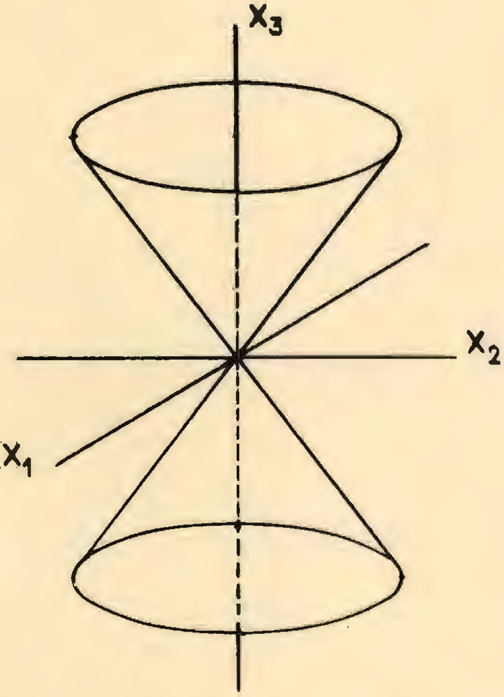
Few-distance sets

DOI:
10.6100/IR53747

Document status and date:
Published: 01/01/1983

Document Version:
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

FEW-DISTANCE SETS



A. BLOKHUIS

FEW-DISTANCE SETS

FEW-DISTANCE SETS

PROEFSCHRIFT

TER VERKRIJGING VAN DE GRAAD VAN DOCTOR IN DE TECHNISCHE WETENSCHAPPEN AAN DE TECHNISCHE HOGESCHOOL EINDHOVEN, OP GEZAG VAN DE RECTOR MAGNIFICUS, PROF. DR. S.T.M. ACKERMANS, VOOR EEN COMMISSIE AANGEWEZEN DOOR HET COLLEGE VAN DEKANEN IN HET OPENBAAR TE VERDEDIGEN OP VRIJDAG 30 SEPTEMBER 1983 TE 16.00 UUR

DOOR

AART BLOKHUIS

GEBOREN TE ALKMAAR

Dit proefschrift is goedgekeurd
door de promotoren

Prof. dr. J.J. Seidel

en

Prof. dr. J.H. van Lint

Aan Cecilia

ACKNOWLEDGEMENTS

I would like to thank Jaap Seidel for his continuous support and patience during the period of my research. I am also grateful to the following people for the interest they showed in my work during their stay in Eindhoven: Tor Helleseth, Arnold Neumaier, Navim Singhi, David Klarner and John Jarratt.

CONTENTS

CHAPTER 1

INTRODUCTION

The vertices of a regular $(2s+1)$-gon in the plane form a set of points on the circle with the property that the distance between different points assumes only s different values. It is easy to see that $2s+1$ is the maximal cardinality of such a set since, starting with any point on the circle, there are at most two points at a prescribed distance away from it. If we denote by $f(s,d)$ the maximal number of points on the unit sphere in d-dimensional space R^d, constituting an s-distance set, then exactly the same reasoning yields an exponential bound in d by the inequality $f(s,d) \leq 1 + sf(s,d-1)$. If s is small compared to d, all known examples indicate that the proper bound should be polynomial in d, of degree s. Using ingredients from the theory of harmonic analysis, especially the addition theorem for Gegenbauer polynomials, Delsarte, Goethals and Seidel [DGS] showed that this is the case. Koornwinder [K] gave a simpler argument, yielding the same absolute bound and avoiding harmonics. His method is to associate with an s-distance set X on the unit sphere in R^d, an independent set of $|X|$ polynomials of degree s in d variables. Hence the cardinality of X is bounded by dim Pol(s,d), i.e., the dimension of the space of polynomials of degree at most s, in d variables.

Koornwinder's method is applicable in many cases, however if we consider sets of vectors with few inner products in an arbitrary inner product space, this method does not depend on the signature of the inner product. With the harmonic method we can do better in case of an indefinite inner product, i.e., the vector space $R^{p,q}$ provided with the inner product $(x,y) = x_1y_1 + x_2y_2 + .. +x_py_p - x_{p+1}y_{p+1} - .. -x_{p+q}y_{p+q}$, of signature (p,q). This is done in chapter 2, which is joint work with Bannai, Delsarte and Seidel [BBDS]. First we prove a generalized version of the addition formula, which is of independent interest. Then we apply it to few-distance sets in indefinite inner product spaces. For example theorem 2.8.1. reads as follows: Let X be a set of unit vectors in $R^{d-1,1}$, such that the inner product between different

elements of X assumes only s different values (all different from 1). Then $\mathrm{card}(X) \le \binom{d+s-1}{s}$.
We conclude this chapter with examples, e.g.: The maximal number of vectors in $R^{9,1}$ having inner products $\{0, \pm \frac{1}{2}\}$ is exactly 165.

Another way to obtain better bounds is to start with Koornwinder's method, but to show that one can actually construct a larger independent set of polynomials. In chapter 3 this approach yields an essentially sharp bound on the number of equiangular lines in $R^{d,1}$ viz. theorem 3.2.1. : Let X be a set of equiangular lines in $R^{d,1}$ at angle $\arccos(\alpha)$. Then

(i) if $(d+1)\alpha^2 < 1$, $\mathrm{card}(X) \le d(1-\alpha^2)/(1-d\alpha^2)$;

(ii) if $(d+1)\alpha^2 \ge 1$, $\mathrm{card}(X) \le \frac{1}{2}d(d+1)$.

The first case is proved using the eigenvalue method and is called the special bound.

In chapter 4, we apply the same idea to improve the bounds for s-distance sets in Euclidean d-space, E^d, and hyperbolic d-space, H^d. In these cases we get the following result: Let X be an s-distance set in E^d or H^d, then $\mathrm{card}(X) \le \binom{d+s}{s}$.
The bound for H^d can also be derived from the results in chapter 2. It is still an open question whether an harmonic analysis approach could give the bound for E^d as well.

An interesting idea, due to Frankl and Wilson [FW], is to consider sets of points with few distances modulo a prime. In chapter 5 a useful number theoretic lemma is combined with Koornwinder's argument to give a.o. the following result (theorem 5.3.1.): Let X be a set of vectors in R^d such that there are integers $a_1, \dots, a_s$ with

(i) $(x,x) \not\equiv a_i \pmod p$, $(x,x) \in Z$ for all $x \in X$, $1 \le i \le s$.

(ii) $(x,y) \equiv a_i \pmod p$ for some i, $1 \le i \le s$, if $x \ne y \in X$.

Then $\mathrm{card}(X) \le \binom{d+s}{s}$.

In chapter 6, the same lemma is applied to the more natural question of few-distance sets modulo a prime in Delsarte spaces, a notion

due to Neumaier [N1] and Delsarte. Since the basic text is not generally available, we repeat the basic theory of Delsarte spaces and association schemes in this chapter. As a corollary of the mod p bound for Delsarte spaces we obtain the result of Frankl and Wilson and also the following theorem: Let X be a collection of subsets from an n-set, such that for any $x \neq y \in X$: $|x \Delta y| \in T$, where T is the union of t non-zero residue classes mod p. Then $\mathrm{card}(X) \leq \binom{n}{t}$.
This chapter finishes with a series of examples meeting this bound. Part of the work in this chapter is joint work with Singhi.

In chapter 7 a relation between two-distance sets and a problem of Erdös is demonstrated. Isosceles sets are sets of points , such that each triple among them determines an isosceles triangle. We show that an isosceles set in E^d can be decomposed in a collection of "mutually orthogonal" two-distance sets. As a result the following bound is obtained (theorem 7.2.5.): Let X be an isosceles set in E^d, then $\mathrm{card}(X) \leq \frac{1}{2}(d+1)(d+2)$. Equality implies that X is a two-distance set or a spherical two-distance set together with its center.
Crucial in the proof of the decomposition theorem is the following graph-theoretical proposition: Let the edges of the complete graph on n vertices be colored by k colors, such that

(i) each triangle has at most two colors ;

(ii) the induced graph on each color is connected.

Then there are at most two colors.

In chapter 8 , which contains joint work with Wilbrink and Kloks, the same proposition plays a key rôle in the study of the structure of graphs satisfying the following two regularity conditions:

(i) There is a constant K, such that every maximal clique has size K.

(ii) There is a constant e, such that for every maximal clique C and every vertex p not in C , there are exactly e vertices in C , adjacent to p.

These graphs were introduced by Zara [Z] in an attempt to characterize polar spaces (in the sense of Veldkamp and Tits). The main result in this chapter is theorem 8.5.11 : Let G be a coconnected Zara-graph of rank r, then the reduced graph of G, say G', is again a coconnected Zara-graph and the partially ordered set of closed cliques in G' is an M_r-space in the sense of Neumaier [N].

CHAPTER 2

THE ADDITION FORMULA FOR $R^{p,q}$

§2.1 Introduction

In [DGS] , the authors investigate few-distance sets on the sphere in Euclidean d-space, R^d. If a two-distance set is considered, then a "lifting" process results in a set of equiangular lines, either in R^{d+1} cf. [vLS] , or in $R^{d,1}$. In this way the 5 points of the regular pentagon correspond to the 6 diagonals of the icosahedron. This is one of the reasons to study the problem of few-distance sets and sets of lines with few angles in the more general setting of an arbitrary inner product space.

If we want to apply the same techniques as in [DGS] we need a generalization of the addition formula for Gegenbauer polynomials. The addition formula reads as follows:

$$\gamma_k C_k^{(d-2)/2}((x,y)) = \sum_{i=1}^{\mu_k} f_{k,i}(x) f_{k,i}(y) \quad .$$

Here $C_k^{(d-2)/2}$ is a Gegenbauer polynomial, with a scaling factor γ_k , while x and y are unit vectors in R^d, provided with the standard inner product (x,y). The $\{f_{k,i}\}$ form an orthonormal basis of the space of the homogeneous harmonic polynomials of degree k, with respect to the inner product

$$\langle f,g\rangle = \frac{1}{|\Omega|} \int_\Omega f(x)g(x)d\omega(x) \ .$$

Here Ω stands for the unit sphere in R^d .

From this representation of the inner product the difficulty in deriving a generalized addition formula becomes apparent: In the case of an indefinite space we no longer have a compact unit sphere, so we have to define the inner product on the space harm(k) of homogeneous harmonic polynomials of degree k in d variables in a different way. To do this we introduce differential operators and the algebra of symmetric tensors ,cf. [BBDS] . It turns out that the new inner product gives back the "old" addition formula in the Euclidean case, while in the indefinite case we still get Gegenbauer polynomials, the only difference being that the inner product on the space harm(k) is no longer positive definite. This fact enables us to improve the bounds for few-distance sets in indefinite space. In the most interesting case of hyperbolic space, $R^{d,1}$, we obtain equality in a number of examples.

The main objective in this chapter is to give the setting for the more general inner product. The application to few-distance sets is essentially the same as in [DGS].

§2.2. Polynomials and tensors

Let V denote a real d-dimensional vector space and let $(v^1,v^2, \dots ,v^d)$ be any basis of V. Let S^* denote the algebra of polynomial functions on V; thus S^* consists of the functions $f : V \to R$ that are represented by polynomials in the coordinates with respect to the basis $(v^1, \dots ,v^d)$. Next let S denote the symmetric algebra on V , consisting of the symmetric tensors

$$s = \sum_a s_{a_1 a_2 \dots a_d} \otimes^{a_1} v^1 \dots \otimes^{a_d} v^d ,$$

with $s_a \in R$ and $a=(a_1,a_2,\dots,a_d)$, only a finite number of the s_a being non-zero.

Let Aut V denote the automorphism group of V. The action of an element $\sigma \in$ Aut V will be written in the form $x \in V \to x^\sigma \in V$. The group Aut V acts as an algebra automorphism group on both S^* and S according to the following rules. The image f^σ of a polynomial $f \in S^*$ is defined by $f^\sigma(x) = f(x^{\sigma^{-1}})$. The image of a symmetric tensor $s \in S$

is defined by

$$s^{\sigma} = \sum_a s_a \otimes^{a_1}(v^1)^{\sigma} \ldots \otimes^{a_d}(v^d)^{\sigma} .$$

§2.3. Differential operators.

To any vector $w \in V$ corresponds the directional derivative ∂_w, which is the linear operator on S^* defined by

$$(\partial_w f)(x) = \lim_{h\to 0} h^{-1} [f(x+hw) - f(x)] , \qquad (1)$$

for $x \in V$ and $f \in S^*$. We extend this definition to the whole algebra S by associating the differential operator $\partial_s = \Sigma s_a \partial_1^{a_1} \ldots \partial_d^{a_d}$, where $\partial_i = \partial_{v^i}$, to the symmetric tensor

$$s = \sum_a s_a \otimes^{a_1} v^1 \otimes^{a_2} v^2 \ldots \otimes^{a_d} v^d .$$

Note the property $\partial_{s\otimes t} = \partial_s \partial_t$ for all s and t in S.
A nonsingular linear pairing $\langle \, | \, \rangle$ between S and S^* is defined by

$$\langle s|f\rangle = (\partial_s f)(0) \quad , \quad s \in S \quad , \quad f \in S^* . \qquad (2)$$

Since $\partial_{s\otimes t} = \partial_s \partial_t$ we have $\langle s\otimes t|f\rangle = \langle s|\partial_t f\rangle$.
Let $\hom(d,k)$ denote the space of the homogeneous polynomials of degree k in d variables. For later use we prove the following lemmas.

<u>LEMMA 2.3.1.</u> *For all* $x \in V$, *and* $f \in \hom(d,k)$ *we have*

$$\langle \otimes^k x | f\rangle = k! \; f(x) \quad .$$

PROOF. For $k=1$ the statement follows from the definition of $\partial_x f$. Indeed $\langle x|f\rangle = \partial_x f(0) = f(x)$ since f is linear. For $k>1$ we have

$$\langle \otimes^k x|f\rangle = \langle \otimes^{k-1} x|\partial_x f\rangle = (k-1)!\ (\partial_x f)(x)$$

Now if f is homogeneous of degree k then $(\partial_x f)(x) = kf(x)$ since

$$(\partial_x f)(x) = \lim h^{-1}\ [f((1+h)x)-f(x)] = \lim h^{-1}((1+h)^k-1)f(x)\ .$$

This finishes the proof. □

<u>LEMMA 2.3.2.</u> *For all* $\sigma \in \mathrm{Aut}\ V$, $s \in S$ *and* $f \in S^*$ *we have*

$$\langle s^\sigma|f^\sigma\rangle = \langle s|f\rangle\ .$$

PROOF. First note that for $x \in V$ we have $\partial_{x^\sigma} f^\sigma = (\partial_x f)^\sigma$. By induction on the degree of s we then can prove $\partial_{s^\sigma} f^\sigma = (\partial_s f)^\sigma$, and this implies $\langle s^\sigma|f^\sigma\rangle = \langle s|f\rangle$. □

§2.4. Bilinear form spaces.

Let $B(.,.)$ denote any nondegenerate symmetric bilinear form on V. Then B induces a vector space isomorphism $\mathcal{B}: V \to V^*$ (the dual of V), given by $x \to B(x,.)$ for all $x \in V$. This vector space isomorphism naturally extends to the algebra isomorphism $\mathcal{B}: S \to S^*$ given by

$$\sum_a s_a \otimes^{a_1} v^1 \ldots \otimes^{a_d} v^d \to \sum_a s_a B(v^1,.)^{a_1} \ldots B(v^d,.)^{a_d}\ .$$

It is clear from the definition that we have, for all x,y in V :

$$\langle x|By\rangle = B(x,y) = \langle y|Bx\rangle \quad .$$

More generally we have

<u>LEMMA 2.4.1.</u> $\langle s|Bt\rangle = \langle t|Bs\rangle$ *for* $s,t \in S$. (3)

PROOF. Let $v^1, v^2, \ldots, v^d$ be an <u>orthogonal</u> basis of V , with $B(v^i, v^i) = \phi_i$, and let

$$s = \otimes^{a_1} v^1 \ldots \otimes^{a_d} v^d \quad , \quad t = \otimes^{b_1} v^1 \ldots \otimes^{b_d} v^d \quad .$$

Then $\langle s|Bt\rangle = 0$ if there is an index i with $a_i \neq b_i$, while if $s = t$ we have, with $\phi = \Pi\phi_i$:

$$\langle s|Bt\rangle = \phi \prod_{i=1}^{d} a_i! = \phi \prod_{i=1}^{d} b_i! \quad .$$

Since tensors of the form $\otimes^{a_1} v^1 \ldots \otimes^{a_d} v^d$ constitute a basis for S the proof is finished. □

The isomorphism B allows one to interpret the pairing in (2) between S and S^* as an inner product on the space S^* ; the definition of this inner product is as follows:

$$\langle f,g\rangle = \langle B^{-1}f|g\rangle \quad ; \quad \text{for } f,g \in S^* . \tag{5}$$

From (3) it follows that this inner product is symmetric, i.e., $\langle f.g\rangle = \langle g,f\rangle$. To any polynomial $g \in S^*$ let us now associate the differential operator ∂_g defined by $\partial_g = \partial_{B^{-1}g}$. Then multiplication and differentiation with respect to a given polynomial are adjoint operations with respect to the inner product defined in (5) , in the sense that

$$\langle gh,f\rangle = \langle h,\partial_g f\rangle \quad , \quad \text{for } f,g,h \in S^* . \tag{6}$$

Let Aut B denote the automorphism group of the bilinear form B, i.e., the subgroup of Aut V containing all σ such that $B(x^\sigma,y^\sigma) = B(x,y)$ for all $x,y \in V$. Using $\langle s^\sigma|f^\sigma\rangle = \langle s|f\rangle$ together with the property $\mathcal{B}(s^\sigma) = (\mathcal{B}s)^\sigma$ for all $\sigma \in \mathrm{Aut}\ B$, one can show that the inner product defined in (5) is invariant under Aut B , i.e.,

<u>THEOREM 2.4.2.</u> $\langle f^\sigma,g^\sigma\rangle = \langle f,g\rangle$ *for all* $\sigma \in \mathrm{Aut}\ B$ *and* $f,g \in S^*$.□

§2.5. Harmonic polynomials.

We now fix a bilinear form B of inertia (p,q), with $p+q = d$, so that B is nondegenerate. Thus for a suitable basis $v^1, \ldots ,v^d$ of V we may write

$$B(x,y) = x_1y_1 + \ldots + x_py_p - \ldots - x_{p+q}y_{p+q} \quad .$$

Let $s = \otimes^{a_1}v^1 \ldots \otimes^{a_d}v^d$. Then the polynomial corresponding to s is:

$$f = \mathcal{B}s = (-1)^{a_{p+1}+\ldots+a_d}\, x_1^{a_1}x_2^{a_2}\ldots x_d^{a_d} \ .$$

Hence, given a polynomial g , we may write the associated differential operator as follows:

$$\partial_g = \partial_{\mathcal{B}^{-1}g} = g(\partial) \quad , \text{ with } \partial = (\partial_1, \ldots,\partial_p,-\partial_{p+1},\ldots,-\partial_d) \ .$$

Here ∂_i stands for ∂_{v^i} . The inner product (5) takes the following form:

$$\langle f,g\rangle = (f(\partial)g)(0) \ .$$

Let us mention in particular the differential operator associated to the quadratic form B itself: $\beta(x) := B(x,x)$:

$$\partial_\beta = \partial_1^2+\dots+\partial_p^2-\partial_{p+1}^2-\dots-\partial_d^2 \quad .$$

∂_β is called the Laplacian (associated to the bilinear form B).
Define the space $\underline{\mathrm{harm}_B(k)}$ to consist of the polynomials $f \in S^*$ which are homogeneous of degree k and satisfy the Laplace equation $\partial_\beta f = 0$; thus

$$\mathrm{harm}_B(k) = \mathrm{Ker}\ \partial_\beta \cap \mathrm{hom}(d,k) \ .$$

Let us mention the following important decomposition (cf. [V] page 446) of hom(d,k) into the kernel and the image of the operator $\beta\partial_\beta$:

$$\mathrm{hom}(d,k) = \mathrm{harm}_B(k) \perp \beta(.)\mathrm{hom}(d,k-2) \quad . \tag{7}$$

The orthogonality of the summands on the right hand side of (7) is an immediate consequence of (6) . When no confusion is possible we shall write hom(k) instead of hom(d,k).

The monomials $x^a = x_1^{a_1} x_2^{a_2} \dots x_d^{a_d}$ with $\sum_{i=1}^{d} a_i = k$, form an orthogonal basis for the space hom(k); furthermore we have

$$\langle x^a, x^a \rangle = (-1)^{a_{p+1}+\dots+a_d} \prod_{i=1}^{d} a_i! \quad .$$

as a direct consequence of (4). This leads us to the following decomposition of hom(k)

$$\mathrm{hom}(k) = \mathrm{hom}^+(k) \perp \mathrm{hom}^-(k) \quad .$$

Here $\mathrm{hom}^+(k) = \langle x^a \mid \sum_{i=p+1}^{d} a_i \equiv 0 \pmod 2 \rangle$;

and $\mathrm{hom}^-(k) = \langle x^a \mid \sum_{i=p+1}^{d} a_i \equiv 1 \pmod 2 \rangle$.

Clearly the restriction of the innerproduct to $hom^+(k)$ is positive definite, while the restriction to $hom^-(k)$ is negative definite. We will show that $harm_B(k)$ splits in a similar way into subspaces $harm_B^+(k)$ and $harm_B^-(k)$, and we shall compute the dimensions of these subspaces.

Let H denote the projection $H: hom(k) \to harm_B(k)$, with respect to the decomposition

$$hom(k) = harm_B(k) \oplus \beta(.)hom(k-2) .$$

<u>LEMMA 2.5.1.</u> *If* $f \in hom^+(k)$ *then also* $Hf \in hom^+(k)$ *and* $f \in hom^-(k)$ *implies* $Hf \in hom^-(k)$.

PROOF. Analogous to [V] , page 445 (13), one can prove that Hf may be written in the following form:

$$Hf = \sum_{i=0}^{\lfloor k/2 \rfloor} c_i \beta^i (\partial_\beta)^i f \quad , \tag{8}$$

for some constants $c_0, \ldots, c_{\lfloor k/2 \rfloor}$. It therefore suffices to show that $\beta\partial_\beta f$ is in $hom^+(k)$, resp. $hom^-(k)$, if f is. This however follows from the fact that $x_i^2 \partial_j^2 f$ is in $hom^+(k)$, resp. $hom^-(k)$, if f is, for all i,j. □

The lemma gives us the following decomposition:

$$harm_B(k) = harm_B^+(k) \perp harm_B^-(k) ,$$

where $harm_B^\varepsilon(k) := hom^\varepsilon(k) \cap harm_B(k)$ for $\varepsilon = +/-$.

Finally we shall use this information to determine the dimensions of $harm_B^+(k)$ and $harm_B^-(k)$, and hence the inertia of the inner product.

<u>THEOREM 2.5.2.</u> *The dimensions of the spaces considered in this section are as follows:*

(i) $\dim hom(d,k) = \binom{d+k-1}{k}$

(ii) $\dim \mathrm{harm}_B(k) = \binom{d+k-1}{k} - \binom{d+k-3}{k-2}$;

(iii) $\dim \mathrm{hom}^+(d,k) = \sum_{j=0}^{k/2} \binom{p+k-2j-1}{k-2j}\binom{q+2j-1}{2j}$;

(iv) $\dim \mathrm{hom}^-(k) = \sum_{j=0}^{(k-1)/2} \binom{p+k-2j-2}{k-2j-1}\binom{q+2j}{2j+1}$;

(v) $\dim \mathrm{harm}_B^+(k) = \dim \mathrm{hom}^+(d,k) - \dim \mathrm{hom}^+(d,k-2) =$

$$= \sum_{j=0}^{k/2} \binom{p+k-2j-1}{k-2j}\binom{q+2j-1}{2j} - \sum_{j=0}^{(k-2)/2} \binom{p+k-2j-3}{k-2j-2}\binom{q+2j-1}{2j} ;$$

(vi) $\dim \mathrm{harm}_B^-(k) = \dim \mathrm{hom}^-(d,k) - \dim \mathrm{hom}^-(d,k-2) =$

$$= \sum_{j=0}^{(k-1)/2} \binom{p+k-2j-2}{k-2j-1}\binom{q+2j}{2j+1} - \sum_{j=0}^{(k-3)/2} \binom{p+k-2j-4}{k-2j-3}\binom{q+2j}{2j+1} .$$

PROOF. *(i)* is well-known ; *(ii)* follows from the decomposition $\mathrm{hom}(d,k) = \mathrm{harm}_B(k) \perp \beta(.)\mathrm{hom}(d,k-2)$. To see *(iii)* we construct an explicit basis of $\mathrm{hom}^+(k)$: Write $a = (a_+;a_-)$ where $a=(a_1, \dots ,a_{p+q})$, $a_+ = (a_1, \dots ,a_p)$ and $a_- = (a_{p+1}, \dots ,a_{p+q})$. Then $x^a = x^{a_+}.x^{a_-}$ and $x^a \in \mathrm{hom}^+(k)$ iff $\sum_{i=1}^{d} a_i = k$ and $\sum_{i=p+1}^{d} a_i \equiv 0 \pmod 2$. Hence

$$\dim \mathrm{hom}^+(k) = \sum_{j=0}^{k/2} \dim \mathrm{hom}(p,k-2j).\dim \mathrm{hom}(q,2j) .$$

The proof of *(iv)* is entirely similar. Statements *(v)* and *(vi)* follow from the following decomposition:

$$\mathrm{hom}^\varepsilon(d,k) \simeq \mathrm{harm}_B^\varepsilon(k) \oplus \mathrm{hom}^\varepsilon(d,k-2) \quad ; \varepsilon= +/- \quad . \qquad \square$$

§2.6. The addition formula.

Let B be a bilinear form of inertia (p,q). For any vector $x \in V$ the map $f \to f(x)$ defines a linear functional on the space $\mathrm{harm}_B(k)$; Hence there exists a unique polynomial $\tilde{x} \in \mathrm{harm}_B(k)$ with the following "reproducing" property :

$$\langle \tilde{x}, f \rangle = f(x) \quad \text{for all} \quad f \in \mathrm{harm}_B(k) \quad . \tag{9}$$

Note that for all $\sigma \in \mathrm{Aut}\, B$ we have $\tilde{x^\sigma} = \tilde{x}^\sigma$, since for all $f \in \mathrm{harm}_B(k)$

$$\langle \tilde{x^\sigma}, f \rangle = f(x^\sigma) = f^{\sigma^{-1}}(x) = \langle \tilde{x}, f^{\sigma^{-1}} \rangle = \langle \tilde{x}^\sigma, f \rangle \; .$$

Next write $q(x,y) = \tilde{x}(y)$. Since $\tilde{x^\sigma} = \tilde{x}^\sigma$ we have

$$q(x^\sigma, y^\sigma) = q(x,y) \quad \text{for} \quad x,y \in V \quad \text{and} \quad \sigma \in \mathrm{Aut}\, B \; .$$

Consider an "orthonormal" basis $\{f_{k,i}; g_{k,j} \mid i=1,\ldots,\mu_k; j=1,\ldots,\nu_k\}$, i.e., a basis of $\mathrm{harm}_B(k)$ such that

$$\langle f_{k,i}, f_{k,u} \rangle = \delta_{iu} \; ; \; \langle g_{k,j}, g_{k,v} \rangle = -\delta_{jv} \; ;$$

$$\langle f_{k,i}, g_{k,j} \rangle = 0 \quad \text{for all } i,j,u,v \; .$$

The harmonic polynomial $\tilde{x}$ has the following expansion in this basis :

$$\tilde{x} = \sum_{i=1}^{\mu_k} \langle \tilde{x}, f_{k,i} \rangle f_{k,i} - \sum_{j=1}^{\nu_k} \langle \tilde{x}, g_{k,j} \rangle g_{k,j} \quad . \tag{10}$$

Combining this with (9) yields :

$$q(x,y) = \sum_{i=1}^{\mu_k} f_{k,i}(x) f_{k,j}(y) - \sum_{j=1}^{\nu_k} g_{k,j}(x) g_{k,j}(y) \quad .$$

Next we show that we may identify the function $q(x,y)$ in terms of the Gegenbauer polynomial of order $(d-2)/2$ and degree k in the variable $[x,y] := B(x,y)$. By lemma 2.3.1. we have $< \otimes^k x, f> = k!f(x)$ for $x \in V$ and $f \in \mathrm{hom}(k)$. The polynomial corresponding to $\otimes^k x$ is

$$[x,.]^k \in \mathrm{hom}(k) \quad ,$$

hence

$$<[x,.]^k, f> = k!f(x) \ .$$

As before, let H denote the projection $H\colon \mathrm{hom}(k) \to \mathrm{harm}_B(k)$, according to decomposition (7). From the uniqueness of the harmonic polynomial $\tilde{x}$ and the orthogonality of decomposition (7) we then have :

$$\tilde{x} = \frac{1}{k!} H[x,.]^k \ . \tag{11}$$

For the explicit determination of $\tilde{x}$ we need the following identity for $f \in \mathrm{hom}(k)$, which is easy to verify (cf. [V] page 446):

$$\partial_\beta(\beta^i \partial_\beta f) = \beta^i \partial_\beta^{i+1} f + 2i(d+2k-2i-2)\beta^{i-1}\partial_\beta{}^i f \ . \tag{12}$$

In view of (8) we may write

$$H[x,.]^k = \sum_{i=0}^{m} a_i \beta^i \partial_\beta{}^i [x,.]^k \quad ,$$

with $a_0 = 1$ and $m = \lfloor k/2 \rfloor$.
To determine the other coefficients a_i, apply ∂_β to both sides and use (12). From this one can derive the following recurrence relation:

$$a_i + (2i+2)(d+2k-2i-4)a_{i+1} = 0 \ .$$

Together with the following observation

$$\partial_\beta{}^i[x,.]^k = \frac{k!}{(k-2i)!}[x,.]^{k-2i}\beta^i(x) \quad ,$$

we obtain along the lines of [V] page 458 :

$$H[x,.]^k = k!\gamma_k\beta(x)^{k/2}\beta(.)^{k/2}C_k^{(d-2)/2}([x,.]/\beta(x)^{\frac{1}{2}}\beta(.)^{\frac{1}{2}}) \ , \quad (13)$$

where $\gamma_k = [(d-2)(d)\ldots(d+2k-4)]^{-1}$, and $C_k^{(d-2)/2}$ is a Gegenbauer polynomial. The Gegenbauer polynomial C_m^p is defined as follows :

$$C_m^p(t) = \frac{2m\ (p+m)}{m!\ (p)}[t^m - \frac{m(m-1)}{2^2(p+m-1)} + \frac{m(m-1)(m-2)(m-3)}{2^4.1.2.(p+m-1)(p+m-2)} \pm ..]$$

(cf. [V] page 458). An alternative definition is the following ([V] p. 492)

$$(1-2th+h^2)^{-p} = \sum_{m=0}^{\infty} C_m^p(t)h^m \ .$$

We now may combine (10),(11) and (13) to obtain the generalized addition formula.

THEOREM 2.6.1. $\gamma_k\beta(x)^{k/2}\beta(y)^{k/2}C_k^{(d-2)/2}(B(x,y)/\beta(x)^{\frac{1}{2}}\beta(y)^{\frac{1}{2}}) =$

$$= \sum_{i=1}^{\mu_k} f_{k,i}(x)f_{k,i}(y) - \sum_{j=1}^{\nu_k} g_{k,j}(x)g_{k,j}(y) \quad .$$

Here $\mu_k = \dim \mathrm{harm}_B^+(k)$, $\nu_k = \dim \mathrm{harm}_B^-(k)$ (cf. theorem 2.5.2) , while $\gamma_k = [(d-2)d\ \ldots\ (d+2k-4)]^{-1}$.

§2.7. Applications to few-distance sets in $R^{p,q}$.

In this section we shall use the generalized addition formula and the knowledge of the inertia of the inner product on $\mathrm{harm}_B(k)$ to obtain bounds on the size of s-distance sets of unit vectors in $R^{p,q}$, and in particular $R^{p,1}$ and $R^{1,q}$.

<u>LEMMA 2.7.1.</u> *Let* A *be a* v x m *matrix,* $I_{s,t} = \mathrm{diag}(1^s,-1^t)$, *where* $s + t = m$, *and suppose* $AI_{s,t}A^t = I_v$. *Then* $v \leq s$.

PROOF. Suppose that $v > s$, then certainly $\mathrm{rank}(A) > s$, and there exists an $x \in R^v$ with the property that $(x^tA)I_{s,t}(A^tx) < 0$. Since $AI_{s,t}A^t = I_v$ this implies that $x^tx < 0$, contradiction.

Let X be a set of points on the "unit sphere" of $V = R^{p,q}$:

$$S_{p,q} := \{x \in R^{p,q} \mid B(x,x) = 1\} ,$$

with $\mathrm{card}(X) = v$. Again we shall write $[x,y]$ for $B(x,y)$. Let $A := \{[x,y] \mid x,y \in X , x \neq y\}$ and suppose that $1 \notin A$. Also put $A' := A \cup \{1\}$. We define the following matrices :

$$F_k = F_k(x,i) = [f_{k,i}(x)]_{x\in X \; ; \; i=1,..,\mu_k} \; ;$$

$$G_k = G_k(y,j) = [g_{k,j}(y)]_{y\in X \; ; \; j=1,..,\nu_k} \; ;$$

$$D_\alpha = [d_\alpha(x,y)]_{x\in X \; ; \; y\in X} \; ; \quad d_\alpha(x,y) = 1 \quad \text{if } [x,y] = \alpha ,$$
$$d_\alpha(x,y) = 0 \quad \text{otherwise.}$$

As a direct consequence of the addition formula the following holds :

$$F_kF_k^t - G_kG_k^t = \sum_{\alpha\in A'} Q_k(\alpha)D_\alpha .$$

Here $Q_k = \gamma_k C_k^{(d-2)/2}$. Define the "annihilator polynomial" ϕ of X:

$$\phi(t) = \prod_{\alpha\in A} \frac{t-\alpha}{1-\alpha} ,$$

and expand ϕ in the "normalized" Gegenbauer polynomials Q_k

$$\phi = \sum_{k=0}^{s} \phi_k Q_k \quad , \quad \text{where} \quad s = \mathrm{card}(A) \ .$$

Then

$$\sum_{k=0}^{s} \phi_k \{F_k F_k^t - G_k G_k^t\} = \sum_{\alpha\in A'} \phi(\alpha) D_\alpha = I_v \ ,$$

i.e.,

$$H \ . \ \bigoplus_{k=0}^{s} \phi_k I_{\mu_k,\nu_k} \ . \ H^t = I_v \ .$$

Here $H = [F_0;F_1;G_0;G_1; \ \ldots \ ;F_d;G_d]$, and $I_{\mu_k,\nu_k} = \mathrm{diag}(1^{\mu_k},(-1)^{\nu_k})$.

The following theorem is now an immediate consequence of lemma 2.7.1.:

<u>THEOREM 2.7.2.</u> *Let* X *be a set of unit vectors in* $R^{p,q}$ *, such that, for* $x,y \in X$, $[x,y]$ *assumes only* s *different values, all different from* 1. *Let* $\phi = \Sigma\, \phi_k Q_k$ *be the expansion of the annihilator polynomial in the normalized Gegenbauer polynomials. Then*

$$\mathrm{card}(X) \le \sum_{k=0}^{s} \sigma_k \quad , \quad \textit{where} \quad \begin{aligned} \sigma_k &= \mu_k \quad \textit{if} \quad \phi > 0 \ , \\ \sigma_k &= \nu_k \quad \textit{if} \quad \phi < 0 \ , \\ \sigma \ &= 0 \quad \ \textit{if} \quad \phi = 0 \ . \end{aligned}$$

□

Here $\mu_k = \dim \mathrm{harm}_B^+(k)$, $\nu_k = \dim \mathrm{harm}_B^-(k)$. (cf. theorem 2.5.2).

§2.8. Examples.

In this section we shall compute the bounds explicitly for the case $p=d-1$, $q=1$. According to theorem 2.5.2. , μ_k and ν_k have the following values:

$$\mu_k = \dim\mathrm{harm}_B^+(k) = \binom{d+k-2}{k-1} \ ; \quad \nu_k = \binom{d+k-3}{k-1} \ .$$

Hence we get the following absolute bound:

THEOREM 2.8.1. *Let* X *be a set of unit vectors in* $R^{d-1,1}$ *such that the inner product between different elements of* X *assumes only* s *different values, all different from* 1, *then*

$$\mathrm{card}(X) \le \binom{d+s-1}{s}.$$

PROOF. $\mathrm{Card}(X) \le \sum_{k=0}^{s} \mu_k = \sum_{k=0}^{s} \binom{d+k-2}{k} = \binom{d+s-1}{s}$,since $\nu_k \le \mu_k$. □

In certain cases we can improve the bound, using the expansion of the annihilator polynomial in Gegenbauer polynomials explicitly. We give the first Gegenbauer polynomials:

$$Q_0(t) = 1 \quad ; \quad Q_1(t) = dx \quad ;$$

$$Q_2(t) = \frac{1}{2}d(d+2)(x^2 - \frac{1}{d}) \quad ;$$

$$Q_3(t) = \frac{1}{6}d(d+2)(d+4)(x^3 - \frac{3}{d+2}x) \quad ;$$

$$Q_4(t) = \frac{1}{24}d(d+2)(d+4)(d+6)(x^4 - \frac{6}{d+4}x^2 + \frac{3}{(d+2)(d+4)}) \quad ;$$

$$Q_5(t) = \frac{1}{120}d \ \ldots \ (d+8)(x^5 - \frac{10}{d+6}x^3 + \frac{15}{(d+4)(d+6)}x) \quad .$$

EXAMPLE 2.8.2. Let X be a set of unit vectors in $R^{9,1}$ with inner products $\{0,-\frac{1}{2},+\frac{1}{2}\}$. The annihilator polynomial in this case is

$$\phi(t) = \frac{4}{3}t(t+\tfrac{1}{2})(t-\tfrac{1}{2}) \quad .$$

Sinde $d=10$ the annihilator polynomial is an exact multiple of Q_3. Hence the bound of theorem 2.7.2. yields $\mathrm{card}(X) \le \dim \mathrm{harm}^{+}_{9,1}(3) = 165$. Equality is realized by the following set of vectors in $R^{10,1}$, in the orthoplement of the vector $(3;1^{10})$:

$$(0;1,-1,0^8) \quad \text{and} \quad (1;1^3,0^7) \quad .$$

There are 90 vectors of the first type, which fall in 45 antipodal pairs, and 120 of the second type. This system can be regarded as an extension of the rootsystem E_8 in the following representation :

$\pm(0;1,-1,0^7)$ and $\pm(1;1^3,0^6)$,

in the orthoplement of the isotropic vector $(3;1^9)$ in $R^{9,1}$.

EXAMPLE 2.8.3. Let X be a set of vectors with inner products $\{+1/3,-1/3\}$ in $R^{9,1}$. The annihilator polynomial $(9t^2-1)/8$ is a multiple of Q_2. We get $\text{card}(X) \leq \dim \text{harm}^+_{8,1}(2) = 36$. Equality is realized by the following vectors in $R^{9,1}$ in the orthoplement of $(2\sqrt{2};1^9)$:

$(\frac{1}{2}\sqrt{2};1^2,0^7)$.

This system can be seen as a subsystem of the previous example in the following way: Fix a vector and consider all vectors with inner product $+\frac{1}{2}$ with this vector. Now project this system on the orthoplement of the fixed vector.

NON-EXAMPLE 2.8.4. Let X be a set of vectors in $R^{3,1}$, with inner products $\{0,\pm\frac{1}{2},\pm\frac{1}{2}\sqrt{3}\}$. Then $\phi(t) = t(4t^2-1)(4t^2-3)/3$ is an exact multiple of Q_5 . From this we get that $\text{card}(X) \leq 21$. However this bound cannot be achieved, as was established by Bussemaker using a computer search.

EXAMPLE 2.8.5. Let X be a set of vectors in $R^{25,1}$, with inner products $\{0,\pm\frac{1}{2},\pm\frac{1}{4}\}$. Then $\phi(t)$ is a multiple of Q_5 and we get $\text{card}(X) \leq \binom{29}{5}$. This example is analogous to example 2.8.2. in the following sense. Example 2.8.2. is a system of vectors that is an extension of a (1,1)- dimensional lower extremal system. In this case the extremal system in R^{24} indeed exists, consisting of the $\binom{28}{5}$ antipodal pairs of vectors closest to the origin in the Leech lattice. Whether this system can be extended in a certain sense to $\binom{29}{5}$ vectors in $R^{25,1}$ is unknown.

EXAMPLE 2.8.6. Let X be a set of vectors in $R^{24,1}$, with inner products $\{0,\pm 1/3\}$. The annihilator polynomial is a multiple of Q_3 , and the bound yields $2600 = \binom{26}{3}$. There do exist 2300 vectors with the prescribed inner products in R^{23}. So far the best we can realize in $R^{24,1}$ is 2324, viz. the following set of vectors: $(8;4^2,0^{22})$,giving $\binom{24}{2}$ vectors, and the vectors $(0;(\pm 1)^{24})$ where the +1 positions correspond to a word in the extended binary Golay code, 2048 pairs.

CHAPTER 3

EQUIANGULAR LINES IN $R^{d,1}$

§3.1. Introduction.

Let $R^{d,1}$ be the (d+1)-dimensional vector space over the reals, provided with the following inner product:

$$(x,y) = -x_0y_0 + x_1y_1 + \dots . x_dy_d \quad .$$

If two lines through the origin span a plane on which the inherited inner product is positive definite, we can define their angle to be $\arccos|(x,y)|$ where x and y are unit vectors along the lines. A set of equiangular lines is a set of lines, such that for each pair the angle is defined and equal to the same value, $\arccos\alpha$ say. Using an argument based on an idea of Koornwinder [K], and on eigenvalue techniques of van Lint and Seidel [vLS] we obtain sharp bounds on the cardinality of sets of equiangular lines in $R^{d,1}$.

§3.2. The theorem

THEOREM 3.2.1. *Let* X *be a set of equiangular lines in* $R^{d,1}$ *at angle* $\arccos(\alpha)$ *, then*

(i) if $(d+1)\alpha^2 \le 1$ *, then* $\mathrm{card}(X) \le d(1-\alpha^2)/(1-d\alpha^2)$;

(ii) if $(d+1)\alpha^2 > 1$ *, then* $\mathrm{card}(X) \le \frac{1}{2}d(d+1)$,

and equality in (i) can only be realized if the set is in a positive definite subspace of dimension d . *Also, an infinite series of sets realizing equality in (ii) exists.*

PROOF. Let U be a set of unit vectors, one along each line of X. The Gram matrix G of the set U has at most d positive eigenvalues. Hence $C = \alpha^{-1}(G - I)$ has v−d eigenvalues less than or equal to $-\alpha^{-1}$, with $v = \mathrm{card}(X)$. Call the other eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_d$.

Since the matrix C has zeros on the diagonal and ± 1 elsewhere

$$0 = \operatorname{tr} C \le \lambda_1 + \lambda_2 + \ldots + \lambda_d - \frac{v-d}{\alpha} \quad ,$$

$$v(v-1) = \operatorname{tr} C^2 \ge \lambda_1^2 + \ldots + \lambda_d^2 + \frac{v-d}{\alpha^2} \quad .$$

As a consequence the following inequalities hold:

$$\frac{(v-d)^2}{\alpha^2} \le (\lambda_1 + \ldots + \lambda_d)^2 \le d(\lambda_1^2 + \ldots + \lambda_d^2) \le d(v(v-1) - \frac{v-d}{\alpha^2}) \quad .$$

In case $d < 1/\alpha^2$ this is equivalent to

$$v \le d(1-\alpha^2)/(1-d\alpha^2) \; .$$

Note that equality can only occur if $\lambda_{d+1}, \ldots, \lambda_v$ are all equal to $-1/\alpha$ and this implies that the subspace $\langle U \rangle$ is actually positive definite.

To prove the second part we proceed as follows. For each $u \in U$ define $F_u : R^{d,1} \to R$ by

$$F_u(x) = (u,x)^2 - \alpha^2 (x,x) \quad ,$$

and define $d+1$ additional functions

$$f_0(x) = (x,x) \quad ; \quad f_i(x) = x_0 x_i \quad , \text{ for } i=1,2,\ldots,d \; .$$

We will show that the set $F = \{F_u, f_0, f_i \mid i=1,\ldots,d \;, u \in U\}$ is independent. This implies our claim, since all these functions are homogeneous of degree 2 and therefore $\operatorname{card}(F) \le \frac{1}{2}(d+1)(d+2)$.

Suppose there is a dependency relation for the functions in F :

$$\sum_{u \in U} a_u F_u(x) + \sum_{i=1}^{d} a_i f_i(x) + a_0 f_0(x) \equiv 0 \; . \tag{1}$$

For $u,v \in U$ always $F_u(v) = (1-\alpha^2)\delta_{uv}$, hence when we insert $u \in U$ in this relation the following results:

$$a_u(1-\alpha^2) + \sum_{i=1}^{d} a_i u_0 u_i + a_0 = 0 \quad (2)$$

Comparing coefficients of x_0^2, x_i^2, and $x_0 x_i$ in (1) yields :

$$\sum_{u\in U} a_u(u_0^2 + \alpha^2) - a_0 = 0 \quad ; \quad (3)$$

$$\sum_{u\in U} a_u(u_i^2 - \alpha^2) + a_0 = 0 \quad ; \quad (4)$$

$$-2 \sum_{u\in U} a_u u_0 u_i + a_i = 0 \quad . \quad (5)$$

Now add (3) and (4) :

$$\sum_{u\in U} a_u u_0^2 = - \sum_{u\in U} a_u u_i^2 \ .$$

Summation of both sides of this equation, and putting $(u,u)=1$ yields:

$$d \sum_{u\in U} a_u u_0^2 = - \sum_{u\in U} a_u(1+u_0^2) \ .$$

From (3) one obtains

$$a_0 = (\alpha^2 - \frac{1}{d+1}) \sum_{u\in U} a_u \ . \quad (6)$$

Now if $(d+1)\alpha^2 = 1$ this implies $a_0=0$. Otherwise we can multiply (1) by a_u and sum over u (using (5) and (6)) to obtain

$$\sum_{u\in U} a_u^2(1-\alpha^2) + \tfrac{1}{2} \sum_{i=1}^{d} a_i^2 + \frac{d+1}{(d+1)\alpha^2-1} a_0^2 = 0 \ .$$

This is a sum of squares since $(d+1)\alpha^2 - 1 > 0$, hence all a_i are 0. If $(d+1)\alpha^2 = 1$ we get the same relation except for the term involving a_0 and we are done as well. So $\mathrm{card}(U) = \mathrm{card}(F)-(d+1) \le \tfrac{1}{2}d(d+1)$. □

An infinite series of sets realizing the bound is provided by:

In $R^{d+1,1}$ the vector $w=(2\sqrt{2};1^{d+1})$ satisfies $(w,w) = d-7$. Therefore we may identify $w^{\perp}$ with $R^{d,1}$ for $d > 7$. The set of $\frac{1}{2}d(d+1)$ vectors of the form

$$(\tfrac{1}{2}\sqrt{2};1^2,0^{d-1})$$

is in $w^{\perp}$ and spans a set of equiangular lines at arccos(1/3). For d=7, $w^{\perp}/\langle w\rangle$ is isomorphic to R^7 and the construction yields 28 equiangular lines. More on this system can be found in [LS] and [vLS] . This representation is due to Seidel (unpublished). For $\alpha=1/5$, d=23 , there exists a set of 276 lines (cf. [LS]). With the help of the Steiner system 4-(23,7,1) they can be nicely described as a set of lines in $R^{23,1}$ as follows: (For details about Steiner systems see [CvL])

$$23 \text{ vectors : } \quad (3\ 2;-1^1,1^{22}) \quad ,$$

$$253 \text{ vectors : } \quad (\ 2;1^7,0^{16}) \quad ,$$

where the positions of the seven ones in the last type corresponds to the blocks of the Steiner system 4-(23,7,1).
Related to this example are sets of lines at arccos(1/5) in R^{22} and R^{21} realizing the bound in part (i) of the theorem. For $\alpha < 1/5$ no case of equality is known.

<u>REMARK 3.2.2.</u> In the case $(d+2)^{-1} < \alpha^2 < (d+1)^{-1}$ we have

$$d(1-\alpha^2)/(1-d\alpha^2) < \tfrac{1}{2}d(d+1) \ .$$

This set of values for α is excluded however by the following theorem.

<u>THEOREM 3.2.3.</u> *If* $v < 2d+2$ *then* α^{-1} *is an integer.*

PROOF. This is essentially theorem 3.4. from [LS], due to Neumann. Let $A = \alpha^{-1}(G-I)$ where G is the Gram matrix of U. Then A is an integral matrix, and has eigenvalue $-\alpha^{-1}$ with multiplicity $m=v-d-1$. Therefore, $-\alpha^{-1}$ is an algebraic integer, and every algebraic conjugate is an eigenvalue with the same multiplicity m. Since $2m=2v-(2d+2) > v$, there is at most one eigenvalue of multiplicity m, which implies that

$-\alpha^{-1}$ is rational, and hence an integer. (In fact one can prove that α^{-1} is an odd integer.)

CHAPTER 4

FEW-DISTANCE SETS IN E^d AND H^d

§4.1. Introduction.

Using Koornwinders argument one obtains the same bounds for s-distance sets in E^d , d-dimensional Euclidean space, and H^d , d-dimensional hyperbolic space , viz.

$$\binom{d+s}{s} + \binom{d+s-1}{s-1} .$$

In both cases it is possible to reduce the bounds using the trick of finding an additional set of independent functions. As a consequence we get the following

<u>THEOREM 4.1.1.</u> *Let* X *be an s-distance set in* E^d *or* H^d *, then*

$$\text{card}(X) \le \binom{d+s}{s} .$$ □

§4.2. Preliminaries and notation.

The vector space R^d together with the usual metric, coming from the inner product $(x,y) = x_1y_1 + \dots + x_dy_d$, will be called E^d ,i.e., d-dimensional Euclidean space. By H^d we denote d-dimensional hyperbolic space. H^d can be realized as follows : Let $R^{1,d}$ be a (d+1)-dimensional vector space over R provided with the inner product

$$\langle x,y\rangle = x_0y_0 - x_1y_1 - \dots - x_dy_d .$$

The points of H^d are the 1-dimensional subspaces $\langle x\rangle$, with $\langle x,x\rangle > 0$. Distance is defined by

$$d(\langle x\rangle,\langle y\rangle) = \operatorname{arcosh}\left|\frac{\langle x,y\rangle}{\langle x,x\rangle^{\frac12}\langle y,y\rangle^{\frac12}}\right| .$$

If we take for x and y unit vectors with positive first coordinate, this becomes $d(x,y) = \operatorname{arcosh}(-\langle x,y\rangle)$. Vectors in R^d or $R^{1,d}$ will be denoted by u,v,x,y,z, where $x=(x_1,x_2,\dots,x_d)$ or $x=(x_0,x_1,\dots,x_d)$. By $b,c,\dots,g$ we denote vectors of length d or $d+1$ with nonnegative integral entries.

The monomial $x_0^{e_0}x_1^{e_1}\dots x_d^{e_d}$ is denoted by the symbol x^e. An appropriate greek letter will denote the sum of the entries of an integral vector ($\beta = b_0+b_1+\dots+b_d$ etc.) . Also

$$\binom{\beta}{b} = \frac{\beta!}{b_0!b_1!\dots b_d!} .$$

Let $\sigma(j)$ be the elementary symmetric function in the variables $\alpha_1,\dots,\alpha_s$, of degree j. So

$$\prod_{i=1}^{s} (t+\alpha_i) = \sum_{j=0}^{s} \sigma(j)t^{s-j} .$$

Denote by $\sigma_u(j)$ the elementary symmetric function of degree j in the variables $(u,u) - \alpha_i$; $i=1,\dots,s$. So

$$\prod_{i=1}^{s} (t+(u,u)-\alpha_i) = \sum_{j=0}^{s} \sigma_u(j)t^{s-j}.$$

Note that $\sigma_u(j) = \sum_{i=0}^{j} \binom{s-i}{j-i}(-1)^i(u,u)^{j-i}\sigma(i)$.

Finally if V is a vector space with basis A , we write $p= \sum_{a\in A} [p,a]a$ for $p \in V$, so $[p,a]$ are the coordinates of p relative to the basis A.

§4.3. The bound in Euclidean space.

THEOREM 4.3.1. *Let X be an s-distance set in E^d, then*

$$\operatorname{card}(X) \le \binom{d+s}{s} .$$

PROOF. Let $\alpha_1, \alpha_2, \ldots, \alpha_s$ be the squares of the distances that occur in X. For each $u \in X$ define the polynomial

$$F_u(x) = \prod_{i=1}^{s} \{(x-u, x-u) - \alpha_i\} = \prod_{i=1}^{s} \{(x,x) - 2(x,u) + (u,u) - \alpha_i\} .$$

For $u,v \in X$ we have $F_u(v) = 0$ iff $u \neq v$. This implies that the polynomials $F_u(x)$ are independent. We may expand F_u as follows:

$$F_u(x) = \sum_{j=0}^{s} \sigma_u(s-j)[(x,x) - 2(x,u)]^j =$$

$$= \sum_{\substack{\varepsilon;g \\ \varepsilon+\gamma \le s}} \sigma_u(s-\varepsilon-\gamma) \binom{\varepsilon+\gamma}{\gamma} (-2)^\gamma \binom{\gamma}{g} u^g x^g (x,x)^\varepsilon . \qquad (1)$$

The summation in (1) is over all nonnegative integral d-vectors g and nonnegative integers ε, such that $\varepsilon + g_1 + g_2 + \quad + g_d \le s$.

The F_u are linear combinations of the functions in the set

$$\{(x,x)^\delta x^b \mid \delta + \beta = s \ \underline{\text{or}}\ \delta = 0 \text{ and } \beta < s\} .$$

The following bound is a direct consequence of this:

$$\text{card}(X) \le \binom{d+s}{s} + \binom{d+s-1}{s-1} .$$

We now proceed to show that in fact the set

$$\{F_u(x) \ , \ x^b \mid u \in X \ , \beta < s\}$$

is independent. This yields the desired result :

$$\text{card}(X) + \binom{d+s-1}{s-1} \le \binom{d+s}{s} + \binom{d+s-1}{s-1} .$$

Suppose then, there is a dependency relation:

$$\sum_{u \in X} a_u F_u(x) + \sum_{b:\beta<s} a_b x^b = 0 \qquad . \qquad (2)$$

<u>LEMMA 4.3.2.</u> *Relation (2) implies :*

$$\forall b \ \textit{with} \ \beta < s : \sum_{u\in X} a_u u^b = 0 \ .$$

PROOF. We shall use induction. First consider the part of (2) that is homogeneous of maximal degree 2s in x. From the explicit expansion (1) of F_u we see that this only happens for $\varepsilon = s$, $\delta = 0$, and we obtain $\sum_{u\in X} a_u = 0$. So the lemma is true for $\beta = 0$. Now suppose

$$\sum_{u\in X} a_u u^b = 0 \ , \quad \text{for all } b \text{ with } 0 \le \beta < t < s \ .$$

Consider the part of (2) that is homogeneous of degree 2s−t in x. This yields

$$\sum_{u\in X} a_u \Big[\sum_{\substack{\varepsilon;g \\ 2\varepsilon+\gamma=2s-t}} \sigma_u(s-\varepsilon-\gamma)\binom{\gamma+\varepsilon}{\gamma}\binom{\gamma}{g}(-2)^{\gamma} u^g (x,x)^{\varepsilon} x^g \Big] = 0 \ .$$

Since

$$\sigma_u(s-\varepsilon-\gamma) = \binom{s}{s-\varepsilon-\gamma}(u,u)^{s-\varepsilon-\gamma} - \binom{s-1}{s-\varepsilon-\gamma-1}(u,u)^{s-\varepsilon-\gamma-1} \pm \ldots \ ,$$

we may, after changing the order of summation, use the induction hypothesis:

$$\sum_{u\in X} a_u (u,u)^{s-\varepsilon-\gamma-i} u^g = 0 \quad , \quad \text{for all } i > 0 \ .$$

Hence

$$\sum_{\substack{\varepsilon;g \\ 2\varepsilon+\gamma=2s-t}} \binom{\varepsilon+\gamma}{\gamma}\binom{\gamma}{g}(-2)^{\gamma}\binom{s}{s-\varepsilon-\gamma}\Big[\sum_{u\in X} a_u (u,u)^{s-\varepsilon-\gamma} u^g (x,x)^{\varepsilon} x^g\Big] = 0.$$

Finally, substituting $x=v$, multiplying by $a_v(v,v)^{s-t}$ and summing over all $v \in X$ yields:

$$\sum_{\substack{\varepsilon;g \\ 2\varepsilon+\gamma=2s-t}} \binom{\gamma+\varepsilon}{\gamma}\binom{\gamma}{g}(-2)^{\gamma}\binom{s}{\gamma+\varepsilon}\Big[\sum_{u\in X} a_u (u,u)^{s-\varepsilon-\gamma} u^d\Big]^2 = 0 .$$

This is a sum of squares, with all coefficients of same sign, therefore

$$\sum_{u\in X} a_u (u,u)^{s-\varepsilon-\gamma} u^g = 0 \quad , \quad \text{if} \quad 2\varepsilon+\gamma = 2s-t \quad ,$$

and in particular

$$\sum_{u\in X} a_u u^d = 0 \qquad \text{if} \qquad \gamma = t . \qquad \square$$

We now proceed with the proof of the theorem. From (2) it follows in particular, with $\pi = \prod_{i=1}^{s} (-\alpha_i)$:

$$a_u \pi \; + \sum_{b:\beta<s} a_b u^b = 0 .$$

The second term of the left hand side is 0, by lemma 4.3.2., so finally we arrive at $a_u = 0$ for all $u \in X$. This finishes the proof of theorem 4.3.1. $\square$

4.4. The bound in hyperbolic space.

<u>THEOREM 4.4.1.</u> *Let* X *be an s-distance set in* H^d *, then*

$$\operatorname{card}(X) \le \binom{d+s}{s} .$$

PROOF. We use the representation of H^d described in 4.2., each point will be identified with a unit vector in $R^{1,d}$ with positive first coordinate. Let $\alpha_1, \alpha_2, \ldots, \alpha_s$ denote the different values of $\langle u,v\rangle$ for distinct $u,v \in X$. For each $u \in X$ define

$$F_u(x) = \prod_{i=1}^{s} (\langle u,x\rangle - \alpha_i) ,$$

and consider these polynomials as elements of the ring

$$R[x_0, x_1, \dots, x_d]/(\langle x,x\rangle - 1) .$$

Since $x_0^2 = 1+x_1^2+ \dots +x_d^2$ in this ring, a basis is formed by the set $\{x^e \mid e_0 \in \{0,1\}\}$. The F_u are independent and they are linear combinations of the basis elements x^e with $\varepsilon \le s$. From this it follows that

$$\operatorname{card}(X) \le \binom{d+s}{s} + \binom{d+s-1}{s-1} .$$

In this case we will show that in fact the following set is independent:

$$\{F_u(x) \ , \ x^e \mid u \in X \ , \ \varepsilon \le s \ , \ e_0 = 1\} .$$

From this we get $\operatorname{card}(X) \le \binom{d+s}{s}$. We shall write

$$E_i = \{e \mid \varepsilon \le s \ , \ e_0 = i\} \ , \ i=0,1 \ ; \ E = E_0 \cup E_1 .$$

Also, $[x^f, x^e]$ will be abbreviated by $[f,e]$ (see 4.2. last line).

Suppose then we have the following dependence relation:

$$\sum_{u \in X} a_u F_u(x) + \sum_{e \in E_1} a_e x^e = 0 . \tag{3}$$

Then, with $\pi = \prod_{i=1}^{d} (1-\alpha_i)$, we have in particular

$$a_u \pi + \sum_{e \in E_1} a_e u^e = 0 , \qquad \text{for all } u \in X . \tag{4}$$

The $F_u(x)$ may be represented relative to the basis $\{x^e \mid e \in E\}$ as follows:

$$F_u(x) = \sum_{f:\phi \le s} \binom{\phi}{f} (s-\phi)(-1)^{s-\phi} u^f x^f (-1)^{\phi - f_0} =$$

$$= \sum_{f:\phi \le s} (-1)^{s-f_0} (s-\phi) \binom{\phi}{f} u^f \Big[\sum_{e \in E} [f,e] x^e \Big] .$$

Note that $[f,e] = 0$ either for all $e \in E_0$ or for all $e \in E_1$ depending on whether f_0 is odd or even. So, comparing coefficients of the respective basis elements we get:

$$(-1)^{s-1} \sum_{u \in X} a_u \sum_{f:\phi \leq s} \binom{\phi}{f} [f,e] u^f \sigma(s-\phi) + a_e = 0 \qquad \forall e \in E_1 \quad , \qquad (5)$$

and

$$\sum_{u \in X} a_u \sum_{f:\phi \leq s} \binom{\phi}{f} [f,e] u^f \sigma(s-\phi) = 0 \qquad \forall e \in E_0 \quad . \qquad (6)$$

Multiplication of (5) by v^e and of (6) by $(-1)^{s-1} v^e$ and summation over $e \in E$ yields:

$$(-1)^{s-1} \sum_{f:\phi \leq s} \binom{\phi}{f} \sigma(s-\phi) \sum_{u \in X} a_u u^f \sum_{e \in E} [f,e] v^e + \sum_{e \in E_1} a_e v^e = 0 \ .$$

Since $\sum_{e \in E} [f,e] v^e = v^f$, this together with (4) implies

$$(-1)^{s-1} \sum_{f:\phi \leq s} \binom{\phi}{f} \sigma(s-\phi) \sum_{u \in X} a_u u^f v^{f'} - a_v \pi = 0 \ .$$

Finally, after multiplication by a_v , and summation over all $v \in X$:

$$(-1)^{s-1} \sum_{f:\phi \leq s} \binom{\phi}{f} \sigma(s-\phi) [\sum_{u \in X} a_u u^f]^2 - \pi \sum_{u \in X} a_u^2 = 0,$$

Now $(-1)^s \pi > 0$ since $a_i > 1$ for all i. Therefore we have again a sum of squares, and $a_u = 0$ for all $u \in X$. This finishes the proof of theorem 4.4.1. . □

CHAPTER 5

FEW-DISTANCE SETS MOD p

5.1. Introduction.

In [FW] the authors proved the following theorem:

<u>THEOREM 5.1.1.</u> *Let* $F = \{F_i | i \in I\}$ *be a collection of subsets of an n-set, and let* $\mu_0, \mu_1, \ldots, \mu_s$ *be distinct residues modulo a prime* p, *such that* $|F_i| = k$, *with* $k \equiv \mu_0 \pmod p$, *and* $|F_i \cap F_j| \equiv \mu_h \pmod p$ *for some* h, $1 \le h \le s$. *Then* $|F| \le \binom{n}{s}$.

In this chapter we shall generalize this theorem to arbitrary bilinear form spaces in two ways. Central to the proof is the following lemma, where ZM denotes the set of all Z-linear combinations of elements from the set M.

<u>LEMMA 5.1.2.</u> *Let* M *be a nonempty finite set of real numbers. If* $M \subset pZM$ *for some prime* p, *then* $M = \{0\}$.

PROOF. QM is a finite dimensional vector space over Q, the field of rational numbers. Write the elements of M as vectors expressed in some fixed basis of this vector space. For $m \in QM$ let $v_p(m)$ be the minimal exponent of p in all coordinates of m relative to this basis, where the exponent of p in 0 is to be taken $+\infty$. Since $v_p(m \pm n) \ge \min(v_p(m), v_p(n))$, we have the following :

$$\min_{m \in ZM} v_p(m) = \min_{m \in M} v_p(m) = \min_{m \in pM} v_p(m) = 1 + \min_{m \in M} v_p(m) .$$

Hence $M = \{0\}$.

5.2. The mod p-bound , first version.

Let $V = R^d$ be equipped with a bilinear form B , say

$$B(x,y) = x_1y_1 + \dots + x_qy_q - x_{q+1}y_{q+1} - \dots - x_dy_d \,.$$

THEOREM 5.2.1. *Let* X *be a set of vectors in* V *such that there are* $a_0, a_1, \dots, a_s \in Z$ *all distinct* mod p *with*

(i) $B(x,x) = a_0$ *for all* $x \in X$ *;*

(ii) $B(x,y) \equiv a_i \pmod p$ *for some* $i,\ 1 \le i \le s$ *if* $x \neq y \in X$*;*

then $\operatorname{card}(X) \le \binom{d+s-1}{d-1} + \binom{d+s-2}{d-1}$.

PROOF. Let Pol(s,d) denote the set of all polynomials of degree at most s in d variables restricted to the "sphere" $B(x,x) = a_0$. Then $\dim \mathrm{Pol}(s,d) = \binom{d+s-1}{d-1} + \binom{d+s-2}{d-1}$ (unless q=0 or d, and $a_0 \ge 0$ resp. $a_0 \le 0$). Again we associate to $x \in X$ the polynomial $f_x(y) = \prod_{i=1}^{s} ((x,y)-a_i)$ where $(x,y) = B(x,y)$. We then have :

$$f_x(x) \not\equiv 0 \pmod p \qquad \text{for all } x \in X \,;$$

$$f_x(y) \equiv 0 \pmod p \qquad \text{for } x \neq y \in X \,.$$

Assume there is a relation $\sum_{x \in X} m_x f_x = 0$. Inserting $x \in X$ in this relation yields:

$$m_x f_x(x) = -\sum_{y \neq x} m_y f_y(x) \in pZM \quad ,$$

where $M = \{m_x \mid x \in X\}$. Since $f_x(x) \not\equiv 0 \pmod p$ this implies that $m_x \in pZM$ for all x , hence $M \subset pZM$. Lemma 5.1.2. now yields that $M = \{0\}$, i.e., the polynomials are independent. This finishes the proof. □

5.3. The mod p-bound second version.

THEOREM 5.3.1. *Let* X *be a set of vectors in* V *such that there are* $a_1, \dots, a_s \in Z$ *with*

(i) $B(x,x) \in Z$ *and* $B(x,x) \not\equiv a_i \pmod p$ *for all* $x \in X$ *and* $1 \le i \le s$;

(ii) $B(x,y) \equiv a_i \pmod p$ *for some* i , $1 \le i \le s$ *and* $x \ne y \in X$; *then* $\mathrm{card}(X) \le \binom{d+s}{d}$.

PROOF. The proof is entirely similar to the previous one. The only difference is that one takes instead of Pol(s,d) the space of all polynomials of degree at most s, i.e., no longer restricted to the "sphere".

EXAMPLE 5.3.2. Let X be a set of vectors in R^d all with norm $\sqrt{7}$. Assume the inner products that are allowed are 0,2,3,5,6. The bound in theorem 5.2.1. with p=3 yields $\mathrm{card}(X) \le \frac{1}{2}d(d+3)$. So far the best bound was $\binom{d+9}{10} + \binom{d+8}{9}$.

For more significant and realistic examples we refer to the end of the next chapter.

CHAPTER 6

ASSOCIATION SCHEMES, DELSARTE SPACES AND THE MOD p-BOUND

§6.1 Introduction.

The theorem of Frankl and Wilson of the previous chapter deals with collections of k-subsets of an n-set, i.e., sets of points in the Johnson scheme $J(n,k)$. This scheme as well as the Hamming scheme are examples of Q-polynomial association schemes. These schemes have central properties in common with finite dimensional projective spaces over the real or the complex numbers. Neumaier [N1] proposed a common generalization which he calls Delsarte spaces. It is our aim in this chapter to present the basic facts concerning association schemes and Delsarte spaces, to prove the generalization of Frankl and Wilson's theorem for Delsarte spaces and to give examples meeting the bound, in particular for the Hamming scheme.

§6.2. Association schemes.

Let X be a finite set with cardinality n. An s-class association scheme on X is a partition of $X \times X$ into $s+1$ symmetric relations $\Gamma_0, \Gamma_1, \ldots, \Gamma_s$ having the following properties :

(i) Γ_0 is the identity : $\Gamma_0 = \{(x,x) \mid x \in X\}$.

(ii) There are constants v_k , $k=0,1,\ldots,s$ such that for all $x \in X$:

$$|\{y \in X \mid (x,y) \in \Gamma_k\}| = v_k \quad .$$

(iii) There are constants a_{ij}^k , $i,j,k = 0,1,\ldots,s$ with $\forall (x,y) \in \Gamma_k$:

$$|\{z \in X \mid (x,z) \in \Gamma_i \wedge (z,y) \in \Gamma_j\}| = a_{ij}^k \quad .$$

The a_{ij}^k are called the intersection numbers of the scheme, the v_k the valencies. Note that (iii) implies (ii) since $v_k = a_{kk}^0$.

Another way to characterize the defining properties of an association scheme is by means of the adjacency matrices $A_0,\ldots,A_s$ defined by

$$A_i(x,y) = \begin{cases} 1 & \text{if } (x,y) \in \Gamma_i , \\ 0 & \text{otherwise} . \end{cases}$$

Since Γ_0 is the identity $A_0 = I$. The Γ_i partition $X \times X$, hence

$$A_0 + A_1 + \ldots + A_s = J .$$

Property (ii) implies $A_k J = v_k J$ and (iii): $A_i A_j = \sum_{k=0}^{s} a_{ij}^k A_k$.

Since the relations Γ_k are symmetric , so are the matrices A_k . The vector space $\langle A_0,A_1,\ldots,A_s\rangle_R$ is therefore a commutative algebra called the Bose-Mesner algebra of the association scheme.

EXAMPLES 6.2.2. Let X be the collection of all k-subsets of an n-set. Put $(x,y) \in \Gamma_i$ if $|x\Delta y| = 2i$, for $i=0,1,\ldots,k$, where $k \le \frac{1}{2}n$. This defines an association scheme called the Johnson scheme $J(n,k)$. This scheme has the following intersection numbers :

$$a_{ij}^h = \sum_{t=0}^{h} \binom{h}{k-i-t}\binom{k-h}{t}\binom{h}{k-j-t}\binom{n-k-h}{t+i+j-k} .$$

Next let X be the collection of all subsets of an n-set , and put $(x,y) \in \Gamma_i$ if $|x\Delta y| = i$, for $i = 0,1,\ldots,n$. This association scheme is called the Hamming scheme $H(n,2)$ and has the following intersection numbers:

$$a_{ij}^h = \begin{cases} \binom{h}{\frac{1}{2}(i-j+h)}\binom{n-h}{\frac{1}{2}(i+j-h)} & \text{if } i+j+h \text{ is even} , \\ 0 & \text{otherwise} . \end{cases}$$

§6.3. The Bose-Mesner algebra.

An important rôle in the theory is played by the basis of orthogonal minimal idempotents (cf [D],[BM]). They are precisely the projectors on the common eigenspaces of the matrices $A_0, A_1, \ldots, A_s$, and are denoted by $E_0, E_1, \ldots, E_s$ with $E_0 = \frac{1}{n}J$. The Bose-Mesner algebra is also closed under Schur (or Hadamard) multiplication, defined by $A \circ B(x,y) = A(x,y).B(x,y)$. This implies the existence of constants b_{ij}^k such that $E_i \circ E_j = \frac{1}{n}\sum_{k=0}^{s} b_{ij}^k E_k$. Moreover $b_{ij}^k \geq 0$ for all i,j,k since $E_i \circ E_j$ is a principal minor of $E_i \otimes E_j$ which is positive semidefinite. The b_{ij}^k are called the <u>Krein parameters</u>. Summarizing :

$$\text{(i)} \quad E_i E_j = \delta_{ij} E_i \quad ; \quad E_i \circ E_j = \frac{1}{n}\sum_{k=0}^{s} b_{ij}^k E_k \quad ;$$

$$\text{(ii)} \quad A_i \circ A_j = \delta_{ij} A_i \quad ; \quad A_i A_j = \sum_{k=0}^{s} a_{ij}^k A_k \quad .$$

The matrices $P = (p_{ik})$ and $Q = (q_{ik})$, $i,k=0,1,\ldots,s$ are defined by the following relations :

$$A_k = \sum_{i=0}^{s} p_{ik} E_i \quad ; \quad E_i = \frac{1}{n}\sum_{k=0}^{s} q_{ki} A_k \quad .$$

Note that p_{ik} is an eigenvalue of A_k with multiplicity $\mu_i = \text{rk } E_i = \text{tr } E_i = q_{0i}$. The μ_i are called the <u>multiplicities</u> of the scheme. Let $\Delta_\mu = \text{diag}(\mu_i)_{i=0}^s$ and $\Delta_v = \text{diag}(v_k)_{k=0}^s$. The multiplicities and the valencies are related as follows :

<u>THEOREM 6.3.1.</u> $\Delta_\mu P = Q^t \Delta_v$.

PROOF. $\mu_i p_{ik} = p_{ik} \text{tr} E_i = \text{tr } A_k E_i = \sum_{\text{elts}} E_i \circ A_k = \frac{q_{ki}}{n} \sum_{\text{elts}} A_k = q_{ki} v_k$.

Define a graph on X by $x \sim y$ if $(x,y) \in \Gamma_1$. If $(x,y) \in \Gamma_i$ iff $d(x,y) = i$ in this graph the scheme is called <u>metric</u>. The Johnson scheme and the Hamming scheme are examples of metric schemes. In a metric scheme $a_{ij}^k = 0$ if $i+j < k$ because of the triangle inequality (similarly $a_{kj}^i = 0$ if $i+j < k$, etc.). As a consequence there are polynomials $f_o, f_1, \ldots, f_s$, with f_k of degree k, such that $A_k = f_k(A_1)$ and therefore $p_{zk} = f_k(p_{z1})$.

Thus the elements of the k-th column of P are polynomials of degree k in the elements of the "first" column. Therefore metric schemes are also called P-polynomial. Of more importance to us is the notion Q-polynomial. An association scheme is called Q-polynomial, if there exist polynomials $g_0, g_1, \dots, g_s$, with g_k of degree k, satisfying $q_{zk} = g_k(q_{z1})$. Q-polynomial schemes are sometimes also called cometric. As a consequence of theorem 6.3.1., which can also be written in the form $P^t \Delta_\mu P = n\Delta_v$, or $n\Delta_\mu = Q^t \Delta_v Q$ we get

$$\sum_{z=0}^{s} \mu_z p_{zk} p_{zm} = n v_k \delta_{k,m}$$

and

$$\sum_{z=0}^{s} v_z q_{zk} q_{zm} = n \mu_k \delta_{k,m} \quad .$$

That means, that in case the scheme is P-polynomial the f_k are orthogonal polynomials with respect to the weight μ_z. And similar in case of a Q-polynomial scheme.

Let A be a matrix and f a polynomial. Then f o A is the matrix defined by f o A(x,y) = f(A(x,y)). The following is an alternative definition of Q-polynomiality: There exist polynomials $g_0, g_1, \dots, g_s$, with g_k of degree k, such that $E_k = g_k \circ E_1$.

§6.4. Delsarte spaces.

In this section we present the theory of Delsarte spaces from Neumaier [N1]. A finite Delsarte space is the same as a Q-polynomial association scheme.

Let (X,d) be a metric space with finite diameter $\sqrt{\delta}$, together with a finite measure ω. We put $\omega(X) = w$. Write $c_{xy} = d^2(x,y)$ for $x,y \in X$, then $0 \le c_{xy} \le \delta$. There is an induced measure $\hat{\omega}$ on X x X. We define the measure μ on $[0,\delta]$ by

$$\mu(A) = w^{-1}\, \hat{\omega}(\{\{x,y\} \mid c_{xy} \in A\}) \quad , \quad A \subset [0,\delta].$$

For every polynomial f the following holds:

$$\int_{[0,\delta]} f(\alpha)\, d\mu(\alpha) = w^{-1} \int_X \int_X f(c_{xy})\, d\omega(x)\, d\omega(y) \quad .$$

If X is finite, ω and μ are taken to be multiples of counting measures, and all integrals are finite sums. Suppose X has s non-zero distances, i.e., $s+1$ is the smallest cardinal of a set T satisfying $\mu([0,\delta]\setminus T) = 0$. We call s the degree of X.

THEOREM 6.4.1. *There exists a family* $\{q_i\}$, $i=0,1,\ldots,s$, *if* $s < \infty$, *resp.* $i=0,1,\ldots$ *if* s *is infinite, of orthogonal polynomials, with* $\deg(q_i) = i$ *, i.e., the* q_i *satisfy*

$$\int_{[0,\delta]} q_i(\alpha)q_j(\alpha)d\mu(\alpha) = \delta_{ij} \ .$$

PROOF. $(f,g) = \int f(\alpha)g(\alpha)d\mu(\alpha)$ is a positive definite inner product on the space of all polynomials of degree at most s, since $(f,f) = 0$ implies $f(\alpha) = 0$ a.e.. Using Gram-Schmidt on the basis $\{1,x,\ldots,x^s\}$ (if s is finite) yields the family $\{q_i\}$.

The following definition is the analogue for metric spaces of the notion of Q-polynomiality.

DEFINITION 6.4.2. (X,d,ω) is a Delsarte space if for each pair of nonnegative integers i,j, there exists a polynomial f_{ij} of degree at most $\min\{i,j\}$ such that for all $a,b \in X$:

$$\int_X c_{ax}^i c_{bx}^j \, d\omega(x) = f_{ij}(c_{ab}) \ .$$

THEOREM 6.4.3. *Let* X *be a Delsarte space with degree* s. *Then for all* $i,j \in \{0,1,\ldots,s\}$ *and* $a,b \in X$:

$$\int_X q_i(c_{ax})q_j(c_{bx})d\omega(x) = q_i(0)^{-1}q_i(c_{ab})\delta_{ij} \ . \tag{1}$$

PROOF. By induction: assume (1) is true for all $i \le i_0$, $j \le j_0$, but $(i,j) \ne (i_0,j_0)$. The definition of Delsarte space implies the existence of constants $u_{i_0j_0}^k$ such that

$$\int_X q_{i_0}(c_{ax})q_{j_0}(c_{bx})d\omega(x) = \sum_{k=0}^{m} u_{i_0j_0}^k q_k(c_{ab}) \ . \tag{2}$$

Here $m = \min(i_0,j_0)$. Take $i_0 \le j_0$ without loss of generality. For $h<i_0$, multiplication of (2) by $q_h(c_{by})$ followed by integration over b yields (using the induction hypothesis and changing the order of integration):

$$0 = \int_X q_{i_0}(c_{ax})\{\int_X q_{j_0}(c_{bx})q_h(c_{by})d\omega(b)\}\ d\omega(x) =$$

$$= \sum_{k=0}^{i_0} u^k_{i_0 j_0} \int_X q_k(c_{ab})q_h(c_{by})d\omega(b) = u^h_{i_0 j_0} q_h(0)^{-1} q_h(c_{ay}) \quad ,$$

whence $u^h_{i_0 j_0} = 0$ for all $h < i$. Therefore

$$\int_X q_{i_0}(c_{ab})q_{j_0}(c_{bx})d\omega(x) \quad = \quad u^{i_0}_{i_0 j_0}\ q_{i_0}(c_{ab}) \ .$$

Finally let $a = b$ and integrate over a:

$$\delta_{ij}w = w\int q_i(\alpha)q_j(\alpha)d\mu = \int\int q_i(c_{ax})q_j(c_{ax})d\omega(a)d\omega(x) =$$

$$= \int u^{i_0}_{i_0 j_0}\ q_i(0)d\omega(a) \quad = \quad u^{i_0}_{i_0 j_0}\ q_i(0)w \ .$$

Hence $q_i(0) \neq 0$ and $u^{i_0}_{i_0 j_0} = q_{i_0}^{-1}\delta_{i_0 j_0}$, proving (1) . □

Let $H(t)$ denote the space of all functions on X , that can be written as linear combinations of functions in the set $\{c^i_{ax} \mid a \in X\}$ and $0 \le i \le t$. Then $H(t)$ is a positive definite inner product space when we define $(f,g) = \int_X f(x)g(x)d\omega(x)$.
The subspace of $H(t)$ generated by the functions $x \to q_i(c_{ax})$, $a \in X$, is called harm(i) . From theorem 6.4.3. we have the following decomposition:

$$H(t) = \mathrm{harm}(0) \perp \mathrm{harm}(1) \perp \dots \perp \mathrm{harm}(t) \ .$$

<u>THEOREM 6.4.4.</u> Dim harm(i) $= q_i(0)^2 w \geq 0$ *for* $0 \leq i \leq s$.

PROOF. Consider an orthonormal basis $\{s_h \mid h \in L\}$. For certain functions p_h, and a finite set $A_h \subset X$:

$$s_h(x) = \sum_{b\in A_h} p_h(b) q_i(c_{bx}) \quad . \tag{3}$$

Also for certain functions r_h:

$$q_i(c_{ax}) = \sum_{h\in L} r_h(a) s_h(x) \quad , \tag{4}$$

where for each $a \in X$ only finitely many $r_h(a) \neq 0$. Using (3),(4) and theorem 6.4.2. one obtains

$$r_h(a) = \langle q_i(c_{ax}), s_h(x)\rangle = \int q_i(c_{ax}) s_h(x) d\omega(x) =$$

$$= \int_X \sum_{b\in A_h} p_h(b) q_i(c_{ax}) q_i(c_{bx}) d\omega(x) =$$

$$= \sum_{b\in A_h} p_h(b) q_i(0)^{-1} q_i(c_{ab}) = q_i(0)^{-1} s_h(a) \quad .$$

Hence $s_h(a) = q_i(0) q_i(c_{ax})$ and by (4):

$$\sum_{h\in L} s_h(a) s_h(x) = q_i(0) q_i(c_{ax}) \quad , \tag{5}$$

where for each $a \in X$ only finitely many $s_h(a) \neq 0$. Hence for all $x \in X$

$$\sum_{h\in L} s_h(x)^2 = q_i(0)^2 \quad ,$$

and

$$\mathrm{card}(L) = \sum_{h\in L} (s_h, s_h) = \sum_{h\in L} \int_X s_h(x)^2 d\omega(x) =$$

$$= \int \sum_{h\in L} s_h(x)^2 d\omega(x) = \int_X q_i(0)^2 d\omega(x) = q_i(0)^2 w \quad . \qquad \square$$

The precise relation between Delsarte spaces and Q-polynomial association schemes is provided by

THEOREM 6.4.5. *A finite metric space with distance matrix* C *is a Delsarte space (with respect to the discrete measure) iff its distribution scheme is a Q-polynomial association scheme.*

PROOF. The distance matrix of a finite metric space X is defined by $C(x,y)= d^2(x,y)$ for $x,y \in X$. The associated distribution scheme has as relations the distances that occur in X. We will show that the minimal idempotents can be labeled in such a way that $E_k = g_k \circ C$, for the following polynomials g_k of degree $k: g_k(x)= q_k(0)q_k(x)$.

By theorem 6.4.3. :

$$\int_X q_k(c_{ax})q_j(c_{bx})d\omega(x) = q_k(0)^{-1}q_k(c_{ab})\delta_{ij} \quad .$$

Multiplying this equation by $q_k(0)q_j(0)$ yields

$$\sum_{x\in X} g_k(c_{ax})g_j(c_{bx}) = g_k(c_{ab})\delta_{kj} \quad ,$$

so

$$(g_k \circ C)(g_j \circ C) = (g_k \circ C)_{kj} \qquad : \quad E_kE_j = \delta_{kj}E_k \quad .$$

Therefore $E_0,E_1,\dots,E_s$ are $s+1$ mutually orthogonal idempotents forming a basis. For the <u>if</u> part, and the implicitly used fact that the distibution scheme is an association scheme we refer to [N1].

A Delsarte space is a metric space. This seems to suggest that only Q-polynomial schemes that are metric, i.e., P-polynomial, are Delsarte spaces. However the two "metrics" are different:

REMARK 6.4.6. *Every finite scheme can be realized as the distribution scheme of a spherical metric space.*

For the proof we refer again to [N1].

In case of a Q-polynomial scheme, dim harm(i) is equal to μ_i=rk E_i. For a number of infinite Delsarte spaces dim harm(i) has been computed by Hoggar [H].

§6.5. The mod p-bound in Delsarte spaces.

THEOREM 6.5.1. *Let* X *be a Delsarte space and* B *a set of points in* X. *Suppose there is a prime* p, *and integers* $a_1,\ldots,a_t \not\equiv 0 \pmod p$ *such that for all* $a \neq b$ *in* B: $c_{ab} \equiv a_i \pmod p$ *for some* $i: 1 \le i \le t$. *Then*

$$\mathrm{card}(B) \le \sum_{i=0}^{t} \dim \mathrm{harm}(i) .$$

PROOF. $H(t)$ has finite dimension $\sum_{i=0}^{t} \dim \mathrm{harm}(i)$, and the inner product ((1) in theorem 6.4.2.) is nondegenerate. Hence for all $x \in X$, there is an $\tilde{x} \in H(t)$ satisfying $\langle \tilde{x}, f \rangle = f(x)$. We will show, using lemma 5.1.2. that $\tilde{B} := \{\tilde{b} \mid b \in B\}$ is an independent subset of $H(t)$. Suppose

$$\sum_{b \in B} m_b \tilde{b} = 0 \quad , \tag{6}$$

for certain coefficients m_b. For each $a \in B$ define $f_a(x) = F(c_{ax})$, where $F(u) := \prod_{i=1}^{t} (a_i - u)$. Since F is a polynomial of degree t, f_a is in $H(t)$. Taking the inner product of f_a with (6) yields

$$\sum_{b \in B} m_b \langle \tilde{b}, f_a \rangle = \sum_{b \in B} m_b f_a(b) = 0 .$$

Now $f_a(b) \equiv 0 \pmod p$ if $b \neq a$ and $f_a(a) = \prod_{i=1}^{t} a_i \not\equiv 0 \pmod p$. Let $M = \{m_b \mid b \in B\}$, then $m_a \in p\mathbb{Z}M$ with a arbitrary. Therefore $M \subset p\mathbb{Z}M$ and we may apply lemma 5.1.2., so $M = \{0\}$.

§6.6. Examples.

The Johnson scheme $J(n,k)$ is a Delsarte space if we define $c_{xy} = \frac{1}{2}|x \Delta y|$. In this case $\dim \mathrm{harm}(i) = \binom{n}{i} - \binom{n}{i-1}$. Hence we get the following bound for a t-distance set mod p: $\sum_{i=0}^{t} [\binom{n}{i} - \binom{n}{i-1}] = \binom{n}{t}$. This is exactly

Frankl and Wilsons result (cf. theorem 5.1.1.).

The Hamming scheme $H(n,2)$ is a Delsarte space for $c_{xy} = |x \Delta y|$. Dim harm(i) = $\binom{n}{i}$ and the bound for a t-distance set mod p becomes

$$\sum_{i=0}^{t} \binom{n}{i} .$$

There seem to be many examples realizing this bound :

EXAMPLE 6.6.1. Let p be any prime. B is the collection of subsets with even cardinality of a (2p-1)-set. No distance in B is 0(mod p)

EXAMPLE 6.6.2. Let $n \equiv 3 \pmod p$. B is the collection of subsets of an n-set with cardinality 0 or n-1. All distances are 2 (mod p).

EXAMPLE 6.6.3. Let $n \equiv 2 \pmod 3$. B consists of the empty set, all 2-sets and all (n-1)-sets. Distance 0 (mod 3) does not occur.

EXAMPLE 6.6.5. Let $n \equiv 2 \pmod 5$. B consists of all singletons, 3-sets, (n-2)-sets and the complete set. Distances are 1,2 and 4 (mod 5).

EXAMPLE 6.6.5. Let $n=m^2+m+1$ be the order of a projective plane, $p|(m-2)$, and p odd. The set of all lines, together with the complete set realizes the bound. All distances are 4 (mod p).

EXAMPLE 6.6.6. Let P be a projective plane of order n. We can define a Q-polynomial association scheme as follows : X consists of the points and lines of the projective plane; relation 1 consists of all incident point line pairs; relation 2 of all point point and all line line pairs; relation 3 is the rest. For a,b in X the following, normalized, non-zero values occur : $\{n\sqrt{n},\ n\sqrt{n} + n + \sqrt{n},\ n\sqrt{n} + \sqrt{n} + n + 1\}$. Unfortunately, these never reduce to less nonzero numbers modulo a prime. Hence we do not obtain new criteria for the existence of projective planes.

In a similar way one can see that no now existence conditions for strongly regular graphs are obtained.

CHAPTER 7

ISOSCELES POINT SETS

§ 7.1. Introduction and notation.

In this chapter we will solve a problem, due to Paul Erdös, related to two-distance sets in Euclidean space. An isosceles set is a set of points such that among any three of them at most two distances occur, i.e., every triangle is isosceles. Two-distance sets are isosceles sets. We will show that essentially the converse is also true. More precisely we prove that isosceles sets can be decomposed in a collection of mutually "orthogonal" two-distance sets. This gives the bound $\frac{1}{2}(d+1)(d+2)$ for an isosceles set in Euclidean d-space. It also shows that maximal two-distance sets yield maximal isosceles sets. Throughout this chapter X will denote an isosceles set in R^d, $X = \{x_1, x_2, \ldots, x_v\}$, and we assume

$$\mathrm{aff}(X) := \{\sum_{i=1}^{v} a_i x_i \mid \Sigma\, a_i = 1\} = R^d .$$

For any subset $X_1 \subset X$, $\dim(X_1)$ will denote the dimension of $\mathrm{aff}(X_1)$. The set X is called decomposable if there is a partition $X = X_1 \cup X_2$, with $\mathrm{card}(X_2) > 1$ and $X_1 \neq \emptyset$, such that any point of X_1 is equidistant to all points of X_2 (this distance may vary for different points of X_1).

§ 7.2. The structure of isosceles sets.

LEMMA 7.2.1. *If* (X_1, X_2) *is a decomposition for* X *, then*

$$\dim(X_1) + \dim(X_2) \leq \dim(X) .$$

PROOF. Let P be the orthogonal projection on $\mathrm{aff}(X_2)$. Then for any $x_1 \in X_1$, Px_1 is the center of a sphere in $\mathrm{aff}(X_2)$ containing X_2. Since X_2 spans $\mathrm{aff}(X_2)$, P maps X_1 onto a single point. Therefore the flats $\mathrm{aff}(X_1)$ and $\mathrm{aff}(X_2)$ are orthogonal.

THEOREM 7.2.2. *Let* X *be an isosceles set. If* X *is indecomposable then it is a two-distance set.*

PROOF. Consider the complete graph on the points of X, with the following edge coloring: to each Euclidean distance between different points x,y of X we associate a unique color $c(x,y)$. The set of colors thus obtained will be called C. For each $c \in C$, X_c denotes the induced graph on the color c, that is, the graph with point set X and edges the pairs $\{x,y\}$ with $c(x,y) = c$. The following two lemmas together provide the proof of theorem 7.2.2.:

LEMMA 7.2.3. *If* X *is an indecomposable isosceles set, then for each* $c \in C$ *the graph* X_c *is connected.*

PROOF. Let c be a color for which X_c is disconnected and let X_2 be a connected component of X_c having more than one point. From the isosceles property it now follows that each point not in X_2 is joined to the points of X_2 with edges of the same color. Indeed, if yz is a c-colored edge in X_2 and $x \in X\ X_2$ then $c(x,y)$ and $c(x,z)$ are different from c since X_2 is a component of X_c. Hence they are equal. This implies that $(X\setminus X_2, X_2)$ is a decomposition of X, contradicting the assumption that X is indecomposable. □

LEMMA 7.2.4. *Let the edges of the complete graph* X *be colored with* k *colors, such that*

(i) for each $c \in C$, X_c *is connected ;*

(ii) in each triangle at most two colors occur .

Then $k \leq 2$.

PROOF. We distinguish two cases. First we assume that there is a color $c \in C$ for which the diameter of X_c exceeds 2. Secondly we treat the case that $\mathrm{diam}(X_c) \leq 2$ for all $c \in C$.

CASE 1. Let $c \in C$ and suppose u and v have distance 3 in the graph X_c. Put $c(u,v) = a$. Let U be the set of points in X that are closer to u than to v in the graph X_c and put $V = X\setminus U$.

For any $z \in U$ there is (u,z)-path entirely in U, so by the isosceles property (ii), $c(v,z) = a$. Similarly $c(u,w) = a$ for all $w \in V$. Now take $z_1 \in U$ and $z_2 \in V$ and let P_1 be a shortest (z_1,u)-path and P_2 a shortest (z_2,v)-path. We will show that $c(z_1,z_2) \in \{a,c\}$. If $z_1 \sim z_2$ in X_c then $c(z_1,z_2) = c$. If z_1 is not adjacent to any point on P_2 then $c(z_1,z_2) = a$ by the isosceles property (ii). The same is true if z_2 is not adjacent to any point of P_1. Finally let z_1 have a neighbor z_1' on P_2 and $z_2 \sim z_2'$ on P_1. Then

$$d_c(v,z_1) \le d_c(v,z_2')+1 = d_c(v,z_2) \le d_c(v,z_1')+1 = d_c(u,z_1) .$$

This contradicts the fact that $z_1 \in U$ (d_c denotes the distance in the graph X_c). So indeed for all $z_1 \in U$ and $z_2 \in V$, $c(z_1,z_2) \in \{a,c\}$. But now for any further color b, the graph X_b cannot be connected, since no edge of color b joins U with V. Hence $k \le 2$.

CASE 2. We now assume that X_c is connected and has diameter at most 2 for each $c \in C$. Let a,b,c be three different colors in C. We shall construct an infinite subset of X, thus obtaining a contradiction. Let z be an arbitrary point in X, and a_1 a point with $c(a_1,z) = a$. Since $\mathrm{diam}(X_b) \le 2$, there is a point b_1 having $c(b_1,z) = c(b_1,a_1) = b$. Similarly there is a point c_1 with $c(c_1,z) = c(c_1,b_1) = c$. Since c_1a_1 is both in triangle $c_1a_1b_1$ and c_1a_1z, $c(c_1,a_1) = c$ also. Next let a_2 be a point satisfying $c(a_2,c_1) = c(a_2,z) = a$ and define $b_2,c_2,a_3,\ldots$ analogously. We will show that at each stage the new constructed point has edges of the same color to all previous points. Suppose the new point is a_k, and assume that our induction hypothesis holds for $a_1,b_1,\ldots,c_{k-1}$. By definition $c(a_k,z) = c(a_k,c_{k-1}) = a$. Comparing za_kb_j and $c_{k-1}a_kb_j$ we see that $c(a_kb_j) = a$. By comparison of za_kc_j and $b_{j+1}a_kc_j$ (where $j+1 \le k$) we conclude that $c(a_k,a_j) = a$. For b_k and c_k a similar proof holds. Since all points are new this procedure produces an infinite subset, contradiction. Hence k is at most 2. □

The lemmas 7.2.3. and 7.2.4. together yield the proof of theorem 7.2.2. □

<u>THEOREM 7.2.5.</u> *Let* X *be an isosceles set in* $\mathbb{R}^d$, *then* $\mathrm{card}(X) \le \frac{1}{2}(d+1)(d+2)$. *Equality implies that* X *is a two-distance set, or a spherical two-distance set together with its center.*

PROOF. The proof is by induction on d. If $d = 1$ then $|X| \leq 3$. For $d = 2$, Kelly proved [K] that the maximum is 6, realized only by the centered regular pentagon. Now let $d > 2$. If X is a two-distance set, then we have the required inequality from theorem 4.1.1. If X has more distances, then by theorem 7.2.2., X is decomposable. Let (X_1, X_2) be a decomposition.

Case 1. $\mathrm{Dim}(X_1) \neq 0$. It follows from lemma 7.2.1., with $\dim(X) = d$ that $0 < \dim(X_1) < d$, since $|X_2| > 1$. Let $\dim(X_i) = d_i$, then by induction it follows that

$$|X| = |X_1| + |X_2| \leq \sum_{i=1}^{2} \tfrac{1}{2}(d_i+1)(d_i+2) < \tfrac{1}{2}(d+1)(d+2) .$$

Case 2. $\mathrm{Dim}(X_1) = 0$. In this case X_1 is a singleton and X_2 lies on a sphere. If X_2 is not a two-distance set it is again decomposable and we are in case 1 again. Otherwise

$$|X| = 1 + |X_2| \leq 1 + \tfrac{1}{2}d(d+3) = \tfrac{1}{2}(d+1)(d+2) .$$

Equality therefore implies that X is a centered maximal two-distance set.

□

CHAPTER 8

GRAPHS RELATED TO POLAR SPACES

§8.1. Introduction.

Let $\mathcal{P}$ be a finite projective geometry, that is, the collection of all subspaces of a finite projective space. A polarity π on $\mathcal{P}$ is a permutation of $\mathcal{P}$ of order 2, reversing inclusion:

$$\forall S,T \in \mathcal{P} : (S \subset T) \Rightarrow (T^{\pi} \subset S^{\pi}) \quad \text{and} \quad \pi^2 = 1 .$$

A subspace $S \in \mathcal{P}$ is called totally isotropic if $S \subset S^{\pi}$. The set $S(\pi)$ of all (totally) isotropic points of π is provided with three essentially equivalent structures, namely (cf. [BS]) :

(i) A graph structure: $p \sim q$ if $p \in q^{\pi}$, for $p,q \in S(\pi)$.

(ii) The structure of the totally isotropic lines.

(iii) The structure of the totally isotropic subspaces, partially ordered by inclusion.

The set $S(\pi)$ provided with any of the structures (i), (ii) and (iii) is called the polar space relative to π. All maximal totally isotropic subspaces have the same dimension d and $d+1$ is called the rank of $S(\pi)$. Also given a maximal t.i. subspace L and a point $p \in S(\pi)\backslash L$ there is a unique maximal t.i. subspace M such that $p \in M$ and $M \cap L$ has dimension $d-1$ ($M = \langle p^{\pi} \cap L, p \rangle$). Hence the graph (i) defined on $S(\pi)$ has the following two properties:

(i) $\exists K$: every maximal clique has size K.

(ii) $\exists e$: given a maximal clique C and a point $p \notin C$, there are precisely e points in C adjacent to p.

In this chapter we shall investigate graphs satisfying these two conditions. A finite graph satisfying (i) and (ii) will be called a Zara-graph, after

F. Zara who introduced the concept in [Z].

§8.2. Preliminaries and notation.

Following Higman [Hi] we use the following graph theoretical notation. Let $G = (V,E)$ be a simple graph. We write $x \sim y$ or $x \perp y$ if $\{x,y\} \in E$ and $x^{\perp} = \{y \in V(G) \mid x=y \text{ or } x \sim y\}$. A graph G is called connected if for all $x,y \in V(G)$ there is a sequence $x=x_0,x_1,\ldots,x_n=y$, such that $x_i \sim x_{i+1}$ for $i=0,\ldots,n-1$. G is called coconnected if the complement of G is connected. If G_1 is a Zara-graph with parameters (K_1,e_1) and G_2 is a Zara-graph with parameters (K_2,e_2), then the graph obtained by joining all points of G_1 to all points of G_2 is a Zara graph whenever $K_1+e_2 = K_2+e_1$. Every Zara-graph can be built from coconnected Zara-graphs in this way. Our main concern will therefore be the structure of coconnected or cc-Zara-graphs.

Note that if G is a Zara-graph with parameters (K,e), then the induced subgraph on $x^{\perp}\setminus\{x\}$ is a Zara-graph with parameters $(K-1,e-1)$. This graph is called the residue of x, or $\mathrm{Res}(x)$. For arbitrary $S \subset V$, we define $S^{\perp} = \bigcap_{x\in S} x^{\perp}$. If S is a clique, $\mathrm{Res}(S)$ is defined analogously, i.e., $\mathrm{Res}(S)$ is the induced subgraph on $S^{\perp}\setminus S$. Again $\mathrm{Res}(S)$ is a Zara-graph with parameters $(K-|S|,e-|S|)$. An equivalence relation $\approx$ is defined on V by $x \approx y \iff x^{\perp} = y^{\perp}$. The equivalence classes $[x]$ are cliques and if x and y are adjacent then all points in $[x]$ are adjacent to all points in $[y]$. The graph $G/\approx$ is defined on $V/\approx$ by $[x] \sim [y]$ whenever $x \sim y$ and $[x] \neq [y]$. This graph is called the reduced graph of G. In general a graph H is called reduced if $[x] = x$ for each point $x \in V(H)$. In §8.6. we will show that the reduced graph of a cc-Zara-graph is a (reduced) cc-Zara-graph.

Let S be a clique in a graph H. Then $S^{\perp\perp}$ is again a clique since $S \subset S^{\perp\perp} \subset S^{\perp}$. Note that $S^{\perp\perp} = (S^{\perp\perp})^{\perp\perp}$. We call $S^{\perp\perp}$ the closure of S, in particular $x^{\perp\perp} = [x]$. An equivalent way of defining reduced is to say that each point is closed. The key theorem, which allows us to use induction in the proofs that follow, is the fact that for each x in a cc-Zara-graph the residue of the closure of x, $\mathrm{Res}([x])$, is again a cc-Zara-graph (theorem 8.5.3.). Using this we can prove that all equivalence classes under $\approx$ have the same size. It follows that if G is a cc-Zara-graph with parameters (K,e), then $G/\approx$ is again a cc-Zara-graph with parameters $(K/|[x]|, e/|[x]|)$. Closures of cliques are called singular subsets or closed cliques. The closure of the empty set is called the radical of G, rad(G). The intersection of two singular subsets is again a singular subset. For $x,y \in X$ we define:

$$d(x) = |x^{\perp}| - 1 \quad ; \quad d(x) \text{ is called the degree of } x \; ;$$

$$\lambda(x,y) = |x^{\perp} \cap y^{\perp}| - 2 \quad , \text{ if } x \sim y \; ;$$

$$\mu(x,y) = |x^{\perp} \cap y^{\perp}| \quad , \text{ if } x \not\sim y \; .$$

If d, λ and μ are constant the graph is called strongly regular. We will show that a reduced cc-Zara-graph is strongly regular. The collection of singular subsets forms a partially ordered set under inclusion. In a polar space this is exactly the structure of all totally isotropic subspaces. This poset will be investigated in §§8.5 and 6. Following Neumaier [N1] we define the notion of an M_r-space: (cf. also [N3])

Let P be a set of points and $X_1, X_2, \ldots, X_r$ sets of subsets of P. Write $X = X_1 \cup \ldots \cup X_r$. Elements of X_i are called i-varieties, r-varieties are also called blocks. X is an M_r-space if it satisfies:

(i) X_1 is the set of all singletons $\{a\}$, $a \in P$.

(ii) There are constants $1 = K_1 < \ldots < K_r$, such that an i-variety contains exactly K_i points.

(iii) There are constants $R_1 > \ldots > R_r = 1$, such that an i-variety is contained in exactly R_i blocks.

(iv) The intersection of two varieties is a variety or empty.

(v) If x is an i-variety, z a block containing x and p a point in z but not in x, then there is an $(i+1)$-variety $y \subset z$ containing x and p.

The main result in this chapter is that a reduced cc-Zara-graph is an M_r-space for some r, called the rank of the Zara-graph.

§8.3. Examples of Zara-graphs.

In [Z] Zara gives the following examples of (cc-) Zara-graphs.

1. Polar spaces. Let W be an m-dimensional vector space, m finite, over a finite field F, together with a field automorphism β satisfying $\beta^2 = 1$. Let F_0 denote the subfield fixed by β. Put $|F_0| = q$, then $|F| = q$ or $|F| = q^2$.

Let $\phi : W \times W \to F$ be a β-sesquilinear form, nondegenerate and reflexive. $Q : W \to F$ is a quadratic form with an associated bilinear nondegenerate form $\phi_1 : W \times W \to F$. The following graphs are Zara-graphs. In each case V is the set $\{\langle a \rangle \mid a \in V \setminus \{\underline{0}\},\ \langle a \rangle$ isotropic, resp. singular$\}$, and $\langle a \rangle \sim \langle b \rangle$ if $\phi(a,b) = 0$, resp. $\phi_1(a,b) = 0$ and $\langle a \rangle \neq \langle b \rangle$.
The following cases occur :

(Sp). ϕ alternating, $m = 2m_1$, $\beta = 1$;

$$(|V|,K,e) = ((q^m-1)/(q-1),\ (q^{m_1}-1)/(q-1),\ (q^{m_1}-1)/(q-1)) .$$

(Q). Q quadratic, $\beta = 1$;

(i) $m=2m_1+1$; $((q^{m-1}-1)/(q-1),\ (q^{m_1}-1)/(q-1),\ (q^{m_1-1}-1)/(q-1))$.

(ii) $m=2m_1$, maximal Witt index ;

$$((q^{m_1}-1)(q^{m_1-1}-1)/(q-1),\ (q^{m_1}-1)/(q-1),\ (q^{m_1-1}-1)/(q-1)) .$$

(iii) $m=2m_1$, non-maximal Witt index ;

$$((q^{m_1}+1)(q^{m_1-1}-1)/(q-1),\ (q^{m_1-1}-1)/(q-1),\ (q^{m_1-2}-1)/(q-1) .$$

(U). ϕ a non-degenerate β-hermitean form, $|F| = q^2$;

(i) $m=2m_1 \geq 4$

$$((q^m-1)(q^{m-1}+1)/(q^2-1),\ (q^m-1)/(q^2-1),\ (q^{m-2}-1)/(q^2-1)) .$$

(ii) $m=2m_1+1 \geq 3$

$$((q^m+1)(q^{m-1}-1)/q^2-1),\ (q^{m-1}-1)/(q^2-1),\ q^{m-3}-1)/(q^2-1)) .$$

(GQ). Rank 2 polar spaces, or generalized quadrangles $GQ(s,t)$. For definition and examples of generalized quadrangles see [Th].

$$(|V|,K,e) = ((s+1)(st+1),\ s+1,\ 1) \ .$$

2. Let W be a 2m-dimensional vector space over $GF(2)$, together with a quadratic form Q of maximal Witt index, for which the associated alternating bilinear form is non-degenerate. $V = \{x | x \in W,\ Q(x) = 1\}$, and $x \sim y$ if $x \neq y$ and $\phi_1(x,y) = 0$.

$$(|V|,K,e) = (2^{m-1}(2^m-1),\ 2^{m-1},\ 2^{m-2}) \ .$$

3. V consists of all triples from a 7-set.

(i) $x \sim y$ if $|x \cap y| = 1$; (35, 7, 3) ;

(ii) $x \sim y$ if $|x \cap y| \neq 1$; (35, 5, 2) .

Note that case (i) is the same as Q(ii) with $m=6$, $q=2$.

4. Let W be a 6-dimensional vector space over $GF(3)$ together with a non-degenerate symmetric bilinear form ϕ , such that W admits an orthonormal basis. $V = \{\langle a\rangle \mid a \in W,\ \phi(a,a) = 1\}$ and $\langle a\rangle \sim \langle b\rangle$ if $\langle a\rangle \neq \langle b\rangle$ and $\phi(a,b) = 0$; (126, 6, 2).

5. The strongly regular graph of McLaughlin (cf. [GS]); (275, 5, 2).

6. Let W be a 2m-dimensional vector space over $GF(q)$, together with a quadratic form Q of maximal Witt index. $V = W$, and $x \sim y$ if $Q(x-y) = 0$ and $y \neq x$; $(q^{2m},\ q^m,\ q^{m-1})$.

7. $\overline{L_2(n)}$. Points are all ordered pairs from an n-set, and $(a,b) \sim (c,d)$ if $a \neq c$ and $b \neq d$; $(n^2,\ n,\ n-2)$.

8. $\overline{T(2n)}$. V = all pairs from a 2n-set, $x \sim y$ if $x \cap y = \emptyset$; $(n(2n-1),\ n,\ n-2)$.

§8.4. Regularity properties of Zara-graphs.

All examples given in the previous section are strongly regular graphs. As a consequence of the results in the present section we will see that a reduced cc-Zara-graph, i.e., $\{x\} = [x]$ for each point, is strongly regular. In the following G will always denote a Zara-graph.

LEMMA 8.4.1. *Let* C *be a maximal clique in* G *and* $p \notin C$. *There is a unique maximal clique containing* p *and* e *points of* C.

PROOF. The statement is equivalent to : two distinct maximal cliques intersect in at most e points; this is a direct consequence of property (ii), defining e. □

LEMMA 8.4.2. *Let* C, C_1 *and* C_2 *be different maximal cliques in* G *such that* C_1 *and* C_2 *intersect* C *in* e *points. Then* $C_1 \cap C_2 \subset C$.

PROOF. If $C_1 \cap C_2 \not\subset C$, then $|(C_1 \cup C_2) \cap C| > e$ and there is a point $x \in C_1 \cap C_2 \setminus C$. This point is joined to more then e points of C, contradiction. □

As a consequence of lemmas 8.4.1 and 2 we can start with any maximal clique C, take for each point outside C the unique clique through this point and e points of C. This way we obtain a collection of cliques $C_1,\dots,C_s$ inducing a partition of $V \setminus C$. This collection is called the C-decomposition.

THEOREM 8.4.3. *Let* $x,y \in V(G)$. *If* $x \not\sim y$ *then* $d(x) = d(y)$.

PROOF. Let C be a maximal clique containing x. Then $y \notin C$. Consider the C-decomposition $\{C_1,\dots,C_s\}$ with $y \in C_1$ and put $C \setminus C_1 = \{x = x_1, x_2, \dots, x_{K-e}\}$. For each $z \in C_1 \setminus C$ we have

$$d(z) = \sum_{i=2}^{s} (e - |C_1 \cap C_i|) + K - 1 .$$

Indeed, the number of points in $C_i \setminus C_1$ adjacent to z is $e - |C_1 \cap C_i|$, and since $C_1 \cap C_i \subset C$, all these points are outside C, hence no points are counted twice. Rewriting this yields

$$d(z) = \sum_{i=2}^{s} \{ \sum_{m:x_m \in C_i} 1 \} + K - 1 ,$$

since $\sum_{m:x_m \in C_i} 1 = e - |C_1 \cap C_i|$. Changing the order of summation yields:

$$d(z) = \{ \sum_{m=1}^{K-e} (d(x_m) - (K-1))/(K-e) \} + K-1 = \frac{1}{K-e} \sum_{m=1}^{K-e} d(x_m) .$$

Hence $d(z_i) = d(z_j)$ for all $z_i, z_j \in C_1 \setminus C$, and by symmetry $d(x_i) = d(x_j)$ for all $x_i, x_j \in C \setminus C_1$. This implies $d(y) = d(x)$. □

COROLLARY 8.4.4. *A cc-Zara-graph is regular.* □

THEOREM 8.4.5. *Let* G *be a cc-Zara-graph. There exists a constant* μ *, such that* $\mu(x,y) = \mu$ *for all* $x,y \in V(G)$, $x \not\sim y$.

PROOF. We will show that $\mu(x,y_1) = \mu(x,y_2)$ for each triple x,y_1,y_2 with $x \not\sim y_1$ and $x \not\sim y_2$. First assume $y_1 \sim y_2$. Take a clique C_1 containing y_1 and y_2 and a clique C with $x \in C$ and $|C \cap C_1| = e$. Consider the C-decomposition $\{C_1, C_2, \ldots, C_s\}$. For $i=1,2$:

$$\mu(x,y_i) = \sum_{k:x \in C_k} (e - |C_1 \cap C_k|) + e ,$$

independent of i. Hence $\mu(x,y_1) = \mu(x,y_2)$.

Next let $y_1 \not\sim y_2$. Claim: there either exists a point z with $z \not\sim x$, and $z \sim y_1, y_2$ or for all $z \sim x$, we have $y_1 \sim z \Leftrightarrow y_2 \sim z$. To see this suppose $z \sim x$, $z \sim y_1$ and $z \not\sim y_2$ and let C be a clique containing y_1 and z. Then $x^{\perp} \cap C$ and $y_2^{\perp} \cap C$ are different sets of the same cardinality e. Hence there is a point $z' \in y_2^{\perp} \cap C$ not adjacent to x. This proves the claim. In the first case $\mu(x,y_1) = \mu(x,z) = \mu(x,y_2)$. In the second case $x^{\perp} \cap y_1^{\perp} = x^{\perp} \cap y_2^{\perp}$, hence also $\mu(x,y_1) = \mu(x,y_2)$. Since G is coconnected,

μ is constant for the whole graph.

THEOREM 8.4.6. *Let* G *be a co-Zara-graph. There exists a constant* λ *such that* $\lambda(x,y) = \lambda$ *for* $x,y \in V(G)$, $x \sim y$ *and* $x \not\approx y$.

PROOF. First recall lemma 7.2.4.: let the edges of the complete graph $X = K_n$ be colored with k colors such that (i) for each color c, the induced graph on this color, X_c, is connected; (ii) in each triangle at most two colors are used. Then k is at most 2.
Now let $H = G/\approx$ be the reduced graph of G. Note that H is also coconnected. We are going to color the edges and non-edges of H. All non-edges get the same color ∞, while if $[x] \sim [y]$ the edge $([x],[y])$ gets the color $\lambda(x,y)$, i.e., the number of common neighbors of x and y in G.
This coloring satisfies the hypotheses (ii) and (i) of lemma 7.2.4.:
(ii) : Triangles with less than two edges satisfy the requirements automatically. Next consider $[y] \sim [x] \sim [z]$, $[y] \not\sim [z]$ in H. In G we have $y \sim x \sim z$, $y \not\sim z$. Since Res(x) is a Zara-graph, theorem 8.4.3. tells us that $d_{Res(x)}(y) = d_{Res(x)}(z)$. This just means $\lambda(x,y) = \lambda(x,z)$. Hence triangles with two edges also satisfy (ii). Finally let $[x] \sim [y] \sim [z] \sim [x]$ in H, or x,y,z mutually adjacent and non-equivalent in G. If there is a point u in G adjacent to precisely one of x,y,z, say to x, then by the previous reasoning $\lambda(u,x) = \lambda(y,x)$ and $\lambda(u,x) = \lambda(z,x)$ and we are done. If not, then, writing $\lambda(x,y,z)$ for the number of common neighbors of x,y and z in G:

$$d(x) = \lambda(x,y) + \lambda(x,z) - \lambda(x,y,z) ;$$

$$d(y) = \lambda(y,z) + \lambda(y,x) - \lambda(x,y,z) ;$$

$$d(z) = \lambda(z,x) + \lambda(z,y) - \lambda(x,y,z) .$$

Since G is coconnected it is regular and therefore $\lambda(x,y)=\lambda(y,z)=\lambda(z,x)$ in this case. This shows that for each triangle (ii) holds.
(i): Let H_c be a connected component for the color c, $|H_c| > 1$, and suppose H_c has not all of the vertices of H. A point outside H_c is joined to all points of H_c with edges (or non-edges) of the same color, by the isosceles property and the fact that H_c is connected and a component. In particular a point outside H_c is either adjacent to <u>all</u>

points of H_c, or to <u>no</u> point of H_c. Let A be the set of points that are adjacent to all points of H_c and N the set of points adjacent to none. Note that N is certainly non-empty, since H is coconnected. In case A is empty H is not connected and also G is not connected, i.e., $e=0$. In this case $x \sim y$ implies $x \approx y$ and the theorem is void. So let $A \neq \emptyset$. Now H_c is not a clique, since in that case $[x]$ and $[y]$ in H_c would have the same neighbors, i.e., $x \approx y$. Take $[h] \in H_c$, $[a] \in A$ and construct a maximal clique C <u>in G</u> containing $[a]$ and $[h]$. Let A' be the "preimage" of A in G, similarly define H'_c and N'. Any point $n \in N'$ has e neighbors in $A' \cap C$, hence $|A' \cap C| \geq e$. There is a point $h' \in H' \setminus C$ having a neighbor in $H'_c \cap C$, since H'_c is connected and not a clique. But this point is also adjacent to all points of A', therefore it has more than e neighbors in C, contradiction. So $H_c = H$, i.e., the induced graph on c is connected. This shows (i) and the theorem is proved, because since there are at most two colors, one of them ∞, the other one must be the constant λ. □

<u>COROLLARY 8.4.7.</u> *Let* G *be a reduced cc-Zara-graph, i.e.,* $G = G/\approx$. *Then* G *is strongly regular.* □

§8.5. The poset of singular subsets.

In this section we study the partially ordered set of closed cliques. Crucial steps in the investigation that allow us to study the structure by induction are:

(i) If G is a cc-Zara-graph and $x \in V(G)$ then $\text{Res}([x])$ is again a cc-Zara-graph.

(ii) All equivalence classes of points have the same size.

We start off with two simple lemmas. Throughout this section G will be a Zara-graph.

<u>LEMMA 8.5.1.</u> *If* u *and* v *are connected by a path in* $\overline{G}$, *then the distance of* u *and* v *in* $\overline{G}$, $d_{\overline{G}}(u,v)$ *is at most* 2.

PROOF. The points u and v are in the same coconnected component of G . But coconnected components of a Zara-graph are cc-Zara-graphs.

LEMMA 8.5.2. *Let* x,y,z $\in$ V(G) *, where* G *is a cc-Zara-graph. Suppose* Res([x]) *is not coconnected, and* y,z *are in different cc-components of* Res([x]). *Then* Res([y]) *is not coconnected , and* x,z *are in different cc-components of* Res([y]).

PROOF. We show that the following statements are equivalent:

(i) Res([x]) is not coconnected and y,z are in different cc-components.

(ii) There is no point u adjacent to x and not to y,z.

(iii) There is no point v adjacent to y and not to x,z.

(iv) Res([y]) is not coconnected and x,z are in different cc-components.

(i) => (ii) : By definition. (ii) => (i): Lemma 8.5.1..
(ii)<=>(iii): x,y and z are mutually adjacent and non-equivalent. Let $\lambda_1(x)$ be the number of points adjacent to x and not to y,z. Then

$$d(x) = \lambda_1(x) + \lambda(x,y) + \lambda(x,z) - \lambda(x,y,z) =$$

$$= \lambda_1(x) + 2\lambda - \lambda(x,y,z) .$$

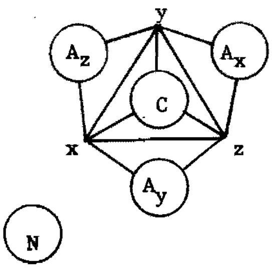
$$d(y) = \lambda_1(y) + 2\lambda - \lambda(x,y,z) ,$$

where again (x,y,z) is the number of common neighbors of x,y and z. This shows that $\lambda_1(x) = \lambda_1(y)$.
(iii)<=> (iv): This is the same as (i)<=>(ii) . □

Triples x,y,z as in the lemma will be called trios. Note that the lemma says that the order of x,y,z is irrelevant.

THEOREM 8.5.3. *If* G *is a cc-Zara-graph ,* x $\in$ V(G) *, then* Res([x]) *is a cc-Zara-graph.*

PROOF. It is enough to show that trios do not exist. Let $\{x,y,z\}$ be a trio, then no point of G is adjacent to exactly one point of $\{x,y,z\}$. Let $A_x = \{u \in V(G) \mid u \not\sim x , u \sim y , u \sim z\}$, A_y and A_z similar; $C = \{u \mid u \sim x,y,z\}$; $N = \{u \mid u \not\sim x,y,z\}$. Picture:



Observe: (i) $N \neq \emptyset$ (lemma 8.5.1.) .

(ii) There are no edges between N and A_x, A_y and A_z. This is shown as follows: If $x' \in A_x$, then x',y,z is again a trio, for x' and x are in the same cc-component of Res([y]) and therefore x' and z in different cc-components. Since the points of N are not adjacent to y and z, they are also not adjacent to x'. The proof is finished by deriving a contradiction. Let $x' \in A_x$. Since x' and x have μ common neighbors, x' has less than μ neighbors in C (at most $\mu-2$). On the other hand $n \in N$ and x' must have μ common neighbors in C. This is a contradiction, hence trios do not exist and the proof is finished. □

In order to investigate the poset of closed cliques we need the following characterization of singular subsets. Here $\mathcal{C}$ denotes the set of all maximal cliques in G.

<u>LEMMA 8.5.4.</u> *Let* S *be a clique in* G *, then*

$$S^{\perp\perp} = \cap\{C \in \mathcal{C} \mid S \subset C\} .$$

PROOF. $S^{\perp\perp} = \cap\{y^{\perp} \mid S \subset y^{\perp}\} = \bigcap_{\substack{C \in \mathcal{C} \\ S \subset y^{\perp}}} \{y^{\perp} \mid y \in C\} =$

$$= \cap\{C^{\perp} \mid S \subset C \in \mathcal{C}\} = \cap\{C \in \mathcal{C} \mid S \subset C\} ,$$

since $C^{\perp} = C$ for all $C \in \mathcal{C}$.

Notation: $(\mathcal{S},\subset)$ is the poset of singular subsets, for $C \in \mathcal{C}$ define

$$\mathcal{S}(C) = \{S \in \mathcal{S} \mid S \subset C\} .$$

Let X,Y be different elements from a lattice $(L,\subset)$. If $X \subset Y \subset Z$ implies $X=Z$ or $Y=Z$ we say that Y covers X and write $X < Y$. A lattice is semi-modular if for all X,Y: $(X > X\wedge Y) \Leftrightarrow (X\vee Y > Y)$. The following two lemmas enable us to show that $(\mathcal{S}(C),\subset)$ is a semi-modular lattice for all $C \in \mathcal{C}$.

<u>LEMMA 8.5.5.</u> *The graph defined on* $\mathcal{C}$ *by* $C \sim D$ *if* $|C\cap D| = e$ *is connected.*

PROOF. We show that two maximal cliques C and D are joined by a path using induction on $|C\cap D|$.

(i) If $|C\cap D| = e$ then $C \sim D$ and there is nothing to prove.

(ii) If $|C\cap D| < e$ take $x \in C\backslash D$ and a clique E containing x and e points of D, then $|E\cap D| = e$ and $|C\cap E| > |C\cap D|$, hence C and E are joined by a path. Since $E \sim D$ we are done. □

<u>LEMMA 8.5.6.</u> *Let* $S \in \mathcal{S}$, $C \in \mathcal{C}$, $S \subset C$. *Then there exists a* $D \in \mathcal{C}$ *such that* $S = C \cap D$.

PROOF. By induction on the size of S.

(i) $|S| = e$. This case is trivial.

(ii) $|S| < e$. Choose closed cliques S_1 and S_2 minimal with respect to $S \subsetneq S_i \subset C$. This is possible since $S = \cap\{T \in \mathcal{S} \mid T \supset S\}$.

Since S_1 and S_2 are minimal, $S_1 \cap S_2 = S$ and there are maximal cliques D_1 and D_2 such that $S_i = C \cap D_i$, $i=1,2$. Choose $x \in D_2\backslash(C \cup D_1)$ such that x is not adjacent to all of $S_1\backslash S$ (and hence to none of $S_1\backslash S$). Let D_3 be the closure of $(x^\perp\cap C_1) \cup \{x\}$. Then $D_3\cap C = S$. To see this, suppose $y \in (D_3\cap C)\backslash S$. Then either $y \in S_1$, which implies $y \sim x$, or $y \notin S_1$, but then $|y^\perp\cap D_1| > e$, contradiction.

We define the binary operations $\wedge$ and $\vee$ on $\mathcal{S}$ as follows :

$$S \wedge T = S \cap T \quad ; \quad S \vee T = \cap\{U \in \mathcal{S} \mid U \supset S\cup T\} .$$

$S \cap T$ is again a singular subset since $(S\cap T)^{\perp\perp} = S^{\perp\perp} \cap T^{\perp\perp}$ (cf 8.6).

THEOREM 8.5.7. *Let* G *be a cc-Zara-graph, and* C *a maximal clique in* G. *Then* $(S(C),\subset)$ *is a semi-modular lattice.*

PROOF. Let $X,Y \in S(C)$ with $X \cap Y < X$ and suppose $X \vee Y \underset{\neq}{\supset} Z \underset{\neq}{\supset} Y$. Then $Z \cap X = Y \cap X$, for otherwise $X \cap Y \underset{\neq}{\subset} X \cap Z \underset{\neq}{\subset} X$. Take a point $z \in Z \backslash Y$ and $x \in X \backslash Y$. Apparently $x^{\perp} \subset z^{\perp}$ in the Zara-graph $Res(Y)$. To see this let u be adjacent to x and Y. Since X covers $X \cap Y$, u is joined to all of X, and if is u is joined to X and Y it is joined to all of $X \vee Y$, including z. By repeated application of theorem 8.5.3. $Res(Y)$ is a cc-Zara-graph, hence $x^{\perp} = z^{\perp}$ in $Res(Y)$. This is a contradiction since $z \in Z$ while $x \notin Z$.

The semi-modularity of the lattice $S(C)$ allows us to introduce a rank fuction on $S(C)$ satisfying $rk(S) = rk(T) + 1$ whenever $S < T$, and $rk(\emptyset) = 0$, cf. [Bi]. By lemma 8.5.5. this rank function can be extended to the poset S. Indeed, for a given set E of cardinality e in S, the rank in $S(C)$ is the same for all $C \supset E$. All maximal cliques have the same rank r. This r is called the rank of the Zara-graph.

§8.6. Zara-graphs and M_r-spaces.

In this section the main structure theorem for cc-Zara-graphs is proved. We show that the poset of singular subsets of the reduced graph of a rank r Zara-graph is an M_r-space (for the definition see §8.2.). Write $S = S_0 \cup S_1 \cup \dots \cup S_r$. Recall that S_i is the collection of singular subsets of rank i. We shall prove the following properties:

(i) There are constants $R_0,\dots,R_r$ such that each rank i singular subset is in R_i maximal cliques.

(ii) There are constants $K_0,\dots,K_r$ such that each rank i singular subset has K_i points.

(iii) The intersection of two singular subsets is again a singular subset.

(iv) If x is a rank i singular subset, and C a maximal clique containing x and $p \in C \backslash x$, then there is a rk (i+1) singular subset y, containing x and p, and contained in C.

Note that it follows from (ii) that all equivalence classes have the same size K_0, and that (i),...,(iv) imply that $G/\approx$ is an M_r-space. Property (iv) is a consequence of the semi-modularity of the lattice $S(C)$ for each $C \in \mathcal{C}$. Property (iii) follows from the observation that $(S \cap T)^{\perp\perp} = S^{\perp\perp} \cap T^{\perp\perp}$, if S and T are singular subsets. Indeed, for arbitary sets A and B we have $(A \subset B) \Rightarrow B^{\perp} \subset A^{\perp}$, and if A is a clique then $A \subset A^{\perp\perp}$. Hence $(S \cap T \subset (S \cap T)^{\perp\perp}$ and $(S \cap T)^{\perp\perp} \subset S^{\perp\perp} \cap T^{\perp\perp}$.

The following theorems establish (i) and (ii).

THEOREM 8.6.1. *Let G be a cc-Zara-graph. There are constants* $R_0,\ldots R_r$, *such that each* $S \in S_i$ *is contained in precisely* R_i *maximal cliques.*

PROOF. By induction in i. For $i = 0$ there is nothing to prove. Rank 1 sets are the equivalence classes of points. Let [x] and $[y] \in S_1$, $x \not\sim y$. For each maximal clique C containing x, and hence [x], there is a unique clique containing y and intersecting C in e points. This establishes a one to one correspondence between the cliques containing [x] and those containing [y]. Since G is coconnected we are done.
Finally let $i > 1$, $S,T \in S_i$. If $S \cap T \neq \emptyset$ then we may use the induction hypothesis since $\mathrm{Res}(S \cap T)$ is again a cc-Zara-graph. Hence in this case S and T are in the same number of maximal cliques. However, the graph defined on S_i by $S \sim T$ if $S \cap T \neq \emptyset$ is connected if $i > 1$, since every edge of G is in a rank i set, and G is connected if the rank of G as a Zara-graph is greater than 1. So for all $S,T \in S_i$ the number of maximal cliques containing them is constant. □

THEOREM 8.6.2. *Let G be a cc-Zara-graph of rank r. There are constants* $K_0,\ldots,K_r$, *such that each* $S \in S_i$ *has* K_i *points.*

In order to prove this we need the following lemma.

LEMMA 8.6.3. *Let G be a cc-Zara-graph of rank r, and suppose* $|S| = K_i$ *for all* $S \in S_i$, $i=0,\ldots,r$. *Then the number of rank* i *sets in a given maximal clique C equals*

$$\prod_{j=0}^{i-1} \frac{K_r - K_j}{K_i - K_j} \quad .$$

PROOF of the lemma. We use induction on r, the case $r=1$ being trivial, using the convention that the empty product equals 1. Now let $r > 1$, and C a maximal clique containing c_i rank i sets. Since C is partitioned into rank 1 sets $c_1 = K_r/K_1$. Next let $i > 1$. Counting in two ways the pairs $S,T \subset C$, $S \in \mathcal{S}_1$, $T \in \mathcal{S}_i$ satisfying $S \subset T$ and using the induction hypothesis yields

$$\frac{K_r}{K_1} \prod_{j=1}^{i-1} \frac{(K_r - K_1) - (K_j - K_1)}{(K_i - K_1) - (K_j - K_1)} = c_i \frac{K_i}{K_1} \; .$$

This proves lemma 8.6.3. . □

PROOF of the theorem. Again we use induction on r. If $r=1$ or 2 the statement is true by definition. Let $r > 2$, and take $S \in \mathcal{S}_1$ with $|S| = s$. By induction $\mathrm{Res}(S)$ has parameters $K^1_{r-1},\ldots,K^1_0=0$. So each rank i set containing S has cardinality $K^1_{i-1} + s$. We allready noticed that the graph defined on $\mathcal{S}_i$ by $S \sim T$ if $S \cap T \neq \emptyset$ is connected. Hence there allready exist constants $K_2,K_3,\ldots,K_r$. Count the number of points inside and outside a given maximal clique C, observing that G is regular, say of degree k. Hence, using the lemma:

$$k-s+1 = |\mathrm{Res}(S)| = K^1_{r-1} + \prod_{j=0}^{r-3} \frac{K^1_{r-1} - K^1_j}{K^1_{r-2} - K^1_j} \; (R_{r-1}-1)(K^1_{r-1}-K^1_{r-2}) \; .$$

To explain this note that each point in $\mathrm{Res}(S)$ outside C determines a unique clique intersecting C in e points, while each e-set in $\mathcal{S}_{r-1}$ is in R_{r-1} maximal cliques. For $i > 1$ we may put $K^1_{i-1} = K_i - s$, whence

$$k-s+1 = K_r - s + \frac{K_r - s}{K_{r-1} - s} \prod_{j=1}^{r-3} \frac{K_r - K_{j+1}}{K_{r-1} - K_{j+1}} (R_{r-1} - 1)(K_r - K_{r-1}) \; .$$

Considered as an equation in s we see that there is only one solution. Indeed, rewrite the equation to get

$$k+1-K_r = \left(1+\frac{K_r-K_{r-1}}{K_{r-1}-s}\right)\prod_{j=1}^{r-3}\frac{K_r-K_{j+1}}{K_{r-1}-K_{j+1}}\,(R_{r-1}-1)(K_r-K_{r-1}) ,$$

and notice that $(K_r-K_{r-1})/(K_{r-1}-s)$ is monotonic. Hence s is constant i.e., $K_1=s$. This finishes the proof of the theorem. □

MAIN THEOREM 8.6.4. *Let* G *be a cc-Zara-graph of rank* r *, then* G' *, the reduced graph of* G *is also a cc-Zara-graph, and the poset of closed cliques of* G' *is an* M_r*-space.* □

§8.7. Final remarks.

In the previous section it was proved that the reduced graph of a cc-Zara-graph is strongly regular. The parameters of this strongly regular graph can be computed in terms of K, e, and the smallest eigenvalue (cf. [N4]). The integrality of the multiplicity of the eigenvalues puts further restrictions on the feasibility of parameter sets. Another related subject is the classification of completely regular two-graphs (cf. [N5]). To each completely regular two-graph there is related at least one Zara-graph. More about these aspects will appear in a forthcoming article by Wilbrink, Kloks and the author. The list in §8.3. contains all examples known to the authors of reduced cc-Zara-graphs. More about M_r-spaces can be found in [N1,3] . Neumaier gives a.o. the following examples:

(i) All $\leq r$ subsets of an n-set.

(ii) All $\leq r$ dimensional subspaces of a projective space PG(n,q).

(iii) All subspaces of a polar space over GF(q).

The graph associated with these structures is the complete graph in (i) and (ii). Only in case (iii) we have a "proper" Zara-graph . The structure of all varieties in a fixed block of an M_r-space , or the lattice $(S(C),\subset)$ in case of a Zara-graph is a perfect matroid design [We] . Our closure operator $^{\perp\perp}$ coincides with the usual closure operator for matroids. The singular subsets are called subspaces or flats in this terminology.

REFERENCES

B BANNAI, E. (82) *On s-distance sets in real hyperbolic space,* Hokkaido J. of Math. 11 nr 2, 201-204.

BB BANNAI, E. and BANNAI, E. (81) *An upper bound for the cardinality of an s-distance subset in Euclidean space,* Combinatorica 2 , 99-103.

BBDS BANNAI, E., BLOKHUIS, A., DELSARTE, Ph. and SEIDEL, J.J. (83) *The addition formula for hyperbolic space,* to appear in J. Comb. Theory Ser. A.

BM BOSE, R.C. and MESNER, D.M. (59) *On linear associative algebras corresponding to association schemes of partially balanced designs,* Ann. Math. Statist. 30, 21-38.

BS BUEKENHOUT, F. and SHULT, E. (74) *On the foundations of polar geometry,* Geom. Dedicata 3, 155-170.

Bi BIRKHOFF, G. (67) *Lattice theory,* 3rd new edition, American Mathematical Society (AMS colloquium publications vol. 25).

CvL CAMERON, P.J. and van LINT, J.H. (80) *Graphs, codes and designs,* Cambridge: Cambridge university press (London Mathematical Society lecture notes series 43).

D DELSARTE, Ph. (73) *An algebraic approach to the association schemes of coding theory,* Philips Res. Rep. Supplement nr 10 (thesis).

DGS DELSARTE, Ph., GOETHALS, J.-M. and SEIDEL, J.J. (77) *Spherical codes and designs,* Geom. Dedicata 6, 363-388.

EMOT ERDELYI, A., MAGNUS, W., OBERHETTINGER, F. and TRICOMI, F.G. (53), *Higher trancendental functions,* vol. II, (Bateman project) McGraw Hill.

FW FRANKL, P. and WILSON, R.M. (81) *Intersection theorems with geometric consequences,* European J. of Combinatorics 4 , 357-369.

GS GOETHALS, J.-M. and SEIDEL J.J. (75) *The regular two-graph on 276 vertices,* Discrete Math. 12 , 143-158.

H HOGGAR, S.G. (82) *t-designs in projective spaces,* European J. of Combinatorics 3 , 233-254.

HC HARISH CHANDRA (57) *Differential operators on a semi simple Lie-algebra,* American J. of Math. 79 , 87-120.

Hi HIGMAN, D.G. (83) *Admissible graphs,* In: Finite geometries (Lecture notes in pure and applied mathematics 82) ed. by N.L. Johnson, M.J. Kallaher and C.T. Long, 211-222.

K KELLY, L.M. (47) *Elementary problems and solutions, isosceles n-points,* American Math. Monthly 54 , 227-229.

Ko KOORNWINDER, T. (76) *A note on the absolute bound for systems of lines,* Proc. K.N.A.W. Amsterdam Ser. A 79 (=Indag. Math. 38), 152-153.

L LUCQUIAUD, J.C. (78) *Expression sous forme covariante des fonctions sphériques zonales attachées aux groupes* SO(N) *et* SH(N). CRAS Paris 287 , A67-A69.

LRS LARMAN, D.G., ROGERS, G.A. and SEIDEL, J.J. (77) *On two-distance sets in Euclidean space,* Bull. London Math. Soc. 9, 261-267.

LS LEMMENS, P.W.H. and SEIDEL, J.J. (73) *Equiangular lines,* J. Algebra 24 , 494-512.

vLS van LINT, J.H. and SEIDEL J.J. (66) *Equilateral point sets in elliptic geometry,* Proceedings K.N.A.W. Amsterdam Ser. A 69 (=Indag. Math. 28), 335-348.

N1 NEUMAIER A. (81) *Combinatorial configurations in terms of distances,* Eindhoven: Technological University dept. of Math. and Comp. Sci. (T.H.-Memo 81-09).

N2 --- (80) *Distances, graphs and designs,* European J. of Combinatorics 1 , 163-174.

N3 --- (81) *Distance matrices and n-dimensional designs,* European J. of Combinatorics 2 , 165-172.

N4 --- (81) *Regular cliques in graphs and special 1½-designs,* In: Finite geometries and designs, LMS Lecture notes series 49, Cambridge Univ. Press, 244-259.

N5 --- (82) *Completely regular two-graphs,* Arch. Math. 38 , 378-384.

Na NAGATA, M. (62) *Local rings,* Interscience tracts in pure and applied math. 13, Ed. L. Bers, R. Courant and J.J. Stoker.

T TAYLOR, D.E. (77) *Regular two-graphs,* Proceedings of the London Math. Society (3) 35 , 257-274.

Th THAS, J.A. (77) *Combinatorics of partial geometries and generalized quadrangles,* In: Higher combinatorics, Ed. by M. Aigner, Dordrecht Reidel, 183-199.

V VILENKIN, N.J. (68) *Special functions and the theory of group representations,* Translations American Math. Soc. Vol 22.

W WEYL, J. (46) *The classical groups,* Princeton University Press.

We WELSH, D.J.A. (76) *Matroid theory,* Academic Press, London/New York.

Z ZARA, F. (83) *Graphes liés aux espaces polaires,* preprint.

INDEX

LIST OF SYMBOLS

SAMENVATTING

Het voornaamste onderwerp van dit proefschrift is het bepalen van grenzen voor de cardinaliteit van puntverzamelingen met weinig afstanden. Voor puntverzamelingen op de eenheidsbol in de Euclidische ruimte E^d, werden reeds scherpe grenzen afgeleid in [DGS]. Koornwinder gaf later een simpeler bewijs voor een apart geval hiervan, namelijk verzamelingen van gelijkhoekige rechten in E^d.

In hoofdstuk 2 wordt de theorie ontwikkeld, die het mogelijk maakt om de methoden uit [DGS] toe te passen op puntverzamelingen op de "eenheidsbol" in inprodukt ruimten met een willekeurige signatuur. Vooral het geval van de hyperbolische ruimte $R^{d,1}$, levert scherpe grenzen op.

Een verscherping van de methode van Koornwinder stelt ons in staat de grenzen voor s-afstands-verzamelingen in E^d en H^d, d-dimensionale hyperbolische ruimte, te verbeteren. Ook worden op die manier scherpe grenzen voor verzamelingen van gelijkhoekige rechten in $R^{d,1}$ verkregen.

Nemen de afstanden alleen maar bepaalde gehele waarden modulo een priemgetal aan, dan kunnen opnieuw scherpere grenzen worden bereikt. De metrische ruimten waarin dit het meest tot zijn recht komt zijn de zogenaamde Delsarte ruimten. Als corollarium treedt een stelling van Frankl en Wilson op.

Hierna wordt een probleem van Erdős opgelost, nauw verwant met 2-afstands-verzamelingen, namelijk: wat is het maximaal aantal punten in E^d, zodanig dat elke driehoek, die door drie punten uit de verzameling wordt bepaald, gelijkbenig is. Een essentieel lemma uit dit hoofdstuk vormt de verbinding met het laatste onderwerp. Welke grafen voldoen aan de volgende eigenschappen: 1. Er is een K zodanig dat elke maximale kliek omvang K heeft; 2. Er is een e zodanig dat voor elke maximale kliek C en punt p niet in C, het punt p precies e buren in C heeft. Deze grafen werden geïntroduceerd door Zara [Z] in een poging polaire ruimten te karakteriseren. We laten zien dat Zara-grafen die aan enkele noodzakelijke eigenschappen voldoen sterk regulier zijn en verdere regelmatigheidseigenschappen hebben.

CURRICULUM VITAE

De schrijver van dit proefschrift werd geboren op 6 juli 1956 in Alkmaar. Hij beëindigde de gymnasium β opleiding aan het Johannes College in Den Helder in 1974. Daarna studeerde hij wiskunde met bijvak Econometrie aan de Vrije Universiteit in Amsterdam, waar hij in 1979 het doctoraal examen aflegde. Tijdens zijn studie was hij gedurende een half jaar student assistent.

Van oktober 1979 tot oktober 1983 was hij wetenschappelijk assistent bij de onderafdeling der wiskunde en informatica van de Technische Hogeschool Eindhoven.

STELLINGEN

1. Er bestaat geen Zara-graaf met 95 punten , $K = 5$ en $e = 2$.
Er bestaan geen Zara-grafen met $K/2 < e < K - 2$. De enige cc-Zara-grafen met $K = e + 2$ zijn $\overline{L(n)}$ en $\overline{T(2n)}$, met $n \geq 3$.
A. Blokhuis, T. Kloks, H. Wilbrink; *A class of graphs containing the polar spaces*, to appear.

2. Er bestaan geen niet-triviale compleet reguliere "two-graphs" op 96 of op 640 punten.

3. Zij $\sigma(n,k)$ het aantal formulieren dat ingevuld moet worden bij een toto met n wedstrijden en k mogelijke uitslagen per wedstrijd, om zeker een prijs te winnen voor alle of op één na alle goede uitslagen.
Dan geldt, met q is priem en $k = 1 + t(q^{r-1}-1)/(q-1)$:

   (i) $\sigma(k,q) \leq (q-t+1)q^{k-r}$;

   (ii) $\sigma(n,mt) \leq \sigma(n,m)t^{m-1}$;

   (iii) $\sigma(q+1,qt) = q^{q-1}t^{q}$;

   (iv) $\sigma(np+1,p) \leq \sigma(n,p)p^{np-n}$;

   (v) $\sigma(7,3) \leq 216$, $\sigma(10,3) \leq 5.3^{6}$, $\sigma(16,5) \leq 13.5^{12}$.

A. Blokhuis, C. Lam; *More coverings by rook domains*. To appear in the J. of Comb. Theory A.

4. Het is niet mogelijk een eindig aantal even lange lucifers zodanig neer te leggen in het vlak dat twee lucifers nooit over elkaar heen liggen en in elk eindpunt vijf lucifers bij elkaar komen.

5. De volgende formule van N. Bebiano voor de permanent:

$$\exp(\underline{x}\ ,\ A\underline{y})t \ = \ \sum_{k=0} t^{k} \sum_{|\underline{k}|=|\underline{1}|=k} \frac{\underline{x}^{\underline{k}}\cdot\underline{y}^{\underline{k}}}{\underline{k}!\cdot\underline{1}!} \ \text{per}\ A(\underline{1},\underline{k}) \quad ,$$

is eenvoudig met multilineaire algebra te bewijzen. Hier zijn $\underline{x},\underline{y} \in R^{d}$, $\underline{k} = (k_1,\ldots,k_d)$, $\underline{k}! = k_1!k_2! \ldots k_d!$, $\underline{x}^{\underline{k}} = x_1^{k_1}\ldots x_d^{k_d}$. Tenslotte is

$A(\underline{l},\underline{k})$ de matrix die uit A ontstaat door de i-de rij l_i keer en de j-de kolom k_j keer te herhalen. Natália Bebiano; *On the evaluation of permanents*, Pacific J. Math. vol. 101 no. 1, 1982.

6. Zij C een kleuring van de kanten van de volledige graaf op n punten (n eindig), zodanig dat voor elke vijfhoek in K_n geldt dat er twee opeenvolgende zijden zijn met gelijke kleur, terwijl de geïnduceerde graaf op elke afzonderlijke kleur samenhangend is. Dan zijn er hooguit twee kleuren.

7. Als men n koorden trekt in een cirkel, zodanig dat er geen drie door één punt binnen de cirkel gaan, en als deze koorden m snijpunten binnen de cirkel bepalen, dan wordt de cirkel in $n + m + 1$ gebieden verdeeld. Met deze observatie kan men probleem 8.1 uit L. Comtet; *Advanced combinatorics*, p. 74, zeer eenvoudig oplossen.

8. In tegenstelling tot de indruk die bij het middelbaar onderwijs gewekt wordt, houdt een wiskundige zich bezig met onopgeloste problemen.

9. De maximaal toegelaten rugwind bij het lopen of springen van een wereldrecord dient minder te zijn op grote hoogte dan op zeeniveau, in verband met het verschil in luchtweerstand.