Ovals, Unitals And Codes.

Citation

ANDRIAMANALIMANANA, BRUNO RATSIMANDEFITRA. *Ovals, Unitals And Codes.* 1980, https://preserve.lehigh.edu/lehigh-scholarship/graduate-publications-theses-dissertations/theses-dissertations/ovals-unitals.

University
Microfilms
International

300 N. ZEEB ROAD, ANN ARBOR, MI 48106
18 BEDFORD ROW, LONDON WC1R 4EJ, ENGLAND

ANDRIAMANALIMANANA, BRUNO RATSIMANDEFITRA

OVALS, UNITALS AND CODES

Lehigh University PH.D. 1980

University
Microfilms
International 300 N. Zeeb Road, Ann Arbor, MI 48106 18 Bedford Row, London WC1R 4EJ, England

OVALS, UNITALS AND CODES

by

Bruno Ratsimandefitra Andriamanalimanana

A Dissertation
Presented to the Graduate Committee
of Lehigh University
in Candidacy for the Degree of
Doctor of Philosophy
in
Mathematics

Lehigh University
1979

CERTIFICATE OF APPROVAL

Approved and recommended for acceptance as a dissertation in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

November 28, 1979
(date)

E. F. Assmus, Jr.
Professor in Charge

Accepted November 28, 1979

Special committee directing the doctoral work of Mr. Andriamanalimanana.

Chairman

Andrew K. Snyder

Gilbert Stengle

Clifford Queen

ACKNOWLEDGMENTS

I would like to express my gratitude to Professor E. F. Assmus, Jr. for his guidance during this work and his kindness, to the members of my committee especially Dr. A. Odlyzko, to all my professors, to the staff members of the Lehigh Mathematics Department and to all my friends at Lehigh. I also have to thank Ms. Judy Arroyo for typing this thesis expertly.

TABLE OF CONTENTS

ABSTRACT

In Chapter One we define an oval for an arbitrary 2-design. Using very simple counting arguments we obtain numerical values about the size of an oval, the number of tangent, secant and exterior blocks to an oval. Our main result is a generalization of a theorem of Qvist on the tangents of an oval in a projective plane of even order. Namely we show that in a projective design of even order with its index λ dividing $k-1$ the tangents to an oval all meet at the same λ points. We also study the relation between the ovals of a 2-design D of even order with λ dividing r and the vectors of minimum weight in the dual of the code equal to the row span over $GF(2)$ of the incidence matrix of D. Finally we introduce the notion of a Hadamard point on an oval in a projective plane of order divisible by 4. We show in particular that if the plane is Desarguesian and if the oval is a nondegenerate conic together with its "nucleus" then this nucleus is a Hadamard point. In Chapter 2 we study the codes from

the incidence matrix of the unital in a Desarguesian projective plane of order q^2 where q is a prime power. In particular we show that if q is odd then the unital cannot contain any nondegenerate conic. Then using the results of Chapter One we obtain a lower bound for the size of a minimum weight vector in the dual of the above code studied over GF(2). We also present some numerical results obtained on the Lehigh machine CDC 6400. These are mainly about the dimensions of the above codes for small values of q but they do indicate a general pattern that we formulate as a conjecture. In Chapter 3 we define and study codes from the irreducible root systems that arise in the classification of simple Lie algebras over an algebraically closed field of characteristic zero. We concentrate on the codes corresponding to systems whose vectors are all of the same length. These codes or the ones derived from them are good with regard to the bounds of coding theory. We obtain values for the dimension, the minimum weight and the number of vectors of minimum weight in these various codes. A further computation on the Lehigh computer yields the complete weight enumerators of the three exceptional codes corresponding to the systems E_6, E_7 and E_8.

NOTATION AND TERMINOLOGY

A t-(v,k,λ) design consists of a set $\mathbb{P}$ of elements called points, a set $\mathcal{B}$ of elements called blocks and a relation I called incidence between points and blocks (i.e. a subset of $\mathbf{P} \times \mathcal{B}$) such that:

(i) $\mathbf{P}$ has v elements,

(ii) Every block is incident with exactly k points,

(iii) Any t distinct points are incident with exactly λ blocks.

It is immediate that a t-(v,k,λ) design is also a i-(v,k,λ_i) design, for $i = 0,1,\ldots,t$, where the integer λ_i is given by the equation

$$\lambda\binom{v-i}{t-i} = \lambda_i\binom{k-i}{t-i} .$$

The numbers λ_0 and λ_1, i.e. the number of blocks and the number of blocks incident with a given point, will be subsequently denoted b and r and called the block and replication numbers of the design. The number $r-\lambda$ will be called the order of the design.

A 2-(v,k,λ) design such that $v = b$ is said to be projective.

Given a design $(\mathbb{P},\mathcal{B},I)$ we may consider the relation $\tilde{I} = \mathbb{P} \times \mathcal{B} - I$ between points and blocks. By the principle of inclusion and exclusion, $(\mathbb{P},\mathcal{B},\tilde{I})$ is also a design, called the complement of $(\mathbb{P},\mathcal{B},I)$. In particular the complement of a 2-(v,k,λ) design has parameters 2-$(v,v-k,b-2r+\lambda)$; the block numbers are the same but the replication number of the complement is of course $b-r$.

The incidence matrix of a design, with respect to a given ordering of the points and the blocks, is the b-by-v matrix (a_{ij}) where $a_{ij} = 1$ or 0 according as the ith block is incidentor not with the jth point.

An automorphism (or collineation) of a design consists of a permutation α of the points and a permutation β of the blocks such that a point p and a block B are incident if and only if p^{α} and B^{β} are. Of course we need describe only α if the incidence relation is the set membership (we may also define an isomorphism between two designs).

A Steiner system is a t-$(v,k,1)$ design.

A projective plane is a projective 2-$(v,k,1)$ design; the parameters of such design may be written $v = b = n^2 + n + 1$, $r = k = n + 1$.

A Hadamard design is a projective 2-$(4n-1,2n-1,n-1)$ design; such a design arises from a so-called Hadamard matrix but we shall not need that notion here.

A set $D = \{d_1, \ldots, d_k\}$ of distinct elements in a finite group G is called a difference set if there exists a positive integer λ such that for any $g \neq 1$ in G there are exactly λ choices $d_i, d_j \in D$ such that $d_i d_j^{-1} = g$. The existence of a difference set is equivalent to that of a projective design having an automorphism group regular on the points and on the blocks.

An important class of designs is given by the classical geometries over finite fields. Let q be a prime power and n be an integer > 1. The points and hyperplanes of the projective space $PG_n(q)$, i.e. the one-dimensional and n-dimensional subspaces of the standard $(n+1)$-dimensional vector space over $GF(q)$, are the points and blocks of a projective design with parameters

$$v = \frac{q^{n+1}-1}{q-1} \quad , \quad k = \frac{q^{n}-1}{q-1} \quad , \quad \lambda = \frac{q^{n-1}-1}{q-1} \ .$$

By a theorem of J. Singer this design is also a difference set. For $n = 2$ we get the so-called Desarguesian projective planes.

Again let q be a prime power. Let $V_n(q)$ be the standard vector space of dimension n over $GF(q)$. We identify an element of $V_n(q)$ with the n-tuple of its coordinates in a fixed basis of $V_n(q)$. A linear (n,k) code over $GF(q)$ is a k-dimensional subspace of $V_n(q)$. If q is 2 then we shall speak of a binary (n,k) code. The (Hamming) weight of a n-tuple u in $V_n(q)$ is the number of its nonzero coordinates; the minimum weight of a code C is then the smallest weight of a nonzero vector in C.

The dual (or orthogonal) of a linear (n,k) code C is the subspace $C^{\perp}$ consisting of all vectors $v = (v_1,\ldots,v_n)$ of $V_n(q)$ such that $u_1v_1 + \ldots + u_nv_n = 0$ for every $u = (u_1,\ldots,u_n)$ in C. $C^{\perp}$ is an $(n,n-k)$ code.

Let C be a linear (n,k) code. For $i = 0,1,\ldots,n$ let A_i denote the number of vectors of weight i in C (of course $A_0 = 1$). The weight enumerator of C is the polynomial

$$W_C(z) = \sum_{0 \le i \le n} A_i z^i .$$

It is often more convenient to use a homogeneous polynomial of degree n and thus to define the weight enumerator to be

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

The weight enumerators of C and its dual $C^{\perp}$ are related by the equation of MacWilliams, namely

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

Often we desribe a (n,k) code C by a generating set of vectors, i.e. by a ℓ-by-n matrix G whose rows generate C. G is called a generator matrix for C. A parity check matrix for C is a generator matrix for the dual code $C^{\perp}$.

If the weight of any vector in a binary code C is even then we say that C is an even code; if the weight of any vector is divisible by 4 then C is doubly even. Note that a doubly even code is necessarily contained in its dual.

An automorphism of a (n,k) code C is a permutation of the n coordinate places that maps any vector of C onto another vector of C. (We may also define an equivalence or isomorphism between two (n,k) codes).

A way of constructing a code is to consider the row span C of the incidence matrix of a design over a field $GF(p)$ where p is a prime; the idea is to relate the algebraic properties of C with the geometric properties of the design.

A class of codes that we shall encounter here is that of (binary) Hamming codes. Let m be a positive integer. The Hamming code H_m has as parity check matrix the m-by-(2^m-1) matrix whose columns are all nonzero binary m-tuples. H_m is a $(2^m-1, 2^m-m-1)$ code of minimum weight 3.

CHAPTER 1

OVALS IN 2-DESIGNS

§1. Arcs and ovals.

Let $D = (\mathbb{P}, \mathbb{B})$ be a $2\text{-}(v,k,\lambda)$ design with block and replication numbers b and r.

A subset S of $\mathbf{P}$ is called an arc if no three points of S are on a block. If S is an arc and B is a block then B is called an exterior, tangent or secant block to S according as $|B \cap S| = 0$, 1 or 2.

We shall exclude the cases where $k = 2$ for which every subset of points is an arc.

Proposition 1.1. Let S be an arc of the design D. Then

(i) if $r-\lambda$ is odd or $r-\lambda$ is even but λ does not divide r then

$$|S| \leq \frac{r+\lambda-1}{\lambda},$$

(ii) if $r-\lambda$ is even and λ divides r then

$$|S| \leq \frac{r+\lambda}{\lambda}.$$

Proof. Suppose the arc S has at least one tangent with point of tangency p. By counting in two ways the set

$$\{(q,B) \mid q \in \mathbb{P},\ B \in \mathcal{B},\ q \neq p,\ q \in S \cap B,\ p \in B\}$$

we get

$$\lambda(|S|-1) \leq r-1$$

so that

$$|S| \leq \frac{r+\lambda-1}{\lambda} .$$

We remark that if $|S| = \frac{r+\lambda-1}{\lambda}$ then through each point of S there passes a unique tangent.

Now suppose the arc S has no tangent. Fix a point p on S. By counting in two ways the set

$$\{(q,B) \mid q \in \mathbb{P},\ B \in \mathcal{B},\ q \neq p,\ q \in S \cap B,\ p \in B\}$$

we get

$$\lambda(|S|-1) = r$$

so that

$$|S| = \frac{r+\lambda}{\lambda} .$$

In particular λ divides r.

Now fix a point p' not on S (this is possible because of the assumption $k > 2$). Let x blocks pass through p' and be secant to S. By counting in two ways the set

$$\left\{(q,B) \mid q \in \mathbf{P},\ B \in \mathcal{B},\ q \in B \cap S,\ p' \in B\right\}$$

we get

$$\lambda |S| = 2x$$

so that

$$r + \lambda = 2x \ .$$

Hence $r-\lambda$ is even.

Definition. An oval of the design D is an arc of maximum size. So if O is an oval then $|O| = \frac{r+\lambda-1}{\lambda}$, $\frac{r+\lambda}{\lambda}$ or $\frac{r+\lambda-1}{\lambda}$ according as $r-\lambda$ is odd, $r-\lambda$ is even and λ divides r, or $r-\lambda$ is even and λ does not divide r.

Remarks.

(i) The above definition is ambiguous when $\lambda = 1$ and $r-1$ is even. For this case an oval is defined to be an arc of cardinality $r+1$ (note that in the literature for a projective plane of even order n, an arc of size $n+1$ is called an oval while an arc of size $n+2$ is called a hyperoval).

(ii) Suppose the design D has an arc of cardinality i. Then $i \leq \frac{r+\lambda}{\lambda}$ in any case. Since $\frac{r}{\lambda} = \frac{v-1}{k-1}$ it follows that

$$(i-1)(k-1) \leq v-1.$$

(iii) Let Oval (D) denote the set of ovals of the design D. Of course it may happen that Oval (D) is empty. But in case Oval (D) is not empty it sometimes happens that the incidence structure $(\mathbb{P}, \text{Oval } (D))$ is itself a 2-design, for example if D has an automorphism group that is doubly transitive on $\mathbf{P}$.

§2. <u>The odd order case</u>

In this section we assume that the order $r-\lambda$ of D is odd and $\frac{r+\lambda-1}{\lambda}$ is an integer.

<u>Proposition 1.2.</u> Let O be an oval of D. Then through a point not on O there pass either no tangent or at least two tangents to O.

<u>Proof.</u> By §1 through each point of O there passes a unique tangent. Let $p \in O$ and let B be the tangent at p. Let q be a point of B distinct from p.

Suppose B is the only tangent to O through q. Let x be the number of secant blocks and y be the number of exterior blocks through q. Counting in two ways the set

$$\left\{(q',C) \mid q' \in \mathcal{P},\ C \in \mathcal{B},\ q' \neq p,\ q' \in O \cap C,\ q \in C\right\}$$

we get

$$\lambda(|O|-1) = \lambda-1 + 2(x-\lambda+1)$$

i.e.

$$\lambda\left(\frac{r+\lambda-1}{\lambda} - 1\right) = 2x - \lambda + 1$$

$$r + \lambda = 2x + 2$$

so that $r-\lambda$ is even, a contradiction. So through a point noton O there pass either no tangent or at least two.

Definition. Let O be an oval of D and q a point not on O. We call q an interior point if through q there passes no tangent, an exterior point otherwise. In particular the points of a tangent distinct from the point of tangency are exterior.

Proposition 1.3. Let O be an oval of D. The numbers of secant, tangent and exterior blocks are respectively

$\frac{1}{2\lambda}(r-1)(r+\lambda-1)$, $\frac{1}{\lambda}(r+\lambda-1)$, and $\frac{r}{k\lambda}[r(k-1)+\lambda]$ $- \frac{1}{2\lambda}[(r+1)(r+\lambda-1)]$.

Proof. Let x be the number of secant blocks to O. Counting in two ways the set

$$\left\{(\{p,q\},B) \mid p,q \in \mathbb{P},\ B \in \mathcal{B},\ p \neq q,\ p,q \in O \cap B\right\}$$

we get

$$x = \lambda\binom{|O|}{2} = \frac{1}{2\lambda}(r-1)(r+\lambda-1).$$

Of course there are $|O|$ tangents and so there are $b - x - |O|$ exterior blocks.

Remark. If the design D is projective then Assmus and VanLint [1] have shown that:

(i) Through an exterior point there pass exactly two tangents, so that the tangents to the oval O form an oval in the dual design.

(ii) An exterior block contains $\frac{1}{2}(k+\lambda-1)$ exterior points and $\frac{1}{2}(k-\lambda+1)$ interior points, while a secant contains $\frac{1}{2}(k+\lambda-3)$ exterior points and $\frac{1}{2}(k-\lambda-1)$ interior points.

(iii) The design has $\frac{1}{2\lambda}(k-1)(k+\lambda-1)$ exterior points and $\frac{1}{2\lambda}(k-1)(k-\lambda-1)$ interior points.

§3. The even order case with λ dividing r.

For this section we assume that the order $r-\lambda$ of D is even and $\frac{r+\lambda}{\lambda}$ is an integer.

Proposition 1.4. Let O be an oval of D. The numbers of secant and exterior blocks to O are respectively $\frac{1}{2\lambda}\, r(r+\lambda)$ and $\frac{r}{k\lambda}[r(k-1)+\lambda] - \frac{1}{2\lambda}\, r(r+\lambda)$.

Proof. Let x be the number of secant blocks to O. Counting in two ways the set

$$\left\{(\left\{p,q\right\},B) \ \vdots\ p,q \in \mathbb{P},\ p \neq q,\ B \in \mathcal{B},\ p,q \in O \cap B\right\}$$

we get

$$x = \lambda\binom{|O|}{2} = \frac{1}{2\lambda}\, r(r+\lambda) \ .$$

The number of exterior blocks is then $b-x$ since O has no tangent.

Proposition 1.5. Let O be an oval of D and let p be a point not on O. The number of secant and exterior blocks to O through p are respectively $\frac{1}{2}\,(r+\lambda)$ and $\frac{1}{2}\,(r-\lambda)$.

Proof. Let x be the number of secants to O through p. Counting in two ways the set

$$\left\{(q,B) \mid q \in \mathbf{P},\ B \in \mathcal{B},\ q \in O \cap B,\ p \in B\right\}$$

we get

$$2x = \lambda|O| = r + \lambda$$

so that $x = \frac{1}{2}(r+\lambda)$. The number of exterior blocks through p is then $r-x$.

Corollary. If the design D is projective then taking as points the exterior blocks of O and as blocks the points not on O we obtain a $2\text{-}(\frac{1}{2\lambda}(k-2)(k-\lambda), \frac{1}{2}(k-\lambda), \lambda)$ design. Note however that this design may have repeated blocks for $\lambda > 1$ [1].

Proposition 1.6. Assume that Oval (D) is not empty and $(\mathbf{P}, \mathrm{Oval}(D))$ is a 2-design with parameters v', b', k', r', λ'. Then $r'-\lambda'$ is even and λ' divides r', as in the design D.

Proof. We have of course $v' = v$ and $k' = \frac{r+\lambda}{\lambda}$.

Now fix a block B in D. Let x denote the number of ovals meeting B. Counting in two ways the set

$$\left\{(p,O) \mid p \in \mathbf{P},\ O \in \mathrm{Oval}(D),\ p \in O \cap B\right\}$$

we get

$$kr' = 2x.$$

Counting in two ways the set

$$\left\{(\{p,q\},O) \mid p,q \in \mathbf{P},\ p \neq q,\ O \in \mathrm{Oval}(D),\ p,q \in O \cap B\right\}$$

we get

$$\lambda'\binom{k}{2} = x .$$

Hence $r' = \lambda'(k-1)$ and so $\frac{r'+\lambda'}{\lambda'} = k.$

Since the blocks of D are clearly arcs of $(\mathbf{P},\mathrm{Oval}(D))$, they are ovals of the latter which is then of even order with λ' dividing r' as in D.

§4. A generalization of a theorem of Qvist.

In this section we propose to generalize a classical result of Qvist which says that in a projective plane of even order all the tangents to an oval meet at the same point (called the nucleus or knot of the oval) [9].

Proposition 1.7. Let D be a projective design with even order and λ dividing $k-1$. Let O be an oval of D. Then all the tangents to O meet at the same λ points.

Proof. We recall that under the hypotheses through each point of 0 there passes a unique tangent. We set $s = |0|$.

(i) Let p be a point not on 0. Let x be the number of tangents through p and y be the number of secants through p. Counting in two ways the set

$$\{(q,B) \mid q \in \mathbf{P},\ B \in \mathcal{B},\ q \in 0 \cap B,\ p \in B\}$$

we get

$$\lambda s = x + 2y$$

that is

$$\lambda(\frac{k+\lambda-1}{\lambda}) = x + 2y\ .$$

Hence $x = (k+\lambda-1)-2y$ and so x is odd. In particular we have $x \geq 1$. (Thus every point of D is on some tangent to 0).

(ii) Now let x_i be the number of points not on 0 through which there pass i tangents to 0. Of course $x_i = 0$ for $i > s$. Since there are $v-s$ points not on 0 we have

$$v - s = \sum_{\substack{i \text{ odd} \\ 1 \leq i \leq s}} x_i\ .$$

Counting in two ways the set

$$\left\{(p,B) \mid p \in \mathbf{P},\ B \text{ tangent to } O,\ p \in B - O\right\}$$

we get

$$s(k-1) = \sum_{\substack{i \text{ odd} \\ 1 \leq i \leq s}} i x_i \quad .$$

Counting in two ways the set

$$\left\{(p,\left\{B,C\right\}) \mid p \in \mathbf{P},\ B,C \text{ tangents to } O,\ p \in B \cap C\right\}$$

we get

$$\lambda\binom{s}{2} = \sum_{\substack{i \text{ odd} \\ 3 \leq i \leq s}} \binom{i}{2} x_i \quad .$$

Now using the relations $\lambda(v-1) = k(k-1)$ and $s = \frac{k+\lambda-1}{\lambda}$ we note that

$$v-s = \frac{(k-1)^2}{\lambda}$$

$$s(k-1) = \frac{(k-1)^2}{\lambda} + k-1 = v-s+k-1$$

$$\lambda\binom{s}{2} = \frac{1}{2}\, s(k-1) \quad .$$

Hence the following equations follow

$$\sum_{\substack{i \text{ odd} \\ 3\le i\le s}} (i-1)x_i = k-1$$

$$\sum_{\substack{i \text{ odd} \\ 3\le i\le s}} i(i-1)x_i = s(k-1) \ .$$

Multiplying the first equation by s and subtracting the second equation yield

$$\sum_{\substack{i \text{ odd} \\ 3\le i\le s}} (s-i)(i-1)x_i = 0 \ .$$

We conclude that $x_i = 0$ for all i except possibly for $i = 1$ and $i = s$.

Now the equations

$$x_1 + sx_s = s(k-1)$$

$$x_1 + x_s = v-s$$

yield

$$x_1 = v-s-\lambda \quad \text{and} \quad x_s = \lambda \ .$$

Of course $x_s = \lambda$ means that all the s tangents to O meet at the same λ points.

Proposition 1.8. Let D be a projective design with even order and λ dividing $k-1$. If D has an oval then $k-1$ divides $\lambda(\lambda-1)$, (of course this condition is of interest only if $\lambda > 1$).

Proof. Let O be an oval of D with $|O| = s$. Let K denote the set of λ points where the tangents to O meet. For a block B which is not tangent to O, let

$$m = |B \cap K| .$$

Then for any tangent T to O we have

$$|B \cap (T-K)| = \lambda - m .$$

By the previous proposition every point of D is on some tangent to O. Hence $m + s(\lambda-m) = k$. Then

$$m = \frac{k-s\lambda}{1-s} = \frac{\lambda(\lambda-1)}{k-1} .$$

Since m is an integer, we conclude the proposition.

Now we investigate the extremal case in the above proposition, i.e. we assume that D is a projective design, $k-\lambda$ is even, λ divides $k-1$ and $k-1 = \lambda(\lambda-1)$.

If we set $\lambda-1 = q$ then we have

$$k = q(q+1) + 1 = q^2 + q + 1$$

$$v = \frac{k(k-1)}{\lambda} + 1 = q^3 + q^2 + q + 1 \,.$$

Hence the design D has the parameters of the design of points and planes of $PG_3(q)$. Of course the classical design $PG_3(q)$, q a prime power, does not have an oval. Moreover the relation $k-1 = \lambda(\lambda-1)$ implies that $k-\lambda = (\lambda-1)^2$; hence λ must be odd.

For $\lambda = 3$, the parameters of D are (15,7,3). There are precisely five designs having those parameters, the classical $PG_3(2)$ with no oval and four others all with ovals [2], [1].

For $\lambda = 5$, the parameters are (85,21,5). There are precisely two known designs having those parameters, the classical $PG_3(4)$ with no oval and another one with ovals [1].

For $\lambda = 7$, the parameters are (259,43,7). These are the parameters of $PG_3(6)$ whose existence or non-existence has not been settled at the present time (though it is well known that the plane $PG_2(6)$ does not exist).

For $\lambda = 9$, the parameters are (585,73,9). The classical $PG_3(8)$ is such a design but no other design is known.

For $\lambda = 11$ the situation is similar to that of $\lambda = 7$, namely we would have $PG_3(10)$.

§5. Ovals and codes from the incidence matrix of a design

Let $D = (\mathbb{P}, \mathcal{B})$ be a design and M be its incidence matrix. Let C denote the code equal to the span over $GF(2)$ of the rows of M.

Proposition 1.9. If D is of even order and λ divides r then

(i) The minimum weight of the dual $C^{\perp}$ is at least the size of an oval in D, that is, $\frac{r+\lambda}{\lambda}$.

(ii) The vectors of weight $\frac{r+\lambda}{\lambda}$ in $C^{\perp}$ are precisely those whose supports form an oval in D.

Proof. (i) Let $v \in C^{\perp}$ and let $p \in v$ be fixed (we identify a vector of $GF(2)^v$ with its support in $\mathbb{P}$). Counting in two ways the set

$$\left\{(q,B) \mid q \neq p,\ q \in v,\ p,q \in B\right\}$$

we get

$$\lambda(|v|-1) = \sum_{\substack{B \\ p\in B}} |B \cap (v-\{p\})| .$$

Now for each block B through p, $|B \cap (v-\{p\})| \geq 1$ since $v \in C^{\perp}$. Hence

$$\lambda(|v|-1) \geq r$$

that is

$$|v| \geq \frac{r+\lambda}{\lambda} .$$

(iii) Now suppose $v \in C^{\perp}$ and $|v| = \frac{r+\lambda}{\lambda}$. Then we have $\sum_{\substack{B \\ p \in B}} |B \cap (v-\{p\})| = r$ and hence $|B \cap (v-\{p\})| = 1$ for each block B through p. So every block meets v either 0 or 2 times and in particular v is an oval of D.

Conversely suppose v is an oval of D. The relation $|v| = \frac{r+\lambda}{\lambda}$ implies that v has no tangent. So any block meets v either 0 or 2 times and so $v \in C^{\perp}$.

§6. Hadamard points on an oval

In this section we assume that the design D is a projective plane of order n divisible by 4.

Suppose that D has an oval O (which is of cardinality $n+2$). Let a be a point on O and B, C two secants through a. Let

$$B \cap O = \{a,b\}, \; C \cap O = \{a,c\} .$$

Let $\mathcal{A} = B - \{a,b\}$ and $\mathcal{E} = C - \{a,c\}$. Define an incidence relation I on $\mathcal{A}\times\mathcal{E}$ by $p \, I \, q$ if $\{p,q\}$ is in an exterior line to O, for $(p,q) \in \mathcal{A}\times\mathcal{E}$.

Note that $(\mathcal{A},\mathcal{E})$ is a 1-design since by proposition 1.5 every point of D not on O is on exactly $\frac{n}{2}$ exterior lines.

Proposition 1.10. If $(\mathcal{A},\mathcal{E})$ is a 2-design then $(\mathcal{A},\mathcal{E})$ is the complement of a Hadamard design.

Proof. If $(\mathcal{A},\mathcal{E})$ is a 2-design then it is projective since $|\mathcal{A}| = |\mathcal{E}| = n-1$; also every block of $(\mathcal{A},\mathcal{E})$ is incident with $\frac{n}{2}$ points, as remarked above. Then the relation $\lambda(v-1) = k(k-1)$ implies

$$\lambda = \frac{\frac{n}{2}(\frac{n}{2}-1)}{n-2} = \frac{n}{4} .$$

Hence $(\mathcal{A},\mathcal{E})$ is a $(4\lambda-1, 2\lambda, \lambda)$ design, the complement of a Hadamard design $(4\lambda-1, 2\lambda-1, \lambda-1)$.

Definition. Let $a \in O$ and let (B,C) be a pair of secants through a. We say that a is a quasi-Hadamard point if for some choice of (B,C) the incidence structure $(\mathcal{A},\mathcal{E})$ is a 2-design; we say that a is a Hadamard point if for any choice of (B,C) $(\mathcal{A},\mathcal{E})$ is a 2-design.

Now we assume that D is Desarguesian of order $n = 2^d$ and that the oval O is a conic together with its nucleus. We shall consider the usual representation of D, namely the points are the row vectors (x,y,z) with the usual identification, the lines are the column vectors $(a,b,c)^t$ with the usual identification, the point (x,y,z) and the line $(a,b,c)^t$ being incident if $ax + by + cz = 0$. It can be shown [9] that any conic of D is equivalent to the conic C defined by the equation $x^2 + yz = 0$. Thus

$$C = \left\{(t,t^2,1) : t \in GF(2^d)\right\} \cup \left\{(0,1,0)\right\}$$

Clearly the nucleus of C is the point $N = (1,0,0)$. Hence

$$O = \left\{(t,t^2,1) : t \in GF(2^d)\right\} \cup \left\{(0,1,0),(1,0,0)\right\} .$$

Moreover the subgroup G of the projective general linear group stabilizing C is triply transitive on the points of C and obviously fixes the nucleus N [9].

Proposition 1.11. The nucleus N is a Hadamard point on the oval O.

Proof. Because of the transitive properties of the group G we need consider only a particular pair of lines through N. We choose $\ell = (0,1,0)^t$ and $m = (0,0,1)^t$. Let $\ell' = \ell - \left\{(1,0,0),(0,0,1)\right\}$ and $m' = m - \left\{(1,0,0), (0,1,0)\right\}$. We want to know when the incidence structure (m',ℓ') is a 2-design. Clearly the points on ℓ' are the points $(1,0,a)$ where $a \neq 0$, those on m' are the points $(b,1,0)$ where $b \neq 0$. The line through $(1,0,a)$ and $(b,1,0)$ is the line $s = (a,ab,1)^t$. Clearly s does not contain the points $(1,0,0)$ and $(0,1,0)$ since $ab \neq 0$. Hence s is an exterior line if and only if $at + abt^2 + 1 \neq 0$ for any t.

A trivial change of variables shows that the condition can be written $a(t+t^2) \neq b$ for all $t \neq 0,1$. Hence (m',ℓ') is a 2-design if and only if given b, c with $b \neq c$, $bc \neq 0$ there is a fixed number (independent of b and c) of elements a such that

$$a(t+t^2) \neq b, \ a(t+t^2) \neq c$$

for all $t \neq 0,1$. Since (m',ℓ') is a 1-design, i.e.

there is a fixed number (independent of b) of elements a satisfying $a(t+t^2) \neq b$ for all $t \neq 0$ the above condition is equivalent to the following: there is a fixed number of elements a such that

$$a(t_o+t_o^2) = b, \ a(t_1+t_1^2) = c$$

for some t_o, t_1 where $t_o t_1 \neq 0,1$. This last condition is that the set $D = \left\{t+t^2 : t \neq 0,1\right\}$ is a difference set in the multiplicative group of $GF(2^d)$. Now consider the linear transformation $f : t \to t + t^2$ of $GF(2^d)$ considered as a d-dimensional space over $GF(2)$. Clearly $\mathrm{Ker}\ f = \left\{0,1\right\}$, a one-dimensional space so that $\mathrm{Im}\ f$ is a hyperplane. But $D = \mathrm{Im}\ f - \left\{0\right\}$. Hence D generates a difference set since $\mathrm{Im}\ f$ does.

Remark. The above argument also shows that any point of O distinct from N is a quasi-Hadamard point. To see this we consider the point $(0,1,0)$ (since G is transitive on C) and the two lines $m = (0,0,1)^t$ and $w = (1,0,0)^t$; the rest of the argument is the same as above. However we were unable to show that the points of C are not Hadamard points.

The Desarguesian projective plane of order 16.

It is well known that the projective planes of order 4 and 8 are unique up to isomorphism [7] and hence they are Desarguesian. An oval in those planes is necessarily a nondegenerate conic together with its nucleus [6]. In [6] M. Hall shows that in the Desarguesian plane of order 16 there are, up to isomorphism, two ovals one of which is of course the conic with its nucleus. The other oval is acted on transitively by a group of collineations of the plane. Using Hall's representation we have found with the help of the Lehigh computer that no point on this second oval is quasi-Hadamard.

CHAPTER 2

CODES FROM CLASSICAL UNITALS

§1. Correlations and polarities

Let $\mathbf{P}$ be a projective plane. A correlation of $\mathbb{P}$ is a one-to-one mapping θ of the points of $\mathbb{P}$ onto the lines of $\mathbf{P}$ and the lines of $\mathbf{P}$ onto the points of $\mathbf{P}$ such that a point p is on a line L if and only if L^θ is on p^θ. The product of any two correlations is of course a collineation. A polarity of $\mathbb{P}$ is a correlation θ such that θ^2 is the identity collineation.

An absolute point or line of a correlation θ is one that is incident with its image under θ.

Since we are mainly interested in the finite Desarguesian case we shall restrict ourselves to this case. It turns out that then a correlation is given by a sesquilinear form on the underlying space of the geometry. Let V be a vector space of rank 3 over the field $K = GF(\ell)$ and let $\mathbf{P}$ be the projective plane over V. Let α be an automorphism of K. A sesquilinear form on V with companion automorphism α is a mapping $s : V \times V \to K$ such that

(i) s is additive in both variables,

(ii) $s(ax,by) = as(x,y)b^{\alpha}$ for all $a,b \in K$, $x,y \in V$. s is nondegenerate if $s(x,y) = 0$ for all $y \in V$ is equivalent to $x = 0$.

If s is a nondegenerate sesquilinear form on V and S is a one or two-dimensional subspace of V (i.e. a point or a line of $\mathbb{P}$) then it can be shown [5] that the mapping θ given by

$$S^{\theta} = \left\{x \in V : s(x,y) = 0 \text{ for all } y \in S\right\} \qquad (*)$$

defines a correlation of the plane $\mathbb{P}$. Conversely if θ is a correlation of $\mathbf{P}$ then there exists a nondegenerate sesquilinear form s on V such that θ is given by (*). Moreover it is easily seen that a form s on V represents a polarity if and only if

$$s(x,y) = 0 \text{ implies } s(y,x) = 0 \text{ for all } x,y \in V .$$

The following result classifies the polarities of $\mathbf{P}$. Further details may be found in [5].

Proposition 2.1. Let s be a nondegenerate sesquilinear form on V with companion automorphism α. If s represents a polarity θ of the plane $\mathbb{P}$ then one of the following holds:

(i) $\alpha = 1$, $s(x,y) = s(y,x)$ for all $x,y \in V$ and if the characteristic of K is 2 then $s(z,z) \neq 0$ for some $z \in V$ (in this case we say that θ or s is orthogonal).

(ii) $\alpha = 1$, $s(x,x) = 0$ for all $x \in V$ (we then say that θ or s is symplectic).

(iii) α is of order 2, $s(x,y) = s(y,x)^{\alpha}$ for all $x,y \in V$ (we say that θ or s is unitary).

The next result gives all unitary polarities over the finite Desarguesian plane **P**. Further details are also contained in [5].

Proposition 2.2. V admits unitary forms if and only if ℓ is a square, say $\ell = q^2$. In this case any unitary form t is equivalent to the form

$$s : (x,y) \to \sum_{1 \leq i \leq 3} x_i y_i^q$$

i.e. the polarities defined by s and t are conjugate under a collineation of the plane **P**.

§2. The unital.

Let s be the standard unitary form

$$(x,y) \to x_1 y_1^q + x_2 y_2^q + x_3 y_3^q$$

of the space V. Let θ be the polarity of the plane $\mathbb{P}$ given by s. Let $\Gamma U_3(q^2)$, $GU_3(q^2)$ and $SU_3(q^2)$ denote the group of semilinear, linear and determinant 1 linear transformations of V that preserve the form s and let $P\Gamma U_3(q^2)$, $PGU_3(q^2)$ and $PSU_3(q^2)$ be the corresponding central factor groups. Finally let U be the set of absolute points of θ i.e. the points represented by nonzero vectors $x = (x_1,x_2,x_3)$ of V such that $x_1^{q+1} + x_2^{q+1} + x_3^{q+1} = 0$.

The following result may be found in [9].

Proposition 2.3

(i) $|U| = q^3 + 1$.

(ii) A line ℓ of the plane $\mathbb{P}$ intersects U at 1 or $q + 1$ points according as ℓ is absolute or not.

(iii) The groups $P\Gamma U_3(q^2)$, $PGU_3(q^2)$, $PSU_3(q^2)$ act on U as doubly transitive permutation groups.

Hence the points of U together with the non-absolute lines (incidence induced by that of $\mathbb{P}$) form a 2-$(q^3+1,q+1,1)$ design with block and replication numbers

$$b = q^2(q^2-q+1), \quad r = q^2 .$$

This design will be called unital. (In particular through every point $p \in U$ there passes one absolute line, which must be the image of p under θ, and q^2 nonabsolute lines). M. O'Nan [11] has proved that the full automorphism group of this unital is $P\Gamma U_3(q^2)$.

Proposition 2.4. Let p be a point of $\mathbb{P}$ not in U.

(i) Through p there pass $q+1$ absolute lines and q^2-q nonabsolute lines.

(ii) The $q+1$ points of U which are on the $q+1$ absolute lines through p are collinear on a line ℓ which is the image of p under θ.

Proof.

(i) Let x, y be the number of absolute and non-absolute lines through p. We have $x + y = q^2 + 1$. Counting in two ways the set

$$\left\{(a,\ell) : a \in U, \ \ell \text{ a line through } a \text{ and } p\right\}$$

we have

$$x + (q+1)y = q^3 + 1.$$

Hence $x = q + 1$ and $y = q^2 - q$.

(ii) Let a and b be two absolute points on two absolute lines through p. Say a, b and p are given by the nonzero vectors u, v, w of V. Let ℓ be the line through a, b and let c be any absolute point on ℓ. Say c is given by $\alpha u + \beta v$ where $\alpha, \beta \in GF(q^2)$. Then for any $\eta, \zeta \in GF(q^2)$, we have

$$\begin{aligned} & s(\alpha u+\beta v, \eta(\alpha u+\beta v)+\zeta w) \\ & = s(\alpha u+\beta v, \zeta w) \quad \text{since c is absolute} \\ & = s(\alpha u, \zeta w) + s(\beta v, \zeta w) \\ & = 0 \end{aligned}$$

since the lines through p, a and p, b are absolute. Hence the image of c under θ is the line through c and p. Since there are q+1 absolute points on ℓ and q+1 absolute lines through p, our claim is proved. Now ℓ is the image of p under θ since it has two distinct points, a and b, whose images under θ contain p.

§3. Codes from the unital

Let M denote the incidence matrix of the unital U and let C be the code equal to the row span of M over a given field GF(p), where p is a prime. This code C is interesting only if p divides the order of U which is q^2-1 [8]. We note that the projective unitary groups are doubly transitive automorphisms groups of C.

Proposition 2.5.

(i) The code C always contains the all-one vector.

(ii) If q is odd and $p = 2$ then the dual code $C^{\perp}$ also contains the all one vector.

Proof.

(i) Let p be a point not on U. The q^2-q non-absolute lines through p give rise to q^2-q pairwise disjoint blocks of U. Also the block formed by the $q+1$ points of intersection of U with the $q+1$ absolute lines through p is disjoint from anyone of the above q^2-q blocks. Since $(q^2-q+1)(q+1) = |U|$ we conclude that those q^2-q+1 blocks form a partition of U and so the all one vector is in C.

(ii) is clear since each row of M has weight $q+1$.

Consider the particular case $q = 3$, $p = 3$.

A straightforward computer calculation has shown that $C^{\perp}$ is a binary $(28,7)$ code whose weight enumerator is

$$W_{C^{\perp}}(x) = 1 + 63(x^{12}+x^{16}) + x^{28} .$$

Hence C is a $(28,21)$ code whose weight enumerator, by the MacWilliams equation, is

$$W_C(x) = 1 + 3^2.5.7(x^4+x^{24}) + 2^5.3^3.7(x^6+x^{22})$$
$$+ 3^3.7.11.23(x^8+x^{20}) + 2^7.3.7^2.11(x^{10}+x^{18})$$
$$+ 3^2.7.59.127(x^{12}+x^{16}) + 2^6.5.3^3.73x^{14} + x^{28}.$$

Since $C^\perp$ is doubly even we conclude that $C^\perp \subset C$. Also note that here the size of an oval of the unital is $3^2 + 1 = 10$. Since $C^\perp$ has no vectors of weight 10 we conclude from Proposition 1.9 that the unital does not contain any oval. We can prove this in general but first we require a lemma, a proof of which may be found in [12].

Lemma 2.1. Suppose $n \geq 2$. Let $u_1(x_1,\ldots,x_n)$ and $u_2(x_1,\ldots,x_n)$ be polynomials over $GF(\ell)$ of respective total degrees e_1 and e_2, without common factor of positive degree. Then the number of their common zeros in $GF(\ell)^n$ is at most

$$\ell^{n-2}e_1e_2 \min\{e_1,e_2\} .$$

Proposition 2.6. If q is odd, $q \geq 3$, then the unital U does not contain any oval.

Proof. Because of the above discussion we assume that $q \geq 5$. Now the size of an oval in U is $q^2 + 1$ which is also the size of an oval in the ambient plane $\mathbb{P}$. Since a line of $\mathbf{P}$ either meets U at only one point or is a block of U we see that an oval of U is an oval of $\mathbf{P}$. But since here $\mathbf{P}$ is of odd order, an oval of $\mathbf{P}$ must be a nondegenerate conic, by Segre's theorem [9]. Such a conic is given by all nonzero vectors $x = (x_1, x_2, x_3)$ satisfying an irreducible equation

$$ax_1^2 + bx_1x_2 + cx_2^2 + dx_1x_3 + ex_2x_3 + fx_3^2 = 0 .$$

The points of U are given by all nonzero vectors $x = (x_1, x_2, x_3)$ satisfying

$$x_1^{q+1} + x_2^{q+1} + x_3^{q+1} = 0 .$$

By the lemma the number of common zeros to those two equations is at most $4q^2(q+1)$. We conclude that the number of points common to the conic and the unital is at most

$$\frac{4q^2(q+1)-1}{q^2-1} .$$

It is easy to see that this number is less than $q^2 + 1$ since $q \geq 5$. This proves the proposition.

Corollary. If q is odd and $p = 2$ then the minimum weight of $C^\perp$ is at least $q^2 + 3$.

Proof. By Proposition 1.9 the minimum weight d of $C^\perp$ is at least $q^2 + 1$; but $d > q^2 + 1$ since U has no ovals. Hence $d \geq q^2 + 3$ because $C^\perp$ is even.

We would like next to discuss our unsuccessful attempt to give a formula for the dimension of the code C. We have done some computer calculations and come up with the following table:

q	p	dim $C^\perp$	Is $C^\perp \subset C$?
2	3	$3 = q^2 - q + 1$	yes
3	2	$7 = q^2 - q + 1$	yes
4	5	$13 = q^2 - q + 1$	yes
5	2	$21 = q^2 - q + 1$	no
5	3	$21 = q^2 - q + 1$	yes

We remark that for $q = 4$, $p = 3$ we have found that dim $C^\perp = 0$. It seems to us then that for p dividing $q + 1$ the dimension of $C^\perp$ is $q^2 - q + 1$. We would like to formulate this as a conjecture.

Conjecture: If p is a prime dividing $q+1$ then the dimension of $C^\perp$ over $GF(p)$ is $q^2 - q + 1$.

CHAPTER 3

CODES FROM IRREDUCIBLE ROOT SYSTEMS

§1. Root systems

Let V be a real Euclidean space in which the scalar product of two vectors x, y is denoted (x,y).

For any nonzero vector x in V, the reflection in the hyperplane perpendicular to x is the orthogonal transformation w_x of V given by

$$w_x(y) = y - \frac{2(x,y)}{(x,x)} x .$$

A root system in V is a set ϕ of vectors in V satisfying the following conditions:

R1. ϕ is finite and $0 \notin \phi$.

R2. ϕ generates the space V.

R3. For all $x, y \in \phi$, $\frac{2(x,y)}{(x,x)} \in \mathbb{Z}$.

R4. For all $x, y \in \phi$, $w_x(y) \in \phi$.

R5. If $x \in \phi$ and $\lambda x \in \phi$, where $\lambda \in \mathbb{R}$, then $\lambda = \pm 1$.

The elements of such a set are called roots.

The subgroup of the orthogonal group of V generated by all w_x, $x \in \phi$, is called the Weyl group of ϕ. It will be denoted $W(\phi)$ (or simply W if there is no ambiguity). It is easy to see that W is a permutation group of ϕ.

A fundamental system of a root system ϕ is a subset π of ϕ satisfying the following conditions:

F1. π is a basis for the space V.

F2. For every $x = \sum_{i=1}^{\ell} \lambda_i p_i$ in ϕ where $\pi = \left\{p_1, \ldots, p_\ell\right\}$ the coefficients λ_i are rational integers that are all nonnegative or all nonpositive.

Given such a subset π the roots in π will be called the fundamental roots of ϕ. An element $x = \Sigma\, \lambda_i p_i$ in ϕ is called a positive (resp. negative) root with respect to π if $\lambda_i \geq 0$ (resp. $\lambda_i \leq 0$) for all i. The set of all positive (resp. negative) roots with respect to π is denoted ϕ_π^+ (resp. ϕ_π^-) or simply ϕ^+ (resp. ϕ^-) if there is no ambiguity.

It can be shown [4] that any root system admits a fundamental system and that the Weyl group operates sharply transitively on the fundamental systems.

Given a root system ϕ, the coroot associated with $x \in \phi$ is the vector $h_x = \frac{2x}{(x,x)}$. It can be shown [4] that the set $\phi^* = \left\{h_x \mid x \in \phi\right\}$ is also a root system and that the coroots associated with the elements of a fundamental system in ϕ form a fundamental system of ϕ^*. The system ϕ^* will be called the dual of ϕ. We remark that $\phi^{**} = \phi$.

Two root systems ϕ_1 and ϕ_2 are said to be equivalent if there is a bijection $f : \phi_1 \to \phi_2$ and a nonzero real number λ such that $(f(x), f(y)) = \lambda(x,y)$ for all x, y in ϕ_1. A root system ϕ is self-dual if ϕ^* is equivalent to ϕ.

§2. Irreducible root systems

A root system ϕ is said to be irreducible if ϕ cannot be partitioned into two nonempty subsets ϕ_1 and ϕ_2 such that $(x,y) = 0$ for all $x \in \phi_1$ and $y \in \phi_2$.

The following result, a proof of which may be found in [3], allows us to study only irreducible root systems.

Proposition 3.1. Any root system ϕ of the space V is the sum of irreducible root systems, i.e. V can be written as

$$V = \bigoplus_{i \in I} V_i$$

such that:

(i) The subspaces V_i are pairwise orthogonal,

(ii) ϕ is contained in $\bigcup_{i \in I} V_i$, and

(iii) Each $\phi_i = \phi \cap V_i$ is an irreducible root system in V_i.

In fact all irreducible root systems are known. It can be proved [3] that an irreducible root system is equivalent to one of the systems described below.

<u>Type A_ℓ.</u> Let $E = \mathbf{R}^{\ell+1}$, let $\{e_0, e_1, \ldots, e_\ell\}$ be an orthonormal basis for E and let V be the subspace of E consisting of all $x = \sum_{i=0}^{\ell} \lambda_i e_i$ such that $\sum_{i=0}^{\ell} \lambda_i = 0$. The vectors $e_i - e_j$, $i \neq j$, form a root system in V that is said to be of type A_ℓ. A fundamental system consists of the vectors $e_i - e_{i+1}$, $i = 0, 1, \ldots, \ell-1$. With respect to this fundamental system, the positive roots are the vectors $e_i - e_j$ where $0 \leq i < j \leq \ell$.

It can be shown that here the Weyl group is isomorphic to the symmetric group on $\ell+1$ letters.

<u>Type B_ℓ.</u> Let $V = \mathbb{R}^\ell$ and let $\{e_1, e_2, \ldots, e_\ell\}$ be an orthonormal basis for V. The vectors $\pm e_i$, $\pm e_i \pm e_j$ with $i < j$ form a root system in V that is said to

be of type B_ℓ. A fundamental system consists of the vectors $e_i - e_{i+1}$, $i = 1,2,\ldots,\ell-1$ and the vector e_ℓ. With respect to this fundamental system, the positive roots are the vectors e_i, $e_i - e_j$ and $e_i + e_j$ where $1 \leq i < j \leq \ell$. Here the Weyl group is a semidirect product of $\mathbb{Z}_2^\ell$ with the symmetric group on ℓ letters.

Type C_ℓ. The notation is the same as in B_ℓ. The vectors $\pm 2e_i$, $\pm e_i \pm e_j$ with $i < j$ form a root system that is said to be of type C_ℓ. A fundamental system consists of the vectors $e_i - e_{i+1}$, $i = 1,2,\ldots,\ell-1$ and the vector $2e_\ell$. With respect to this fundamental system, the positive roots are the vectors $2e_i$, $e_i - e_j$ and $e_i + e_j$ where $1 \leq i < j \leq \ell$. The Weyl group is the same as that of B_ℓ.

Type D_ℓ. The notation is the same as in B_ℓ. The vectors $\pm e_i \pm e_j$ with $i < j$ form a root system that is said to be of type D_ℓ. A fundamental system consists of the vectors $e_i - e_{i+1}$, $i = 1,2,\ldots,\ell-1$ and the vector $e_{\ell-1} + e_\ell$. With respect to this fundamental system the positive roots are the vectors $e_i - e_j$ and $e_i + e_j$ where $1 \leq i < j \leq \ell$. Here the Weyl group is a semidirect product of $\mathbb{Z}_2^{\ell-1}$ with the symmetric group on ℓ letters.

Type G_2. Let $E = \mathbb{R}^3$. Let $\left\{e_1, e_2, e_3\right\}$ be an orthonormal basis for E and let V be the hyperplane consisting of all $x = \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3$ such that $\lambda_1 + \lambda_2 + \lambda_3 = 0$. The vectors $\pm(e_1-e_2)$, $\pm(e_1-e_3)$, $\pm(e_2-e_3)$, $\pm(2e_1-e_2-e_3)$, $\pm(2e_2-e_1-e_3)$, $\pm(2e_3-e_1-e_2)$ form a root system that is said to be of type G_2. A fundamental system consists of the vectors $p_1 = e_1-e_2$ and $p_2 = -2e_1 + e_2 + e_3$. With respect to this fundamental system the positive roots are the vectors p_1, p_2, $p_1 + p_2$, $2p_1 + p_2$, $3p_1 + p_2$, $3p_1 + 2p_2$. Here the Weyl group is the dihedral group D_6 of order 12.

Type F_4. Let $V = \mathbf{R}^4$ and let $\left\{e_1, e_2, e_3, e_4\right\}$ be an orthonormal basis for V. The vectors $\pm e_i$, $\pm e_i \pm e_j$ $(1 \leq i < j \leq 4)$ and $\frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4)$ form a root system in V that is said to be of type F_4. A fundamental system consists of the vectors e_2-e_3, e_3-e_4, e_4, $\frac{1}{2}(e_1-e_2-e_3-e_4)$. With respect to this fundamental system, the positive roots are e_i, $e_i \pm e_j$ $(1 \leq i < j \leq e)$, $\frac{1}{2}(e_1 \pm e_2 \pm e_3 \pm e_4)$. Here the Weyl group is a semidirect product of the symmetric group on 3 letters with a semidirect product of the symmetric group on 4 letters with $\mathbf{Z}_2^3$.

In the rest of this section we let $E = \mathbb{R}^8$. Let $\left\{e_1,\ldots,e_8\right\}$ be an orthonormal basis for E.

Type E_8. The vectors $\pm e_i \pm e_j$ $(1 \leq i < j \leq 8)$ and $\frac{1}{2}\sum_{i=1}^{8} (-1)^{\varepsilon(i)} e_i$, with $\sum_{i=1}^{8} \varepsilon(i)$ even, form a root system in E that is said to be of type E_8. A fundamental system consists of the vectors $p_1 = \frac{1}{2}(e_1-e_8) - \frac{1}{2}(e_2+e_3+e_4+e_5+e_6+e_7)$, $p_2 = e_1+e_2$, $p_3 = e_2-e_1$, $p_4 = e_3-e_2$, $p_5 = e_4-e_3$, $p_6 = e_5-e_4$, $p_7 = e_6-e_5$, $p_8 = e_7-e_6$. With respect to this fundamental system the positive roots are $\pm e_i + e_j$ $(1 \leq i < j \leq 8)$ and $\frac{1}{2}(e_8 + \sum_{i=1}^{7} (-1)^{\varepsilon(i)} e_i)$ where $\sum_{i=1}^{7} \varepsilon(i)$ is even.

Type E_7. Let V be the hyperplane of E orthogonal to the vector e_7+e_8. The vectors $\pm e_i + e_j$ $(1 \leq i < j \leq 6)$, $\pm(e_7-e_8)$, $\pm\frac{1}{2}(e_7-e_8 + \sum_{i=1}^{6} (-1)^{\varepsilon(i)} e_i)$, with $\sum_{i=1}^{6} \varepsilon(i)$ odd, form a root system in V that is said to be of type E_7. A fundamental system consists of the vectors $p_1, p_2, \ldots p_7$ described above. The positive roots are then $\pm e_i + e_j$

$(1 \leq i < j \leq 6)$, $e_8 - e_7$, $\frac{1}{2}(e_8 + e_7 + \sum_{i=1}^{6} (-1)^{\varepsilon(i)} e_i$ where $\sum_{i=1}^{6} \varepsilon(i)$ is odd.

Type E_6. Let V' be the subspace of E consisting of the vectors whose coordinates (λ_i) satisfy $\lambda_6 = \lambda_7 = -\lambda_8$. The vectors $\pm e_i \pm e_j$ $(1 \leq i < j \leq 5)$, $\pm \frac{1}{2}(e_8 - e_7 - e_6 + \sum_{i=1}^{5} (-1)^{\varepsilon(i)} e_i)$, with $\sum_{i=1}^{5} \varepsilon(i)$ even, form a root system in V' that is said to be of type E_6. A fundamental system consists of the vectors $p_1, p_2, \ldots, p_6$ described above. The positive roots are then $\pm e_i + e_j$ $(1 \leq i < j \leq 5)$ and $\frac{1}{2}(e_8 - e_7 - e_6 + \sum_{i=1}^{5} (-1)^{\varepsilon(i)} e_i)$ where $\sum_{i=1}^{5} \varepsilon(i)$ is even.

§3. Definition of the codes from root systems

Let ϕ be a root system in the space V and let

$$Q = \left\{ v \in V \mid (v, r) \in \mathbb{Z} \text{ for all } r \in \phi^* \right\} .$$

It is known [3] that Q is a free Abelian group of rank equal to the dimension of V. (Q is called the group of weights of Q in the literature). Moreover there exists a basis $\left\{q_1, \ldots, q_\ell\right\}$ for Q such that

$(q_i, h_{p_j}) = \delta_{ij}$ (Kronecher delta) if $\{p_1, \ldots, p_\ell\}$ is a fundamental system of ϕ. Clearly Q is invariant under the Weyl group W.

Now consider the mapping T of Q into the free abelian group $\mathbf{Z}^{\phi^*}$ of all functions from ϕ^* to $\mathbf{Z}$ given by

$$T(q)(r) = (q,r) \quad \text{for all} \quad r \in \phi^* .$$

Clearly T is an Abelian group homomorphism. Moreover it is one-to-one since $T(q) = 0$ means that $(q,r) = 0$ for all $r \in \phi^*$ so that $q = 0$ since ϕ^* generates V. Hence $T(Q)$ is a (n, ℓ) code over $\mathbb{Z}$ where $n = |\phi|$, $\ell = \operatorname{rank} Q = \dim V$. Of course we can read $T(Q)$ over any finite field $GF(p)$ and get a (n,ℓ) code over $GF(p)$.

Lemma 3.1. The Weyl group W acts on the code $T(Q)$.

Proof. The group W acts on $\mathbb{Z}^{\phi^*}$ by the formula $(f\cdot w)(r) = f(w(r))$ where $f \in \mathbf{Z}^{\phi^*}$, $w \in W$, $r \in \phi^*$. Thus for any $q \in Q$, $w \in W$, $r \in \phi^*$ we have

$$[T(q)\cdot w](r) = T(q)(w(r)) = (q, w(r)) = (w^{-1}(q), r)$$

$$= T(w^{-1}(q))(r).$$

Hence $T(q)\cdot w = T(w^{-1}(q)) \in T(Q)$.

Lemma 3.2. A generator matrix for the code $T(Q)$ is given by the ℓ-by-n matrix whose column corresponding to the coroot h_r consists of the coordinates of h_r in the fundamental system $\{h_{p_1},\ldots,h_{p_\ell}\}$ of ϕ^* where $\{p_1,\ldots,p_\ell\}$ is a fundamental system of ϕ.

Proof. Let $\{q_1,\ldots,q_\ell\}$ be the basis for Q such that $(q_i,h_{p_j}) = \delta_{ij}$ for all i,j. Suppose $h_r = \sum \lambda_j h_{pj}$. Then we have

$$(T(q_i))(h_r) = (q_i, \sum \lambda_j h_{pj}) = \lambda_i .$$

From now on we assume that ϕ is an irreducible root system and that the corresponding code is read in GF(2). In this case the generator matrix given by Lemma 2 is of the form $M|M$ where the columns of M correspond to the positive roots in ϕ^*. We will study the binary code whose generator matrix is M and denote that code by A_ℓ, B_ℓ,... etc according as ϕ is of type A_ℓ, B_ℓ,... etc. Note however that the identity is the only element of the Weyl group that is in the automorphism group of any of the codes A_ℓ, B_ℓ,... etc. This is so because the identity is the only element of the Weyl group that fixes the positive roots setwise [4]. The code with generator matrix $M|M$ will be denoted $\tilde{A}_\ell$, $\tilde{B}_\ell$,... etc.

The codes $\tilde{A}_\ell$, $\tilde{B}_\ell, \ldots$ etc. may be useful in studying the codes A_ℓ, $B_\ell, \ldots$ etc. We recall the following fundamental result, a proof of which may be found in [3].

Proposition 3.2. Let ϕ be an irreducible root system. If x and y are roots of the same length then there exists an element $w \in W$ with $w(x) = y$.

Corollary. The Weyl group acts as a transitive automorphism group of the codes $\tilde{A}_\ell$, $\tilde{D}_\ell$, $\tilde{E}_6$, $\tilde{E}_7$ and $\tilde{E}_8$.

Proof. This follows immediately from Lemma 3.1 and Proposition 3.2.

§4. A listing of generator matrices

We use the standard root systems given in §2 to determine explicitly the matrix M of §3 in each case.

$$\begin{array}{cccccccc}
 & 1000\ldots00 & 111\ldots11 & 000\ldots00 & \ldots & 00 & 0 \\
 & 0100\ldots00 & 111\ldots11 & 111\ldots11 & \ldots & 00 & 0 \\
A_\ell & 0010\ldots00 & 011\ldots11 & 111\ldots11 & \ldots & 00 & 0 \\
 & 0001\ldots00 & 001\ldots11 & 011\ldots11 & \ldots & 00 & 0 \\[8pt]
 & 0000\ldots00 & 000\ldots11 & 000\ldots11 & \ldots & 11 & 0 \\
 & 0000\ldots10 & 000\ldots11 & 000\ldots11 & \ldots & 11 & 1 \\
 & 0000\ldots01 & 000\ldots01 & 000\ldots01 & \ldots & 01 & 1 \\[8pt]
 & \ell & \ell-1 & \ell-2 & & 2 & 1
\end{array}$$

$$\begin{array}{cllllllll}
 & 1000\ldots00 & 00\ldots01 & 111\ldots11 & 000\ldots00 & \ldots0 & 111\ldots11 & 000\ldots00 & \ldots0 \\
 & 0100\ldots00 & 00\ldots11 & 111\ldots11 & 111\ldots11 & \ldots0 & 011\ldots11 & 111\ldots11 & \ldots0 \\
C_\ell & 0010\ldots00 & 00\ldots11 & 011\ldots11 & 111\ldots11 & \ldots0 & 001\ldots11 & 011\ldots11 & \ldots0 \\
 & 0001\ldots00 & 00\ldots11 & 001\ldots11 & 011\ldots11 & \ldots0 & 000\ldots11 & 001\ldots11 & \ldots0 \\[1ex]
 & 0000\ldots00 & 01\ldots11 & 000\ldots11 & 000\ldots11 & \ldots1 & 000\ldots11 & 000\ldots11 & \ldots0 \\
 & 0000\ldots10 & 11\ldots11 & 000\ldots01 & 000\ldots01 & \ldots1 & 000\ldots01 & 000\ldots01 & \ldots1 \\
 & 0000\ldots01 & 11\ldots11 & 000\ldots00 & 000\ldots00 & \ldots0 & 000\ldots00 & 000\ldots00 & \ldots0 \\[1ex]
 & \ell & \ell-1 & \ell-2 & \ell-3 & 1 & \ell-1 & \ell-2 & 1
\end{array}$$

Note that the first $\frac{1}{2}\ell(\ell+1)$ columns of the matrix of B_ℓ are just a permutation of the columns of the matrix A_ℓ.

$$\begin{array}{cllllllll}
 & 1000\ldots00 & 00\ldots00 & 111\ldots11 & 000\ldots00 & \ldots0 & 111\ldots11 & 000\ldots00 & \ldots0 \\
 & 0100\ldots00 & 00\ldots00 & 111\ldots11 & 111\ldots11 & \ldots0 & 011\ldots11 & 111\ldots11 & \ldots0 \\
 & 0010\ldots00 & 00\ldots00 & 011\ldots11 & 111\ldots11 & \ldots0 & 001\ldots11 & 011\ldots11 & \ldots0 \\
B_\ell & 0001\ldots00 & 00\ldots00 & 001\ldots11 & 011\ldots11 & \ldots0 & 000\ldots11 & 001\ldots11 & \ldots0 \\[1ex]
 & 0000\ldots00 & 00\ldots00 & 000\ldots11 & 000\ldots11 & \ldots1 & 000\ldots11 & 000\ldots11 & \ldots0 \\
 & 0000\ldots10 & 00\ldots00 & 000\ldots01 & 000\ldots01 & \ldots1 & 000\ldots01 & 000\ldots01 & \ldots1 \\
 & 0000\ldots01 & 11\ldots11 & 000\ldots00 & 000\ldots00 & \ldots0 & 111\ldots11 & 111\ldots11 & \ldots1 \\[1ex]
 & \ell & \ell-1 & \ell-2 & \ell-3 & 1 & \ell-1 & \ell-2 & 1
\end{array}$$

$$\begin{array}{clllllll}
 & 1000\ldots00 & 111\ldots11 & 000\ldots00 & \ldots0 & 111\ldots11 & 000\ldots00 & \ldots00 \\
 & 0100\ldots00 & 111\ldots11 & 111\ldots11 & \ldots0 & 011\ldots11 & 111\ldots11 & \ldots00 \\
 & 0010\ldots00 & 011\ldots11 & 111\ldots11 & \ldots0 & 001\ldots11 & 011\ldots11 & \ldots00 \\
D_\ell & 0001\ldots00 & 001\ldots11 & 011\ldots11 & \ldots0 & 000\ldots11 & 001\ldots11 & \ldots00 \\[1ex]
 & 0000\ldots00 & 000\ldots11 & 000\ldots11 & \ldots1 & 000\ldots11 & 000\ldots11 & \ldots11 \\
 & 0000\ldots10 & 000\ldots01 & 000\ldots01 & \ldots1 & 111\ldots10 & 111\ldots10 & \ldots10 \\
 & 0000\ldots01 & 000\ldots00 & 000\ldots00 & \ldots0 & 111\ldots11 & 111\ldots11 & \ldots11 \\[1ex]
 & \ell & \ell-2 & \ell-3 & 1 & \ell-1 & \ell-2 & 2
\end{array}$$

```
G₂:   101011
      011110

F₄:   100011001110111101111000
      010001111011100110011110
      001011100000000001001011
      000100000000000000111111

      100000111111000000000000001011011111
      010000000011100011100111011111111110
E₆:   001000111111111111000000011101101000
      000100011111111111111111000000000011
      000010001101101101111011111111010000
      000001000100100100101001100101111111

                     000001001010110111111111110
                     000000111111111111110100000
                     000011011111011010000000011
E₇:        E₆        000111111000000000111111000
                     001111111110100000000101111
                     011111111111110100101000000
      000...00111111111111111111111111111

E₈:        E₇          M          N
      000...00
```

where

```
M:    0000001001001011110111
      0000000111111111111111
      0000011011111101011001
      0000111111000000000100
      0001111111101010000000
      0011111111111011100100
      0111111111111111110110
      1111111111111111111111
```

```
     11111111111111101101101101000000000
     01101100100100000000000001010111111
N:   00000000000010011011011111110000000
     11011111101100100000000101111100000
     00001010111111111111010000000001111
     10000000000100100101111111111111000
     11011010010010010000000000000000011
     11111111111111111111111111111111110
```

§5. The code A_ℓ $(\ell \geq 2)$

In this section we let $n = \frac{1}{2}\ell(\ell+1)$.

Proposition 3.3.

(i) A_ℓ is a (n, ℓ) code.

(ii) the minimum weight d of A_ℓ is ℓ.

(iii) A_ℓ is even if and only if ℓ is even.

Proof.

(i) is clear.

(ii) is proved by induction on ℓ. The weight enumerator of A_2 is easily seen to be $1 + 3x^2$. Now consider the generator matrix of A_ℓ, $\ell > 2$. The first and last rows are both of weight ℓ so that $d \leq \ell$. Now if we remove row ℓ and columns ℓ, $\ell+(\ell-1)$, $\ell+(\ell-1)+(\ell-2), \ldots, \frac{1}{2}\ell(\ell+1)$ then we get the generator matrix $A_{\ell-1}$. Then consider a sum S of rows of the matrix of A_ℓ. Using the code $\tilde{A}_\ell$ and the transitivity of the Weyl group on the roots, we may assume that S

involves the last row. Now by the induction hypothesis the weight of S minus the last row is at least $\ell-1$. Hence the weight of S is at least ℓ because the last entry in column ℓ is 1, the other entries zero.

To prove (iii) we note that the weights of the generator matrix for A_ℓ are respectively ℓ, $2(\ell-1)$, $3(\ell-2),\ldots,\ell$.

Proposition 3.4. The dual $A_\ell^\perp$ of A_ℓ, which is a $(n,n-\ell)$ code, has minimum weight equal to 3 and the number of vectors of weight 3 in $A_\ell^\perp$ is $a(\ell)$ where

$$a(\ell) = (\ell-1)^2 + \binom{2}{2} + \binom{3}{2} + \ldots + \binom{\ell-2}{2} .$$

(For $\ell = 2$ and 3 this number is to be interpreted as 1 and 4 respectively)

Proof. Recall that if a generator matrix of a binary (n,ℓ) code is of the form $I_\ell|G$ then a generator matrix of the dual code is $G^t|I_{n-\ell}$. Hence the following matrix is a generator matrix for $A_\ell^\perp$:

$$\begin{array}{lll}
 & 110000\ldots00 & \\
 & 111000\ldots00 & \\
\ell-1 & 111100\ldots00 & \\
 & \vdots & \\
 & 111111\ldots11 & \\
 & 011000\ldots00 & \\
 & 011100\ldots00 & \\
\ell-2 & 011110\ldots00 & \\
 & \vdots & n-\ell \\
 & 011111\ldots11 & \\
 & \quad\vdots & \\
 & 000000\ldots11 & \\
 & \quad\ell &
\end{array}$$

Rows 1, $1+(\ell-1)$, $1+(\ell-1)+(\ell-2),\ldots$ etc. are of weight 3, the other rows of weight grater than 3. If we add up two rows then the sum has at least one nonzero coordinate in its first ℓ coordinates since the rows are all distinct in their first ℓ coordinates. We conclude that the minimum weight of $A_{\ell}^{\perp}$ is 3.

Now there are $\ell-1$ rows of weight 3.

Next we count the number of unordered pairs of rows whose sum has precisely one nonzero coordinate in its first ℓ coordinates. The number of such distinguished pairs for $A_3^{\perp}$ is easily seen to be 2. Assume by induction that the number of such pairs for $A_{\ell-1}^{\perp}$ is

$(\ell-3)(\ell-2)$. A distinguished pair that involves any of the first $\ell-1$ rows in the matrix of $A_\ell^\perp$ has to involve another of those rows or one of the next $\ell-2$ rows. In the first case we have to take two consecutive rows so that we get $\ell-2$ pairs. In the second case we have to match row i of the first $\ell-1$ rows with row $\ell+i-2$ for $2 \leq i \leq \ell-1$ so that we also get $\ell-2$ pairs. Hence the number of distinguished pairs of rows in $A_\ell^\perp$ is

$$(\ell-3)(\ell-2) + 2(\ell-2) = (\ell-2)(\ell-1).$$

Next we count the number of unordered triples of rows whose sum has all of its first ℓ coordinates equal to zero. The number of such distinguished triples of rows is 0 and 1 for $A_3^\perp$ and $A_4^\perp$ respectively. Assume by induction that the number of such triples is $\binom{2}{2} + \binom{3}{2} +\ldots+ \binom{\ell-3}{2}$, $\ell \geq 5$, for $A_{\ell-1}^\perp$. A distinguished triple that involves any of the first $\ell-1$ rows in the matrix of $A_\ell^\perp$ has to involve exactly two of those rows. In fact a row i can combine with rows $i+2, i+3,\ldots,\ell-1$. We then get $(\ell-3) + (\ell-4) +\ldots + 1 = \binom{\ell-2}{2}$ triples involving the first $\ell-1$ rows. We conclude that the number of distinguished triples for $A_\ell^\perp$ is

$$\binom{2}{2} + \binom{3}{2} + \ldots + \binom{\ell-3}{2} + \binom{\ell-2}{2} .$$

Then the number of vectors of weight 3 in $A_\ell^\perp$ is

$$(\ell-1) + (\ell-2)(\ell-1) + \binom{2}{2} + \binom{3}{2} + \ldots + \binom{\ell-2}{2}$$

$$= (\ell-1)^2 + \binom{2}{2} + \binom{3}{2} + \ldots + \binom{\ell-2}{2}$$

as required.

We remark that if ℓ is even the code $A_\ell^\perp$ does not have any vector of weight $n-1$ or $n-2$. A similar result holds for ℓ odd.

Proposition 3.5. If ℓ is odd, $\ell \geq 5$, then the code $A_\ell^\perp$ does not contain any vector of weight n, $n-1$ or $n-2$.

Proof. It is easily seen that the weight enumerator of $A_3^\perp$ is $1 + 4x^3 + 3x^4$ so that $A_3^\perp$ does have a vector of weight $n-2 = 4$. Now assume $\ell \geq 5$. We first remark that this condition implies that no row of the generator matrix for $A_\ell^\perp$ is of weight n, $n-1$ or $n-2$. Now the sum of all the rows is the vector

$$S = \underset{\ell}{0101\ldots010}\ \underset{n-\ell}{1111\ldots11}$$

which is of weight at most $n-3$. To get a vector of weight $n-1$ we need to add to S a row. Looking at the first two coordinates, we see that we never get a vector whose first ℓ coordinates are all 1. Hence there is no vector of weight $n-1$ in $A_\ell^\perp$. To get a vector of weight $n-2$ we need to add to S either a row or two rows. Let r be a row. $S+r$ is of weight $n-2$ if and only if $S+r$ has precisely one zero among its first ℓ coordinates. Now if r is among the first $\ell-2$ rows then coordinates 2 and ℓ of $S+r$ are both zero; if r is the row $\ell-1$ then coordinates 2 and $\ell-1$ of $S+r$ are both zero. If r is not among the first $\ell-1$ rows then the first coordinate of $S+r$ is always zero; if in addition coordinate ℓ of r is zero then coordinate ℓ of $S+r$ is also zero; if coordinate ℓ of r is 1 then its $(\ell-1)$-coordinate is also 1 so that coordinate $\ell-1$ of $S+r$ is zero. We conclude that we do not get a vector of weight $n-2$ by adding a row to S. Now let r, t be two rows. $S+r+t$ is of weight $n-2$ if and only if $S+r+t$ has all of its first ℓ coordinates equal to 1, i.e. if the first ℓ coordinates of $r+t$ are

$$101010\ldots101 .$$

To be so, one of r and t, say r, must be among the first $\ell-1$ rows and t among the next $\ell-2$ rows. Inspection shows however that then $r+t$ is never of the desired form. Thus we do not get a vector of weight $n-2$ by adding two rows to S.

Proposition 3.6.

(i) The code $A_5^\perp$ contains 15 vectors of weight $n-3 = 12$.

(ii) If ℓ is odd and if $\ell \geq 7$ then the code $A_\ell^\perp$ does not contain any vector of weight $n-3$.

Proof. The assertion about $A_5^\perp$ can be deduced directly from the matrix of $A_5^\perp$ or by a slight modification of the following argument for the proof of ii. So assume ℓ is odd and $\ell \geq 7$. Note first that the condition $\ell \geq 4$ implies that no row of the matrix for $A_\ell^\perp$ is of weight $n-3$. Now to get a vector of weight $n-3$ we need to add up at least $n-\ell-3$ rows. The sum of all $n-\ell$ rows is the vector

$$S = \underbrace{010101\ldots010}_{\ell}\ \underbrace{111\ldots11}_{n-\ell}$$

which is of weight at most $n-4$ since $\ell \geq 7$. For convenience let us call cell 1 the set of rows 1 through ℓ-1, cell 2 the set of rows $(\ell-1)+1$ through $(\ell-1)+(\ell-2)$,... etc. Now let r be a row and consider the sum $S+r$. $S+r$ is of weight $n-3$ if and only if it has precisely two zeros among its first ℓ coordinates. This is never so if r is in cell 6, 7,... etc. because then the first five coordinates of r are zero. Suppose r is in cell 1. If the first six coordinates of r are all ones then coordinates 2, 4 and 6 of $S+r$ are zero. If not then coordinates 2 and 7 of $S+r$ are zero; then depending on whether r has 2, 3, 4 or 5 ones among its first ℓ coordinates, coordinate 5, 5, 5 or 4 of $S+r$ is also zero. A similar argument shows that $S+r$ is never of weight $n-3$ if r is in cells 2, 3, 4 and 5. Now let r, s be two rows and consider the sum $S+r+s$. This sum is of weight $n-3$ if and only if it has precisely one zero among its first ℓ coordinates. Clearly one of r and s has to be in cells 1, 2 or 3 since a vector of the other cells has its first three coordinates equal to zero. First assume that r and s are not in cell 1. Then the first coordinate of $S+r+s$ is zero so the remaining of the first ℓ coordinates must be all ones. If r

is in cell 2 then so is s because of the second coordinate, but then the third coordinates of r and s are ones and the third coordinate of $S+r+s$ is also zero. If r is in cell 3 then s has to be in cell 4 because of the third and fourth coordinates, but then the seventh coordinates of r and s must be zero because of the fifth and sixth coordinates and hence the seventh coordinate of $S+r+s$ is also zero. Secondly assume that r is in cell 1. If s is also in cell 1 then the first coordinate of $S+r+s$ is zero so that the remaining of its first ℓ coordinates must be all ones. If the third coordinate of r is one then the third coordinate of s and the fourth coordinate of r must be zero; hence the fifth coordinate of $S+r+s$ is also zero. If the third coordinate of r is zero then the fourth coordinate of s must be zero; again the fifth coordinate of $S+r+s$ is zero. If s is in cell 2 then its third coordinate is one. If the third coordinate of r is also one then the third coordinate of $S+r+s$ is zero so the remaining of its first ℓ coordinates must be ones. But then the fourth coordinates of r and s must be 0 and the fifth coordinate of $S+r+s$ is zero. If the third coordinate of r is zero then both coordinates 7 and 4 or both coordinates 7 and 5 of $S+r+s$ are zero depending on whether the fifth coordinate of s is 1 or 0. If s in not in cell 1 or 2 then the second coordinate of $S+r+s$ is zero, hence the remaining of the first ℓ coordinates must be ones. Hence the fourth coordinates of r and s must be zero and then the fifth coordinate of $S+r+s$ is also zero. So we do not get a vector of weight $n-3$ by adding up $n-\ell-2$ rows. Finally let r, s, t be three rows and consider the sum $S+r+s+t$. This sum is of weight $n-3$ if and only if all of its first ℓ coordinates are ones, i.e. the first ℓ coordinates of $r+s+t$ look like

$$101010\ldots101.$$

A necessary condition for this to be true is that either r, s, t are all in cell 1 or exactly one of them is in cell 1. First assume that r, s and t are in cell 1. Because of coordinate ℓ, t has to be row $\ell-1$ and then s has to be row $\ell-2$ for coordinate $\ell-1$ must be zero. However this implies that the second coordinate of $r+s+t$ is one and not zero as desired. Secondly suppose that only r is in cell 1. Because of the second coordinate, another row, say s, must be in cell 2 and the first two coordinates of the third row t must be zero. Suppose the third coordinate of r is zero. If the fourth coordinate of s is zero then the fifth coordinate of t must be one, hence the sixth coordinate of $r+s+t$ is one. If the fourth coordinate of s is one then the fourth and fifth coordinates of t must be ones, hence the sixth and seventh coordinates of s, t and $r+s+t$ are zero. Now suppose the third coordinate of r is one. Then t must be in cell 3, because of the third coordinate. If the fourth coordinate of r is zero then the fourth coordinate of s is one. If the fifth coordinate of s is zero then the seventh coordinates of s, t and $r+s+t$ are zero. If the fifth coordinate of s is one then the fifth coordinate of t must be zero and again the seventh coordinate of $r+s+t$ is zero. We can show similarly that if the fourth coordinate of r is one then the seventh coordinate of $r+s+t$ is always zero. So we do not get a vector of weight $n-3$ by adding up $n-\ell-3$ rows.

§7. The code D_ℓ $(\ell \geq 4)$

In this section we let $n = \ell(\ell-1)$.

Proposition 3.7.

(i) D_ℓ is a (n,ℓ) code.

(ii) The minimum weight d of D_ℓ is $2(\ell-1)$.

(iii) D_ℓ is even if and only if $\ell \equiv 0$ or $1 \bmod 4$.

Proof. (i) is obvious.

We prove (ii) by induction on ℓ. The weight enumerator of D_4 is easily seen to be $1 + 12x^6 + 3x^8$. Now consider the generator matrix for D_ℓ where $\ell > 4$. The first row has weight $1 + (\ell-2) + (\ell-1) = 2(\ell-1)$ so that $d \leq 2(\ell-1)$. Now if we remove row 1, column 1, columns $\ell+1$ through $2(\ell-1)$ and columns $\frac{1}{2}(\ell-1)(\ell-2) + \ell + 1$ through $\frac{1}{2}(\ell-1)(\ell-2) + 2\ell-1$ then we get the generator matrix for $D_{\ell-1}$. Then consider a sum S of rows of the matrix of D_ℓ. Since the roots are all of the same length we may assume, as in A_ℓ, that S involves the first row. By the induction hypothesis the weight of $T = S$ - first row is at least $2(\ell-2)$. Now if T involves none or both of the last two rows, then the weight of S is at least $2(\ell-2) + 2$ because of the entries $(1,1)$ and $(1,\frac{1}{2}(\ell-1)(\ell-2)+\ell+1)$. If T

does not involve the second row then we use the entries (1,1) and $(1,\ell+1)$. Finally if T involves the second row and either one of the last two rows then we use the entries (1,1) and $(1,\frac{1}{2}(\ell-1)(\ell-2)+\ell+2)$.

To prove (iii) we note that the weight of the first $\ell-2$ rows of the matrix of D_ℓ are $2(\ell-1),4(\ell-2),\ldots,2(\ell-2)$ respectively and the weight of either of the last two rows is $\frac{1}{2}\ell(\ell-1)$. Hence D_ℓ is even if and only if $\frac{1}{2}\ell(\ell-1)$ is even. This clearly means that $\ell \equiv 0$ or 1 mod 4.

<u>Proposition 3.8.</u> The dual $D_\ell^\perp$ of D_ℓ, which is a $(n,n-\ell)$ code, has minimum weight 3 and the number of vectors of weight 3 in $D_\ell^\perp$ is equal to $a(\ell) + b(\ell) + c(\ell)$ where

$$a(\ell) = \ell-1 ,$$

$$b(\ell) = \ell(\ell-3) + (\ell-1)(\ell-2)$$

and

$$c(\ell) = \sum_{4\leq i\leq \ell} (i^2-4i+2) + \sum_{4\leq i\leq \ell} \binom{i-3}{2} + \sum_{4\leq i\leq \ell} \binom{i-2}{2} .$$

<u>Proof</u>. The following matrix is a generator matrix for a code equivalent to $D_\ell^\perp$.

$$\begin{array}{lll}
 & 11000\ldots000 & \\
 & 11100\ldots000 & \\
\ell-2 & 11110\ldots000 & \\
 & \vdots & \\
 & 11111\ldots110 & \\
 & 10000\ldots011 & \\
 & 11000\ldots011 & \\
\ell-1 & 11100\ldots011 & \\
 & \vdots & \\
 & 11111\ldots111 & \\
 & 11111\ldots101 & \\
 & 01100\ldots000 & \\
\ell-3 & 01110\ldots000 & \\
 & \vdots & \\
 & 01111\ldots110 & \\
 & 01000\ldots011 & \\
 & 01100\ldots011 & n-\ell \\
\ell-2 & \vdots & \\
 & 01111\ldots111 & \\
 & 01111\ldots101 & \\
 & \vdots & \\
 & 00000\ldots110 & \\
2 & 00000\ldots111 & \\
 & 00000\ldots101 & \\
 & \ell &
\end{array}$$

Rows 1, $(\ell-2)+(\ell-1)+1,\ldots,n-\ell-2$ are of weight 3, the other rows of weight grater than 3. Now any two rows differ in their first ℓ coordinates, hence the minimum weight of $D_{\ell}^{\perp}$ is 3. Now let $a(\ell)$ be the number of rows of weight 3. Then clearly

$$a(\ell) = (\ell-2) + 1 = \ell-1 .$$

Now let $b(\ell)$ be the number of unordered pairs of rows that differ exactly in one coordinate in their first ℓ coordinates. For convenience, let us call cell 1 the set of rows 1 through $\ell-2$, cell 2 the set of rows $(\ell-2)+1$ through $(\ell-2)+(\ell-1)$,... etc. Now it is easily seen that $b(4) = 10$. Assume by induction that $\ell > 4$ and $b(\ell-1) = (\ell-1)(\ell-4) + (\ell-2)(\ell-3)$. Then consider a distinguished pair (r,s) of rows of the above matrix for $D_{\ell}^{\perp}$ that involves cell 1 or cell 2. Note that pair cannot involve cells 5, 6, ... etc. This is so because all the rows of cells 1 and 2 but row $\ell-1$ have their first two coordinates equal to 1 and all the rows of cells 5, 6, ... etc. have their first two coordinates equal to 0. On the other hand, row $\ell-1$ looks like 1000...011 and there is no row of the form 0000...011 in cells 3, 4, 5, ... etc. Now if rows r and s are both in cell 1 or both in cell 2 then clearly they have to be consecutive rows, hence we get $(\ell-3) + (\ell-2)$ distinguished pair that way. Now suppose r is in cell 1 and s is in cell 2. If r is among the first $\ell-4$ rows then its last three coordinates are zero, hence it cannot be paired with any of the rows of cell 2 since the latter have at least two ones among their last three coordinates. Now row $\ell-3$, whose last two coordinates are zero, can be paired only with the last row of cell 2; similarly row $\ell-2$ can be paired only with row $2(\ell-2)$. Hence we get 2 distinguished pairs. Now suppose r is in cell 1 and s is in cell 3. By changing the first coordinate of each row of cell 3 we get the last $\ell-3$ rows of cell 1, hence we get $\ell-3$ distinguished pairs. Note that if r is in cell 1 then s cannot be in cell 4. This is so because a row of cell 1 and a row of cell 4 differ in both coordinates 1 and ℓ. Similarly we get $\ell-2$ distinguished pairs from a row of cell 2 and a row of cell 4. Hence

$$\begin{aligned} b(\ell) &= b(\ell-1) + 2(\ell-2) + 2(\ell-3) + 2 \\ &= \ell(\ell-3) + (\ell-1)(\ell-2) . \end{aligned}$$

Now let $c(\ell)$ be the number of unordered triples of rows whose sum has all of its first ℓ coordinates equal to 0. It is easily checked that $c(4) = 3$. Assume by induction that $\ell > 4$ and that

$$c(\ell-1) = \sum_{4\le i\le \ell-1} \binom{i-3}{2} + \sum_{4\le i\le \ell-1} \binom{i-2}{2} + \sum_{4\le i\le \ell-1} (i^2-4i+2)$$

Consider a distinguished triple (r,s,t) of rows of the matrix for $D_\ell^\perp$ that involves cell 1 or cell 2. Such a triple has to involve exactly two rows, say r and s, from cell 1 and cell 2. If r and s are both in cell 1 then they cannot be consecutive rows but given r, s can be anyone of rows $r+2, r+3, \ldots$ etc. Hence we get $1 + \ldots + (\ell-4) = \binom{\ell-3}{2}$ distinguished triple this way. Similarly we get $\binom{\ell-2}{2}$ distinguished triples (r,s,t) where r and s are both in cell 2. Now suppose r is in cell 1 and s is in cell 2. Suppose r is among the first $\ell-4$ rows of cell 1. Then the last three coordinates of r are zero, its first two coordinates equal to 1. Say $r = 111\ldots\underset{i}{1}0..000$. Then s can be anyone of the rows of cell 2 except row $111\ldots\underset{i}{1}0\ldots011$. Now row $\ell-3$ looks like $111\ldots\underset{\ell-2}{1}00$. Clearly it can be paired with the first $\ell-3$ rows of cell 2, but not the last two. The same is true for the last row of cell 1. Hence we get

$$(\ell-2)(\ell-1) - (\ell-4) - 4 = \ell^2 - 4\ell + 2$$

distinguished triples (r,s,t) where r is in cell 1 and s is in cell 2. We conclude that

$$c(\ell) = c(\ell-1) + \binom{\ell-3}{2} + \binom{\ell-2}{2} + \ell^2 - 4\ell + 2$$

$$= \sum_{4\leq i\leq \ell} \binom{i-3}{2} + \sum_{4\leq i\leq \ell} \binom{i-2}{2} + \sum_{4\leq i\leq \ell} (i^2-4i+2).$$

§8. The Hamming codes and the codes $A_\ell^\perp$ and $D_\ell^\perp$.

We recall that $A_\ell^\perp$ does not contain the all-one vector j if and only if ℓ is odd. Hence for ℓ odd the augmented code

$$\overline{A}_\ell = A_\ell^\perp \cup \left\{j+A_\ell^\perp\right\}$$

is a $(n,n-\ell+1)$ code where $n = \frac{1}{2}\ell(\ell+1)$. Moreover, according to proposition 3.5 if $\ell \geq 5$ then the minimum distance of $\overline{A}_\ell$ is 3 and according to proposition 3.6 if $\ell \geq 7$ then the number of vectors of weight 3 in $\overline{A}_\ell$ is

$$a(\ell) = (\ell-1)^2 + \sum_{2\leq i\leq \ell-2} \binom{i}{2} .$$

We also know that $D_\ell^\perp$ does not contain j if and only if ℓ is congruent to 2 or 3 mod 4. However the augmented code is of no particular interest because the code $D_\ell^\perp$, $\ell \geq 6$, contains a vector of weight $n-2$, for instance the sum of all the rows of the generator matrix for $D_\ell^\perp$. We give below a table for the small parameters of the code $\overline{A}_\ell$, $D_\ell^\perp$ and the Hamming code (we set $\overline{A}_\ell = A_\ell^\perp$ if ℓ is even).

$\overline{A}_\ell$:	length	6	10	15	21	28	36	45	55	66	78	91
	dimension	3	6	11	15	22	28	37	45	56	66	79

$D_\ell^\perp$:	length	12	20	30	42	56	72	90	110
	dimension	8	15	24	35	48	63	80	99

Hamming:

length	7	15	31	63	127	255
dimension	4	11	26	57	120	247

§9. On the automorphism groups of A_ℓ and D_ℓ

We have remarked earlier that the identity is the only element of the Weyl group that is in the automorphism group of A_ℓ or D_ℓ. We can show however that this automorphism group is not trivial.

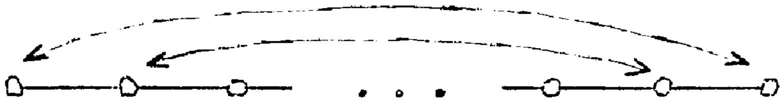
We recall that the Dynkin diagram D of a root system ϕ is the graph (with multiple edges) defined as follows:

—the vertex set consists of the roots in a given fundamental system π in ϕ.

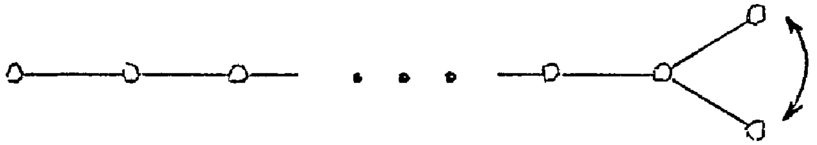
—the number of edges joining two vertices p_i, p_j is equal to $n_{ij} = 4 \cos^2\theta_{ij}$ where θ_{ij} is the angle between p_i, p_j.

Let σ be a nontrivial symmetry of the Dynkin diagram. We depict below the Dynkin diagrams for the systems of type A_ℓ and D_ℓ with their nontrivial symmetries.

A_ℓ:



D_ℓ:



(note that D_4 has another aymmetry of order 3, fixing one vertex and cycling the three others.)

Since σ permutes the elements of a basis for the space V, σ determines a linear transformation τ of V.

Lemma 3.3. τ is an isometry of V and $\tau(\phi) = \phi$.

Proof. See for example [4].

In fact $\tau(\phi^+) = \phi^+$ since τ is linear and it preserves the fundamental system π.

Proposition 3.9. The permutation of ϕ^+ induced by τ is an automorphism of the code A_ℓ or D_ℓ.

Proof. Clearly the group of weights Q is invariant under τ. Then as in Lemma 1 we see that, for any $q \in Q$,

$$T(q)\cdot\tau = T(\tau^{-1}(q)) \in T(Q).$$

§10. The codes B_ℓ and C_ℓ.

For this section we let $n = \ell^2$.

Proposition 3.10.

(i) B_ℓ and C_ℓ are (n,ℓ) codes.

(ii) The minimum weight of B_ℓ is $2(\ell-1)$, that of C_ℓ is ℓ.

Proof.

(i) is clear.

(ii) is proved by induction on ℓ. Consider first the code B_ℓ. The weight enumerator of B_2 is easily seen to be $1 + x^2 + 2x^3$. Now assume $\ell > 2$. The first row of the generator matrix is of weight

$1 + (\ell-2) + (\ell-1) = 2(\ell-1)$ so that the minimum weight is not larger than $2(\ell-1)$. Now if we remove row 1, column 1, columns $2\ell-1$ through $3(\ell-1)$ and columns $\frac{1}{2}(\ell-2)(\ell-1) + \ell + 1$ through $\frac{1}{2}(\ell-2)(\ell-1) + 2\ell - 1$ then we get the generator matrix for $B_{\ell-1}$. Then consider a sum S of rows of the matrix for B_ℓ. Using the code $\tilde{B}_\ell$ and the transitivity of the Weyl group on the roots of the same length we may assume that S involves either the first or the last row. Suppose S involves the first row but not the last one. Since the weight of $T = S$ - first row is at least $2(\ell-2)$, the weight of S is at least $2(\ell-2)+2$ because of the entries $(1,1)$ and $(1,\frac{1}{2}(\ell-2)(\ell-1)+\ell+1)$. If S involves the last row but not the first one, we use the entries $(\ell,2\ell-1)$ and $(\ell,\frac{1}{2}(\ell-2)(\ell-1)+\ell+1)$. Finally if S involves both first and last rows, we use the entries $(1,1)$ and $(\ell,2\ell-1)$. The statement about C_ℓ is proved in a similar way.

Remarks.

The dual codes $B_\ell^\perp$ and $C_\ell^\perp$ are of little interest to us since they are easily seen to have minimum weight equal to 2.

§11. The exceptional codes G_2, F_4, E_6, E_7, E_8.

The weight enumerators of the exceptional codes (which we shall write in homogeneous form) were computed either by hand or by computer.

(i) The weight enumerator for G_2, which is a (6,2) code, is

$$x^6 + 3x^2y^4$$

By the MacWilliams theorem, the weight enumerator of the dual code $G_2^{\perp}$ is then

$$\tfrac{1}{4}[(x+y)^6+3(x+y)^2(x-y)^4]$$

$$= x^6 + 3x^4y^2 + 8x^3y^3 + 3x^2y^4 + y^6$$

In particular $G_2^{\perp}$ has minimum weight 2.

(ii) The weight enumerator for F_4, which is a (24,4) code is

$$x^{24} + 3x^{16}y^8 + 12x^{10}y^{14} \; .$$

Then the weight enumerator of $F_4^{\perp}$ is

$$\tfrac{1}{16}[(x+y)^{24}+3(x+y)^{16}(x-y)^8+12(x+y)^{10}(x-y)^{14}].$$

The minimum weight of $F_4^{\perp}$ is also 2.

(iii) E_6 is a doubly even (36,6) code whose weight enumerator is

$$x^{36} + 27x^{20}y^{16} + 36^{16}y^{20} .$$

The weight enumerator of $E_6^{\perp}$ is then

$$\frac{1}{64}[(x+y)^{36}+27(x+y)^{20}(x-y)^{16}+36(x+y)^{16}(x-y)^{20}]$$

$$= x^{36} + 120x^{33}y^3 +\ldots$$

Hence $E_6^{\perp}$ is a (36,30) code with minimum weight equal to 3.

(iv) E_7 is a (63,7) code whose weight enumerator is

$$x^{63} + 28x^{36}y^{27} + 63x^{31}y^{32} + 36x^{28}y^{35} .$$

The weight enumerator of $E_7^{\perp}$ is then

$$\frac{1}{128}[(x+y)^{63}+28(x+y)^{36}(x-y)^{27}+63(x+y)^{31}(x-y)^{32}$$
$$+36(x+y)^{28}(x-y)^{35}]$$

$$= x^{63} + 336x^{60}y^3 +\ldots+ 315x^3y^{60} .$$

Hence $E_7^{\perp}$ is a (63,56) code with minimum weight 3. Now consider the augmented code $\overline{E}_7 = E_7^{\perp} \cup \left\{j+E_7^{\perp}\right\}$ where j is the all-one vector. We see immediately that $\overline{E}_7$ is a (63,57) code of minimum weight 3 (the number of vectors of weight 3 is 336+315 = 651), hence $\overline{E}_7$ must be the Hamming code H_6.

(v) E_8 is a doubly even (120,8) code whose weight enumerator is

$$x^{120} + 120x^{64}y^{56} + 135x^{56}y^{64} .$$

The weight enumerator of $E_8^{\perp}$ is

$$\frac{1}{256}[(x+y)^{120}+120(x+y)^{64}(x-y)^{56}+135(x+y)^{56}(x-y)^{64}]$$

$$= x^{120} + 1120x^{117}y^3 +\ldots$$

Hence $E_8^{\perp}$ is a (120,112) code with minimum weight 3.

Remark.

Consider the code E_6. Since the all-one vector j is not in E_6 we may consider the augmented code

$$\overline{E}_6 = E_6 \cup \left\{j+E_6\right\} .$$

$\overline{E}_6$ is a (36,7) code with weight enumerator

$$x^{36}y^0 + 63x^{20}y^{16} + 63x^{16}y^{20} + x^0y^{36}.$$

In particular $\overline{E}_6$ attains the bound given in the table of Helgert-Stinaff (IEEE Trans. Info. Theory

19(1973), 344-356). Now the dual $\overline{E}_6^{\perp}$ of $\overline{E}_6$ consists of all even weight vectors of the dual $E_6^{\perp}$ of E_6. Hence the minimum distance of $\overline{E}_6^{\perp}$ is at least 4 (we may, if we wish, obtain the weight distribution of $\overline{E}_6^{\perp}$ by the MacWilliams equation). Hence by Assmus-Mattson theorem (see e.g. MacWilliams-Sloane's book, p. 178) the code words of each weight in $\overline{E}_6^{\perp}$ form a 2-design. We conclude (see the same book, p. 165) that the codewords of each weight in $\overline{E}_6$ form a 2-design. Thus we get a 2-(36,16,12) design with $r = 28$ and $b = 63$.

Since E_8 has properties similar to that of E_6 we may apply the above discussion to E_8. $\overline{E}_8 = E_8 \cup E_8 \cup \{j+E_8\}$ is a (120,9) code with weight enumerator

$$x^{120}y^{0} + 255x^{64}y^{56} + 255x^{56}y^{64} + x^{0}y^{120} .$$

This code $\overline{E}_8$ improves the bound in the table of Helgert-Stinaff. Also the vectors of weight 56 in $\overline{E}_8$ form a 2-(120,56,55) design with $r = 119$ and $b = 255$.

BIBLIOGRAPHY

[1] E. F. Assmus and J. H. VanLint, Ovals in projective designs, J. Combinat. Th. (to appear).

[2] V. N. Bhat and S. S. Shrikhande, Nonisomorphic solutions of some balanced incomplete block designs I, J. Combinat. Th., 9 (1970), 174-191.

[3] N. Bourbaki, Groupes et algèbres de Lie, Chap. 4, 5 et 6, Hermann, Paris 1968.

[4] R. W. Carter, Simple groups of Lie type, Wiley, London-New York 1972.

[5] P. Dembowski, Finite geometries, Springer-Verlag, New York 1968.

[6] M. Hall, Ovals in Desarguesian plane of order 16, Am. Math. pura ed appl. IV vol CII (1975), 159-176.

[7] M.-Hall, J. D. Swift and R. J. Walker, Uniqueness of the projective plane of order eight, Math. Tables and other Aids to computation, 10 (1956), 186-194.

[8] N. Hamada, On the p-rank of the incidence matrix of a balanced or partially balanced block design and its applications to error-correcting codes, Hiroshima Math. J., 3 (1973), 153-226.

[9] D. R. Hughes and F. C. Piper, Projective planes, Springer-Verlag, New York-Heidelberg-Berlin 1973.

[10] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, J. Algebra, 32 (1974), 418-443.

[11] M. E. O'Nan, Automorphisms of unitary block designs, J. Algebra, 20 (1972), 495-511.

[12] W. M. Schmidt, Equations over finite fields, Springer-Verlag, Berlin-Heidelberg-New York 1976.

VITA

Bruno R. Andriamanalimanana was born on February 20, 1953 in Imerimandroso-Alaotra, Madagascar. He is the eldest son of Mrs. Séraphine Rahariline and the late Etienne Ratsimandefitra. He graduated from Sainte Famille High School, Mahamasina, Tananarive in 1970. He obtained his license in mathematics from the University of Madagascar in 1974. He cameto the United States in July 1975 and entered Georgetown University, Washington D.C. to learn English. He came to Lehigh University in January 1976 and obtained his Master's degree in mathematics in May 1977.