.1.9)$$

In [5, page 294] it is shown that  $(\lambda - k)x_d(\lambda)$  is a rational multiple of the characteristic polynomial of  $B$  and that  $B$  has distinct eigenvalues. Hence  $x_d(\lambda)$  has zeros  $\lambda_1, \lambda_2, \dots, \lambda_d$  where  $k, \lambda_1, \dots, \lambda_d$  are the distinct eigenvalues of  $B$ .

## 2.2 e-codes in distance-regular graphs

Definitions Let  $\Gamma$  be a distance-regular graph with distance function

$\partial$ . For each non-negative integer  $e$  an e-code in  $\Gamma$  is a subset  $C$  of  $V\Gamma$  such that  $\partial(u,v) \geq 2e + 1$  for each pair  $u,v$  of distinct elements of  $C$ .

If  $v \in V\Gamma$  then we define

$$\Sigma_e(v) = \{w \in V\Gamma \mid \partial(v,w) \leq e\} \quad (2.2.1)$$

and if  $\partial(v,C) = \min_{c \in C} \{\partial(v,c)\} = i$  then for  $0 \leq h \leq d$

$$p_{hi}(C,v) = |C \cap \Gamma_h(v)| \quad (2.2.2)$$

We call the vector  $[p_{0i}(C,v), p_{1i}(C,v), \dots, p_{di}(C,v)]^t$  the weight vector of  $C$  with respect to  $v$ .

In what follows we prove a generalisation (Theorem 2.2.5) of an upper bound obtained by Goethals and Snover [14] who used their bound to define binary nearly perfect codes. In fact their bound is a special case of a result of Johnson [22].

Lemma 2.2.1 If  $\Gamma$  contains an e-code  $C$  then

$$\sum_{h=0}^e p_{hi}(C,v) \leq 1 \quad \text{for each } v \in V\Gamma \text{ with } \partial(v,C) = i \quad (2.2.3)$$

Proof This is immediate from the definition of minimum distance ■

Lemma 2.2.2 If  $C \cap \Gamma_i(v) \neq \emptyset$  for some  $i$  with  $0 \leq i \leq e$  then

$$\sum_{h=0}^e p_{hi}(C,v) = 1 \text{ and } c_{e+1} p_{e+1i}(C,v) \leq b_e p_{ei}(C,v) \quad (2.2.4)$$

for each  $v \in V\Gamma$ .

Proof The first part is obvious from Lemma 2.2.1. The second part is obvious if  $p_{ei}(C,v) = 0$ , so we suppose  $p_{ei}(C,v) = 1$  in which case  $i=e$ .  $\Gamma_1(v)$  contains vertices at distance  $e$  or less from  $C$  so

$$\begin{aligned} k &= |\Gamma_1(v)| \geq p_{ee}(C,v)((B_{e-1})_{1e} + (B_e)_{1e}) + p_{e+1e}(C,v)(B_e)_{1e+1} \\ &= (B)_{e-1e} + (B)_{ee} + p_{e+1e}(C,v)(B)_{ee+1}([4,4.4.4]) \\ &= c_e + a_e + p_{e+1e}(C,v)c_{e+1} \end{aligned}$$

Using  $k = c_e + a_e + b_e$  the result follows ■

Consider the set  $\Gamma_{e+1}(v)$  of vertices of  $\Gamma$  at distance  $e+1$  from a particular code vertex  $v$ , we partition its elements into two classes:

$$T_\alpha(v) = \{x \in \Gamma_{e+1}(v) \mid \exists c \in C \text{ such that } x \in \Sigma_e(c)\}$$

$$T_\beta(v) = \{x \in \Gamma_{e+1}(v) \mid \partial(x,c) > e \forall c \in C\}$$

Lemma 2.2.3 For each  $v \in C$ ,

$$|T_\alpha(v)| \leq [b_e/c_{e+1}]k_e \quad (2.2.5)$$

Proof Since  $v \in C$   $\partial(v,C) = 0$  and  $p_{00}(C,v) = 1$ ,  $p_{10}(C,v) = \dots = p_{2e0}(C,v) = 0$ . By the definition of  $T_\alpha(v)$  we have

$$|T_\alpha(v)| = (B_e)_{e+1 \ 2e+1} p_{2e+1 \ 0}(C,v) \quad (2.2.6)$$

Now take any  $z \in \Gamma_e(v)$ ; then  $p_{ee}(C,z) = 1$  and by Lemma 2.2.2

$$c_{e+1} p_{e+1e}(C,z) \leq b_e. \quad \text{Hence}$$

$$|\Gamma_{e+1}(z) \cap C| \leq [b_e/c_{e+1}] \quad (2.2.7)$$

Clearly the sets  $\Gamma_{e+1}(z) \cap C$ , for  $z \in \Gamma_e(v)$ , are not necessarily disjoint. In fact if we sum the  $\Gamma_{e+1}(z) \cap C$  we repeat each code vertex in  $\Gamma_{2e+1}(v)$  at least  $(B_e)_{e+1} 2e+1$  times. Hence

$$\begin{aligned} (B_e)_{e+1} 2e+1 p_{2e+1 0}(C, v) &\leq \sum_{z \in \Gamma_e(v)} |\Gamma_{e+1}(z) \cap C| \\ &\leq k_e [b_e / c_{e+1}] \quad \blacksquare \end{aligned}$$

Corollary 2.2.4 For each  $v \in C$ ,

$$|T_\beta(v)| \geq k_{e+1} - k_e [b_e / c_{e+1}] \quad (2.2.8)$$

Proof Using (2.2.5) and  $k_{e+1} = |T_\alpha(v)| + |T_\beta(v)| \quad \blacksquare$

Theorem 2.2.5 For any e-code  $C$  in a distance-regular graph  $\Gamma$  with valency  $k$ ,

$$|C| \cdot (1 + k + \dots + k_e + \frac{k_e}{[k/c_{e+1}]} (b_e / c_{e+1} - [b_e / c_{e+1}])) \leq |v\Gamma| \quad (2.2.9)$$

Proof A given vertex of  $\Gamma$  can belong to at most  $[k/c_{e+1}]$  of the distinct sets  $T_\beta(v)$ . Combining this with Corollary 2.2.4 we obtain

$$\begin{aligned} [k/c_{e+1}] \left| \bigcup_{v \in C} T_\beta(v) \right| &\geq \sum_{v \in C} |T_\beta(v)| \\ &\geq |C| (k_{e+1} - k_e [b_e / c_{e+1}]) \quad (2.2.10) \end{aligned}$$

Since  $|v\Gamma| \geq \left| \bigcup_{v \in C} \Sigma_e(v) \right| + \left| \bigcup_{v \in C} T_\beta(v) \right|$

$$\geq |C| (1 + k + \dots + k_e) + \frac{|C|}{[k/c_{e+1}]} (k_{e+1} - k_e [b_e / c_{e+1}])$$

and  $k_{e+1} = k_e b_e / c_{e+1}$  the result follows  $\blacksquare$

### 2.3 Nearly perfect and perfect codes

Codes satisfying (2.2.9) with equality are called nearly perfect. (We shall often refer to this equality as the sphere packing condition for nearly perfect codes). In the case of binary nearly perfect codes we have  $\Gamma = \Gamma(m, 2)$  the  $m$ -dimensional binary cube. This graph has  $b_e = m - e$  and  $c_{e+1} = e + 1$  and we see that our definition coincides with that of Goethals and Snover [14]. For any nearly perfect  $e$ -code vertices of the graph are at distance at most  $e + 1$  from the code.

Corollary 2.3.1 For any nearly perfect  $e$ -code in a distance-regular graph we have

- (i) any vertex at distance greater than  $e$  from every code vertex is at distance  $e + 1$  from exactly  $[k/c_{e+1}]$  code vertices;
- (ii) any vertex at distance  $e$  from a given code vertex is at distance  $e + 1$  from exactly  $[b_e/c_{e+1}]$  other code vertices.

Proof (i) Let  $M(x) = \{v \in C \mid x \in T_\beta(v)\}$  for  $x \in \bigcup_{v \in C} T_\beta(v)$ .

We have already shown in the proof of Theorem 2.2.5

$$|M(x)| \leq [k/c_{e+1}] \quad (2.3.1)$$

We have equality throughout Theorem 2.2.5 and in particular in (2.2.10)

$$[k/c_{e+1}] \left| \bigcup_{v \in C} T_\beta(v) \right| = \sum_{v \in C} |T_\beta(v)| \text{ and } |M(x)| = [k/c_{e+1}] \quad (2.3.2)$$

(ii) (2.3.2) and equality in (2.2.10) imply

$$\sum_{v \in C} |T_\beta(v)| = |C| (k_{e+1} - k_e \lfloor b_e / c_{e+1} \rfloor)$$

Hence  $|T_\beta(v)| = k_{e+1} - k_e \lfloor b_e / c_{e+1} \rfloor$  and

$$|T_\alpha(v)| = k_e \lfloor b_e / c_{e+1} \rfloor \quad (2.3.3)$$

From the proof of Lemma 2.3.3

$$\begin{aligned} |T_\alpha(v)| &\leq \sum_{z \in \Gamma_e(v)} |\Gamma_{e+1}(z) \cap C| \\ &\leq k_e \lfloor b_e / c_{e+1} \rfloor \end{aligned}$$

and hence  $|\Gamma_{e+1}(z) \cap C| = \lfloor b_e / c_{e+1} \rfloor \quad (z \in \Gamma_e(v)) \quad \blacksquare$

We define a perfect e-code as a subset  $C$  of  $\Gamma$  such that the sets  $\Sigma_e(c)$ , for  $c \in C$ , form a partition of  $V\Gamma$ . A consequence of this partition is that  $|\Sigma_e(c)| \cdot |C| = |V\Gamma|$ . We call this equality the sphere packing condition for perfect codes and write it as

$$|C| x_e(k) = |C| (1 + k + \dots + k_e) = |V\Gamma| = x_d(k) \quad (2.3.4)$$

If we repeat the counting argument used in the proof of Lemma 2.2.2 for a perfect e-code  $C$ , we obtain  $p_{e+1e}(C, u) = b_e / c_{e+1}$  for  $u \in V\Gamma$  and  $\partial(u, C) = e$ .

Hence a necessary condition for the existence of a perfect e-code in  $\Gamma$  is

$$b_e \equiv 0 \pmod{c_{e+1}} \quad (2.3.5)$$

In classical coding theory (2.3.5) is already well known. From (2.3.4), (2.3.5) and the definition of nearly perfect codes we see that perfect codes are nearly perfect.

For the rest of this section we compare the properties of perfect<sup>codes</sup> and nearly perfect codes which are not perfect. The proofs for both classes of codes are similar so we shall prove only the results for nearly perfect codes. Before we do this, however, we shall need some more definitions:

For each  $j = 0, 1, \dots, e+1$  we choose a vertex  $z_j$  in  $\Gamma$  such that  $\partial(z_j, C) = j$  and recalling (2.2.2)

$$p_{ij}(C, z_j) = |\{x \in C \mid \partial(x, z_j) = i\}| \quad (2.3.6)$$

Obviously we can choose  $z_{e+1}$  only if  $b_e \not\equiv 0 \pmod{c_{e+1}}$  i.e. if  $C$  is not perfect.

We define the  $(d+1) \times n$  matrix  $T_j$ , for  $j=0, 1, \dots, e+1$ , as follows:

$$(T_j)_{iu} = \begin{cases} 1 & \text{if } \partial(u, z_j) = i; \\ 0 & \text{otherwise.} \end{cases} \quad (2.3.7)$$

A simple calculation shows that  $T_j A = B T_j$  and then by (2.1.7), for  $0 \leq i \leq d$

$$T_j A_i = B_i T_j \quad (2.3.8)$$

Using Lemma 2.2.1, (2.3.6) and Corollary 2.3.1 we have

$$p_{ij}(C, z_j) = \delta_{ij} \quad (i, j \in \{0, 1, \dots, e\}) \quad (2.3.9)$$

$$p_{e+1e}(C, z_e) = [b_e / c_{e+1}] \quad (2.3.10)$$

$$p_{e+1e+1}(C, z_{e+1}) = [k / c_{e+1}]; \quad p_{ie+1}(C, z_{e+1}) = 0 \quad (0 \leq i \leq e) \quad (2.3.11)$$

If  $X$  is any subset of  $V\Gamma$  we define its  $n \times 1$  characteristic vector  $\underline{c}$  by  $(\underline{c})_v = \begin{cases} 1 & \text{if } v \in X; \\ 0 & \text{otherwise.} \end{cases}$  By a simple calculation we find

Let  $\underline{c}$  denote the characteristic vector of  $C$ . Then

$$(T_{j\underline{c}})_i = |\{x \in C \mid \partial(x, z_j) = i\}| = p_{ij}(C, z_j) \quad (2.3.12)$$

and from (2.3.9), (2.3.10) and (2.3.11) the vectors  $T_{0\underline{c}}, T_{1\underline{c}}, \dots, T_{e+1\underline{c}}$  are linearly independent.

For the rest of this section  $\Gamma$  denotes a distance-regular graph with distance function  $\partial$ , diameter  $d$  and valency  $k$ .  $\underline{u}$  denotes the  $n \times 1$  column vector  $[1, 1, \dots, 1]^t$ .

**Lemma 2.3.2** If  $\Gamma$  contains a nearly perfect  $e$ -code  $C$  with characteristic vector  $\underline{c}$  and

$$S = A_0 + \dots + A_{e-1} + \frac{A_e}{[k/c_{e+1}]} ([k/c_{e+1}] - [b_e/c_{e+1}]) + \frac{A_{e+1}}{[k/c_{e+1}]}, \text{ then}$$

$$S \underline{c} = \underline{u} \quad (2.3.13)$$

**Proof** Let  $w \in V\Gamma$ . If  $\partial(w, C) \leq e-1$  then obviously  $(S\underline{c})_w = 1$ .

a) If  $\partial(w, C) = e$  then

$$\begin{aligned} (S\underline{c})_w &= 1 - \frac{[b_e/c_{e+1}]}{[k/c_{e+1}]} + \frac{|\Gamma_{e+1}(w) \cap C|}{[k/c_{e+1}]} \\ &= 1 \quad (\text{by (2.3.10)}) \end{aligned}$$

b) If  $\partial(w, C) = e+1$  then

$$(S\underline{c})_w = \frac{|\Gamma_{e+1}(w) \cap C|}{[k/c_{e+1}]} = 1 \quad (\text{by (2.3.11)}) \quad \blacksquare$$

Lemma 2.3.2 holds for perfect codes since part b) of the proof is vacuously true. We state a related result first proved by Biggs [5] for perfect codes in distance-transitive graphs. Distance-transitive graphs are a subclass of the class of distance-regular graphs and the result generalises easily. The author would like to point out that many of the ideas used in this chapter are taken from [5].

Lemma 2.3.3 (Biggs [5]) If  $\Gamma$  contains a perfect  $e$ -code  $C$  with characteristic vector  $\underline{c}$  and  $S_e = A_0 + A_1 + \dots + A_e$ , then

$$S_e \underline{c} = \underline{u} \quad (2.3.14) \blacksquare$$

If we define

$$\hat{S} = B_0 + \dots + B_{e-1} + \frac{B_e}{[k/c_{e+1}]} \cdot ([k/c_{e+1}] - [b_e/c_{e+1}]) + \frac{B_{e+1}}{[k/c_{e+1}]} \quad (2.3.15)$$

then by (2.3.8)

$$T_j S = \hat{S} T_j \quad (0 \leq j \leq e+1) \quad (2.3.16)$$

Lemma 2.3.4 If  $\Gamma$  contains a nearly perfect  $e$ -code and  $b_e \not\equiv 0 \pmod{c_{e+1}}$  then  $\dim \ker \hat{S} \geq e+1$ .

Proof By applying  $T_j$  to (2.3.13) we obtain

$$\hat{S} T_j \underline{c} = T_j \underline{u} = \underline{k} \quad (0 \leq j \leq e+1) \quad (2.3.17)$$

where  $\underline{k} = [1, k, \dots, k_d]^t$ .  $\{T_0 \underline{c}, T_1 \underline{c}, \dots, T_{e+1} \underline{c}\}$  is a set of linearly independent vectors and hence the vectors

$T_0 \underline{c} - T_1 \underline{c}, \dots, T_0 \underline{c} - T_{e+1} \underline{c}$  are linearly independent. From (2.3.17)

we have  $\hat{S}(T_j \underline{c} - T_0 \underline{c}) = \hat{S} T_j \underline{c} - \hat{S} T_0 \underline{c} = 0$  for  $0 \leq j \leq e+1$  and hence the kernel of  $\hat{S}$  has dimension at least  $e+1$  ■

Lemma 2.3.5 (Biggs) If  $\Gamma$  contains a perfect  $e$ -code and

$\hat{S}_e = B_0 + B_1 + \dots + B_e$  then  $\dim \ker \hat{S}_e \geq e$  ■

proving

Of course in Lemma 2.3.5 we shall obtain

$$\hat{S}_e T_j \underline{c} = \underline{k} \quad (0 \leq j \leq e) \quad (2.3.18)$$

$B$  is tri-diagonal so  $\hat{S}_e$  is  $2e+1$ -diagonal and the entries on the uppermost diagonal,  $(\hat{S}_e)_{i, e+i}$  ( $0 \leq i \leq d-e$ ), are all non-zero. We know, by (2.3.9), that  $(T_j \underline{c})_i$  ( $0 \leq i \leq e$ ) are independent of the choice of  $z_j$  so we can use (2.3.18) to find  $(T_j \underline{c})_i$  ( $e+1 \leq i \leq d$ ). Thus  $T_j \underline{c}$  is independent of the choice of  $z_j$  for  $0 \leq j \leq e$ .

A similar proof holds when a nearly perfect  $e$ -code exists. In this case  $\hat{S}$  is  $2e+3$ -diagonal and the entries,  $(\hat{S})_{i, e+1+i}$  ( $0 \leq i \leq d-e-1$ ) are all non-zero. We know, by (2.3.9), (2.3.10) and (2.3.11), that  $(T_{j, \underline{c}})_i$  ( $0 \leq i \leq e+1$ ) are independent of the choice of  $z_j$  so we can find  $(T_{j, \underline{c}})_i$  ( $e+2 \leq i \leq d$ ) from (2.3.17). Thus  $T_{j, \underline{c}}$  is independent of the choice of  $z_j$  for each  $j$  with  $0 \leq j \leq e+1$ .

We now prove a result which is analogous to Lloyd's theorem and generalises a result of Goethals and Snover [14, Theorem 4.3]. Biggs [5] proved a generalisation of Lloyd's theorem for perfect codes in distance-transitive graphs; we state the result (Theorem 2.3.8) for distance-regular graphs.

Theorem 2.3.6 If  $\Gamma$  contains a nearly perfect  $e$ -code and  $b_e \not\equiv 0 \pmod{c_{e+1}}$  then in the ring  $\mathbb{Q}[\lambda]$  we have the condition,

$$x(\lambda) = x_{e-1}(\lambda) + \frac{v_e(\lambda)}{[k/c_{e+1}]} ([k/c_{e+1}] - [b_e/c_{e+1}]) + \frac{v_{e+1}(\lambda)}{[k/c_{e+1}]} \quad (2.3.19)$$

divides  $x_d(\lambda)$ , or alternatively the zeros of  $x(\lambda)$  are eigenvalues of  $\Gamma$ .

Proof From (2.3.15) and (2.1.7) we have

$$\hat{S} = x(B) \quad (2.3.20)$$

Hence the eigenvalues of  $\hat{S}$  are  $x(k)$ ,  $x(\lambda_1)$ , ...,  $x(\lambda_d)$  where  $k$ ,  $\lambda_1$ , ...,  $\lambda_d$  are the eigenvalues of  $B$ . By Lemma 2.3.4 at least  $e+1$  eigenvalues of  $\hat{S}$  are zero so that the polynomial  $x(\lambda)$  has at least  $e+1$  zeros in the set  $\{k, \lambda_1, \dots, \lambda_d\}$ .  $x(\lambda)$  is of degree  $e+1$  and from the sphere packing condition  $|C| \cdot x(k) = |V\Gamma|$ . Hence  $x(\lambda)$  is a rational multiple of  $(\lambda - \mu_1)(\lambda - \mu_2) \dots (\lambda - \mu_{e+1})$  where  $\{\mu_1, \mu_2, \dots, \mu_{e+1}\}$  is a subset of  $\{\lambda_1, \lambda_2, \dots, \lambda_d\}$ .

Finally as mentioned earlier  $x_d(\lambda)$  is a rational multiple of  $(\lambda - \lambda_1)(\lambda - \lambda_2) \dots (\lambda - \lambda_d)$  and the result follows. ■

We recall the definition of the binary Lloyd polynomial of degree  $i$

$$Q_i(x) = \sum_{j=0}^i (-1)^j \binom{m-x}{i-j} \binom{x-1}{j} \quad (0 \leq i \leq m)$$

We now prove a result of Goethals and Snover [14, Theorem 4.3]

Corollary 2.3.7 If there exists a nearly perfect binary  $e$ -code of length  $m$ , with  $m+1 \not\equiv 0 \pmod{e+1}$ , then the polynomial

$$Q(x) = Q_{e-1}(x) + \frac{Q_{e+1}(x) - Q_{e-1}(x)}{[(m+1)/(e+1)]} \quad (2.3.21)$$

has  $e+1$  distinct zeros in  $\{1, 2, \dots, m\}$ .

Proof We apply Theorem 2.3.6 to the distance-regular graph  $\Gamma(m, 2)$ , the generalised binary cube. The necessary polynomial condition is that in  $\mathbb{Q}[\lambda]$

$$x(\lambda) = x_{e-1}(\lambda) + \frac{v_e(\lambda)}{[m/(e+1)]} ([m/(e+1)] - [(m-e)/(e+1)]) + \frac{v_{e+1}(\lambda)}{[m/(e+1)]} \quad (2.3.22)$$

divides  $x_m(\lambda)$ , provided  $m-e \not\equiv 0 \pmod{e+1}$  or equivalently  $m+1 \not\equiv 0 \pmod{e+1}$ . Reducing the coefficient of  $v_e(\lambda)$  in (2.3.22) and using  $[m/(e+1)] = [(m+1)/(e+1)]$  for  $m+1 \not\equiv 0 \pmod{e+1}$

$$\begin{aligned} x(\lambda) &= x_{e-1}(\lambda) + \frac{(v_e(\lambda) + v_{e+1}(\lambda))}{[(m+1)/(e+1)]} \\ &= x_{e-1}(\lambda) + \frac{x_{e+1}(\lambda) - x_{e-1}(\lambda)}{[(m+1)/(e+1)]} \end{aligned}$$

From [5, page 296] we have  $x_i(\lambda) = Q_i(x)$   $(0 \leq i \leq m)$

where

$$x = m - \frac{(m+\lambda)}{2} \quad (2.3.23)$$

and also  $x_m(\lambda) = Q_m(x)$  is a rational multiple of  $(x-1)(x-2)\dots(x-m)$ .

The result follows ■

Theorem 2.3.8 If  $\Gamma$  contains a perfect  $e$ -code  $C$  then in the ring  $\mathbb{Q}[\lambda]$  we have the condition

$x_e(\lambda)$  divides  $x_d(\lambda)$ , or alternatively the zeros of  $x_e(\lambda)$  are eigenvalues of  $\Gamma$  ■

#### 2.4 The weight vector of a nearly perfect code

The related weight vectors of a code can be useful in proving non-existence results for codes in distance-regular graphs. In this section we obtain expressions connecting the related weight vectors of a nearly perfect  $e$ -code.

Lemma 2.4.1 If  $\Gamma$  contains a nearly perfect  $e$ -code and  $0 \leq i \leq e+1$ , then

$$\sum_{h=1}^{e-1} p_{hi}(C) + \frac{p_{ei}(C)}{\lfloor k/c_{e+1} \rfloor} (\lfloor k/c_{e+1} \rfloor - \lfloor b_e/c_{e+1} \rfloor) + \frac{p_{e+1i}(C)}{\lfloor k/c_{e+1} \rfloor} = 1 \quad (2.4.1)$$

Proof The result follows by considering the first component of (2.3.17) and using  $(B_h)_{os} = \delta_{hs}$  ■

$$\begin{aligned} \text{Lemma 2.4.2} \quad \text{If } \hat{S} = B_0 + \dots + B_{e-1} + B_e \frac{(\lfloor k/c_{e+1} \rfloor - \lfloor b_e/c_{e+1} \rfloor)}{\lfloor k/c_{e+1} \rfloor} \\ + \frac{B_{e+1}}{\lfloor k/c_{e+1} \rfloor} \end{aligned}$$

then  $\dim \ker \hat{S} \leq e + 1$ .

Proof Let  $r(\hat{S})$  denote the rank of  $\hat{S}$ .  $B$  is tri-diagonal so  $\hat{S}$  is  $2e+3$ -diagonal with non-zero elements on the uppermost diagonal. Then  $r(\hat{S}) \geq d-e$  and  $\dim \ker \hat{S} = d+1-r(\hat{S}) \leq e+1$  ■

Similarly we can prove that  $\dim \hat{S}_e \leq e$ .

We now define a more convenient notation for the related weight vectors of a nearly perfect  $e$ -code  $C$ . For each  $j=0,1,\dots,e+1$  we define the vector  $p(j)$  as follows:

$$[p(j)]_i = p_{ij}(C) \quad (0 \leq i \leq d)$$

$$\text{and hence } p(j) = T_{j\underline{c}} \quad (0 \leq j \leq e+1)$$

$$\text{and by (2.3.17) } \hat{S}p(j) = \underline{k} \quad (0 \leq j \leq e+1)$$

N.B. We recall that  $p(e+1)$  is only defined when  $b_e \not\equiv 0 \pmod{c_{e+1}}$ .

If  $\Gamma$  contains a nearly perfect  $e$ -code and  $b_e \not\equiv 0 \pmod{c_{e+1}}$  then by Lemmas 2.3.4 and 2.4.2  $\dim \ker \hat{S} = e+1$  and hence  $\{T_{1\underline{c}} - T_{0\underline{c}}, T_{2\underline{c}} - T_{0\underline{c}}, \dots, T_{e+1\underline{c}} - T_{0\underline{c}}\} = \{p(1) - p(0), p(2) - p(0), \dots, p(e+1) - p(0)\}$  is a basis for  $\ker \hat{S}$ . We are now in a position to obtain expressions for  $p(1), \dots, p(e+1)$  in terms of  $p(0)$ .

#### Theorem 2.4.3

$$(i) \quad p(i) = B_i p(0) / k_i \quad (0 \leq i \leq e);$$

$$(ii) \quad p(e+1) = \frac{B_{e+1} - [b_e / c_{e+1}] B_e}{k_{e+1} - [b_e / c_{e+1}] k_e} \cdot p(0).$$

Proof We suppose  $i > 0$  because (i) is trivial otherwise.  $k$  is an eigenvalue of  $B$  associated with the eigenvector  $\underline{k}$ . Thus from (2.1.7)

$$B_i \underline{k} = k_i \underline{k} \text{ and}$$

$$\begin{aligned} \hat{S}(B_i p(0) - k_i p(0)) &= \hat{S}B_i p(0) - k_i \hat{S}p(0) \\ &= B_i \underline{k} - k_i \underline{k} \\ &= 0 \end{aligned}$$

Hence  $B_i p(0) - k_i p(0) \in \ker \hat{S}$  and

$$B_i p(0) = k_i p(0) + \sum_{s=1}^{e+1} \eta_s (p(s) - p(0)) \quad (2.4.2)$$

The  $j$ th component of  $B_i p(0)$  is

$$\sum_{t=0}^d (B_i)_{jt} p_{t0}(C) = (B_i)_{j0} + \sum_{t=2e+1}^d (B_i)_{jt} p_{t0}(C)$$

since  $C$  has minimum distance  $2e+1$ .

Equating the first components of both sides of (2.4.2)

$$k_i = \sum_{s=1}^{e+1} \eta_s \quad (2.4.3)$$

(i) Let  $1 \leq i \leq e$ ; if  $0 < j \leq e$  then the  $j^{\text{th}}$  component of (2.4.2) gives

$$\eta_j = \begin{cases} (B_i)_{i0} = k_i & \text{if } j=i; \\ 0 & \text{otherwise,} \end{cases}$$

and then (2.4.3) gives  $\eta_{e+1} = 0$ . Hence

$$B_i p(0) = k_i p(\hat{1}) \quad (0 \leq i \leq e).$$

(ii) Let  $i=e+1$ ; if  $0 < j < e$  we have  $\eta_j = 0$ . If  $j=e$

$$\text{we obtain } \eta_e = (B_{e+1})_e p_{2e+1,0}(C)$$

$$= k_e [b_e / c_{e+1}] \quad \text{by (2.3.3) and (2.2.6).}$$

(2.4.3) implies  $\eta_{e+1} = k_{e+1} - k_e [b_e / c_{e+1}]$  which with

$$B_e p(0) = k_e p(e) \text{ gives (ii) } \blacksquare$$

Corollary 2.4.4 If  $\Gamma$  contains a nearly perfect  $e$ -code and  $b_e \not\equiv 0 \pmod{c_{e+1}}$  then

$$\underline{k} = \sum_{i=0}^e k_i p(i) + \frac{k_e}{[k/c_{e+1}]} (b_e/c_{e+1} - [b_e/c_{e+1}]) p(e+1) \quad (2.4.4)$$

Proof The result follows from Theorem 2.4.3 and  $\hat{S}_p(0) = \underline{k}$  ■

We can derive similar results for a perfect code. In fact if  $\Gamma$  contains a perfect  $e$ -code then by the above methods we have

$$\dim \ker \hat{S}_e = e; \quad B_i p(0) = k_i p(i) \quad (0 \leq i \leq e) \quad (2.4.5)$$

and

$$\underline{k} = \sum_{i=0}^e k_i p(i) \quad (2.4.6)$$

## 2.5 Constructing perfect codes from nearly perfect codes

Suppose that the distance-regular graph  $\Gamma$  contains a nearly perfect  $e$ -code  $C$  (with  $e$  even) and let  $D$  denote the set of vertices of  $\Gamma$  at distance greater than  $e$  from every member of  $C$ . If  $b_e \not\equiv 0 \pmod{c_{e+1}}$  and we can establish that  $D$  has minimum distance at least  $e+1$  then  $C \cup D$  is an  $e/2$ -code in  $\Gamma$ . An interesting problem is to find values of the parameters  $e$ ,  $[k/c_{e+1}]$ ,  $[b_e/c_{e+1}]$  for which  $C \cup D$  is a perfect  $(e/2)$ -code in  $\Gamma$ .

We suppose that this is the case; since  $C$  is nearly perfect we have

$$|C| x_e(k) + |D| = |V\Gamma| \quad (2.5.1)$$

where

$$\begin{aligned} |D| &= \frac{|C| k_e}{[k/c_{e+1}]} (b_e/c_{e+1} - [b_e/c_{e+1}]) \\ &= \frac{|C| k_e \beta}{k - \chi} \end{aligned}$$

for  $b_e \equiv \beta \pmod{c_{e+1}}$ ,  $k \equiv \chi \pmod{c_{e+1}}$  and  $0 \leq \chi < c_{e+1}$ ,  $1 \leq \beta < c_{e+1}$ .

From the fact that CUD is a perfect  $(e/2)$ -code

$$|CUD| x_{e/2}(k) = |V\Gamma| \quad (2.5.2)$$

Combining (2.5.1) and (2.5.2) and using the disjointness of C and D

$$|C| (x_e(k) - x_{e/2}(k)) = |D| (x_{e/2}(k) - 1) \quad (2.5.3)$$

and hence,

$$\chi = k - \frac{(x_{e/2}(k) - 1)}{(x_e(k) - x_{e/2}(k))} \cdot k_e \beta \quad (2.5.4)$$

Substituting  $e=2$  in (2.5.4) gives  $\chi = k - k\beta$  so  $k$  divides  $\chi$  and hence  $\chi = 0$  and  $\beta = 1$ . We have a possible set of parameters  $e=2$ ,  $k \equiv 0 \pmod{c_3}$  and  $b_2 \equiv 1 \pmod{c_3}$ . Before we investigate the case  $e=2$  further we prove that there are no other possible parameter sets for graphs with  $k_i > k_{i-1}$  ( $1 \leq i \leq e$ ) and  $2 < e \leq \lfloor (d-1)/2 \rfloor$ . Each of the infinite families of distance-regular graphs we consider later has  $k_i > k_{i-1}$  ( $1 \leq i \leq e$ ).

If  $e > 2$  and  $k_i > k_{i-1}$  ( $1 \leq i \leq e$ ), then

$$k_e \sum_{i=1}^{e/2} k_i > k \sum_{i=1}^{e/2} k_{(e/2)+i}$$

which we write as

$$k_e (x_{e/2}(k) - 1) > k (x_e(k) - x_{e/2}(k)) \quad (2.5.5)$$

But (2.5.5) and  $\beta \geq 1$  imply that  $\chi < 0$  which is impossible.

**Theorem 2.5.1** Let  $\Gamma$  be a distance-regular graph with valency  $k$ .

Suppose that  $\Gamma$  contains a nearly perfect 2-code and let D denote the set of vertices of  $\Gamma$  at distance greater than 2 from every code vertex.

If  $k \equiv 0 \pmod{c_3}$  and  $b_2 \equiv 1 \pmod{c_3}$ , then CUD is a perfect 1-code in  $\Gamma$ .

Proof If  $e=2$  (2.5.1) becomes

$$|C| (1+k+k_2) + |D| = |V\Gamma| \quad (2.5.6)$$

where  $|D| = |C|k_2/k$ . Substituting for  $|C|k_2$  in (2.5.6) gives

$$|C \cup D| (1+k) = |V\Gamma| \quad (2.5.7)$$

It only remains to show that every vertex at distance 2 from some code vertex is at distance one from some vertex in  $D$ . Take  $u \in C$  and  $z \in \Gamma_2(u)$ . Let  $C^* = C \setminus \{u\}$ , then for  $c \in C^*$

$$|\Gamma_1(z) \cap \Sigma_2(c)| = \begin{cases} c_3 & \text{if } z \in T_\alpha(c); \\ 0 & \text{otherwise.} \end{cases} \quad (2.5.8)$$

$z$  is at distance three from exactly  $[b_2/c_3] = (b_2-1)/c_3$  vertices of  $C$  so

$$|\Gamma_1(z) \cap (\bigcup_{c \in C^*} \Sigma_2(c))| = \sum_{c \in C^*} |\Gamma_1(z) \cap \Sigma_2(c)| = b_2 - 1.$$

Hence  $|\Gamma_1(z) \cap T_\beta(u)| = 1$  and  $z$  is at distance one from exactly one element of  $T_\beta(u) \subseteq D$  ■

We shall give an application of this result in a later chapter. With the same hypotheses as Theorem 2.5.1 we find the weight vector of  $D$ .

Corollary 2.5.2 If  $p(C) = p(0)$  for the nearly perfect 2-code  $C$  and  $p(D)$  is the weight vector of  $D$  with respect to any element of  $C$  then

$$p(D) = k_2 p(3)/k = (c_3 B_3 - (b_2 - 1) B_2) p(C)/k \quad (2.5.9)$$

Proof  $C$  is a nearly perfect 2-code and  $C \cup D$  is a perfect 1-code.

If  $\hat{S} = \frac{c_3 B_3}{k} + \frac{B_2}{k} (k - b_2 + 1) + B + I$  then

$$\hat{S} p(C) = \underline{k} \quad (2.5.10)$$

$$\text{and } (B+I) p(C \cup D) = \underline{k} \quad (2.5.11)$$

where  $p(C \cup D)$  is the weight vector of  $C \cup D$  with respect to a vertex of  $C$ .

$$\begin{aligned} BB_2 &= c_3 B_3 + a_2 B_2 + b_1 B \\ BB_1 &= c_2 B_2 + a_1 B_1 + kI, \end{aligned}$$

with which we find  $\hat{S} = (B+I)(B_2+B)/k$ .  $C$  and  $D$  are disjoint and by multiplying (2.5.11) by  $(B_2+B)/k$

$$\hat{S}_P(C) + \hat{S}_P(D) = (B_2+B)\underline{k}/k = (k_2+k)\underline{k}/k$$

which combined with (2.5.10) gives

$$\hat{S}_P(D) = k_2 \underline{k}/k \quad (2.5.12)$$

(2.5.10) and (2.5.12) imply that  $p(D) - \frac{k_2}{k} p(C)$  is an element of  $\ker \hat{S}$  whence

$$p(D) = \frac{k_2}{k} p(C) + \sum_{i=1}^3 \alpha_i (p(i) - p(C)) \quad (2.5.13)$$

Equating the first three components of (2.5.13)

$$\alpha_i = 0 \quad (1 \leq i \leq 2) \text{ and } \alpha_3 = k_2/k.$$

$$\text{Hence } p(D) = \frac{k_2}{k} p(3) = \frac{k_2}{k} \frac{(B_3 - [b_2/c_3] B_2)}{k_3 - [b_2/c_3] k_2} \cdot p(C), \text{ by Theorem 2.4.3 (ii),}$$

and the result follows ■

### 3. Completely Regular Codes

In Chapter 2 we have compared the properties of perfect codes and nearly perfect codes which are not perfect. We have seen that for a perfect  $e$ -code vertices of the graph are at distance at most  $e$  from the code and for a nearly perfect  $e$ -code vertices are at distance at most  $e+1$  from the code.

Suppose now that we have an  $e$ -code  $C$  with the property that any vertex of the graph is at most at distance  $e+m$  from  $C$ . We pose the obvious questions:

- (i) What conditions must  $C$  satisfy in order that we can prove a result analogous to Lloyd's theorem?
- (ii) What properties does  $C$  have in common with perfect and nearly perfect codes when it satisfies these conditions?

In the present chapter we hope to answer these interesting questions.

#### 3.1 Definitions

We continue to denote a distance-regular graph by  $\Gamma$ . If  $C$  is an  $e$ -code in  $\Gamma$  we say that it has external distance  $e+m$  if the maximum distance of any vertex of  $\Gamma$  from  $C$  is  $e+m$ . We point out that this is what Delsarte [9] defines as "true external distance", his external distance being an upper bound for this number.

We choose  $z_j \in V\Gamma$  such that  $\partial(z_j, C) = j$  ( $j \in \{0, 1, \dots, e+m\}$ ) and call  $C$  completely regular if the numbers

$$p_{ij}(C, z_j) = p_{ij}(C) \quad (i \in \{0, 1, \dots, d\}, j \in \{0, 1, \dots, e+m\})$$

depend only on  $i$  and  $j$  and not on the choice of  $z_j$ . (Notice that both nearly perfect and perfect codes are completely regular). We say that  $C$  is locally regular if the numbers

$$p_{ij}(C, z_j) = p_{ij}(C) \quad (i, j \in \{0, 1, \dots, e+m\})$$

depend only on  $i$  and  $j$  and not on the choice of  $z_j$ . We shall prove that an analogue of Lloyd's theorem holds for locally regular codes and that such codes are necessarily completely regular.

### 3.2 An analogue of Lloyd's theorem for completely regular codes

(except Section 3.6)

In this chapter  $C$  denotes a locally regular  $e$ -code with external distance  $e+m$  in the distance-regular graph  $\Gamma$ . By the definition of minimum distance it is easy to see

$$p_{ij}(C) = \delta_{ij} \quad (i, j \in \{0, 1, \dots, e\}) \quad (3.2.1)$$

$$p_{ij}(C) = 0 \quad \text{for } i < j \text{ and } i, j \in \{0, 1, \dots, e+m\} \quad (3.2.2)$$

$$p_{ii}(C) \neq 0 \quad (i \in \{0, 1, \dots, e+m\}) \quad (3.2.3)$$

Lemma 3.2.1 There exist rational numbers  $\alpha_0, \alpha_1, \dots, \alpha_{e+m}$  such that

$$\sum_{i=0}^{e+m} \alpha_i p_{ij}(C) = 1 \quad (j \in \{0, 1, \dots, e+m\}) \quad (3.2.4)$$

Proof By (3.2.2) and (3.2.3) the system of equations is triangular and can be solved uniquely for the  $\alpha_i$ 's ■

Lemma 3.2.2 If  $S = \sum_{i=0}^{e+m} \alpha_i A_i$  and  $\underline{c}$  is the characteristic vector of  $C$  then

$$S\underline{c} = \underline{u} \quad (3.2.5)$$

Proof Suppose  $\partial(w, C) = j$ . Then

$$(S_{\underline{c}})_{\underline{w}} = \sum_{i=0}^{e+m} \alpha_i (A_{i, \underline{c}})_{\underline{w}} = \sum_{i=0}^{e+m} \alpha_i p_{ij}(C) = 1 \blacksquare$$

We define the  $(d+1) \times n$  matrices  $T_0, T_1, \dots, T_{e+m}$  as follows:  
for  $j \in \{0, 1, \dots, e+m\}$

$$(T_j)_{i\mathbf{w}} = \begin{cases} 1 & \text{if } \partial(z_j, \mathbf{w}) = i \\ 0 & \text{otherwise} \end{cases},$$

and from (2.1.7) we find

$$T_j A_i = B_i T_j \quad (i \in \{0, 1, \dots, d\}) \quad (3.2.6)$$

and

$$T_j S = \hat{S} T_j \quad \text{where} \\ \hat{S} = \sum_{i=0}^{e+m} \alpha_i B_i = \sum_{i=0}^{e+m} \alpha_i v_i(B) \quad (3.2.7)$$

Lemma 3.2.3 If  $\Gamma$  contains a locally regular  $e$ -code  $C$  with external distance  $e+m$  then  $\dim \ker \hat{S} \geq e+m$ .

Proof We follow the proof of Lemma 2.3.4 to obtain

$$\hat{S} T_{j, \underline{c}} = \underline{k} \quad (j \in \{0, 1, \dots, e+m\}) \quad (3.2.8)$$

We also have an equality analogous to (2.3.12), namely

$$(T_{j, \underline{c}})_i = p_{ij}(C) \quad (i \in \{0, 1, \dots, d\}, j \in \{0, 1, \dots, e+m\})$$

By (3.2.1), (3.2.2) and (3.2.3) the vectors  $T_{1, \underline{c}} - T_{0, \underline{c}}, T_{2, \underline{c}} - T_{0, \underline{c}}, \dots, T_{e+m, \underline{c}} - T_{0, \underline{c}}$  are linearly independent and  $\hat{S}(T_{j, \underline{c}} - T_{0, \underline{c}}) = 0$  for  $j \in \{1, 2, \dots, e+m\}$ .

The result follows  $\blacksquare$

Using the eigenvector sequence we define the polynomial

$$x(\lambda) = \sum_{i=0}^{e+m} \alpha_i v_i(\lambda) \quad (3.2.9)$$

Theorem 3.2.4 If  $\Gamma$  contains a locally regular e-code with external distance  $e+m$  then, in the ring  $\mathbb{Q}[\lambda]$ , we have the condition,

$$x(\lambda) \text{ divides } x_d(\lambda), \text{ or alternatively,}$$

the zeros of  $x(\lambda)$  are eigenvalues of  $\Gamma$ .

Proof The proof is essentially the same as for Theorem 2.3.6.

$\hat{S} = x(B)$  has eigenvalues  $x(k), x(\lambda_1), \dots, x(\lambda_d)$ . By Lemma (3.2.3)  $x(\lambda)$  has at least  $e+m$  zeros in the set  $\{k, \lambda_1, \dots, \lambda_d\}$ . If we pre-multiply (3.2.5) by the row vector  $[1, 1, \dots, 1]$  we obtain

$$\sum_{i=0}^{e+m} \alpha_i k_i \cdot |C| = |V\Gamma| \quad \text{and since } k_i = v_i(k)$$

$$x(k) \cdot |C| = |V\Gamma| \quad (3.2.10)$$

Hence  $x(k) \neq 0$  and the zeros of  $x(\lambda)$  are elements of  $\{\lambda_1, \lambda_2, \dots, \lambda_d\}$ . The result follows since  $x_d(\lambda)$  is a rational multiple of  $(\lambda - \lambda_1)(\lambda - \lambda_2) \dots (\lambda - \lambda_d)$  ■

N.B. (3.2.10) will also be referred to as the 'sphere packing condition'. There should be no confusion between the various forms of the sphere packing condition once the code is specified.

Theorem 3.2.5 A locally regular e-code  $C$  with external distance  $e+m$  is completely regular.

Proof  $\hat{S}$  is a polynomial of degree  $e+m$  in the tri-diagonal matrix  $B$  and so  $\hat{S}$  is  $2(e+m) + 1$  diagonal. If we know  $p_{ij}(C, z_j)$  for  $i=0, 1, \dots, e+m$  then for any fixed  $j$  we can solve (3.2.8) uniquely to determine  $p_{ij}(C, z_j)$  for  $i=0, 1, \dots, d$ . So if  $p_{ij}(C, z_j)$  does not depend on the choice of  $z_j$  for  $i=0, 1, \dots, e+m$  it does not depend on the choice of  $z_j$  for  $i=0, 1, \dots, d$ . Hence if the code is locally regular then it is completely regular ■

We end this section with a generalisation of a result first proved for perfect codes by O. Heden [21].

By counting the edges of  $\Gamma$  between  $\Gamma_{i-1}(z)$  and  $\Gamma_i(z)$  (for any  $z \in V\Gamma$ ) we obtain

$$k_i c_i = b_{i-1} k_{i-1} \quad (1 \leq i \leq d) \quad (3.2.11)$$

Using (3.2.11) and the definition of the right eigenvector  $\underline{v}(\lambda) = [v_0(\lambda), v_1(\lambda), \dots, v_d(\lambda)]^t$  of  $B$  it is not difficult to show that  $\underline{u}(\lambda) = [v_0(\lambda)/k_0, v_1(\lambda)/k_1, \dots, v_d(\lambda)/k_d]$  is a left eigenvector of  $B$  corresponding to the eigenvalue  $\lambda$ .

**Theorem 3.2.7** If the distance-regular graph  $\Gamma$  contains a locally regular  $e$ -code with external distance  $e+m$  then, in the ring  $\mathbb{Q}[\lambda]$ , we have the condition:

for each  $j=0, 1, \dots, e+m$ ,

$$x_d(\lambda) \text{ divides } x(\lambda) \cdot \sum_{i=0}^d \frac{v_i(\lambda)}{k_i} p_{ij}(C) \quad .$$

**Proof** For the left eigenvector  $\underline{u}(\lambda)$

$$\underline{u}(\lambda)B = \lambda \underline{u}(\lambda) \quad (3.2.12)$$

and hence,

$$\underline{u}(\lambda)\hat{S} = x(\lambda)\underline{u}(\lambda) \quad (3.2.13)$$

We post-multiply (3.2.13) by  $T_{j,c}$  and use (3.2.8) to obtain

$$\underline{u}(\lambda)\underline{k} = x(\lambda)\underline{u}(\lambda)T_{j,c}$$

which can be written as

$$\sum_{i=0}^d u_i(\lambda)k_i = x(\lambda) \sum_{i=0}^d u_i(\lambda)p_{ij}(C)$$

that is

$$\sum_{i=0}^d v_i(\lambda) = x(\lambda) \sum_{i=0}^d \frac{v_i(\lambda)}{k_i} p_{ij}(C).$$

$\lambda$  is an eigenvalue of  $B$  so  $\sum_{i=0}^d v_i(\lambda) = x_d(\lambda) = 0$  and the result follows ■

### 3.3 Antipodal distance-regular graphs

In this section we shall show Theorem 3.2.4 can be strengthened for the case of antipodal distance-regular graphs. The idea of applying the analogous Lloyd's theorem to the derived graph of an antipodal graph is due to D.H. Smith [36]. In fact by using this method he has obtained an improved version of Lloyd's theorem which shortens the proof of the non-existence of binary <sup>perfect</sup>  $\lambda$ -e-codes for  $e \geq 4$ .

A distance-regular graph  $\Gamma$  is antipodal if for all  $u, v \in \Gamma_0(z) \cup \Gamma_d(z)$  either  $\partial(u, v) = d$  or  $u = v$ . The basic results on antipodal distance-transitive graphs are contained in [7]. The results which do not involve transitivity generalise directly to distance-regular graphs [13].

For an antipodal distance-regular graph  $\Gamma$  we can define a derived graph  $\Gamma'$ . The vertices of  $\Gamma'$  are the sets  $\Gamma_0(z) \cup \Gamma_d(z)$  ( $z \in V\Gamma$ ), and the vertices  $\Gamma_0(z) \cup \Gamma_d(z)$  and  $\Gamma_0(z') \cup \Gamma_d(z')$  are adjacent in  $\Gamma'$  if and only if there are vertices  $v \in \Gamma_0(z) \cup \Gamma_d(z)$  and  $v' \in \Gamma_0(z') \cup \Gamma_d(z')$  such that  $\partial(v, v') = 1$  in  $\Gamma$ . If  $d > 2$ ,  $\Gamma'$  is distance-regular with valency  $k$  and diameter  $\lfloor d/2 \rfloor$ .

Lemma 3.3.1 If  $\Gamma$  is an antipodal distance-regular graph with intersection array

$$\begin{Bmatrix} * & c_1 & c_2 & \dots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \dots & a_{d-1} & a_d \\ k & b_1 & b_2 & \dots & b_{d-1} & * \end{Bmatrix}$$

and the derived graph  $\Gamma'$  has intersection array

$$\begin{Bmatrix} * & C_1 & \dots & C_{D-1} & C_D \\ 0 & A_1 & \dots & A_{D-1} & A_D \\ k & B_1 & \dots & B_{D-1} & * \end{Bmatrix}$$

then  $D = \lfloor d/2 \rfloor$  and  $c_i = C_i, a_i = A_i, b_i = B_i$  for  $1 \leq i \leq \lfloor d/2 \rfloor$ .

Proof This is contained in [13, Proposition 4.2] ■

Lemma 3.3.2 If  $\Gamma$  is an antipodal distance-regular graph with derived graph  $\Gamma'$  then the polynomial  $x(\lambda)$  defined by (3.2.9) is the same in both cases provided  $e+m < \lfloor d/2 \rfloor$ .

Proof This follows immediately from Lemma 3.3.1 ■

We shall generalise Corollary 2.4.5 and use the generalisation to show that under certain conditions the derived graph contains a locally regular  $e$ -code which itself is 'derived' from the locally regular  $e$ -code in the antipodal graph.

Lemma 3.3.3 There exist rational numbers  $f_{e+1}, f_{e+2}, \dots, f_{e+m}$  such that for  $m \leq e$  and  $1 \leq t \leq m$

$$\sum_{s=1}^m f_{e+s} p_{e+t, e+s}(C) = k_{e+t} - \sum_{i=0}^e k_i p_{e+t, i}(C) \quad (3.3.1)$$

Proof By (3.2.2) and (3.2.3) the system of equations (3.3.1) is triangular and we can solve uniquely for  $f_{e+1}, f_{e+2}, \dots, f_{e+m}$  ■

Lemma 3.3.4 Suppose  $m \leq e$ . Write  $[p(j)]_i = p_{ij}(C)$  then

$$\underline{k} = \sum_{j=0}^e k_j p(j) + \sum_{s=1}^m \notag_{e+s} p(e+s). \quad (3.3.2)$$

Proof  $\underline{k}$  is an eigenvector of  $B$  corresponding to the eigenvalue  $k$  so

$$\hat{S}\underline{k} = x(B)\underline{k} = x(k)\underline{k} = x(k)\hat{S}p(0)$$

and  $\underline{k} - x(k)p(0) \in \ker \hat{S}$ . We have already mentioned in <sup>proving</sup>Theorem 3.2.5 that  $\hat{S}$  is  $2(e+m)+1$  diagonal so by using the method of proof of Lemma 2.4.2 we have  $\dim \ker \hat{S} \leq e+m$ . We combine this with Lemma (3.2.3) and so a basis for  $\ker \hat{S}$  is the set  $\{p(1) - p(0), \dots, p(e+m) - p(0)\}$ .

Hence

$$\underline{k} = x(k)p(0) + \sum_{s=1}^{e+m} \beta_s (p(s) - p(0)).$$

The first  $e+m+1$  components give  $x(k) - \sum_{s=1}^{e+m} \beta_s = 1$ ,  $k_i = \beta_i$  ( $1 \leq i \leq e$ ) and

$$k_{e+t} = \sum_{s=1}^m \beta_{e+s} p_{e+t, e+s}(C) + \sum_{i=0}^e k_i p_{e+t, i}(C) \quad (1 \leq t \leq m).$$

Hence

$$\beta_{e+s} = \notag_{e+s} \quad (s \in \{1, 2, \dots, m\}) \quad \blacksquare$$

Gardiner [13, Corollary 4.4] has shown that for an antipodal distance-regular graph  $k_d < k$ .

Lemma 3.3.5 If  $m \leq e$ ,  $k_j > k$  for  $j \leq [d/2]$  and  $\notag_{e+s} > k_d$  ( $1 \leq s \leq m$ ) then  $\Gamma_d(c) \subseteq C$  for each  $c \in C$ .

Proof From Lemma 3.3.4

$$k_d = \sum_{j=0}^e k_j p_{dj}(C) + \sum_{s=1}^m \notag_{e+s} p_{de+s}(C).$$

$p_{dj}(C)$  is a non-negative integer for each  $j \in \{0, 1, \dots, e+m\}$  and since  $k_j > k$  for  $j \in \{2, \dots, e+m\}$  so  $p_{d0}(C) = k_d$  and the result follows ■

**Lemma 3.3.6** If  $e+m < \lfloor d/2 \rfloor$  and  $\Gamma_d(c) \subseteq C$  for all  $c \in C$  then the derived graph  $\Gamma'$  contains a locally regular  $e$ -code  $C'$  with external distance  $e+m$ .

**Proof** We define the subset  $C'$  of  $V\Gamma'$  as follows.  $\Gamma_0(c) \cup \Gamma_d(c) \in C'$  if and only if  $c \in C$ . We show

- a)  $C'$  has external distance  $e+m$ ;
- b)  $p_{ij}(C', \Gamma_0(z_j) \cup \Gamma_d(z_j)) = p_{ij}(C, z_j)$  ( $i, j \in \{0, 1, \dots, e+m\}$ ).

Let  $C'$  have external distance  $e+m'$ . Clearly the maximum distance of a vertex from the code cannot be greater in the derived graph so  $m' \leq m$ . Let

$$\Sigma_{e+m-1}(x) = \{w \in V\Gamma \mid \partial(w, x) \leq e+m-1\}$$

and

$$\Sigma'_{e+m-1}(X) = \{W \in V\Gamma' \mid \partial(W, X) \leq e+m-1 \text{ in } \Gamma'\}$$

Suppose  $\partial(x, C) = e+m$ . Every pair of vertices in  $\Sigma_{e+m-1}(x)$  are at distance strictly less than  $d$  and so no two vertices of  $\Sigma_{e+m-1}(x)$  belong to the same set  $\Gamma_0(v) \cup \Gamma_d(v)$  ( $v \in V\Gamma$ ).  $|\Sigma_{e+m-1}(x)| = |\Sigma'_{e+m-1}(X)|$  for  $X = \Gamma_0(x) \cup \Gamma_d(x)$  so  $\Sigma'_{e+m-1}(X)$  consists of the sets  $\Gamma_0(y) \cup \Gamma_d(y)$  ( $y \in \Sigma_{e+m-1}(x)$ ) none of which are code vertices of  $\Gamma'$ . Hence  $m' \geq m$ .

Before we can prove part b) we need a result of D.H. Smith [35, Lemma 8]. Although the result is proved for distance-transitive graphs the generalisation to distance-regular graphs is direct:

$$\Gamma_i(z_j) \cup \Gamma_{d-i}(z_j) = \bigcup_{v \in \Gamma_i(z_j)} (\Gamma_0(v) \cup \Gamma_d(v)) \quad (3.3.3)$$

If  $i < \lfloor d/2 \rfloor$  then by (3.3.3) the vertices of  $\Gamma'$  in  $\Gamma_i(\Gamma_0(z_j) \cup \Gamma_d(z_j))$  are the sets  $\Gamma_0(v) \cup \Gamma_d(v)$  ( $v \in \Gamma_i(z_j)$ ). Hence

$$\begin{aligned} |C \cap \Gamma_i(\Gamma_0(z_j) \cup \Gamma_d(z_j))| &= |C' \cap \{\Gamma_0(v) \cup \Gamma_d(v) \mid v \in \Gamma_i(z_j)\}| \\ &= |\{\Gamma_0(v) \cup \Gamma_d(v) \mid v \in \Gamma_i(z_j) \cap C\}| \\ &= |C \cap \Gamma_i(z_j)|. \end{aligned}$$

Hence  $p_{ij}(C', \Gamma_0(z_j) \cup \Gamma_d(z_j)) = p_{ij}(C, z_j) = p_{ij}(C)$  for  $i, j \in \{0, 1, \dots, e+m\}$  ■

**Theorem 3.3.7** Suppose  $\Gamma$  is antipodal and  $C$  is a locally regular  $e$ -code with external distance  $e+m$  and  $e+m < \lfloor d/2 \rfloor$ . If  $\Gamma_d(c) \subseteq C$  for each  $c \in C$  then the roots of the polynomial  $x(\lambda)$  are eigenvalues of the intersection matrix of the derived graph  $\Gamma'$ .

**Proof** This follows from Lemma 3.3.2, Lemma 3.3.6 and an application of Theorem 3.2.4 to the derived graph  $\Gamma'$  ■

Since  $\Gamma$  has  $d+1$  eigenvalues and  $\Gamma'$  has  $\lfloor d/2 \rfloor + 1$  eigenvalues Theorem 3.3.7 is stronger than Theorem 3.2.4.

### 3.4 Locally regular $e$ -codes with external distance $e$

If  $m=0$  we obviously have the class of perfect  $e$ -codes in  $\Gamma$ . If  $\Gamma$  is antipodal we can apply the argument of Lemma 3.3.5 to (3.3.2) with  $d \geq 2e+1$  (or in fact to (2.4.4)) and obtain  $\Gamma_d(c) \subseteq C$  for each  $c$  in the perfect  $e$ -code  $C$  (a result proved by O.Heden [21] using different methods). Then by Theorem 3.3.7 the roots of  $x_e(\lambda)$  are eigenvalues of the derived graph  $\Gamma'$ , (see also [18, Theorem 2]).

### 3.5 Locally regular e-codes with external distance e+1

If  $m=1$  we can solve the equations of Lemma 3.2.1 to obtain:

$$\left. \begin{aligned} \alpha_i &= 1 \quad (i \in \{0, 1, \dots, e-1\}); \\ \alpha_e &= 1 - (p_{e+1e}(C)/p_{e+1 \ e+1}(C)); \\ \alpha_{e+1} &= 1/p_{e+1 \ e+1}(C) \end{aligned} \right\} \quad (3.5.1)$$

Equations (3.3.1) imply

$$j_{e+1} = (k_{e+1} - k_e p_{e+1e}(C))/p_{e+1 \ e+1}(C) \quad (3.5.2)$$

A locally regular e-code with external distance e+1, then, has parameters e,  $p_{e+1e}(C)$ ,  $p_{e+1 \ e+1}(C)$ .

We wish to point out that the result of Delsarte [9, Theorem 5.13] that codes with 'external distance' e+1 are completely regular does not apply to our more natural definition of external distance. For example the binary 1-code  $C = \{(0,0,0,0), (1,1,1,0)\}$  has external distance 2 but  $p_{41}(C, (0,0,0,1)) = 1$  and  $p_{41}(C, (1,0,0,0)) = 0$  and so C is not completely regular.

We have already remarked that a nearly perfect e-code is locally regular. The associated parameters are  $p_{e+1e}(C) = \lfloor b_e/c_{e+1} \rfloor$  and  $p_{e+1 \ e+1}(C) = \lfloor k/c_{e+1} \rfloor$ . Next we state the improved polynomial condition necessary for the existence of a nearly perfect e-code in an antipodal distance-regular graph.

**Theorem 3.5.1** Let  $\Gamma$  be an antipodal distance-regular graph with diameter d and valency k. If there exists a nearly perfect e-code in  $\Gamma$  with  $d \geq 2e+1$ ,  $k_d < k_e/k$  and  $b_e \not\equiv 0 \pmod{c_{e+1}}$  then there exists a nearly perfect e-code in the derived graph  $\Gamma'$  and the zeros of

$$x(\lambda) = x_{e-1}(\lambda) + v_e(\lambda) \left(1 - \frac{[b_e/c_{e+1}]}{[k/c_{e+1}]}\right) + \frac{v_{e+1}(\lambda)}{[k/c_{e+1}]}$$

are eigenvalues of  $\Gamma'$ .

Proof The proof follows from Lemma 3.3.5, Theorem 3.3.7 and the

fact that  $\delta_{e+1} = \frac{k_e}{[k/c_{e+1}]} (b_e/c_{e+1} - [b_e/c_{e+1}]) \geq \frac{k_e}{k}$  ■

Another family of locally regular codes with external distance  $e+1$  is the family of binary uniformly packed codes (**[26]** and **[32]**) first defined by Semakov, Zinov'ev and Zaitsev. In fact the definition generalises directly to distance-regular graphs:

Definition A uniformly packed  $e$ -code  $C$  with external distance  $e+1$  in a distance-regular graph  $\Gamma$  is a code such that

- a) if  $\partial(C, z_e) = e$  then  $1 + p_{e+1e}(C, z_e) = r(z_e)$ ;
- b) if  $\partial(C, z_{e+1}) = e+1$  then  $p_{e+1 e+1}(C, z_{e+1}) = r(z_{e+1})$ ,

where  $r(z_e) = r(z_{e+1}) = r$  is independent of the vertex  $z_e$  or  $z_{e+1}$  chosen.

Then  $p_{e+1e}(C, z_e) = p_{e+1e}(C)$  and  $p_{e+1 e+1}(C, z_{e+1}) = p_{e+1 e+1}(C)$  are both independent of the vertex chosen and so the code is locally regular and hence completely regular.

From (3.5.1) we have

$$x(\lambda) = x_{e-1}(\lambda) + \frac{v_e(\lambda) + v_{e+1}(\lambda)}{r} \quad (3.5.3)$$

and Theorems 3.2.4 and 3.3.7 apply. With particular reference to Lemma 3.3.5 and (3.5.2)

$$\delta_{e+1} = (k_{e+1} - (r-1)k_e)/r \quad (3.5.4)$$

van Lint [26, page 173] has already noted that a binary uniformly packed code with  $r = \lfloor (m+1)/(e+1) \rfloor$  is nearly perfect. For an arbitrary distance-regular graph this is not necessarily true because we would require  $\lfloor k/c_{e+1} \rfloor$  to be equal to  $1 + \lfloor b_e/c_{e+1} \rfloor$ .

### 3.6 Generalised uniformly packed codes

The definition of generalised uniformly packed codes [32] extends directly to distance-regular graphs:

Definition An  $m^{\text{th}}$  order generalised uniformly packed  $e$ -code  $C$  of external distance  $e+m$  ( $m \leq e$ ) in a distance-regular graph  $\Gamma$  is an  $e$ -code such that if  $\partial(C, z_{e-m+j}) = e-m+j$  and

$$\sum_{i=e-m+1}^{e+m} p_{ie-m+j}(C, z_{e-m+j}) = r(z_{e-m+j}, C) \quad (3.6.1)$$

then  $r(z_{e-m+j}, C) = r$  is independent of  $j$  and of the choice of  $z_{e-m+j}$  for  $1 \leq j \leq 2m$ .

Although this definition does not immediately imply that the code is locally regular, we can still prove Theorem 3.2.4 for these codes.

If we have

$$S = A_0 + A_1 + \dots + A_{e-m} + (A_{e-m+1} + \dots + A_{e+m})/r$$

it is easily seen that  $S\bar{c} = \bar{u}$  as in Lemma 3.2.2. We can prove Lemma 3.3.6 and Theorem 3.2.4 in exactly the same way with

$$x(\lambda) = x_{e-m}(\lambda) + (x_{e+m}(\lambda) - x_{e-m}(\lambda))/r \quad (3.6.2)$$

#### 4. Codes in the graphs $\Gamma(m,q)$

##### 4.1 Introduction

We have already given a brief description of the classical perfect code problem in the case when the alphabet is a finite field. Recently progress has been made for non-field alphabets. The non-existence of perfect 2-codes over alphabets with 6 or 10 elements has been proved by van Lint ( [24] and [26] ). Reuvers [31] has extended these results to  $q = 2p$  and  $p < 20$  for  $e = 2$ . The results of Zinov'ev et al [43] cover  $q = 2^a \cdot 3^b$  for  $e \geq 2$  and the most general result so far, for  $q = p_1^a p_2^b$  and  $e \geq 2$ , is due to Tietäväinen[39] .

The binary nearly perfect code problem, very recently settled by Lindström [23], relies on a computer search for  $e \leq 100$  and  $n \leq 10,000$ . In §4.3 we shall prove algebraically the non-existence of binary nearly perfect codes for odd  $e$  with  $5 \leq e \leq 17$ . Although it is likely that this method will easily extend to other odd values of  $e$  it does not help at all when  $e$  is even. We also consider nearly perfect 1-codes and 2-codes over an arbitrary alphabet.

Finally in §4.4 we briefly discuss completely regular codes and obtain an interesting connection with orthogonal latin squares.

##### 4.2 The eigenvector sequence for $\Gamma(m,q)$

The graph  $\Gamma(m,q)$ , for  $m$  and  $q$  not less than two, represents the  $m$ -dimensional vector space over  $q$  elements where  $q$  is arbitrary. Two vertices of  $\Gamma(m,q)$  are joined by an edge if and only if they differ in one component. These graphs correspond to the Hamming schemes of Delsarte [9] .

$\Gamma(m, q)$  has diameter  $m$ , valency  $m(q-1)$  and intersection array:

$$\left\{ \begin{array}{ccccccc} * & 1 & \dots & i & \dots & m-1 & m \\ 0 & q-2 & \dots & i(q-2) & \dots & (m-1)(q-2) & m(q-2) \\ m(q-1) & (m-1)(q-1) & \dots & (m-i)(q-1) & \dots & q-1 & * \end{array} \right\}$$

The eigenvector sequence is defined as follows:

$$v_0(\lambda)=1, \quad v_1(\lambda)=\lambda, \quad \text{and for } 1 \leq i \leq m-1$$

$$(i+1)v_{i+1}(\lambda) + i(q-2)v_i(\lambda) + (m-i+1)(q-1)v_{i-1}(\lambda) = \lambda v_i(\lambda) \quad (4.2.1)$$

In [5] it is shown that  $\Gamma(m, q)$  has eigenvalues  $m(q-1)-q\xi$  where  $\xi \in \{0, 1, \dots, m\}$ . Hence if  $v$  is a root of  $x_d(\lambda)$  for  $\Gamma(m, q)$  then  $\xi = m - (m+v)/q$  for some  $\xi \in \{1, 2, \dots, m\}$  and

$$m + v \equiv 0 \pmod{q} \quad (4.2.2)$$

We recall the connection between the eigenvector sequence and the Lloyd polynomial

$$x_i(\lambda) = Q_i(x) = \sum_{s=0}^i (-1)^s \binom{m-x}{i-s} \binom{x-1}{s} (q-1)^s \quad (4.2.3)$$

where

$$x = m - (m+\lambda)/q \quad (4.2.4)$$

It is not difficult to see that  $\Gamma(m, 2)$  is an antipodal distance-regular graph and Smith [36] has calculated the eigenvalues of the derived graph  $\Gamma(m, 2)/2$  which are:

$$\left. \begin{array}{ll} m, -m, m-4, -(m-4), \dots, 4, -4, 0 & (m \equiv 0 \pmod{4}); \\ m, -(m-2), m-4, -(m-6), \dots, -3, 1 & (m \equiv 1 \pmod{4}); \\ m, -m, m-4, -(m-4), \dots, -6, 2, -2 & (m \equiv 2 \pmod{4}); \\ m, -(m-2), m-4, -(m-6), \dots, 3, -1 & (m \equiv 3 \pmod{4}). \end{array} \right\} \quad (4.2.5)$$

The following lemma is proved for  $\Gamma(m, 2)$  only.

Lemma 4.2.1 Let  $0 \leq i \leq [(m-1)/2]$ . Then

$$(i) \quad x_{2i}(0) = x_{2i+1}(0) = (-1)^i \binom{\frac{m-2}{2}}{i};$$

$$(ii) \quad x_{2i}(1) = (-1)^i \frac{(m-4i-1)}{(m-1)} \binom{\frac{m-1}{2}}{i},$$

$$x_{2i+1}(1) = (-1)^i 2 \binom{\frac{m-3}{2}}{i};$$

$$(iii) \quad x_{2i}(3) = (-1)^i \frac{(m^2 - 4m(4i+1) + 32i^2 + 16i + 3)}{(m-1)(m-3)} \binom{\frac{m-1}{2}}{i},$$

$$x_{2i+1}(3) = (-1)^i 4 \frac{(m-4i-3)}{(m-3)} \binom{\frac{m-3}{2}}{i}.$$

Proof From (4.2.3), (4.2.4) and  $q=2$  we have  $x = \frac{m-\lambda}{2}$  and

$$\begin{aligned} x_r(\lambda) &= \sum_{j=0}^r (-1)^j \binom{m-x}{r-j} \binom{x-1}{j} \\ &= \text{coefficient of } u^r \text{ in } (1-u)^{x-1} (1+u)^{m-x} \\ &= \text{coefficient of } u^r \text{ in } (1-u^2)^{x-1} (1+u)^{m-2x+1} \\ &= \sum_{j=0}^{[r/2]} (-1)^j \binom{m-2x+1}{r-2j} \binom{x-1}{j} \\ &= \sum_{j=0}^{[r/2]} (-1)^j \binom{\lambda+1}{r-2j} \binom{\frac{m-\lambda}{2}-1}{j}. \end{aligned}$$

The results follow by substitution ■

#### 4.3 Nearly perfect codes in $\Gamma(m, q)$

We consider the binary case initially. If there exists a nearly perfect binary e-code with  $m+1 \not\equiv 0 \pmod{e+1}$  then by Corollary 2.3.7 the polynomial

$$Q(x) = Q_{e-1}(x) + (Q_{e+1}(x) - Q_{e-1}(x)) / [(m+1)/(e+1)] \quad (4.3.1)$$

has distinct <sup>integer</sup>  $\lambda$  roots between 1 and m.

$\Gamma(m,2)$  is antipodal and by Theorem 3.5.1 the derived graph  $\Gamma(m,2)/2$  contains a nearly perfect e-code provided  $k_e = \binom{m}{e} > m$ . Hence for  $e > 1$  the zeros of

$$x(\lambda) = x_{e-1}(\lambda) + (x_{e+1}(\lambda) - x_{e-1}(\lambda)) / [(m+1)/(e+1)]$$

are eigenvalues of the derived graph  $\Gamma(m,2)/2$ . We combine this with (4.2.4) and the form of the eigenvalues in (4.2.5) to infer that the zeros of  $Q(x)$  are even.

Notice from (4.2.3) that if  $q=2$  and  $\alpha$  is a root of  $Q(x)$  then  $m+1-\alpha$  is also a root. Both of these roots must be even so  $m$  must be odd. Further suppose  $a$  is the smallest non-negative integer such that  $e+1$  divides  $m+1-a$ . If  $e$  is odd then  $a$  is even.

We make the substitution  $z = (m+1-2x)^2$  introduced by van Lint[26] and write  $Q(x)$  as  $Q^*(z)$ . The relationship between  $x(\lambda)$  and  $Q^*(z)$  is given by  $z = (\lambda+1)^2$ .

Lemma 4.3.1 If  $e$  is odd and  $e \geq 3$

$$(i) \quad Q^*(1) = x(0) = \frac{(-1)^{\frac{e+1}{2}} (m-2)(m-4) \dots (m-e+1)(a-1)}{(m+1-a)(e-1)(e-3) \dots 2} \quad ;$$

$$(ii) \quad Q^*(4) = x(1) = (-1)^{\frac{e+1}{2}} \frac{((a-4)m-2e(a-2)+a)}{(m+1-a)} \cdot \begin{pmatrix} \frac{m-3}{2} \\ \frac{e-3}{2} \end{pmatrix};$$

$$(iii) \quad Q^*(16) = x(3) = (-1)^{\frac{e+1}{2}} \frac{((a-16)m^2+m(48e+16-8ae+4a))+8e^2(a-4)-8e(a+2)+3a}{(m+1-a)(m-1)(m-3)} \cdot \begin{pmatrix} \frac{m-1}{2} \\ \frac{e-3}{2} \end{pmatrix}.$$

Proof Each of the above results follows from Lemma 4.2.1 and the definition of  $Q^*(z)$  ■.  
 We suppose in Lemmas 4.3.2 and 4.3.3 that  $\Gamma(m,2)$  contains a non-trivial nearly perfect  $e$ -code.  
Lemma 4.3.2  $Q^*(1)$  and  $Q^*(16)$  are non-zero and of opposite sign for odd  $e$  with  $5 \leq e \leq 17$ .

Proof  $e > 1$  so  $\Gamma(m,2)/2$  contains a nearly perfect  $e$ -code. We can exclude the case where there is a single code vertex and since the diameter of  $\Gamma(m,2)/2$  is  $(m-1)/2$  we have  $m \geq 4e+3$ . Combining this with  $a = 2, 4, \dots, e-1$  we easily obtain the result ■

It now follows that if a binary nearly perfect  $e$ -code exists with  $e$  odd and  $5 \leq e \leq 17$  then we must have  $Q^*(4) = 0$ .

Lemma 4.3.3  $Q^*(4) \neq 0$  for odd  $e$  with  $5 \leq e \leq 17$ .

Proof Suppose  $Q^*(4) = 0$ . From <sup>the proof of</sup> Lemma 4.3.2  $m \geq 4e + 3$ . Hence for  $a \neq 2$

$$(4e+3)(a-4) + a - 2ae + 4e \leq 0$$

which implies  $a \leq \frac{6(e+1)}{(e+2)}$  and so  $a = 2$  or  $4$ . If  $a = 4$ ,  $Q^*(4) = 0$  implies  $e = 1$ . If  $a = 2$ ,  $Q^*(4) = 0$  implies  $m = 1$  ■

Combining these results we have

Theorem 4.3.4 There are no non-trivial nearly perfect binary  $e$ -codes for odd  $e$  with  $5 \leq e \leq 17$  ■

We now consider the existence of nearly perfect 1-codes and 2-codes over arbitrary alphabets.

**Lemma 4.3.5** The only nearly perfect 1-codes in  $\Gamma(m, q)$  which are not perfect are binary.

**Proof** For nearly perfect 1-codes which are not perfect we must have  $(m-1)(q-1) \not\equiv 0 \pmod{2}$  i.e. both  $m$  and  $q$  are even. Then the required polynomial  $x(\lambda) = \frac{\lambda(\lambda+2)}{m(q-1)}$  has distinct integer roots. By (4.2.2)  $q$  divides both  $m$  and  $m-2$ , hence  $q=2$  ■

Goethals and Snover [14] have shown that any binary nearly perfect 1-code is either perfect or a shortened perfect 1-code.

If  $\Gamma(m, q)$  contains a nearly perfect 2-code then the required polynomial  $x(\lambda)$  has three distinct integer roots which we denote by  $\lambda_1, \lambda_2, \lambda_3$ . From (4.2.2) we infer

$$3m + \sum \lambda_i \equiv 0 \pmod{q} \quad (4.3.2)$$

$$3m^2 + 2m \sum \lambda_i + \sum \lambda_i \lambda_j \equiv 0 \pmod{q^2} \quad (4.3.3)$$

$$m^3 + m^2 \sum \lambda_i + m \sum \lambda_i \lambda_j + \lambda_1 \lambda_2 \lambda_3 \equiv 0 \pmod{q^3} \quad (4.3.4)$$

(4.3.2) and (4.3.3) imply

$$m \sum \lambda_i + \sum \lambda_i \lambda_j \equiv 0 \pmod{q} \quad (4.3.5)$$

**Lemma 4.3.6** The only nearly perfect 2-codes in  $\Gamma(m, q)$  which are not perfect are binary.

**Proof** We must have  $b_2 = (m-2)(q-1) \not\equiv 0 \pmod{3}$  and so  $m \not\equiv 2 \pmod{3}$  and  $q \not\equiv 1 \pmod{3}$ . Let  $k = m(q-1) \equiv \alpha \pmod{3}$  and  $b_2 = (m-2)(q-1) \equiv \beta \pmod{3}$  where  $0 \leq \alpha < 3$  and  $0 < \beta < 3$ . Then by calculation we find

$$\Sigma \lambda_i = \alpha - \beta + q - 4 \quad (4.3.6)$$

$$\Sigma \lambda_i \lambda_j = q(\alpha - \beta - m) + m + 2\beta - 4\alpha + 2 \quad (4.3.7)$$

$$\lambda_1 \lambda_2 \lambda_3 = 2\alpha - m(q-1)(\alpha - \beta) \quad (4.3.8)$$

If we substitute for  $\Sigma \lambda_i$  and  $\Sigma \lambda_i \lambda_j$  in (4.3.2) and (4.3.5) and eliminate  $m$  then

$$(\alpha - \beta)^2 + 5\alpha + \beta + 6 \equiv 0 \pmod{q} \quad (4.3.9)$$

We consider the four possibilities:

(i) If  $m \equiv 0 \pmod{3}$  and  $q \equiv 2 \pmod{3}$  then  $\alpha = 0$  and  $\beta = 1$ . (4.3.9)

implies that  $q$  divides 8. Hence  $q = 2$  or 8. (4.3.2) implies that  $q$  divides  $3m-5$  and by inspection  $x(-1) = 0$  and so  $q$  divides  $m-1$ .

Hence  $q$  divides  $m+1$  and so  $q = 2$ .

(ii) If  $m \equiv 1 \pmod{3}$  and  $q \equiv 2 \pmod{3}$  then  $\alpha = 1$  and  $\beta = 2$ . (4.3.9)

implies that  $q$  divides 14. Hence  $q = 2$  or 14. As in (i)  $x(-1) = 0$  and the only possibility is  $q = 2$ . The sphere packing condition implies that  $(m+1)(m+2)$  divides  $2^{m+1}$  which is impossible.

(iii) If  $m \equiv 0 \pmod{3}$  and  $q \equiv 0 \pmod{3}$  then  $\alpha = 0$  and  $\beta = 2$ .

(4.3.9) implies that  $q$  divides 12. The sphere packing condition implies that

$$x(k) = (m^2(q-1)^2 - m(q-1)(q-5) - 2(q-2))/2$$

divides  $q^m$ . Since  $x(k) \equiv 2 \pmod{3}$   $q$  cannot be 3 and hence  $x(k) = 2^{2r-1}$  for some integer  $r$ . Then

$$m(q-1)(m(q-1) - q + 5) = 2^{2r} + 2(q-2) \quad (4.3.10)$$

and if  $q=6$  the right hand side of (4.3.10) must be divisible by 5 which is impossible since  $2^{2r} + 8$  always ends in 2 or 4.

If  $q = 12$  then  $4^r + 20$  must be divisible by 11 which is impossible.

(iv) If  $m \equiv 1 \pmod{3}$  and  $q \equiv 0 \pmod{3}$  then  $\alpha=2$  and  $\beta=1$ . (4.3.9)

implies that  $q$  divides 18. (4.3.5) and (4.3.2) imply that  $q$  divides  $m-7$  and (4.3.4) implies that  $q$  divides  $(m-1)(m^2-m-4)$ . Hence  $q$  divides 6.38 and so  $q = 3$  or  $6$ .

If  $q=3$  then  $x(k) = 2m^2+m+1$  is not divisible by 3. If  $q=6$  then

$$x(\lambda) = (\lambda^3 - 3\lambda^2 - 5(m-2)\lambda + 5m - 4)/(5m-2)$$

and the eigenvalues of  $\Gamma(m,6)$  are  $5m, 5m-6, \dots, 5, -1, \dots, -m$ .

By inspection we see that  $x(\lambda)$  has exactly one negative root. Let

$r, s, -t$  denote the roots of  $x(\lambda)$  where  $r, s, t$  are positive integers.

Hence  $r \geq 5, s \geq 5, t \geq 1$  and

$$rs - rt - st = -5m + 2$$

$$rst = 5m - 4$$

which imply

$$(st-2)/(st+s-t) = r \geq 5$$

and so

$$\begin{aligned} s &\leq (5t-2)/(4t+5) \\ &= 1 + (t-7)/(4t+5) . \end{aligned}$$

This is impossible since  $s \geq 5$  ■

Also in [14] Goethals and Snover have shown that any binary nearly perfect 2-codes have  $m = 4^r - 1$  and in fact one such family is the Preparata codes [30] .

#### 4.4 Completely regular codes in $\Gamma(m,q)$

Independently of [14] Goethals and van Tilborg [15] have defined completely regular codes in the case corresponding to the graph  $\Gamma(m,q)$ . They have also given definitions of  $t$ -regular and generalised  $i^{\text{th}}$  uniformly packed codes. Their paper contains many examples of completely regular 1-codes with external distance 2.

It is worth remarking that every example of a binary completely regular  $e$ -code in [15] with external distance  $e+1$  satisfies the condition  $\lambda_{e+1} > 1$  so the derived graph  $\Gamma(m,2)/2$  contains a completely regular  $e$ -code with the same parameters.

In this section we do not wish to repeat the work of Goethals and van Tilborg in [15] but we shall give two examples of parameter sets not contained therein. The first of these examples is connected with orthogonal latin squares and the second is still an open case.

##### Example 1

A latin square is a square matrix with  $q^2$  entries of  $q$  different symbols (usually the integers  $0, 1, \dots, q-1$ ) none of which occur twice within any row or column of the matrix. The integer  $q$  is called the order of the latin square.

Two latin squares  $L_1 = [a_{ij}]$  and  $L_2 = [b_{ij}]$  on  $q$  symbols  $0, 1, \dots, q-1$  are said to be orthogonal if every ordered pair of symbols occurs exactly once among the  $q^2$  pairs  $(a_{ij}, b_{ij})$  for  $i, j \in \{0, 1, \dots, q-1\}$ .

Using  $t$  latin squares we can construct a  $q$ -ary code in  $\Gamma(t+2, q)$  ([11, page 355]). Let  $L_s = [a_{ij}(s)]$  ( $s=1, 2, \dots, t$ ) be

$t$  latin squares of order  $q$ . Then the  $q^2$   $t+2$ -tuples  $(i, j, a_{ij}(1), \dots, a_{ij}(t))$  may be regarded as a set of code vertices in  $\Gamma(t+2, q)$ .

In [16] Golomb and Posner obtained the following connection between mutually orthogonal latin squares and error-correcting codes:

Theorem 4.4.1 (Golomb and Posner). The following concepts are equivalent :

- (i) a set of  $t$  mutually orthogonal latin squares of order  $q$ ;
- (ii) a code of length  $t+2$  and minimum distance  $t+1$  having  $q^2$  elements constructed from a  $q$ -ary alphabet.

We illustrate Theorem 4.4.1 with an example. We use two orthogonal latin squares of order 3

$$L_1 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \quad \text{and} \quad L_2 = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix}$$

and construct the 1-code  $C$  in  $\Gamma(4, 3)$  with elements

$$\begin{array}{lll} (0, 0, 0, 0) & (1, 1, 2, 0) & (2, 2, 1, 0) \\ (0, 1, 1, 2) & (1, 2, 0, 2) & (1, 0, 1, 1) \\ (0, 2, 2, 1) & (2, 0, 2, 2) & (2, 1, 0, 1) \end{array}$$

In fact  $C$  is a perfect 1-code in  $\Gamma(4, 3)$  and this is the only occasion when a perfect 1-code arises from this construction. However, in our next result we prove that for  $q > 3$  we obtain a completely regular 1-code with external distance 2.

Theorem 4.4.2 The following are equivalent for  $q > 3$ :

- (i) a pair of orthogonal latin squares of order  $q$ ;
- (ii) a completely regular 1-code in  $\Gamma(4, q)$  with external distance 2 and parameters  $p_{21}(C) = 3$ ,  $p_{22}(C) = 6$ .

Proof To prove (ii)  $\Rightarrow$  (i) we need only use the fact that the code has  $q^2$  elements and apply Theorem 4.4.1.

In order to prove the converse we first show that the 1-code  $C$  constructed from  $L_1 = [a_{ij}]$  and  $L_2 = [b_{ij}]$  has external distance 2. If  $u = (\alpha, \beta, \gamma, \delta)$  is any vertex of  $\Gamma(4, q)$  then the code vertex  $x = (\alpha, \beta, a_{\alpha\beta}, b_{\alpha\beta})$  satisfies  $\partial(u, x) \leq 2$ . If the code is perfect then by the sphere packing condition  $q^2 = 1 + 4(q-1)$  and so  $q=1$  or  $3$ . Hence  $C$  has external distance 2.

It only remains to show that  $p_{21}(C, u)$  and  $p_{22}(C, y)$  are independent of the choice of  $u$  and  $y$  and take the values 3 and 6 respectively. Let  $\partial(u, v) = 1$  for  $v \in C$  and  $\partial(x, u) \geq 2$  for all  $x \in C \setminus \{v\}$ . Suppose  $v = (\alpha, \beta, \gamma, \delta)$  and  $u = (\alpha, \beta, \gamma', \delta)$  where  $\gamma \neq \gamma'$ . If  $w \in C$  and  $\partial(u, w) = 2$  then  $w = (\epsilon, \xi, \gamma', \eta)$  where exactly one of the equations  $\epsilon = \alpha, \xi = \beta, \eta = \delta$  holds. Having decided which of these does hold, the remaining components of  $w$  are uniquely determined by the definition of orthogonal latin squares. Hence  $p_{21}(C, u) = 3$ . A similar argument holds when  $u \in \{(\alpha', \beta, \gamma, \delta), (\alpha, \beta', \gamma, \delta), (\alpha, \beta, \gamma, \delta')\}$ .

Let  $\partial(y, v) = 2$  for  $v \in C$  and  $\partial(y, x) \geq 2$  for all  $x \in C$ . Suppose  $v = (\alpha, \beta, \gamma, \delta)$  and  $y = (\alpha', \beta', \gamma, \delta)$ . If  $w = (\epsilon, \xi, \eta, \theta) \in C$  and  $\partial(w, y) = 2$  then either  $\epsilon = \alpha'$  or  $\xi = \beta'$  (but not both) and exactly one of  $\eta = \gamma, \theta = \delta$  holds or  $\epsilon = \alpha', \xi = \beta', \eta \neq \gamma$  and  $\theta \neq \delta$ . In each of these five cases the remaining unknown components of  $w$  are uniquely determined by the definition of orthogonal latin

squares. Hence  $p_{22}(C, y) = 6$ . A similar argument holds if  $y \in \{(\alpha', \beta, \gamma', \delta), (\alpha', \beta, \gamma, \delta'), (\alpha, \beta', \gamma', \delta), (\alpha, \beta', \gamma, \delta'), (\alpha, \beta, \gamma', \delta')\}$  ■

We apply the polynomial condition with  $x(\lambda) = (\lambda - q + 4)(\lambda + 4)/12$ . The roots of  $x(\lambda)$  are always eigenvalues of  $\Gamma(4, q)$ . This is to be expected since it is known ([8]) that a pair of orthogonal latin squares exists for every order  $q$  except  $q=6$  in which case such a pair does not exist ([42]).

Example 2 We end this section with an example of a set of parameters which is still an open case.

Let  $\alpha^2 = 4^s$  where  $s$  is a positive integer and let  $m = 2\alpha^2 + \alpha$ . Suppose that  $C$  denotes a completely regular 1-code in  $\Gamma(m, 2)$  with external distance 2 and parameters

$$p_{22}(C) = p_{21}(C) = (\alpha^2 + \alpha)/2.$$

Then by simple calculation we find

$$x(\lambda) = (\lambda - \alpha)(\lambda + \alpha)/(\alpha^2 + \alpha)$$

and

$$x(k) = 4\alpha^2 = 4^{s+1}.$$

These parameters satisfy both the polynomial and sphere packing conditions.

Since  $j_2 = (2\alpha + 1)(\alpha - 1) > 1$   $\alpha$  and  $-\alpha$  must be eigenvalues of  $\Gamma(m, 2)/2$ .

This is also true provided  $s \geq 2$ .

One possible construction of a code with these parameters arises from a result of Goethals and van Tilborg [15]. Before we discuss this, however, we must define some concepts of classical coding theory.

We say that a code  $C$  in  $\Gamma(m, q)$  is linear if  $C$  is a subspace of the vector space represented by  $\Gamma(m, q)$ . The dual (orthogonal) code  $C^\perp$  of a linear code  $C$  is defined by:

$$C^\perp = \{u \in \Gamma(m, q) \mid (u, v) = 0 \text{ for each } v \in C\}$$

where  $(u, v)$  denotes the usual inner product of vectors over a  $q$ -ary field.

The weight vector  $p(0)$  of  $C$  in  $\Gamma(m, q)$  is sometimes expressed as a polynomial  $A(z)$  in an indeterminate  $z$

$$A(z) = \sum_{i=0}^m p_{i0}(C) z^i = \underline{z} \cdot \underline{p}(0)$$

where  $\underline{z} = [1, z, z^2, \dots, z^m]$ . If  $A(z)$  and  $B(z)$  respectively represent the weight vectors of a linear code  $C$  and its dual code  $C^\perp$  then the following equality holds ( [24, page 121] )

$$|C| \cdot B(z) = (1 + (q-1)z)^m A\left(\frac{1-z}{1+(q-1)z}\right) \quad (4.4.1)$$

((4.4.1) is usually called the MacWilliams identity.)

Theorem 4.4.3 (Goethals and van Tilborg). A linear 1-code  $C$  is completely regular with external distance 2 if and only if its dual code  $C^\perp$  contains only vertices at two distinct distances from the code vertex  $(0, 0, \dots, 0)$  ■

In the proof of the above theorem ( [15, page 21] ) Goethals and van Tilborg establish that if  $C^\perp$  has weight enumerator  $B(z) = 1 + N_1 z^{w_1} + N_2 z^{w_2}$  then the parameters of  $C$  are given by

$$2p_{21}(C) = (m-1)(q-1) + (m(q-1) - qw_1 + 1)(m(q-1) - qw_2 + 1) \quad (4.4.2)$$

$$2p_{22}(C) = m(q-1) + (m(q-1) - qw_1)(m(q-1) - qw_2) \quad (4.4.3)$$

We return now to the case in hand. If a linear binary code  $D$  exists with weight vector represented by

$$D(z) = 1 + (2^{\alpha^2 - \alpha - 1})z^{\alpha^2} + (2^{\alpha^2} + \alpha)z^{\alpha^2 + \alpha}$$

then the dual code  $D^\perp$  has, by (4.4.1), weight enumerator

$$A(z) = \frac{1}{4^{\alpha^2}} ((1+z)^{2^{\alpha^2} + \alpha} + (2^{\alpha^2} + 1)(1-z)^{2^{\alpha^2}} \{ (\alpha+1)(1+z)^\alpha + \alpha(1-z)^\alpha \})$$

$D^\perp$  is obviously a 1-code and if we let  $C = D^\perp$  and apply Theorem 4.4.3 we see that  $C$  is completely regular with parameters given by (4.4.2) and (4.4.3). By substitution we find  $p_{21}(C) = p_{22}(C) = (\alpha^2 + \alpha)/2$ . So one method of construction of a completely regular 1-code with these parameters would be to construct first a linear code with weight vector represented by  $D(z)$ .

## 5. Codes in the graphs $O_k$

5.1 The graphs  $O_k$  (sometimes referred to as the odd graphs) have been studied by various authors ([7], [18], [29]). The vertex set of  $O_k$  is the set of  $(k-1)$ -subsets of  $\{1, 2, \dots, 2k-1\}$  and two vertices are joined if and only if their labels are disjoint. For example  $O_2$  is the complete graph on three vertices and  $O_3$  is Petersen's graph.

For  $k \geq 2$  the graphs  $O_k$  are distance-regular with diameter  $k-1$ . The intersection array is

$$\left\{ \begin{array}{ccccccc} * & 1 & 1 & \dots & r-2 & r-2 & r-1 & r-1 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & r \\ 2r-1 & 2r-2 & 2r-2 & \dots & r+1 & r+1 & r & * \end{array} \right\} \quad \begin{array}{l} \text{for } k=2r-1, \\ \text{and} \end{array}$$

$$\left\{ \begin{array}{ccccccc} * & 1 & 1 & \dots & r-1 & r-1 & r \\ 0 & 0 & 0 & \dots & 0 & 0 & r \\ 2r & 2r-1 & 2r-1 & \dots & r+1 & r+1 & * \end{array} \right\} \quad \text{for } k=2r$$

The eigenvalues of  $O_k$  are  $\lambda_i = (-1)^i (k-i)$  ( $0 \leq i \leq k-1$ ). The labels of a vertex  $u$  and any vertex  $v \in \Gamma_i(u)$  have  $(i-1)/2$  elements in common if  $i$  is odd and  $k-1-(i/2)$  if  $i$  is even. Then for vertices  $x$  and  $y$  of  $O_k$

$$\partial(x, y) \geq 2e+1 \text{ if and only if } e \leq |x \cap y| \leq k-e-2 \quad (5.1.1)$$

Using the graph  $O_k$  we can construct another distance-regular graph  $2.O_k$ . The  $k$ -valent graph  $2.O_k$  has  $2 \cdot \binom{2k-1}{k-1}$  vertices indexed by the sets  $(x, i)$  where  $x$  is a  $k-1$  subset of  $\{1, 2, \dots, 2k-1\}$  and  $i \in \{0, 1\}$ . Two vertices  $(x, i)$  and  $(y, j)$  are adjacent if and only if  $x$  and  $y$  are disjoint and  $i \neq j$ .  $2.O_k$  has intersection array

$$\left\{ \begin{array}{cccccc} * & 1 & 1 & \dots & k-1 & k-1 & k \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ k & k-1 & k-1 & \dots & 1 & 1 & * \end{array} \right\}$$

and eigenvalues  $\lambda_i = \pm(k-i)$  ( $0 \leq i \leq k-1$ ).

We note that  $2.O_k$  is an antipodal distance-regular graph with derived graph  $O_k$ .

## 5.2 Construction of codes in $O_k$

The main result of this section is that given an e-code in  $\Gamma(2k-1, 2)$  we can, under certain circumstances, construct an e-code in  $O_k$ . We illustrate this result by investigating the possibility of constructing a perfect 1-code in  $O_k$  using the binary Hamming codes mentioned earlier.

The graph  $\Gamma(m, 2)$  is antipodal and each vertex  $x$  of  $\Gamma(m, 2)$  has a unique antipodal vertex  $x' = (1, 1, \dots, 1) + x$  (the component addition being modulo 2). We shall call an e-code  $C$  in  $\Gamma(m, 2)$  antipodal if the antipodal vertex of each element of  $C$  is also contained in  $C$ .

Lemma 5.2.1 If  $C$  is an antipodal e-code in  $\Gamma(2k-1, 2)$  then the vertices of weight  $k-1$  form an e-code in  $O_k$ .

Proof Suppose  $x, y$  are elements of  $C$  of weight  $k-1$ . From the definition of the distance function  $\partial'$  in  $\Gamma(2k-1, 2)$

$$\begin{aligned} \partial'(x, y) &= \text{number of places in which } x \text{ and } y \text{ differ} \\ &= 2k-2-2|x \cap y| \end{aligned} \quad (5.2.1)$$

$C$  is antipodal so  $y' = (1, 1, \dots, 1) + y \in C$  and  $\partial'(x, y') \geq 2e+1$ .  
 Then  $2e+1 < \partial'(x, y') = 2k-1 - \partial'(x, y)$  and using (5.2.1)  $|x \wedge y| \geq e$ .  
 Similarly  $\partial'(x, y) \geq 2e+1$  implies that  $|x \wedge y| \leq k-e-2$  and the result follows from (5.1.1) ■

The perfect binary Hamming 1-codes in  $\Gamma(m, 2)$  have vertices of weight  $(m+1)/2$  where  $m=2^r-1$  ([24, page 25]). If  $k = 2^{r-1}$  and  $m = 2k-1$  then by applying Lemma 5.2.1 we obtain a 1-code in  $O_k$ .

The perfect Hamming 1-code in  $\Gamma(7, 2)$  is the first non-trivial case to consider. This code has seven vertices of weight 3 which form the perfect 1-code  $\{123, 145, 167, 246, 257, 347, 356\}$  in  $O_4$ .

We prove now that this is the only occasion when the construction gives a perfect 1-code in  $O_k$ .

Lemma 5.2.2 If  $k \geq 4$  the vertices of weight  $k-1$  in the Hamming code in  $\Gamma(2k-1, 2)$  form a 1-code in  $O_k$  which is not perfect.

Proof Let  $k = 2^{r-1}$  and suppose  $r \geq 4$ . If  $p(0)$  is the weight vector of the binary Hamming code in  $\Gamma(2k-1, 2)$  and  $\underline{z} = [1, z, z^2, \dots, z^{2k-1}]$  then from [24, page 25]

$$\begin{aligned} \underline{z}p(0) &= \frac{1}{2k} (1+z)^{2k-1} + \frac{2k-1}{2k} (1+z)^{k-1} (1-z)^k \\ &= \frac{1}{2k} (1+z)^{2k-1} + \frac{2k-1}{2k} (1-z^2)^{k-1} (1+z) \end{aligned} \quad (5.2.2)$$

From (5.2.2)  $p_{k-1, 0}(C) = \frac{1}{2k} \binom{2k-1}{k-1} + \frac{2k-1}{2k} \binom{k-1}{k/2-1}$ . If these vertices of weight  $k-1$  form a perfect 1-code in  $O_k$  then by the sphere packing condition

$$\frac{1}{2k} \binom{2k-1}{k-1} + \frac{2k-1}{2k} \binom{k-1}{k/2-1} = \frac{1}{1+k} \binom{2k-1}{k-1} \quad (5.2.3)$$

Let  $\alpha_r = \binom{2r-1}{r-1}$  then (5.2.1) can be rewritten as

$$(k+1)(2k-1)\alpha_{k/2} = (k-1)\alpha_k \quad (5.2.4)$$

Now  $\alpha_k = 2^{k/2} (2-1/k) (2-1/(k-1)) \dots (2-1/(k/2+1)) \alpha_{k/2}$  and hence

$$\alpha_k \geq 2^{k/2} \alpha_{k/2} \quad (5.2.5)$$

(5.2.4) and (5.2.5) imply that  $2^{k/2} \leq 2k+4$  which is impossible for  $k=2^{r-1}$  unless  $k=8$ . The result follows because  $k=8$  does not satisfy (5.2.3) ■

### 5.3 The eigenvector sequence for $O_k$

We use the eigenvector sequence for  $O_k$  to obtain results about the roots of  $x_e(\lambda)$  for  $e > 1$ . We hope that these results may prove to be useful in future work on non-existence results for  $O_k$ .

Some of the results require only a simple inductive proof which we shall sometimes omit or indicate briefly.

The eigenvector sequence for  $O_k$  is defined as follows:

$$v_0(\lambda) = 1, v_1(\lambda) = \lambda,$$

$$(s+1)v_{2s+1}(\lambda) + (k-s)v_{2s-1}(\lambda) = \lambda v_{2s}(\lambda) \quad (1 \leq s \leq [(k-2)/2]) \quad (5.3.1)$$

$$(s+1)v_{2s+2}(\lambda) + (k-s)v_{2s}(\lambda) = \lambda v_{2s+1}(\lambda) \quad (0 \leq s \leq [(k-3)/2]) \quad (5.3.2)$$

A much more useful form of these equations can be obtained from a simple inductive argument applied to (5.3.1) and (5.3.2) :

$$\text{for } x_i(\lambda) = \sum_{j=0}^i v_j(\lambda)$$

$$(s+1)x_{2s+1}(\lambda) + (k-s)x_{2s-1}(\lambda) = (\lambda+1)x_{2s}(\lambda) \quad (1 \leq s \leq [(k-2)/2]) \quad (5.3.3)$$

$$(s+1)x_{2s+2}(\lambda) + (k-s-1)x_{2s}(\lambda) = \lambda x_{2s+1}(\lambda) \quad (0 \leq s \leq [(k-3)/2]) \quad (5.3.4)$$

Lemma 5.3.1 For  $s=0,1,\dots, [(k-2)/2]$

$$x_{2s+1}(-1) = 0 \quad (5.3.5)$$

Proof This follows from an inductive argument applied to (5.3.3) ■

Corollary 5.3.2 If  $O_k$  contains a perfect  $e$ -code with  $e$  odd, then  $k$  is even.

Proof Suppose  $O_k$  contains a perfect  $e$ -code with  $e$  odd. By Theorem 2.3.8 the roots of  $x_e(\lambda)$  are eigenvalues of  $O_k$ . Then  $-1$  is an eigenvalue and since the eigenvalue of smallest absolute value is  $(-1)^{k+1}$   $k$  is even ■

Lemma 5.3.3 For  $0 \leq s \leq [(k-2)/2]$

- (i)  $x_{2s}(0) = x_{2s+1}(0) = (-1)^s \binom{k-1}{s}$  ;
- (ii)  $x_{2s}(1) = (-1)^s \frac{(k-2s-1)}{(k-1)} \binom{k-1}{s}$ ,  $x_{2s+1}(1) = (-1)^s 2 \binom{k-2}{s}$  ;
- (iii)  $x_{2s}(2) = (-1)^s \frac{(k^2-3k+6ks+6s^2+6s+2)}{(k-1)(k-2)} \binom{k-1}{s}$  ,  
 $x_{2s+1}(2) = (-1)^s 3 \frac{(k-2s-2)}{(k-2)} \binom{k-2}{s}$  .

Proof These results follow from inductive arguments applied to (5.3.3) and (5.3.4) ■

Lemma 5.3.4 For  $0 \leq s \leq [(k-2)/2]$

- (i)  $x_{2s}(\lambda) = x_{2s}(-\lambda-1)$  ;
- (ii)  $\lambda x_{2s+1}(\lambda) = -(\lambda+1)x_{2s+1}(-\lambda-1)$ .

Proof By simple calculation we can show that (i) and (ii) hold for  $s=0$  and  $1$ . We suppose inductively that (i) and (ii) hold

for  $s \leq m$ . If we replace  $\lambda$  by  $-\lambda-1$  in (5.3.4) and use the inductive hypothesis

$$(m+1)x_{2m+2}^{(-\lambda-1)} + (k-m-1)x_{2m}^{(\lambda)} = \lambda x_{2m+1}^{(\lambda)} \quad (5.3.6)$$

$$\text{Comparing (5.3.6) and (5.3.3) } x_{2m+2}^{(\lambda)} = x_{2m+2}^{(-\lambda-1)}.$$

Similarly from (5.3.3) for  $s=m+1$

$$-(\lambda+1)(m+2)x_{2m+3}^{(-\lambda-1)} + (k-m-1)x_{2m+1}^{(\lambda)} = (\lambda^2 + \lambda)x_{2m+2}^{(\lambda)} \quad (5.3.7)$$

Comparing (5.3.7) and (5.3.3) for  $m+1$  we have

$$-(\lambda+1)x_{2m+3}^{(-\lambda-1)} = \lambda x_{2m+3}^{(\lambda)}$$

and this completes the proof ■

From Lemma 5.3.4 we can already see that if  $\alpha$  is a root of  $x_e(\lambda)$  and  $\alpha \neq -1$  then  $-\alpha-1$  is also a root.

Theorem 5.3.5 If  $x_e(\lambda)$  has roots  $\lambda_1, \lambda_2, \dots, \lambda_e$  then

$$\lambda_1 + \lambda_2 + \dots + \lambda_e = -[(e+1)/2] \quad (5.3.8)$$

$$\lambda_1 \lambda_2 \dots \lambda_e = (-1)^{e+[e/2]} [(e+1)/2]! [e/2]! \binom{k-1}{[e/2]} \quad (5.3.9)$$

Proof (5.3.8) follows from Lemma 5.3.1 and the observation made after Lemma 5.3.4.

By differentiating (5.3.3) and (5.3.4) to the order of the highest power of  $\lambda$  and using the notation  $f^{(t)}(\lambda) = \left(\frac{d}{d\lambda}\right)^t(f(\lambda))$

$$[(r+2)/2] x_{r+1}^{(r+1)}(0) = (r+1) x_r^{(r)}(0) \quad (0 \leq r \leq k-2) \quad (5.3.10)$$

and so,

$$x_{r+1}^{(r+1)}(0) = \frac{(r+1)!}{[(r+2)/2]! [(r+1)/2]!} \quad (0 \leq r \leq k-2) \quad (5.3.11)$$

Hence the coefficient of  $\lambda^e$  in  $x_e(\lambda)$  is  $1/[(e+1)/2]![e/2]!$  and

$$\begin{aligned}\lambda_1 \lambda_2 \dots \lambda_e &= (-1)^e [(e+1)/2]![e/2]! x_e(0) \\ &= (-1)^{e+[e/2]} [(e+1)/2]![e/2]! \binom{k-1}{[e/2]}\end{aligned}$$

by Lemma 5.3.3 ■

It will be useful to separate the odd and even cases of  $e$ .

We suppose that  $x_{2r}(\lambda)$  has roots  $\alpha_1, \alpha_2, \dots, \alpha_r, -(\alpha_1+1), \dots, -(\alpha_r+1)$ . In order that we can find  $\sum_{i=1}^r \alpha_i(\alpha_i+1)$  we shall need  $\sum_i \lambda_i$  which involves our finding the coefficient of  $\lambda^{r-2}$  in  $x_r(\lambda)$ .

Lemma 5.3.6 (i)  $x_{2r+1}^{(2r)}(0) = \binom{2r}{r}$ ,  $x_{2r+2}^{(2r+1)}(0) = \binom{2r+1}{r}$  ;

$$(ii) \quad x_{2r+1}^{(2r-1)}(0) = -\frac{(6k-4r-5)}{6} \binom{2r-1}{r-1},$$

$$x_{2r+2}^{(2r)}(0) = \frac{((r+2)(4r+3)-6k(r+1))}{6(r+1)} \binom{2r}{r}.$$

Proof (i) From (5.3.3) and (5.3.4)

$$\begin{aligned}x_{2s+1}^{(2s)}(0) &= \frac{2s}{s+1} \cdot x_{2s}^{(2s-1)}(0) + \frac{x_{2s}^{(2s)}(0)}{s+1} \\ &= \frac{2s}{s+1} x_{2s}^{(2s-1)}(0) + \frac{(-1)^s (2s)!}{(s+1)!s!}\end{aligned} \quad (5.3.12)$$

and

$$x_{2s+2}^{(2s+1)}(0) = \frac{2s+1}{s+1} x_{2s+1}^{(2s)}(0) \quad (5.3.13)$$

The proof follows from an inductive argument on (5.3.12) and (5.3.13).

(ii) Also from (5.3.3) and (5.3.4) we have

$$\begin{aligned}x_{2s+2}^{(2s)}(0) &= \frac{2s}{s+1} \cdot x_{2s+1}^{(2s-1)}(0) - \frac{(k-s-1)}{(s+1)} \cdot x_{2s}^{(2s)}(0) \\ &= \frac{2s}{s+1} \cdot x_{2s+1}^{(2s-1)}(0) - \frac{(k-s-1)}{s+1} \cdot (-1)^s \binom{2s}{s}\end{aligned} \quad (5.3.14)$$

and

$$\begin{aligned}
 x_{2s+1}^{(2s-1)}(0) &= \frac{(2s-1)}{s+1} \cdot x_{2s}^{(2s-2)}(0) + \frac{x_{2s}^{(2s-1)}(0)}{s+1} - \frac{(k-s)}{s+1} \cdot x_{2s-1}^{(2s-1)}(0) \\
 &= \frac{(2s-1)}{s+1} \cdot x_{2s}^{(2s-2)}(0) - \frac{(k-s-1)}{s+1} \cdot \binom{2s-1}{s-1} \quad (5.3.15)
 \end{aligned}$$

The proof is completed by an inductive argument on (5.3.14) and (5.3.15) ■

If  $e=2r+1$  then

$$\Sigma \lambda_i \lambda_j = \frac{x_{2r+1}^{(2r-1)}(0)}{(2r-1)!} \cdot \frac{(2r+1)!}{x_{2r+1}^{(2r+1)}(0)} = \frac{-r(r+1)(6k-4r-5)}{6}$$

and since  $\Sigma \lambda_i \lambda_j = \frac{r(r+1)}{2} - \sum_{i=1}^r \alpha_i(\alpha_i+1)$

$$\sum_{i=1}^r \alpha_i(\alpha_i+1) = \frac{r(r+1)}{3} (3k-2r-1) \quad (5.3.16)$$

Similarly if  $e = 2r$

$$\Sigma \lambda_i \lambda_j = \frac{-r}{6} (6kr - (r+1)(4r-1))$$

and

$$\sum_{i=1}^r \alpha_i(\alpha_i+1) = \frac{r}{3} (3kr - 2r^2 - 1) \quad (5.3.17)$$

#### 5.4 Perfect codes in $O_k$

We shall divide §5.4 into five parts: in part (a) we obtain a lower bound on  $k$ ; in parts (b), (c), (d) and (e) we investigate the existence of perfect 1-codes, 2-codes, 3-codes and 4-codes respectively.

A result which seems worth mentioning is that  $O_k$  contains a perfect  $e$ -code if and only if  $2.O_k$  contains a perfect  $e$ -code.

This follows easily from the results of §3.3 and the definitions of  $O_k$  and  $2.O_k$ .

a) A lower bound

The method we use here has already been employed by D.H. Smith to obtain an analogous bound in  $\Gamma(m, 2)$  [26, page 162].

Theorem 5.4.1 If  $O_k$  contains a non-trivial  $e$ -code then  
 $k \geq \frac{e^2+4e+2}{2}$  ( $e$  even) and  $k \geq \frac{e^2+4e+3}{2}$  ( $e$  odd).

Proof Case 1  $e=2r$ . We assume that  $p_{2e+1,0}(C)$  is non-zero. Notice that  $\partial(x, y) = e-2, e-1, e$  respectively as the labels of  $x$  and  $y$  have  $k-r, r-1, k-r-1$  elements in common. Also the labels of  $\Gamma_0(x)$  and  $\Gamma_{e+1}(x)$ ,  $\Gamma_{e+2}(x)$ ,  $\Gamma_{e+3}(x)$  have respectively  $r, k-2-r, r+1$  elements in common.

Similarly, the labels of  $\Gamma_0(x)$  and  $\Gamma_{2e+1}(x)$ ,  $\Gamma_{2e+2}(x)$ ,  $\Gamma_{2e+3}(x)$  have respectively  $2r, k-2-2r, 2r+1$  elements in common.

First we count in two ways the vertices of  $\Gamma_{e+1}(x)$ . Each vertex of  $\Gamma_{e+1}(x)$  is at distance  $e$  from exactly one code vertex of  $\Gamma_{2e+1}(x)$ . Let the vertex of  $\Gamma_{e+1}(x)$  have  $q$  elements of the labelling set in common with  $\Gamma_0(x)$  and the code vertex of  $\Gamma_{2e+1}(x)$ :

$$\begin{aligned} k_{e+1} &= \binom{k-1}{r} \binom{k}{r+1} = p_{2e+1,0}(C) \cdot \sum_{q=0}^r \binom{2r}{q} \binom{k-1-2r}{r-q} \binom{k-1-2r}{k-1-r-q} \binom{2r+1}{q} \\ &= p_{2e+1,0}(C) \binom{2r}{r} \binom{2r+1}{r}. \end{aligned}$$

Similarly, counting in two ways the vertices of  $\Gamma_{e+2}(x)$ :

$$k_{e+2} = \binom{k-1}{r+1} \binom{k}{r+1} = p_{2e+2,0}(C) \cdot \sum_{q=0}^{k-2-2r} \binom{k-2-2r}{q} \binom{2r+1}{k-2-r-q} \binom{2r+1}{k-1-r-q} \binom{k-2r-1}{q-k+2r+2}$$

$$\begin{aligned}
& + p_{2e+1,0}(C) \cdot \sum_{q=0}^{r-1} \binom{2r}{q} \binom{k-1-2r}{r-1-q} \binom{k-1-2r}{k-2-r-q} \binom{2r+1}{q+2} \\
& = p_{2e+2,0}(C) \binom{2r+1}{r} \binom{2r+1}{r+1} + p_{2e+1,0}(C) \binom{2r}{r-1} \binom{2r+1}{r+1}
\end{aligned}$$

We combine these equations to obtain

$$\frac{k-r+1}{r+1} = \frac{r}{r+1} + \frac{2r+1}{r+1} \cdot (p_{2e+2,0}(C)/p_{2e+1,0}(C)).$$

Now counting  $\Gamma_{e+3}(x)$  in two ways:

$$\begin{aligned}
k_{e+3} &= \binom{k-1}{r+1} \binom{k}{r+2} = p_{2e+3,0}(C) \cdot \sum_{q=0}^{m+1} \binom{2r+1}{q} \binom{k-2r-2}{r+1-q} \binom{k-2r-2}{k-1-r-q} \binom{2r+2}{q-1} \\
& + p_{2e+2,0}(C) \cdot \sum_{q=0}^{m-1} \binom{k-2-2r}{q} \binom{2r+1}{r+1-q} \binom{2r+1}{r-1-q} \binom{k-2r-1}{k-2r-1-q} \\
& + p_{2e+1,0}(C) \cdot \left[ \sum_{q=0}^{r+1} \binom{2r}{q} \binom{k-1-2r}{r+1-q} \binom{k-1-2r}{k-r-q} \binom{2r+1}{q-2} \right. \\
& \quad \left. + \sum_{q=0}^{r+1} \binom{2r}{q} \binom{k-1-2r}{r+1-q} \binom{k-1-2r}{k-1-r-q} \binom{2r+1}{q-1} \right] \\
& = p_{2e+3,0}(C) \cdot \binom{2r+1}{r} \binom{2r+2}{r} + p_{2e+2,0}(C) \binom{2r+1}{r+1} \binom{2r+1}{r-1} \\
& + p_{2e+1,0}(C) \left[ \binom{2r}{r+1} \binom{2r+1}{r-1} + \binom{2r}{r} \binom{2r+1}{r-1} (k-2r-1) + \binom{2r}{r+1} \binom{2r+1}{r} \right]
\end{aligned}$$

Eliminating  $p_{2e+2,0}(C)$  from these two equations gives

$$p_{2e+3,0}(C)/p_{2e+1,0}(C) = \frac{k^2 - 2k(r^2 + 3r + 1) + (4r^3 + 10r^2 + 6r + 1)}{(2r+2)(2r+1)}$$

Because  $p_{2e+3,0}(C)/p_{2e+1,0}(C) \geq 0$ ,  $k \leq \frac{4r+2}{2}$  or

$k \geq \frac{4r^2 + 8r + 2}{2}$ . Hence  $k \leq e+1$ , which corresponds to a trivial code,  
or  $k \geq \frac{e^2 + 4e + 2}{2}$ .

Case 2  $e=2r+1$ . Again we assume  $p_{2e+1,0}(C)$  is not zero. In this case  $\partial(x,y) = e-2, e-1, e$  respectively as the labels of  $x$  and  $y$  have  $r-1, k-r-1, r$  elements in common. Also the labels of  $\Gamma_0(x)$  and  $\Gamma_{e+1}(x), \Gamma_{e+2}(x), \Gamma_{e+3}(x)$  have respectively  $k-2-r, r+1, k-3-r$  elements in common. Similarly the labels of  $\Gamma_0(x)$  and  $\Gamma_{2e+1}(x), \Gamma_{2e+2}(x), \Gamma_{2e+3}(x)$  have respectively  $2r+1, k-3-2r, 2r+2$  elements in common.

The proof goes through in the same way, the relevant equations being

$$\begin{aligned} \binom{k}{r+1} \binom{k-1}{r+1} &= p_{2e+1,0}(C) \cdot \binom{2r+1}{r} \binom{2r+2}{r+1} \\ \binom{k}{r+2} \binom{k-1}{r+1} &= \binom{2r+2}{r+1} \binom{2r+2}{r} p_{2e+2,0}(C) + \binom{2r+1}{r+1} \binom{2r+2}{r} p_{2e+1,0}(C) \\ \binom{k}{r+2} \binom{k-1}{r+2} &= \binom{2r+2}{r} \binom{2r+3}{r+2} p_{2e+3,0}(C) + \binom{2r+2}{r} \binom{2r+2}{r+2} p_{2e+2,0}(C) \\ &\quad + p_{2e+1,0}(C) \cdot \left[ \binom{2r+1}{r-1} \binom{2r+2}{r+2} + (k-2-2r) \binom{2r+1}{r-1} \binom{2r+2}{r+1} \right. \\ &\quad \left. + (k-2-2r) \binom{2r+1}{r} \binom{2r+2}{r+2} \right] \end{aligned}$$

Again eliminating  $p_{2e+2,0}(C)$  we have

$$(2r+2)(2r+3)p_{2e+3,0}(C)/p_{2e+1,0}(C) = k^2 - \frac{k}{2}(2r+6) + \frac{1}{2}(2r+2)^2(2r+4)$$

so  $(k - \frac{(e+1)}{2} \cdot (e+3))(k-e-1) \geq 0$  and the result follows ■

b) Perfect 1-codes in  $O_k$

Perfect 1-codes are known to exist in  $O_4$  and  $O_6$  (and hence in  $2.O_4$  and  $2.O_6$ ) and these codes form Steiner systems  $S(2,3,7)$  and  $S(4,5,11)$  respectively. We shall show, in Theorem 5.4.3, that any perfect 1-code in  $O_k$  is a Steiner system  $S(k-2, k-1, 2k-1)$  (first proved by P.J. Cameron) and a Steiner system  $S(k-2, k-1, 2k-1)$  is a perfect 1-code in  $O_k$ .

Remark We point out that the line graph of  $O_4$  is an example of a non-trivial graph which contains a perfect 1-code but which is not distance-regular.

Lemma 5.4.2 If a Steiner system  $S(k-2, k-1, 2k-1)$  exists then  $k+1$  is prime.

Proof A well known necessary condition for the existence of an  $S_\lambda(t, d, v)$  design is that  $\binom{d-h}{t-h}$  divides  $\lambda \binom{v-h}{t-h}$  for  $h=0, 1, \dots, t-1$ . In this case we have  $k-1-h$  divides  $(2k-1-h)(2k-2-h)\dots(k+2)/(k-2-h)!$  for  $h=0, 1, \dots, k-3$ . Let  $p$  be any prime between 2 and  $k-1$ , then for  $h=k-p-1$ ,  $p$  divides  $(k+p)(k+p-1)\dots(k+2)/(p-1)!$  and so  $p$  does not divide  $k+1$ . Since  $k \geq 2$ ,  $k$  does not divide  $k+1$  and the result follows ■

Theorem 5.4.3 Let  $C$  be a subset of the vertices of  $O_k$ . The labels of the vertices of  $C$  form an  $S(k-2, k-1, 2k-1)$  Steiner system if and only if  $C$  is a perfect 1-code.

Proof Suppose that  $O_k$  contains a perfect 1-code  $C$  and that  $\mathcal{C}$  is the set of labels of the elements of  $C$ . Any pair of elements of  $C$  are at least at distance three apart so their labelling sets cannot have  $k-2$  elements in common. Hence each  $(k-2)$ -subset of the ground set is contained in at most one element of  $\mathcal{C}$ . Since  $|\mathcal{C}|(k-1) = \binom{2k-1}{k-2}$  it follows that each  $(k-2)$ -subset is in fact contained in exactly one element of  $\mathcal{C}$ .

Conversely, suppose that  $\mathcal{C}$  is an  $S(k-2, k-1, 2k-1)$  Steiner system; we show that the set of vertices  $C$  labelled by blocks of  $\mathcal{C}$  forms a perfect 1-code in  $O_k$ . There are  $\binom{2k-1}{k-1}/(k+1)$  such vertices; we show that the minimum distance between them is three. No two blocks of  $\mathcal{C}$  have  $k-2$  elements in common so no two vertices of  $C$  can be at distance two.

We now show that no two blocks of  $\mathcal{C}$  are disjoint in order to show that no two vertices of  $C$  can be at distance one.

Without loss of generality we assume that  $\{1, 2, \dots, k-1\}$  is a block of  $\mathcal{C}$  and show that every other block contains at least one of the elements of  $\{1, 2, \dots, k-1\}$ . We use the notation  $N(a \cup b \cup \dots \cup f)$ ,  $N(a \cap b \cap \dots \cap f)$  to denote the number of blocks of  $\mathcal{C}$  containing the elements  $a$  or  $b$  or  $\dots$  or  $f$ ,  $a$  and  $b$  and  $\dots$  and  $f$  respectively. By the principle of inclusion and exclusion we have

$$N(1 \cup 2 \cup \dots \cup k-1) = N(1) + N(2) + \dots + N(k-1) - N(1 \cap 2) - \dots - N(k-2 \cap k-1) + \dots + (-1)^k N(1 \cap 2 \cap \dots \cap k-1)$$

Let  $r_j$  denote the number of blocks of  $\mathcal{C}$  containing  $j$  particular elements of  $\{1, 2, \dots, k-1\}$ . Then

$$r_j = \frac{(2k-j-1)!}{(k-j-1)!(k+1)!} = \frac{1}{k-j-1} \cdot \binom{2k-j-1}{k-j-2} \quad ([4, \text{page 50}]).$$

Hence

$$\begin{aligned} N(1 \cup 2 \cup \dots \cup k-1) &= \sum_{s=1}^{k-2} (-1)^s \binom{k-1}{s} \binom{k+s}{s-1} \cdot \frac{1}{s} + 1 \\ &= 1 - \frac{1}{(k+1)} \cdot \sum_{s=1}^{k-2} (-1)^{k-1-s} \binom{k-1}{s} \binom{k+s}{s} \end{aligned}$$

By equating the coefficient of  $x^{k-1}$  in  $(1+x)^{k-1}(1+x)^{-k-1}$  and  $(1+x)^{-2}$  we have

$$\sum_{s=1}^{k-1} (-1)^{k-1-s} \binom{k-1}{s} \binom{k+s}{s} = k + (-1)^k.$$

Thus

$$N(1 \cup 2 \cup \dots \cup k-1) = 1 - \frac{1}{k+1} \left[ k+1 - \binom{2k-1}{k-1} \right] = \frac{1}{k+1} \binom{2k-1}{k-1} = |C|$$

and so no two blocks are disjoint ■

Equation (2.3.18) for a perfect 1-code gives  $(B+I)p(0)=k$ .

The component equations are

$$k_{2r} = (k-r)p_{2r-1} + p_{2r} + (r+1)p_{2r+1} \quad (1 \leq r \leq [(k-2)/2])$$

$$k_{2r+1} = (k-r)p_{2r} + p_{2r+1} + (r+1)p_{2r+2} \quad (0 \leq r \leq [(k-3)/2])$$

where  $p_i = p_{i0}(C)$  and  $(k-r)k_{2r} = (r+1)k_{2r+1}$ . These equations enable us to prove inductively that

$$p_{2r0}(C) = \frac{k-r}{r} \cdot p_{2r-1,0}(C) \quad (1 \leq r \leq [(k-1)/2]) \quad (5.4.1)$$

It then follows by counting  $\Gamma_{2r}$  that

$$p_{2r+1,0}(C) = \frac{k_{2r}}{r+1} - p_{2r,0}(C) \quad (0 \leq r \leq [(k-2)/2]) \quad (5.4.2)$$

If we manipulate these two expressions we obtain the following explicit form for  $p_{2r,0}(C)$ :

$$p_{2r,0}(C) = \frac{(-1)^{r-1}}{k+1} \binom{k-1}{r} \sum_{i=1}^{r-1} (-1)^i \binom{k+1}{i+1} \quad (2 \leq r \leq [(k-1)/2])$$

For  $k+1$  prime each term in the summation will be divisible by  $k+1$  and hence  $p_{2r,0}(C)$  ( $r=0,1,\dots, [(k-1)/2]$ ) are integral and positive.

Since  $k_{2r+1} = \frac{k-r}{r+1} \cdot k_{2r}$  and  $k+1$  is prime,  $r+1$  divides  $k_{2r}$  and from (5.4.2)  $p_{2r+1,0}(C)$  ( $r=0,1,\dots, [(k-2)/2]$ ) are positive integers.

(We can prove a similar result if  $p_i = p_{i1}(C)$ ).

Hence we have shown, independently of the existence of a perfect 1-code, that the weight vector always has positive integer components if  $k+1$  is prime. This may be considered as supporting evidence for the possible existence of other perfect 1-codes in  $O_k$ , although Theorem 5.4.3 and the conjecture that no  $t$ -designs exist with  $t > 5$  indicate that no other perfect 1-codes in  $O_k$  are likely to exist.

c) Perfect 2-codes

Theorem 5.4.4 There are no non-trivial perfect 2-codes in  $O_k$  for  $k < 3081$ .

Proof If  $O_k$  contains a perfect 2-code, then by the polynomial condition  $x_2(\lambda) = \lambda^2 + \lambda - k + 1$  has eigenvalues of  $O_k$  as zeros. The roots of  $x_2(\lambda)$  will be of the form  $\alpha, -\alpha-1$  where  $\alpha > 0$  and  $k-1 = \alpha(\alpha+1)$ . Hence  $k$  is odd and so  $\alpha$  is odd, which gives  $k=1-2r+4r^2$  for a positive integer  $r$ .

If  $r=1$  we obtain the trivial perfect 2-code in  $O_3$ , so we assume for the rest of this section that  $k \geq 13$ .

Since  $\hat{S}_2 p(0) = (B^2 + B - (k-1)I)p(0) = 0$  we can obtain explicit expressions for the components of  $p(0)$ . In particular,

$$p_{10,0}(C) = k(k-1)^2(k-3)(k-5)(k^3 - 15k^2 + 87k - 181)/(5!)^2$$

and since  $k^3 - 15k^2 + 87k - 181$  is never divisible by 5,  $5^2$  divides  $k(k-1)^2(k-3)(k-5)$ . But  $k=1-2r+4r^2$  and consequently  $k$  is not divisible by 5 and hence  $5^2$  divides  $r^2(2r-1)^2(2r+1)(r-1)$ . We have four possibilities:

$$(i) \quad r \equiv 0 \pmod{5}, \quad k = 100s^2 + 190s + 91 \quad (s=0,1,\dots) \quad ;$$

$$(ii) \quad r \equiv 3 \pmod{5}, \quad k = 100s^2 + 110s + 31 \quad (s=1,2,\dots) \quad ;$$

$$(iii) \quad r \equiv 1 \pmod{25}, \quad k = 2500s^2 + 150s + 3 \quad (s=1,2,\dots) \quad ;$$

$$(iv) \quad r \equiv 12 \pmod{25}, \quad k = 2500s^2 + 2350s + 553 \quad (s=0,1,\dots) \quad .$$

We can eliminate some of the cases by using the sphere packing condition:  $1+k^2$  divides  $\binom{2k-1}{k-1}$ . Substituting for  $k$  gives  $1+k^2 = 2(4r^2+1)(r^2+(r-1)^2)$ . Let  $p$  denote  $r^2+(r-1)^2$ . Since  $r \geq 3$  we have  $5p > 2k-1 > 4p$ ,  $3p > k$  and  $2p < k-1$ . Consequently when  $p$  is prime it is relatively prime to  $\binom{2k-1}{k-1} = (2k-1)\dots(k+1)/(k-1)!$  and the sphere packing condition is not satisfied.

Case (i)  $r \equiv 0 \pmod{5}$

The first value of  $r$  for which  $p$  is non-prime is  $r=45$  and so for  $k$  of the form  $100s^2+190s+91$  there are no perfect 2-codes in  $O_k$  for  $k < 9901$ .

Case (ii)  $r \equiv 3 \pmod{5}$

The first value of  $r$  for which  $p$  is non-prime is  $r=28$  and so for  $k$  of the form  $100s^2+110s+31$  there are no perfect 2-codes in  $O_k$  for  $k < 3081$ .

Case (iii)  $r \equiv 1 \pmod{25}$

If  $s=1$  then  $p=1301$  which is prime and so for  $k$  of the form  $2500s^2+150s+3$  there are no perfect 2-codes in  $O_k$  for  $k < 10303$ .

Case (iv)  $r \equiv 12 \pmod{25}$

If  $s=0$ ,  $r=12$  and  $p=265=5 \cdot 53$  but 53 is relatively prime to  $\binom{1105}{552}$ . Hence for  $k$  of the form (iv) and  $k < 5403$  there are no perfect 2-codes in  $O_k$ .

By combining the results from these four cases the theorem is proved. ■

d) Perfect 3-codes

Theorem 5.4.5 If  $O_k$  contains a non-trivial perfect 3-code then

$$(i) \quad k = 32r^2 + 20r + 4 \quad (r=1,2,\dots) \quad ; \text{ or}$$

$$(ii) \quad k = 128r^2 - 24r + 2 \quad (r=1,2,\dots) \quad .$$

Proof From (5.3.3) and (5.3.4) we find  $x_3(\lambda) = \frac{(\lambda+1)(\lambda^2+\lambda-2(k-1))}{2}$ .

Since -1 is a root of  $x_3(\lambda)$  and hence an eigenvalue of  $O_k$ ,  $k$  must be even. The other roots of  $x_3(\lambda)$  are of the form  $-(2s-1), 2s$  where  $s > 0$  and  $2s(2s-1) = 2(k-1)$ . But  $k$  is even and so  $s$  is odd and hence  $k = 1 + (4t-1)(2t-1)$  for  $t = 1, 2, \dots$ .

If  $t = 1$  then  $k = 4$  and this corresponds to the trivial perfect 3-code in  $O_4$ . We assume that  $t > 1$ . From  $\hat{S}_3 p(0) = \underline{k}$  we are able to calculate

$$p_{11,0}(C) = k(k-1)^2(k-2)(k-4)(k^3 - 22k^2 + 197k - 584) / 3 \cdot (5!)^2$$

and since  $k$  is even  $2^6$  divides  $k(k-2)(k-4)(k^3 - 22k^2 + 197k - 584)$ .

Let  $q = 4t^2 - 3t + 1$  so that  $k = 2q$  and  $2^2$  divides  $q(q-1)(q-2)(4q^3 - 44q^2 + 197q - 229)$ . Either  $q$  is even or  $q \equiv 1 \pmod{4}$  i.e.  $t$  is odd or divisible by 4. The two possibilities follow ■

e) Perfect 4-codes

Theorem 5.4.6 If  $O_k$  contains a non-trivial perfect 4-code then  $k \geq 4061$ .

Proof By the results of §5.3 we can assume that  $x_4(\lambda)$  has roots  $\gamma, -\gamma-1, \alpha, -\alpha-1$  with  $\gamma$  and  $\alpha$  positive integers. By (5.3.9) and (5.3.17)  $\alpha(\alpha+1)\gamma(\gamma+1) = 2(k-1)(k-2)$  and  $\gamma(\gamma+1) + \alpha(\alpha+1) = 2(2k-3)$ . If  $\eta = \alpha(\alpha+1)$  then

$$\eta^2 - (4k-6)\eta + 2(k-1)(k-2) = 0 \quad \text{and so}$$

$$\eta = 2k-3 \pm (2k^2-6k+5)^{\frac{1}{2}}.$$

If  $O_k$  contains a perfect 4-code then  $\eta$  is integral and  $2k^2-6k+5 = r^2$  for some integer  $r > 1$ . Hence  $(k-1)^2 + (k-2)^2 = r^2$  and the first integer solution  $r=5$ ,  $k=5$  corresponds to the trivial perfect 4-code in  $O_5$ . The next solution is  $k=22$ ,  $r=29$  so we shall assume that  $k \geq 22$ .

The equation  $(k-2)^2 + (k-1)^2 = r^2$  has general solution as follows [20, page 190]:

(i) k even  $k-2=2xy$ ,  $k-1=x^2-y^2$ ,  $r=x^2+y^2$  so that  $x^2-2xy-y^2-1=0$  which gives  $x=y+(1+2y^2)^{\frac{1}{2}}$ . Let  $\xi = x-y$  then the equation  $\xi^2 = 1+2y^2$  ( $\xi > 0$ ,  $y > 0$ ) has general solution given by  $\xi_s = (1+\sqrt{2})^{2s} - y\sqrt{2}$  ( $s=1,2,\dots$ ) [20, page 210] and hence  $k = 2 + 2y(y(1-\sqrt{2}) + (1+\sqrt{2})^{2s})$  for  $s=1,2,\dots$

(ii) k odd  $k-1=2xy$ ,  $k-2=x^2-y^2$ ,  $r=x^2+y^2$  which gives  $k=1+2y(y+\xi_s)$  where  $y, \xi_s$  satisfy  $\xi_s^2 = 2y^2-1$  and  $\xi_s + y\sqrt{2} = (1+\sqrt{2})^{2s+1}$  ( $s=1,2,\dots$ ).

The first four possibilities for  $k$  are 22, 121, 698 and 4061.

From  $\hat{S}_4 P(0) = \underline{k}$  we obtain

$$P_{11,0}(C) = 4k(k-1)^2(k-2)^2(k-5)(k-17)/6!5!$$

We can rule out the first three cases using the fact that

$P_{11,0}(C)$  must be integral ■

Remark We have seen, in sections (b), (c) and (e), how it is possible to consider particular values of  $e$  and obtain reasonable non-existence results. However it appears that without the use of the sphere-packing condition it is not even possible to deal completely with any particular value of  $e$ .

For example, in the case  $e=2$ , if  $k=4r^2-2r+1$  the existence of the factor  $k-1 = r(4r-2)$  in each component  $p_{i0}(C)$  ( $i \geq 5$ ) means that for any fixed value of  $i$   $p_{i0}(C)$ ,  $p_{i-10}(C)$ , ...,  $p_{5,0}(C)$  will be positive integers for some suitable value of  $r$ . Similarly if  $e=3$  we have a factor  $k-2$  in each  $p_{i0}(C)$  ( $i \geq 7$ ).

### 5.5 Nearly perfect codes in $O_k$

Having made the comment above about the perfect code case, we shall show in this section that we can obtain more definite non-existence results for nearly perfect  $e$ -codes which are not perfect and with  $e$  odd.

Suppose  $e=2r+1$  and  $r \geq 1$ . We omit the case  $e=1$  since  $c_2=1$  and all nearly perfect 1-codes are perfect.

Let  $k \equiv a \pmod{(r+1)}$  with  $0 < a \leq r$  then

$$p_{e+1e}(C) = \left[ \frac{(k-r-1)}{(r+1)} \right] = \frac{(k-r-1-a)}{(r+1)} \text{ and}$$

$$p_{e+1e+1}(C) = \left[ \frac{k}{(r+1)} \right] = \frac{(k-a)}{(r+1)}. \quad \text{On substitution into (2.3.19) we find}$$

$$(k-a)x(\lambda) = (r+1)x_{2r+2}(\lambda) + (k-a-r-1)x_{2r}(\lambda)$$

and by (5.3.4)

$$(k-a)x(\lambda) = \lambda x_{2r+1}(\lambda) - ax_{2r}(\lambda) \quad (5.5.1)$$

Theorem 5.5.1 If  $O_k$  contains a nearly perfect  $e$ -code which is not perfect and  $e$  is odd then  $e \geq 15$ .

Proof Suppose that  $O_k$  contains a nearly perfect  $e$ -code which is not perfect and let  $e=2r+1$ . Using (5.5.1) and Lemma 5.3.3 we derive the following:

$$\begin{aligned}
\text{(i)} \quad (k-a)x(0) &= (-1)^{r+1} a \binom{k-1}{r} ; \\
\text{(ii)} \quad (k-a)x(1) &= \frac{(-1)^{r+1}}{k-1} \binom{k-1}{r} (k(a-2) - 2r(a-1) - (a-2)) ; \\
\text{(iii)} \quad (k-a)x(2) &= \frac{(-1)^{r+1}}{(k-1)(k-2)} \binom{k-1}{r} \left[ k^2(a-6) - k(3a+6ar-18r-18) \right. \\
&\quad \left. + a(6r^2+6r+2) - 12r^2 - 24r - 12 \right] .
\end{aligned}$$

By Theorem 2.3.6  $x(\lambda)$  must have roots in the set  $\{-(k-1), k-2, \dots, (-1)^{k+1}\}$ .

If  $1 \leq r \leq 2$  then  $1 \leq a \leq 2$  and obviously  $x(0)$  and  $x(1)$  are non-zero and have opposite signs - a contradiction.

If  $3 \leq r \leq 6$  then  $1 \leq a \leq 6$ . For non-trivial codes we have  $k \geq 2e + 2 = 4r + 4$  which is sufficient to ensure that  $x(0)$  and  $x(2)$  are non-zero and have opposite signs. Hence  $x(1) = 0$  and  $k(a-2) = 2r(a-1) + (a-2)$ . If  $a=1$  or  $2$  then  $k=1$  or  $r=0$  respectively. For  $a > 2$   $k=2r+1 + \frac{2r}{a-2} < 4r+1$  - a contradiction. The result then follows. ■

It seems very likely that by considering  $x(\lambda)$  for other integral values of  $\lambda$  we shall be able to extend this non-existence result.

Suppose now that  $e=2r$  with  $r \geq 1$ . If  $k \equiv a \pmod{r+1}$  then  $0 \leq a \leq r-1$  and

$$(k-a)x(\lambda) = (\lambda+1)x_{2r}(\lambda) - (a+1)x_{2r-1}(\lambda) \quad (5.5.2)$$

We find, when we calculate  $x(0)$ ,  $x(1)$  and  $x(2)$ , that the sign of  $x(1)$  and  $x(2)$  is independent of the value of  $a$ . This means that we cannot repeat the rather simple proof of Theorem 5.5.1 to obtain similar non-existence results.

However, we illustrate the case  $e=2$  since it is an example of an application of Theorem 2.5.1. If  $e=2$  we need  $b_2 = k-1 \not\equiv 0 \pmod{2}$  and hence  $k$  must be even. But then we can apply Theorem 2.5.1 and obtain a

perfect 1-code. We have already established that a perfect 1-code is a Steiner system  $S(k-2, k-1, 2k-1)$  and so it seems unlikely that a nearly perfect 2-code exists in  $O_k$  for  $k > 6$ . In fact  $O_6$  does contain a nearly perfect 2-code indexed by the following  $2-(2, 5, 11)$  design

1 2 3 4 5	2 4 7 8 9
4 5 6 9 10	2 3 9 10 11
3 5 7 8 10	1 5 7 9 11
3 4 6 7 11	1 4 8 10 11
2 5 6 8 11	1 2 6 7 10
1 3 6 8 9	

If we had not already known the Steiner system  $S(4, 5, 11)$  we could have obtained an explicit form from the nearly perfect 2-code above.

From the form of the roots of  $x(\lambda) = (\lambda+1)(\lambda^2 + \lambda - k)/2$   
 $k=2r(2r+1)$  and the next value of  $k$  to satisfy the sphere packing condition is  $k=42$ .

## 6. Codes in $J(a,b)$

### 6.1 Introduction

We have already mentioned Delsarte's investigation [10] of an analogue of a design in association schemes. For the case of the Johnson schemes, which correspond to the graphs  $J(a,b)$ , Delsarte has shown that his definition coincides with the classical combinatorial idea of a design.

Biggs [6] has also extended the concept of a design to a connected finite graph and his definition is of a more combinatorial nature. As in Delsarte's case the definition coincides with the classical designs for the particular case of the graph  $J(a,b)$ .

In §6.5 and §6.6 we investigate some interesting connections between combinatorial designs and completely regular codes in  $J(a,b)$ .

As we shall see later in the chapter the nature of the intersection array of  $J(a,b)$  increases the difficulty of considering the existence of particular codes in the graph. For this reason we can only prove the non-existence of nearly perfect 1-codes in  $J(a,b)$  at present.

### 6.2 Eigenvalues of $J(a,b)$

The graph  $J(a,b)$  has  $\binom{a}{b}$  vertices indexed by the  $b$ -subsets of the set  $\{1,2,\dots,a\}$ . Two vertices are joined if and only if they have  $b-1$  elements in common.  $J(a,b)$  has valency  $k=b(a-b)$  and when  $a \geq 2b$  the graph is connected with distance function

$$\partial(u,v) = b - |u \cap v| \quad (6.2.1)$$

and diameter  $b$ . The graph is distance-regular for  $a \geq 2b$  and has intersection array

$$\left\{ \begin{array}{cccccc} * & 1^2 & . & . & . & i^2 & . & . & . & b^2 \\ 0 & a-2 & . & . & . & i(a-2i) & . & . & . & b(a-2b) \\ b(a-b) & (b-1)(a-b-1) & . & . & . & (b-i)(a-b-i) & . & . & . & * \end{array} \right\}$$

For any distance-regular graph  $x_d(\lambda)$  is a divisor, in  $\mathbb{Q}[\lambda]$ , of the characteristic polynomial of the intersection matrix. To find the eigenvalues of  $J(a,b)$  we need to calculate the roots of  $x_b(\lambda)$ . The eigenvector sequence for  $J(a,b)$  is defined as follows:

$$v_0(\lambda) = 1, \quad v_1(\lambda) = \lambda \quad \text{and for } 0 < i < b$$

$$(i+1)^2 v_{i+1}(\lambda) + i(a-2i)v_i(\lambda) + (b-i+1)(a-b-i+1)v_{i-1}(\lambda) = \lambda v_i(\lambda) \quad (6.2.2)$$

If we make the following substitutions in (6.2.2)

$$\lambda = u(u-a-1) + b(a-b) \quad (6.2.3)$$

$$E_i(u) = v_i(\lambda) \quad (0 \leq i \leq b) \quad (6.2.4)$$

we obtain

$$\begin{aligned} & (i+1)^2 E_{i+1}(u) + (i(a-2i) - u(u-a-1) - b(a-b)) E_i(u) \\ & + (b-i+1)(a-b-i+1) E_{i-1}(u) = 0 \quad (0 < i < b) \end{aligned} \quad (6.2.5)$$

In fact (6.2.5) defines a family of orthogonal polynomials called the Eberlein polynomials ([10], [37]). An explicit form of these polynomials is given in [9, page 70] as follows:

$$E_i(u, a, b) = \sum_{j=0}^i (-1)^j \binom{u}{j} \binom{b-u}{i-j} \binom{a-b-u}{i-j} \quad (0 \leq i \leq b) \quad (6.2.6)$$

Lemma 6.2.1 If  $E_i(u, a, b)$  is defined by (6.2.6) then

$$\sum_{i=0}^r E_i(u, a, b) = E_r(u-1, a-2, b-1) \quad (6.2.7)$$

Proof The proof follows easily by induction. ■

(6.2.4) and (6.2.7) imply

$$x_i(\lambda) = \sum_{j=0}^i (-1)^j \binom{u-1}{j} \binom{b-u}{i-j} \binom{a-b-u}{i-j} \quad (6.2.8)$$

and in particular,

$$x_b(\lambda) = \sum_{j=0}^i (-1)^j \binom{u-1}{j} \binom{b-u}{b-j} \binom{a-b-u}{b-j} \quad (6.2.9)$$

Suppose that  $\alpha \in \{1, 2, \dots, b\}$  and  $\lambda_\alpha = \alpha(\alpha-a-1) + b(a-b)$   
 then  $\alpha-1 \geq 0$ ,  $b-\alpha \geq 0$  and consequently  $\binom{\alpha-1}{j} = 0$  for  $j > \alpha-1$  and  
 $\binom{b-\alpha}{b-j} = 0$  for  $j < \alpha$ . Hence  $x_b(\lambda_\alpha) = 0$  and  $J(a, b)$  has eigenvalues

$$\{\alpha(\alpha-a-1) + b(a-b) : \alpha = 0, 1, \dots, b\}.$$

### 6.3 Nearly perfect 1-codes in $J(a,b)$

Suppose that  $v$  is an eigenvalue of  $J(a,b)$  then there exists  $\alpha \in \{0,1,\dots,b\}$  such that  $\alpha^2 - \alpha(a+1) + ab - b^2 = v$ . Hence there is an integer  $x_v$  such that

$$(a+1)^2 - 4b(a-b) + 4v = x_v^2 \quad (6.3.1)$$

Similarly if  $\mu$  is another eigenvalue of  $J(a,b)$  then there exists an integer  $x_\mu$  such that

$$(a+1)^2 - 4b(a-b) + 4\mu = x_\mu^2 \quad (6.3.2)$$

We combine (6.3.1) and (6.3.2) to obtain

$$(x_v - x_\mu)(x_v + x_\mu) = 4(v - \mu) \quad (6.3.3)$$

and from (6.3.1) it follows that

$$a = 2b - 1 + (x_v^2 - 4v - 4b)^{\frac{1}{2}} \quad (6.3.4)$$

We choose the positive square root in (6.3.4) because  $a \geq 2b$ .

Theorem 6.3.1 There are no non-trivial nearly perfect 1-codes in  $J(a,b)$  with  $(b-1)(a-b-1) \not\equiv 0 \pmod{4}$ .

Proof Since  $b_1 = (b-1)(a-b-1) \not\equiv 0 \pmod{4}$  we have only a small number of cases to consider. We illustrate just two since the method is identical in every case:

(i) If  $b \equiv 2 \pmod{4}$  and  $a \equiv 0 \pmod{4}$  then  $p_{21}(C) = [b_1/c_2] = (b(a-b)-a)/4$  and  $p_{22}(C) = [k/c_2] = b(a-b)/4$ . We substitute these values into (2.3.19) and find  $x(\lambda) = \lambda(\lambda+2)/b(a-b)$ . If  $v = 0$  and  $\mu = -2$  (6.3.3) has solutions  $x_v = \pm 3$ ,  $x_\mu = \pm 1$ . (6.3.4) gives  $a = 2b - 1 + (9-4b)^{\frac{1}{2}}$  and the only possible integer solution is  $a=4, b=2$ .

(ii) If  $b \equiv 2 \pmod{4}$  and  $a \equiv 1 \pmod{4}$  then we find  $x(\lambda) = (\lambda+2)(\lambda-1)/(b(a-b)-2)$ . Let  $v = -2$  and  $\mu = 1$  then (6.3.3) has solutions  $x_v = \mp 2$ ,  $x_\mu = \pm 4$ . (6.3.4) implies  $a = 2b-1+(12-4b)^{\frac{1}{2}}$  and this has integer solution  $a=5$ ,  $b=2$  ■

#### 6.4 Completely regular codes and designs

The first result in this section is due to Delsarte [9]. We include a short proof since Delsarte's proof is not explicit.

Lemma 6.4.1 (Delsarte). If  $J(a,b)$  contains a code  $C$  with minimum distance  $\delta$  and  $|C| = \binom{a}{t} / \binom{b}{t}$ , where  $t=b-\delta+1$ , then the elements of  $C$  form a Steiner system  $S(t,b,a)$ .

Proof Let  $t = b - \delta + 1$  and let  $x$  denote a  $t$ -subset of  $\{1, 2, \dots, a\}$ . If there exist  $u, v \in C$  such that  $u \cap v \neq x$  then  $\partial(u, v) = b - |u \cap v| \leq \delta - 1$ , a contradiction.

If  $x_1, x_2, \dots, x_r$  denote the  $t$ -subsets of  $\{1, 2, \dots, a\}$ , where  $r = \binom{a}{t}$ , and  $x_i$  is contained in  $\lambda_i$  elements of  $C$  then  $\lambda_i = 0$  or  $1$ . Let  $\lambda$  denote the mean of  $\lambda_1, \lambda_2, \dots, \lambda_r$  then

$$\sum_{i=1}^r \lambda_i = |C| \cdot \binom{b}{t} = \binom{a}{t}$$

which implies  $\lambda = 1$  and hence each  $\lambda_i = 1$ . ■

We shall use Lemma 6.4.1 in the following results which connect completely regular codes and designs.

Theorem 6.4.2 If  $J(a,b)$  contains a completely regular 1-code  $C$  with external distance 2 and parameters  $p_{21}(C) = \binom{b-1}{2}$  and  $p_{22}(C) = \binom{b}{2}$ , then  $C$  forms a Steiner system  $S(b-2, b, a)$ .

Conversely a Steiner system  $S(b-2, b, a)$  is a completely regular 1-code in  $J(a, b)$  with the above parameters.

Proof By calculating  $x(k)$  we find  $|C| = \binom{a}{b-2} / \binom{b}{b-2}$  and the result follows from an application of Lemma 6.4.1.

Conversely suppose  $C$  is a Steiner system  $S(b-2, b, a)$ .

Any two blocks of  $C$  have at most  $b-3$  elements in common and hence  $C$  has minimum distance three. Obviously  $C$  has external distance not greater than two. If  $C$  is perfect then  $-1$  is an eigenvalue of  $J(a, b)$  and there exists  $\alpha \in \{1, 2, \dots, b\}$  such that  $\alpha(\alpha-a-1)+b(a-b)=-1$ . If  $\alpha=b$  then  $b=1$ . Let  $\alpha=b-j$  then  $b=j^2+j(a-2b+1)+1$  and since  $j \geq 1$  we have  $a \leq 3b-3$ . By the sphere packing condition for a perfect 1-code

$$1+b(a-b) = \binom{a}{b} / |C| = (a-b+2)(a-b+1)/2$$

and hence

$$a = (4b-3 + (4b^2-12b+17)^{\frac{1}{2}}) / 2 > 3b-3$$

which is a contradiction. We have shown that  $C$  has external distance exactly two.

Suppose  $v$  and  $c$  are vertices of  $J(a, b)$  with  $c \in C$  and  $\partial(c, v) = 1$ . Then  $|c \cap v| = b-1$ . Let  $v \setminus c = \{\pi\}$ . By definition  $p_{21}(C, v) = |\{x \in C \mid \partial(x, v) = 2\}| = |\{x \in C \mid |x \cap v| = b-2\}|$ . If  $|x \cap v| = b-2$  and  $x \in C$  then  $x$  contains  $\pi$  and exactly  $b-3$  elements of  $c$ . In fact  $x$  is the unique block containing these  $b-2$  elements. Hence  $p_{21}(C, v) = \binom{b-1}{b-3} = \binom{b-1}{2}$ .

We can use a similar argument to show that for any vertex  $y$  with  $\partial(y, C) = 2$   $p_{22}(C, y) = 1 + \binom{b-2}{b-3} \binom{2}{1} + \binom{b-2}{b-4} = \binom{b}{2}$ . ■

The polynomial condition is satisfied because the roots of  $x(\lambda) = (\lambda+b)(\lambda-a+3b-2)/2b(b-1)$  are eigenvalues of  $J(a,b)$ .

Theorem 6.4.3 If  $J(a,b)$  contains a completely regular code  $C$  with minimum distance 2 (we consider  $C$  to be a 0-code with  $p_{10}(C) = 0$ ), external distance 1 and parameter  $p_{11}(C) = b$ , then  $C$  forms a Steiner system  $S(b-1, b, a)$ .

Conversely a Steiner system  $S(b-1, b, a)$  is a completely regular code with the above parameters.

Proof We omit the proof since it is almost identical to the proof of Theorem 6.4.2. ■

Once again the polynomial condition is satisfied with  $x(\lambda) = (\lambda+b)/b$ .

Notice also that when  $b=k-1$  and  $a=2k-1$  we have a perfect 1-code in  $O_k$ .

We now use a property of Steiner systems to obtain further completely regular codes.

Theorem 6.4.4 (i) If  $J(a,b)$  contains a completely regular 1-code  $C$  with external distance 2 and parameters  $p_{21}(C) = \binom{b-1}{2}$  and  $p_{22}(C) = \binom{b}{2}$  then  $J(a-i, b-i)$  contains a completely regular 1-code  $C_i$  with external distance 2 and parameters  $p_{21}(C_i) = \binom{b-i-1}{2}$  and  $p_{22}(C_i) = \binom{b-i}{2}$  for each  $i$  with  $0 \leq i \leq b-3$ ;

(ii) If  $J(a,b)$  contains a completely regular code  $C$  with minimum distance 2 and parameter  $p_{11}(C) = b$  then  $J(a-i, b-i)$  contains a completely regular code  $C_i$  with minimum distance 2 and parameter  $p_{11}(C_i) = b-i$  for each  $i$  with  $0 \leq i \leq b-2$ .

Proof The existence of the Steiner system  $S(t,b,a)$  implies the existence of the Steiner system  $S(t-i,b-i,a-i)$  for  $0 \leq i \leq t-1$

[2, page 103]. To obtain (i) and (ii) we simply apply Theorems 6.4.2 and 6.4.3 successively. ■

We mention one other connection between completely regular 1-codes in  $J(a,b)$  and Steiner systems. This result, however, is weaker than Theorem 6.4.2 and Theorem 6.4.3.

Theorem 6.4.5 If  $b$  is even and greater than 2 and  $J(4b-8,b)$  contains a completely regular 1-code  $C$  with external distance 2 and parameters  $p_{22}(C) = b/2$  and  $p_{21}(C) = 0$ , then  $C$  forms a Steiner system  $S(b-3,b,4b-8)$ .

Proof Suppose that  $J(4b-8,b)$  contains such a code  $C$ . The relevant polynomial  $x(\lambda) = (\lambda+b)(\lambda-3b+10)/2$  has eigenvalues as its roots and from the sphere packing condition  $|C| = \binom{4b-8}{b-3} / \binom{b}{b-3}$ . The result follows from an application of Theorem 6.4.1. ■

## 6.5 $J(2b,b)$

The graph  $J(2b,b)$  is obviously antipodal and each vertex has a unique antipodal vertex, namely its complement in the set  $\{1,2,\dots,2b\}$ . The derived graph  $J(2b,b)/2$  has diameter  $\lfloor b/2 \rfloor$ .

With a view to applying the results of §3.3 we consider the codes of Theorem 6.4.2 and Theorem 6.4.3.

The Steiner systems  $S(b-1,b,2b)$  associated with the codes of Theorem 6.4.3 have been studied by several authors ([1], [3], [4]). These designs exist and are unique for  $b=2,4$  and 6. With the assumption that the automorphism group of the design is flag-transitive Assmus and Hermes [3] have shown that the designs exist only in cases  $b=2,4$  and 6.

Returning to the parameters of the code we find  $\lambda_1 = b > 1$  and by Lemmas 3.3.5 and 3.3.6  $J(2b, b)/2$  contains a completely regular code with the same parameters. It seems likely then that the only completely regular codes of this type are in  $J(12, 6)$ ,  $J(8, 4)$ ,  $J(4, 2)$  (and their derived graphs) and by Theorem 6.4.4 in  $J(11, 5)$ ,  $J(10, 4)$ ,  $J(9, 3)$ ,  $J(8, 2)$ ,  $J(8, 4)$ ,  $J(7, 3)$  and  $J(6, 2)$ .

Next we consider the Steiner systems  $S(b-2, b, 2b)$ . Although we omit the details it can be shown that  $\lambda_2 < 0$  and also that the polynomial condition is not satisfied for  $J(2b, b)/2$ . This is not surprising because if the code satisfied the premises of the following result then  $2/(b+2)$  would need to be integral.

Theorem 6.5.1 (Alltop [1]). If an  $S_\lambda(t, b, 2b)$  design exists with  $t$  even and such that the complement of each block is a block, then the design is already an  $S_\eta(t+1, b, 2b)$  design with  $\eta = \lambda(b-t)/(2b-t)$ .

Another result of Alltop [1] which has interesting applications here is the following:

Theorem 6.5.2 If an  $S_\lambda(t, b, 2b)$  design exists with  $t$  even then an  $S_\lambda(t+1, b+1, 2b+1)$  design also exists.

If we apply Theorem 6.5.2 and Theorem 6.4.4 we obtain the following:

Theorem 6.5.3 (i)  $J(2b, b)$  (with  $b$  even) contains a completely regular 1-code  $C$  with external distance 2 and parameters  $p_{21}(C) = \binom{b-1}{2}$ ,  $p_{22}(C) = \binom{b}{2}$  if and only if  $J(2b+1, b+1)$  contains a completely regular 1-code  $C^1$  with parameters  $p_{21}(C^1) = \binom{b}{2}$ ,  $p_{22}(C^1) = \binom{b+1}{2}$ ;

(ii)  $J(2b, b)$  (with  $b$  even) contains a completely regular code  $C$  with minimum distance 2 and parameter  $p_{11}(C) = b$  if and only if  $J(2b+1, b+1)$  contains a completely-regular code  $C^1$  with minimum distance 2 and parameter  $p_{11}(C^1) = b+1$ .

## 6.6 Equidistant codes and finite projective planes

A set of vertices  $C$  with mutual distance  $\delta$  in a distance-regular graph  $\Gamma$  will be called a  $\delta$ -equidistant code. When  $\Gamma = J(a, 2)$ ,  $\delta = 2k$  and  $|C| = m$  our definition coincides with Deza's [4]. Deza calls this latter code an  $(m, 2k, a)$ -code.

A finite projective plane is a finite set  $X$  together with a family  $\mathcal{C}$  of subsets of  $X$  satisfying

- (i) Each distinct pair  $x, y \in X$  belong to exactly one  $c \in \mathcal{C}$ ;
- (ii) Each distinct pair  $c, c^1 \in \mathcal{C}$  contains exactly one common  $x \in X$ ;
- (iii) There are at least four elements of  $X$  having the property that no three of them belong to a single  $c \in \mathcal{C}$ .

It can be shown [11, page 161] that if some  $c \in \mathcal{C}$  contains  $b+1$  elements of  $X$  then all members of  $\mathcal{C}$  contain  $b+1$  elements and  $|\mathcal{C}| = |X| = b^2 + b + 1$ .  $\mathcal{C}$  is then called a finite projective plane of order  $b$ . A finite projective plane of order  $b$  is equivalent to a Steiner system  $S(2, b+1, b^2 + b + 1)$  [4, page 51].

Theorem 6.6.1  $J(b^2 + b + 1, b + 1)$  contains a  $b$ -equidistant code with  $b^2 + b + 1$  elements if and only if there exists a finite projective plane of order  $b$ .

Proof Suppose a projective plane  $\mathcal{C}$  of order  $b$  does exist. Then  $\mathcal{C}$  contains  $b^2+b+1$  elements. If  $x$  and  $y$  are distinct members of then  $|x \wedge y| = 1$  and  $\partial(x, y) = b$  in  $J(b^2+b+1, b+1)$ .

Conversely, suppose  $J(b^2+b+1, b+1)$  contains such a  $b$ -equidistant code  $C$ . Then  $|C| = b^2+b+1 = \binom{b^2+b+1}{2} / \binom{b+1}{2}$  and by Theorem 6.4.1  $C$  is a Steiner system  $S(2, b+1, b^2+b+1)$ . ■

Given a vertex  $x$  of  $J(a, b)$  we can identify  $x$  with a vertex  $x^1$  of  $\Gamma(a, 2)$ . We do this in an obvious way by choosing the components of  $x^1$  to be 1 when indexed by elements of  $x$  and 0 elsewhere. In terms of  $\Gamma(a, 2)$   $x^1$  has weight  $b$ .

Let  $x, y$  be vertices of  $J(a, b)$  and  $x^1, y^1$  respectively be the identified vertices in  $\Gamma(a, 2)$ . If  $\partial$  and  $\partial^1$  denote the distance functions in  $J(a, b)$  and  $\Gamma(a, 2)$  respectively then

$$\partial^1(x^1, y^1) = 2(b - |x \wedge y|) = 2\partial(x, y) \quad (6.6.1)$$

Using this identification and Theorem 6.5.1 we can prove a result of Deza [12].

Corollary 6.6.2 (Deza [12]). If a projective plane of order  $k$  exists then provided  $a$  is sufficiently large a  $(k^2+k+2, 2k, a)$ -code exists.

Proof Suppose  $\mathcal{C}$  is a projective plane of order  $k$  then by Theorem 6.6.1  $\mathcal{C}$  is a  $k$ -equidistant code in  $J(k^2+k+1, k+1)$  with  $k^2+k+1$  elements. We now allow  $\mathcal{C}$  to represent its identification in  $\Gamma(k^2+k+1, 2)$ . By (6.6.1)  $\mathcal{C}$  is a  $2k$ -equidistant set in  $\Gamma(k^2+k+1, 2)$ . If we choose  $a$  large enough we can increase the length of each element of  $\mathcal{C}$  by  $k-1$  1's to give a  $2k$ -equidistant code in  $\Gamma(a, 2)$  where each element has weight  $2k$ . By adding the all-zero vector to this set we have the required  $(k^2+k+2, 2k, a)$ -code. ■

## REFERENCES

1. W.O. Alltop. Extending  $t$ -designs. J. Combinatorial Theory (A) 18(1975) 177-186.
2. I. Anderson. A first course in Combinatorial Mathematics. Clarendon Press, Oxford, 1974.
3. E.F. Assmus and Hermes. Non-existence of Steiner Systems of type  $S(d-1, d, 2d)$ . Math. Z. 138(1974) 171-172.
4. N.L. Biggs. Finite groups of automorphisms (London Math. Soc. Lecture Note Series 6). Cambridge University Press, London, 1974.
5. N.L. Biggs. Perfect codes in graphs. J. Combinatorial Theory (B) 15(1973) 289-296.
6. N.L. Biggs. Designs, factors and codes in graphs, to appear.
7. N.L. Biggs. Algebraic Graph Theory (Cambridge Math. Tracts No. 67). Cambridge University Press, London, 1974.
8. R.C. Bose, S.S. Shrikhande and E.T. Parker. Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture. Canad. J. Math. 12(1960) 189-203.
9. P. Delsarte. An algebraic approach to the association schemes of coding theory. Thesis, Université Catholique de Louvain, 1973.
10. P. Delsarte. Four fundamental parameters of a code and their combinatorial significance. Inf. Control 23(1973) 407-438.
11. J. Denes and A.D. Keedwell. Latin squares and their applications. English Univ. Press, London, 1974.
12. M. Deza. Une propriété extrémale des plans projectifs finis dans une classe de codes équidistants. Discrete Math. 6(1973) 343-352.

13. A. Gardiner. Antipodal covering graphs. J. Combinatorial Theory (B) 16(1974) 255-273.
14. J.M. Goethals and S.L. Snover. Nearly perfect binary codes. Discrete Math. 3(1972) 65-88.
15. J.M. Goethals and H.C.A. van Tilborg. Uniformly packed codes. MBLE Res. Lab. Rpt. 272(1974).
16. S.W. Golomb and E.C. Posner. Rook domains, latin squares, affine planes and error-correcting codes. IEEE Trans. Inform. Theory IT10 (1964) 196-208.
17. P. Hammond. Nearly perfect codes in distance-regular graphs. Discrete Math. 14(1976) 41-56.
18. P. Hammond and D.H. Smith. Perfect codes in the graph  $O_k$ . J. Combinatorial Theory (B) 19(1975) 239-255.
19. P. Hammond and D.H. Smith. An analogue of Lloyd's theorem for completely regular codes. Proc. Brit. Comb. Conf., Aberdeen, to appear.
20. G.H. Hardy and E.M. Wright. The theory of numbers. Oxford (1960).
21. O. Heden. Unpublished.
22. S.M. Johnson. A new upper bound for error-correcting codes. IRE Trans. Information Theory, IT8(1962) 203-207.
23. K. Lindström. On the non-existence of nearly perfect binary codes. Dissertation, Turku Universite (1975).
24. J.H. van Lint. Coding Theory (Lecture Notes in Mathematics 201). Springer-Verlag, Berlin, 1971.
25. J.H. van Lint. On the non-existence of perfect 2- and 3- Hamming-error-correcting codes over  $GF(q)$ . Inf. and Control 16(1970) 396-401.

26. J.H. van Lint. Recent results on perfect codes and related topics. Proc. Advanced Study Institute, Nijerode Castle, Breukelen (Mathematical Centre Tracts 55) (1974) 158-178.
27. J.H. van Lint. A survey of perfect codes. Rocky Mountain J. Math., to appear.
28. S.P. Lloyd. Binary block coding. Bell Syst. Tech. J. 36(1957) 517-535.
29. G.H.J. Meredith and E.K. Lloyd. The Footballers of Croam. J. Combinatorial Theory (B) 15(1973) 161-166.
30. F.P. Preparata. A class of optimum non-linear double-error-correcting codes. Inf. and Control 13(1968) 378-400.
31. H. Reuvers. (1974) unpublished.
32. N.V. Semakov, V.A. Zinov'ev and G.V. Zaitsev. Uniformly packed codes. Problemy Peredači Informacii 7(1971) 38-50.
33. C.E. Shannon. A mathematical theory of communication. Bell Syst. Tech. J. 27(1948) 379-423, 623-656.
34. N.J.A. Sloane. A survey of constructive coding theory and a table of binary codes of highest known rate. Discrete Math. 3(1972) 265-294.
35. D.H. Smith. Primitive and imprimitive graphs. Quarterly J. Maths. Oxford (2), 22(1971) 551-557.
36. D.H. Smith. An improved version of Lloyd's theorem. Discrete Mathematics, to appear.
37. G. Szëgo. Orthogonal Polynomials. Am. Math. Soc. Coll. Publ. 23(1959).
38. A. Tietäväinen. On the non-existence of perfect codes over finite fields. SIAM J. Appl. Math. 24(1973) 88-96.
39. A. Tietäväinen. On the non-existence of perfect codes over non-field alphabets, to appear.
40. A. Tietäväinen and A. Perko. There are no unknown perfect binary codes. Ann. Univ. Turku. Ser. A I 148(1971) 3-10.

41. A. Tietäväinen. Some recent results on perfect and nearly perfect codes, to appear.
42. K. Yamamoto. Euler squares and incomplete Euler squares of even degrees. Mem. Fac. Sci. Kyūsū Univ. Ser. A 8(1954) 161-180.
43. V. A. Zinov'ev, (1974) unpublished.
44. N. S. Mendelsohn, A theorem on Steiner systems, Canad.J. Math. 22 (1970) 1010-1015.