Convex Cone Conditions on the Structure of Designs

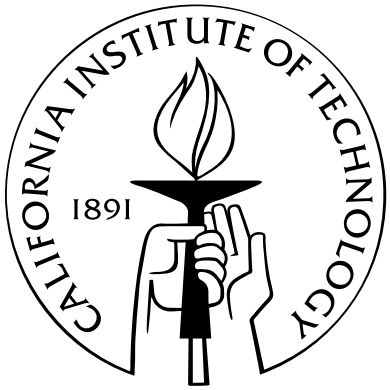
Thesis by

Peter Dukes

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy



California Institute of Technology

Pasadena, California

2003

(Submitted August 7, 2002)

Acknowledgements

My advisor, Professor R. M. Wilson, deserves thanks for a wide variety of reasons. I gratefully acknowledge his suggestion of this research topic and the many helpful ideas arising from our discussions. In this respect alone, I could not have asked for a better mentor. But this is not even to mention his patience, kindness and humor, all of which made my work very enjoyable. Professor Wilson is truly an inspiring role model.

Support from the Department of Mathematics was also indispensable. The secretaries, students, and faculty all made for an excellent experience during my studies at Caltech. Additional thanks extend to the members of my thesis defense committee. Financial assistance, both from the department and my NSERC postgraduate scholarship, was extremely helpful and much appreciated.

Finally, I would like to thank my parents. They lovingly and selflessly captured my passion for learning, while giving me the freedom to discover my own interests.

Abstract

Various known and original inequalities concerning the structure of combinatorial designs are established using polyhedral cones generated by incidence matrices. This work begins by giving definitions and elementary facts concerning t-designs. A connection with the incidence matrix W of t-subsets versus k-subsets of a finite set is mentioned. The opening chapter also discusses relevant facts about convex geometry (in particular, the Farkas Lemma) and presents an arsenal of binomial identities. The purpose of Chapter 2 is to study the cone generated by columns of W, viewed as an increasing union of cones with certain invariant automorphisms. The two subsequent chapters derive inequalities on block density and intersection patterns in t-designs. Chapter 5 outlines generalizations of W which correspond to hypergraph designs and poset designs. To conclude, an easy consequence of this theory for orthogonal arrays is used in a computing application which generalizes the method of two-point based sampling.

Summary of Results

Lemma 1.6: A binomial identity from the Saalschütz formula.

Theorem 2.3: Farkas Lemma for t-vectors invariant under a partition.

Lemma 2.5: Correspondence of facets with maximally vanishing nonzero polynomials.

Theorem 2.6: A characterization of facets invariant under a bipartition.

Theorem 2.7: A proposed generalization of the method of moments.

Theorem 2.9: Equivalence of the cone condition and the classical moment equations.

Theorem 3.1: Alternate proof of a block density inequality in [26].

Theorem 3.4: Necessary and sufficient cone conditions for an enclosing t-vector.

Corollary 3.5: Sharpest inequality from the cone for enclosings of 2-designs.

Corollary 3.6: An inequality for n-fold blocks in t-$(2t+2, t+1, \lambda)$ designs.

Tables 3.1-3.3: Some bounds on n-fold blocks in designs with small parameters.

Theorem 4.1: Alternate proof of the Connor-Wilson inequalities in [27].

Proposition 4.2: Conditions for equality in a block intersection bound when $t = 4$.

Table 4.1: Some improvements on Connor's inequalities for small parameters.

Proposition 4.4: A condition for existence of a block transverse to a parallel class.

Theorem 4.5: Alternate proof of a result on pairwise intersection of several blocks.

Theorem 5.1: Generalization of a hole-size inequality for tBDs in [14].

Theorem 6.2: An error bound for the t-point based sampling technique.

Proposition 6.4: Asymptotic comparison of error bounds with the bound in [11].

Contents

List of Figures

Chapter 1

Preliminaries

1.1 Definitions and facts concerning block designs

Let $\mathbb{N}$ denote the set of positive integers, and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Suppose $t \in \mathbb{N}_0$ and $\lambda \in \mathbb{N}$. A *t-wise balanced block design* (tBD) of *index* λ is a triple $(V, \mathcal{B}, \iota)$, where V and $\mathcal{B}$ are (disjoint) sets of *points* and *blocks*, respectively, and $\iota \subset V \times \mathcal{B}$ is a set of *flags* with the property that for any t-subset T of V, there are precisely λ blocks B of $\mathcal{B}$ satisfying $(x, B) \in \iota$ for all $x \in T$. The *supplement* of such a tBD is $(V, \mathcal{B}, \iota')$ with $\iota' = (V \times \mathcal{B}) \setminus \iota$. When $(x, B) \in \iota$, it is said that x and B are *incident*. For a block $B \in \mathcal{B}$, notation will be abused by writing B also for the set of points in V which are incident with B. In this case, a collection of blocks can be regarded as a multiset of subsets of V. With this in mind, it makes sense to drop the flags from this notation and discuss the "cardinality" of a block, or the "membership" of a point in a block. If the collection of all blocks (each regarded as a set of points) is itself a set, or in other words when there are no repeated blocks, the tBD is called *simple*. Note that these set systems are rather uninteresting when $t = 0, 1$; so it is generally assumed that $t \geq 2$. The well-known Fano plane is an example of a 2BD with index unity and all blocks of size 3. Until Chapter 5, all blocks will be assumed to have a common size k with $t \leq k \leq v = |V|$. The relevant structure is then often referred to by its parameters as a t-(v, k, λ) design, or simply a t-design. However, it is common to use the term "design" when speaking of certain other structures.

A *configuration* $\mathcal{D}$ is a collection of subsets from some relatively small generic set

U. To say that a design $(V, \mathcal{B})$ *contains* a configuration means that there exists an injection $U \hookrightarrow V$ so that (the image of) $\mathcal{D}$ is a subcollection of $\mathcal{B}$. A very large amount of research has gone into the construction and enumeration of designs containing or avoiding various configurations. Under consideration here will be structural constraints, or nonexistence results, for designs containing a given configuration.

The first fact along these lines is a well-known family of necessary numerical conditions on the parameters of a t-design.

Proposition 1.1. *For $0 \leq i \leq t$ and $I \subset V$ with $|I| = i$, the number of blocks containing I in a t-(v, k, λ) design is a constant $\lambda\binom{v-i}{t-i}/\binom{k-i}{t-i}$. In particular, there are $\lambda\binom{v}{t}/\binom{k}{t}$ blocks in a t-(v, k, λ) design.*

Proof: Count in two ways the number of ordered pairs (T, B), where $|T| = t$ and B is a block with $I \subset T \subset B$. □

It follows that every t-design is also an i-design for $i \leq t$. As the count of blocks above is obviously an integer, this result implies the conditions $\binom{k-i}{t-i} \big| \lambda\binom{v-i}{t-i}$ for $0 \leq i \leq t$. Parameters t, k, v, λ which satisfy all these divisibility requirements are said to be *admissible*. A detailed treatment of this and other standard necessary conditions on t-designs can be found in [24], chapter 19.

A somewhat more subtle family of constraints exists on the parameters of a t-design. Let H be any subset of V with $|H| = w$. Suppose there are z_j blocks which intersect H in j points for $j = 0, 1, \ldots, k$. Count the ordered pairs (I, B), where B is a block and $I \subset B \cap H$ with $|I| = i$ in two ways. Starting with a choice of either B (and using the z_j) or I (and using Proposition 1.1) yields the system

$$\sum_{j=0}^{k} \binom{j}{i} z_j = \lambda \binom{w}{i} \binom{v-i}{t-i} \binom{k-i}{t-i}^{-1}, \quad i = 0, 1, \ldots, t. \tag{1.1}$$

These are the *moment equations*. The existence of nonnegative integral z_j solving (1.1) has been frequently exploited to obtain inequalities or other nonexistence results on designs. This technique is often called the method of moments. Dropping one of either the integrality or nonnegativity condition on the z_j makes the solubility issue

for (1.1) more tractable. This work essentially pursues the nonnegativity condition to a more general system. Working from the integrality condition results in *signed designs*; see [28], for example.

Let $t, k, v \in \mathbb{N}$ with $t \leq k \leq v$. From now on, the v-set V will be assumed to have some arbitrary ordering. The term *t-vector* will be employed to mean a vector in $\mathbb{R}^{\binom{v}{t}}$ indexed over t-subsets of V. If $X \subseteq V$, let $\mathbf{e}_X$ be the *characteristic* t-vector of X,

$$\mathbf{e}_X(T) = \begin{cases} 1 & \text{if } T \subseteq X, \\ 0 & \text{otherwise.} \end{cases}$$

The $\binom{v}{t} \times \binom{v}{k}$ matrix W_{tk}^v has rows and columns indexed by all t-subsets and k-subsets of V, respectively, with

$$W_{tk}^v(T, K) = \begin{cases} 1 & \text{if } T \subseteq K, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\mathbf{j}$ denote the vector (whose dimension is understood from context) with all entries equal to 1. In this language, there exists a t-(v, k, λ) design if and only if the equation $W_{tk}^v \mathbf{d} = \lambda \mathbf{j}$ has a nonnegative integral solution $\mathbf{d}$. The vector $\mathbf{d}$ simply encodes the number of occurrences of each possible block. Note that since $W_{tk}^v \mathbf{j} = \binom{v-t}{k-t}\mathbf{j}$, it is always true that this equation has nonnegative *rational* solutions. In the work which follows, two basic modifications of this equation will be used so that the existence of nonnegative rational solutions may, in fact, provide useful results.

First, the structure present in a certain design could allow for restricting the possible choices of blocks. For a set $\mathcal{K}$ of k-subsets of V, define the matrix $W = W_{tk}^v|\mathcal{K}$ to be a $\binom{v}{t} \times |\mathcal{K}|$ submatrix of W_{tk}^v consisting of those columns indexed over $\mathcal{K}$. Additionally, suppose a design contains a certain configuration $\mathcal{D}$. The existence of such a design is equivalent to a nonnegative integral solution $\mathbf{d}$ of

$$W\mathbf{d} = \lambda \mathbf{j} - \sum_{B \in \mathcal{D}} \mathbf{e}_B, \tag{1.2}$$

and relaxing to rational (or real) $\mathbf{d}$ becomes nontrivial in general. It will be shown in Section 2.3 that the case $|\mathcal{D}| = 1$ of (1.2) is equivalent to a variant of equations (1.1).

1.2 Tools from convex geometry

For more on the definitions and proofs omitted in this section, see the book [25]. A (convex) *cone* κ in a finite-dimensional real vector space U is a subset of U, for which $c_1x_1 + c_2x_2 \in \kappa$ whenever $x_1, x_2 \in \kappa$ and $c_1, c_2 \geq 0$. The (polyhedral) cone *generated* by $\{x_1, \ldots, x_n\} \subset U$ is the set $\kappa = \{c_1x_1 + \cdots + c_nx_n : c_i \geq 0\}$. Should these x_i be linearly independent, the cone is said to be of *dimension* n. A cone $\kappa \subset U$ is *full* if its dimension agrees with that of U, and is *pointed* if $x, -x \in \kappa$ implies $x = 0$. Here, all cones will be assumed to be full, pointed, and generated by a finite set. A *face* of κ is a cone $\eta \subset \kappa$ such that for all $x \in \eta$, if $x = x_1 + x_2$ with $x_1, x_2 \in \kappa$, then $x_1, x_2 \in \eta$. A face of dimension 1 is called an *extremal ray* of κ, while a face of codimension 1 is called a *facet* of κ.

The following is a "cone version" of the Krein-Milman Theorem, which states that every compact, convex set in a finite dimensional space is the convex hull of its extreme points.

Proposition 1.2. *Let $\kappa \subset U$ be a (closed, pointed, full, and convex) cone and suppose $\{x_1\}, \ldots, \{x_n\}$ generate all the extremal rays of κ. Then $\{x_1, \ldots, x_n\}$ generates κ.*

Let U' be the dual space of U and let κ be a cone in U. Then $\kappa' = \{y \in U' : yx \geq 0\}$ is a cone called the *dual* of κ. The space U'' will be identified with U so that $\kappa'' = \kappa$. The following correspondence will be of particular interest:

($\star$) The dual of a facet of κ is an extremal ray of κ'.

For $y \in U'$, $y \neq 0$, the dual of the cone generated by $\{y\}$ is a *half-space* of U, and y is a *supporting vector* for any cone contained in this half-space. If y is a supporting vector for κ and $\eta = \kappa \cap y^{\perp}$ is a face of κ, then y is said to *support κ at η*. A result of fundamental importance is that a cone κ is the intersection of all half-spaces

described by supporting vectors of κ. Theorem 1.3 below states this in the concrete setting which shall be used herein.

The discussion from now on focuses on cones in real Euclidean space generated by the columns of some matrix A. The reader is cautioned about a change of notation. The vector $\mathbf{x}$ is used below to represent a (column) vector in the *domain* of A as a linear transformation, rather than a typical element of a cone. After this section, $\mathbf{x}$ will have a different meaning; however, $\mathbf{y}$ should be regarded throughout as a supporting (row) vector in the dual space.

Given an $m \times n$ matrix A, the set $\mathcal{C}A = \{A\mathbf{x} : \mathbf{x} \in \mathbb{R}^n, \mathbf{x} \geq \mathbf{0}\}$ is a closed and polyhedral cone in $\mathbb{R}^m$. The dimension of $\mathcal{C}A$ is equal to the rank of A. The following result provides necessary and sufficient conditions for a point to belong to $\mathcal{C}A$.

Theorem 1.3. (Farkas Lemma) *Let A be an $m \times n$ matrix, and $\mathbf{b} \in \mathbb{R}^m$. The equation $A\mathbf{x} = \mathbf{b}$ has a solution $\mathbf{x} \geq \mathbf{0}$ (that is, $\mathbf{b} \in \mathcal{C}A$) if and only if $\mathbf{y} \cdot \mathbf{b} \geq 0$ for all $\mathbf{y} \in \mathbb{R}^m$ such that $\mathbf{y}A \geq \mathbf{0}$.*

Remarks: One direction of this result is immediate. Suppose $A\mathbf{x} = \mathbf{b}$ has a nonnegative solution $\mathbf{x} \in \mathbb{R}^n$, and let $\mathbf{y}$ be such that $\mathbf{y}A \geq \mathbf{0}$. Then

$$\mathbf{y} \cdot \mathbf{b} = \mathbf{y}(A\mathbf{x}) = (\mathbf{y}A)\mathbf{x} \geq 0.$$

The converse is deeper, relying on the existence of a *separating hyperplane* between $\mathcal{C}A$ and a point not in this cone.

When $\mathcal{C}A$ is full and pointed, it is enough by ($\star$) and Proposition 1.2 to check the condition in Theorem 1.3 for $\mathbf{y}$ corresponding to facets of $\mathcal{C}A$. Roughly speaking, facets of $\mathcal{C}A$ provide the family of strongest tests for $\mathbf{b} \in \mathcal{C}A$. Since there are a finite number of facets of $\mathcal{C}A$, it is a finite problem to determine whether $A\mathbf{x} = \mathbf{b}$ has nonnegative solutions $\mathbf{x}$. However this problem is seldom easy in practice, as evidenced by the expanding study of linear programming. A variant of the well-known *simplex algorithm* can, in principle, be implemented on computer to find facets of $\mathcal{C}A$. This is given below for completeness, with $\mathrm{col}(A)$ denoting the set of columns of A.

1. Start with a random $\mathbf{y} \in \mathbb{R}^m$ such that $\mathbf{y}A \geq \mathbf{0}$.

2. If $\dim(\text{span}\{\mathbf{a} \in \text{col}(A) : \mathbf{y} \cdot \mathbf{a} = 0\}) < m - 1$ (that is, if $\mathbf{y}$ does not already support $\mathcal{C}A$ at a facet), choose a random $\mathbf{z} \in \mathbb{R}^m$ such that $\mathbf{z}A$ has a positive coordinate but vanishes on at least the same coordinates as $\mathbf{y}A$.

3. Let
$$\epsilon = \min \frac{(\mathbf{y}A)_i}{(\mathbf{z}A)_i},$$
where the minimum is taken over all i for which the quantity is defined and positive.

4. Set $\mathbf{y} := \mathbf{y} - \epsilon\mathbf{z}$ and return to step 2.

It should be noted that the columns of W (defined in Section 1.1) are linearly independent and all lie in the nonnegative orthant of $\mathbb{R}^{\binom{v}{t}}$, so step 1 in the above algorithm is trivial. For all $\mathcal{K}$ to be considered, $W = W^v_{tk}|\mathcal{K}$ will be of full rank $\binom{v}{t}$, so $\mathcal{C}W$ is indeed full. Unfortunately, when the parameters (particularly t) are large, the simplex algorithm is too slow to be of much use, though infinite families of facets of may be guessed by observing the output from this algorithm. For proofs, it is often the case that other supporting vectors $\mathbf{y}$ of $\mathcal{C}W$, which do not necessarily define a facet, are easier to use with Theorem 1.3. However, facets of $\mathcal{C}W$ are of some combinatorial interest on their own, as will be seen in Section 2.2. In any case, with $\mathbf{b} = \lambda\mathbf{j} - \sum_{B\in\mathcal{D}} \mathbf{e}_B$, constraints of the form $\mathbf{y} \cdot \mathbf{b} \geq 0$ can be established on t-designs containing $\mathcal{D}$.

1.3 Some binomial identities

For use in later chapters, some identities involving binomial coefficients[1] are presented here. The simple relation

$$\binom{\alpha}{\beta}\binom{\beta}{\gamma} = \binom{\alpha}{\gamma}\binom{\alpha-\gamma}{\beta-\gamma} \tag{1.3}$$

[1] In the usual way, top arguments of binomial coefficients may take on non-integer values.

will be used frequently. For identities involving summations, it may be convenient at times to use the hypergeometric notation

$$ {}_pF_q\left[\begin{array}{cccc} \alpha_1, & \alpha_2, & \ldots, & \alpha_p \\ & \beta_1, & \ldots, & \beta_q \end{array};\xi\right] = \sum_{j=0}^{\infty} \frac{(\alpha_1)_j(\alpha_2)_j\ldots(\alpha_p)_j}{j!(\beta_1)_j\ldots(\beta_q)_j}\xi^j, $$

where $(\alpha)_j = \alpha(\alpha+1)\ldots(\alpha+j-1)$. The transformation from a (finite) sum of products of binomial coefficients into this notation is routine and will be omitted in what follows. References and proofs for many hypergeometric identities can be found in [1]. A vintage formula of Gauss is now given as a starting point.

Proposition 1.4. *If $a, b, c \in \mathbb{R}$ with $c > a + b$, then*

$$ {}_2F_1\left[\begin{array}{cc} a, & b \\ & c \end{array};1\right] = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)}. $$

When meaningful, the right side can be written as a quotient of two binomial coefficients. Some easy consequences are the "convolution" identities

$$ \sum_{j=0}^{t} \binom{x}{j}\binom{y}{t-j} = \binom{x+y}{t}, \tag{1.4} $$

$$ \sum_{j=0}^{t} (-1)^{t-j}\binom{x}{j}\binom{y-j}{t-j} = \binom{x-y+t-1}{t}, \tag{1.5} $$

$$ \sum_{j=0}^{t} \binom{j}{i}\binom{t-j}{r-i}\binom{x}{j}\binom{y}{t-j} = \binom{x+y-r}{t-r}\binom{x}{i}\binom{y}{r-i}, \quad (t \geq r), \tag{1.6} $$

$$ \sum_{h=j}^{r} \binom{h}{j}\binom{j}{r-h}\binom{x}{h} = \binom{x}{j}\binom{x}{r-j}, \tag{1.7} $$

and

$$ \begin{aligned} &\sum_{j=0}^{t-r} (-1)^j \binom{t}{j}^{-1}\binom{x}{j}\binom{y}{t-j} \\ &= \frac{t+1}{x+y-t}\left[\binom{y}{t+1} + (-1)^{t-r}\binom{x}{t-r+1}\binom{y}{r}\binom{t+1}{r}^{-1}\right], \quad (0 \leq r \leq t). \end{aligned} \tag{1.8} $$

Proof of (1.6) *and* (1.7): Apply equation (1.3) to the summand, shift the index of summation, and use (1.4). □

Proof of (1.8): The given (terminating) sum is

$$\left(\binom{y}{t}-(-1)^{t-r+1}\binom{x}{t-r+1}\binom{y}{r-1}\binom{t}{r-1}^{-1}\right){}_2F_1\left[\begin{array}{ccc}1, & -x & ;1\\ & 1-t+y & \end{array}\right],$$

which simplifies to the right side by Proposition 1.4 and the special case $\frac{\beta}{\alpha}\binom{\alpha}{\beta}=\binom{\alpha-1}{\beta-1}$ of equation (1.3). □

For another important summation to be used, a classical identity of Saalschütz is required.

Proposition 1.5. *Suppose* $1+w+x-n=y+z$ *with* $n\in\mathbb{N}_0$. *Then*

$${}_3F_2\left[\begin{array}{ccc}-n, & w, & x\\ & y, & z\end{array};1\right]=\frac{(y-w)_n(y-x)_n}{(y)_n(y-w-x)_n}.$$

Lemma 1.6. *For* $v\geq k+s$,

$$\sum_{j=0}^{s}(-1)^j\binom{v-i-j}{k-i-j}\binom{v-s}{j}\binom{k-j}{s-j}=\binom{v-s}{k-s}.$$

Proof: Let $f(k,i)$ denote the given sum. The familiar $\binom{x-1}{i-1}+\binom{x-1}{i}=\binom{x}{i}$ gives rise to $f(k,i)=f(k,i+1)+f_{\text{Saal}}(k+1,i+1)$, where

$$\begin{aligned}f_{\text{Saal}}(k,i) &= \sum_{j=0}^{s}(-1)^j\binom{v-i-j}{k-i-j}\binom{v-s}{j}\binom{k-1-j}{s-j}\\ &= \binom{v-i}{k-i}\binom{k-1}{s}{}_3F_2\left[\begin{array}{ccc}-s, & s-v, & i-k\\ & 1-k, & i-v\end{array};1\right].\end{aligned}$$

By Proposition 1.5, $f_{\text{Saal}}(k,i)=0$ unless $i=0$. So

$$f(k,i)=f(k,0) = \sum_{j=0}^{s}(-1)^j\binom{v-j}{k-j}\binom{v-s}{j}\binom{k-j}{s-j}$$

$$\begin{aligned} &= \binom{v-s}{k-s} \sum_{j=0}^{s} (-1)^j \binom{v-j}{s-j} \binom{v-s}{j} \\ &= \binom{v-s}{k-s}, \end{aligned}$$

where equations (1.3) and (1.5) have been used. □

Chapter 2

General Theory

2.1 Automorphisms and invariant partitions

In this section, $\mathbf{b}$ is some fixed t-vector as defined in Section 1.1. Consider the action of the symmetric group $\mathcal{S}_V$ on V. For $\sigma \in \mathcal{S}_V$ and $\mathbf{y}$ a t-vector, define $\mathbf{y}^\sigma$ by $\mathbf{y}^\sigma(T) = \mathbf{y}(\sigma^{-1}(T))$. This vector is obtained from $\mathbf{y}$ simply by permuting its coordinates according to the inherited action on t-subsets of V. It is clear that

$$\mathbf{y}^\sigma \cdot \mathbf{b}^\sigma = \sum_{|T|=t} \mathbf{y}(\sigma^{-1}(T))\mathbf{b}(\sigma^{-1}(T)) = \sum_{|T|=t} \mathbf{y}(T)\mathbf{b}(T) = \mathbf{y} \cdot \mathbf{b}. \tag{2.1}$$

If $\mathbf{b}^\sigma = \mathbf{b}$, then it will be said that $\mathbf{b}$ is *invariant* under σ. The set of all such $\sigma \in \mathcal{S}_V$ is a group because $(\mathbf{b}^\sigma)^\tau = \mathbf{b}^{(\sigma\tau)}$ follows immediately from the definition. Define this group to be $\mathrm{stab}(\mathbf{b})$.

Let $\mathbb{H}^d(V)$ denote the set of partitions of V into d parts which are ordered according to the implicit ordering in V. For a set $S \subset V$ and $\Omega = (U_1, \ldots, U_d) \in \mathbb{H}^d(V)$, define $S \cap \Omega = (S \cap U_1, \ldots, S \cap U_d) \in \mathbb{H}^d(S)$. For $s \in \mathbb{N}_0$, define the simplex of lattice points $\mathbb{H}^d(s) = \left\{(n_1, \ldots, n_d) \in \mathbb{N}_0^d : \sum n_i = s\right\}$. Let $|\Omega|$ denote the integer partition $(|U_1|, \ldots, |U_d|) \in \mathbb{H}^d(v)$. The set of $\sigma \in \mathcal{S}_V$ which leave each U_i invariant is the subgroup $\mathrm{stab}(\Omega) = \mathcal{S}_{U_1} \times \cdots \times \mathcal{S}_{U_d}$ of $\mathcal{S}_V$. Consider the usual ordering $\preceq$[1] and the associated lattice structure on $\mathbb{H}^d(V)$.

Call $\Omega \in \mathbb{H}^d(V)$ an *invariant partition* for $\mathbf{b}$ if $\mathrm{stab}(\Omega) \subseteq \mathrm{stab}(\mathbf{b})$. Of primary

[1] If each part of Ω_1 belongs to a single part of Ω_2, then $\Omega_1 \preceq \Omega_2$.

interest will be invariant partitions which are maximal in $\mathbb{H}^d(V)$, in the sense that any other such Ω' satisfies $\Omega' \preceq \Omega$. For the remainder of this section, assume $\Omega = (U_1, \ldots, U_d)$ is some invariant partition for $\mathbf{b}$, with $\omega = |\Omega|$.

Define

$$\overline{\mathbf{y}} = \frac{1}{|\mathrm{stab}(\Omega)|} \sum_{\sigma \in \mathrm{stab}(\Omega)} \mathbf{y}^\sigma.$$

An elementary consequence of the definitions and equation (2.1) is that $\mathbf{y} \cdot \mathbf{b} = \overline{\mathbf{y}} \cdot \mathbf{b}$. for any $\mathbf{y} \in \mathbb{R}^{\binom{v}{t}}$.

Two subsets $S, S' \subset V$, which satisfy $\tau(S) = S'$ for some $\tau \in \mathrm{stab}(\Omega)$, will be called *equivalent* under Ω. Note that S, S' are equivalent under Ω if and only if $|S \cap \Omega| = |S' \cap \Omega| \in \mathbb{H}^d(s)$, where $s = |S| = |S'|$.

Lemma 2.1. *Let $T_1, T_2 \subset V$ be t-sets equivalent under Ω. Then $\overline{\mathbf{y}}(T_1) = \overline{\mathbf{y}}(T_2)$.*

Proof: Let $\tau \in \mathrm{stab}(\Omega)$ be such that $\tau(T_1) = T_2$. Then

$$\begin{aligned} |\mathrm{stab}(\Omega)|\ \overline{\mathbf{y}}(T_1) &= \sum_{\sigma \in \mathrm{stab}(\Omega)} \mathbf{y}^\sigma(T_1) = \sum_{\sigma \in \mathrm{stab}(\Omega)} \mathbf{y}(\sigma^{-1}(T_1)) \\ &= \sum_{\sigma \in \mathrm{stab}(\Omega)} \mathbf{y}(\sigma^{-1}\tau^{-1}(T_2)) = \sum_{\sigma \in \mathrm{stab}(\Omega)} \mathbf{y}^{\tau\sigma}(T_2) \\ &= \sum_{\sigma' \in \mathrm{stab}(\Omega)} \mathbf{y}^{\sigma'}(T_2) = |\mathrm{stab}(\Omega)|\ \overline{\mathbf{y}}(T_2). \end{aligned}$$

□

This allows for writing

$$\overline{\mathbf{y}} = \sum_{\varphi \in \mathbb{H}^d(t)} a_\varphi \sum_{|T \cap \Omega| = \varphi} \mathbf{e}_T \tag{2.2}$$

for some real coefficients a_φ. Of course, the contribution to the sum is 0 unless $\varphi \leq \omega$.

For $\mathbf{x} = (x_1, \ldots, x_d)$ and $\varphi \in \mathbb{N}_0^d$, define

$$\mathbf{x}^\varphi = \prod_{i=1}^d x_i^{\varphi_i} \quad \text{and} \quad \binom{\mathbf{x}}{\varphi} = \prod_{i=1}^d \binom{x_i}{\varphi_i}.$$

Let $k \in \mathbb{N}$. Consider the real algebra $\Lambda = \mathbb{R}[x_1, \ldots, x_d]/(-k + \sum_1^d x_i)$. Then Λ can

be expressed as an increasing union $\Lambda = \cup_{t=0}^{\infty} \Lambda_t$, where

$$\Lambda_t = \text{span}\{[\mathbf{x}^\varphi] : \varphi \in \mathbb{H}^d(t)\}.$$

It is easy to show that another basis for Λ_t is $\{[\binom{\mathbf{x}}{\varphi}] : \varphi \in \mathbb{H}^d(t)\}$. Indeed, the transition matrix expressing the binomial coefficients in terms of the monomials is upper triangular (after appropriate indexing) with diagonal entries $1/\varphi!$. Consider any $[f] \in \Lambda_t$. It follows that when $\sum_1^d x_i = k$,

$$f(\mathbf{x}) = \sum_{\varphi \in \mathbb{H}^d(t)} a_\varphi \binom{\mathbf{x}}{\varphi}$$

for some $a_\varphi \in \mathbb{R}$. For such an f expressed in this way, define the corresponding t-vector $\mathbf{y}_f$ as on the right side of equation (2.2).

Lemma 2.2. *Suppose K is a k-set with $|K \cap \Omega| = \psi \in \mathbb{H}^d(k)$. Then $\mathbf{y}_f \cdot \mathbf{e}_K = f(\psi)$*

Proof: The dot product on the left counts a_φ times the number of t-subsets T of K for which $|T \cap \Omega| = \varphi$, summed over all $\varphi \in \mathbb{H}^d(t)$. There are $\binom{\psi}{\varphi}$ such t-sets for a given φ, so this count agrees with the right hand side. □

Theorem 2.3. *Suppose $\Omega \in \mathbb{H}^d(V)$ is an invariant partition for $\mathbf{b}$, and let $\omega = |\Omega|$. Define $W = W_{tk}^v|\mathcal{K}$. Then $\mathbf{b} \in \mathcal{C}W$ if and only if*

$$\mathbf{y}_f \cdot \mathbf{b} = \sum_{\varphi \in \mathbb{H}^d(t)} a_\varphi b_\varphi \binom{\omega}{\varphi} \geq 0$$

for all $f \in \mathbb{R}[x_1, \ldots, x_d]$ of degree $\leq t$ nonnegative on $\{|K \cap \Omega| : K \in \mathcal{K}\}$, where $f(\mathbf{x}) = \sum_{\varphi \in \mathbb{H}^d(t)} a_\varphi \binom{\mathbf{x}}{\varphi}$ and $\mathbf{b} = \sum_{\varphi \in \mathbb{H}^d(t)} b_\varphi \sum_{|T \cap \Omega| = \varphi} \mathbf{e}_T$.

Proof: By Lemma 2.2, the nonnegativity constraint on f is equivalent to $\mathbf{y}_f \cdot \mathbf{e}_K \geq 0$ for all k-sets K, or $\mathbf{y}_f W \geq \mathbf{0}$. Theorem 1.3 states that $\mathbf{b} \in \mathcal{C}W$ if and only if $\mathbf{y} \cdot \mathbf{b} \geq 0$ whenever $\mathbf{y}W \geq \mathbf{0}$. Thus it is enough to prove this condition is equivalent to that when quantified over the Ω-invariant vectors $\mathbf{y}_f$. Suppose $\mathbf{y}W \geq \mathbf{0}$ implies $\mathbf{y} \cdot \mathbf{b} \geq 0$ for all $\mathbf{y} \in \mathbb{R}^{\binom{v}{t}}$. Then certainly $\mathbf{y}_f W \geq \mathbf{0}$ implies $\mathbf{y}_f \cdot \mathbf{b} \geq 0$ for all polynomials f

of the given form. Conversely, suppose $\mathbf{y}_f W \geq \mathbf{0}$ implies $\mathbf{y}_f \cdot \mathbf{b} \geq 0$ for all f. Let $\mathbf{y} \in \mathbb{R}^{\binom{v}{t}}$ be arbitrary and assume $\mathbf{y}W \geq \mathbf{0}$. Observe for any $\sigma \in \mathcal{S}_V$ that the vector $\mathbf{y}^\sigma W$ is a rearrangement of $\mathbf{y}W$. So $\overline{\mathbf{y}}W \geq \mathbf{0}$. But $\overline{\mathbf{y}}$ is of the form $\mathbf{y}_f$ for some f. So $\mathbf{y} \cdot \mathbf{b} = \overline{\mathbf{y}} \cdot \mathbf{b} \geq 0$. □

2.2 Facets and the extremal polynomials

Here, let $W = W^v_{tk}$. Define $W^\sigma(T, K) = W(\sigma^{-1}(T), K)$. This can be viewed as changing W by either a row or column permutation. For $\Omega \in \mathbb{H}^d(V)$, set

$$W_\Omega = \frac{1}{|\mathrm{stab}(\Omega)|} \sum_{\sigma \in \mathrm{stab}(\Omega)} W^\sigma.$$

Note that the cone $\mathcal{C}W_\Omega$ is full if and only if $d \geq 2$. It is a straightforward observation that $\Omega' \preceq \Omega$ implies $\mathcal{C}W_\Omega \subseteq \mathcal{C}W_{\Omega'}$. This motivates the view of $\mathcal{C}W$ as a refinement of cones

$$\mathcal{C}W = \bigcup_{\Omega \in \mathbb{H}^d(V)} \mathcal{C}W_\Omega$$

indexed over the lattice of partitions of V.

Proposition 2.4. *Suppose $\Omega \in \mathbb{H}^d(V)$, $(d \geq 2)$ is an invariant partition for $\mathbf{y}$. Then $\mathbf{y}W_\Omega \geq \mathbf{0}$ implies $\mathbf{y}W \geq \mathbf{0}$. Moreover, if $\mathbf{y}$ supports W_Ω at a facet, then $\mathbf{y}$ supports W at a facet.*

Proof: Since $\mathbf{y}$ is Ω-invariant,

$$\mathbf{y}W = \frac{1}{|\mathrm{stab}(\Omega)|} \sum_{\sigma \in \mathrm{stab}(\Omega)} \mathbf{y}^{\sigma^{-1}} W = \frac{1}{|\mathrm{stab}(\Omega)|} \sum_{\sigma \in \mathrm{stab}(\Omega)} \mathbf{y}W^\sigma = \mathbf{y}W_\Omega.$$

This proves the first statement and, since each column of W_Ω is in the span of the columns of W,

$$\mathrm{span}\{\mathrm{col}(W_\Omega) : \mathbf{y}W_\Omega = 0\} \subseteq \mathrm{span}\{\mathrm{col}(W) : \mathbf{y}W = 0\}.$$

So if the subspace on the left has codimension 1, then so does the subspace on the right provided it is not full. But $\mathbf{y}$ supporting a facet of W_Ω implies $\mathbf{y} \cdot \sum_{\sigma \in \mathrm{stab}(\Omega)} \mathbf{e}_{\sigma K} > 0$ for some K. Again by invariance under Ω, it must be that $\mathbf{y} \cdot \mathbf{e}_K > 0$, and so $\mathbf{y}$ does in fact support a facet of $\mathcal{C}W$. □

Theorem 2.3 essentially describes the dual cone of $\mathcal{C}W_\Omega$. Rather than directly considering the supporting vectors, it is interesting to view this dual as the cone of d-variable polynomials of degree $\leq t$ which are nonnegative on the appropriate lattice points. By the remarks in Section 1.2, there is a correspondence between facets of $\mathcal{C}W$ and extremal rays of these cones of polynomials. It is not the aim of this work to thoroughly investigate such extremal rays. Indeed, this appears to be related to the subject of polynomial interpolation in several variables, for which relatively little is known in general [9]. However, the remainder of this section will contribute some initial observations along these lines.

For a set $S \subset \mathbb{R}^d$, let $P_t^d(S)$ denote the cone of d-variable polynomials of degree $\leq t$ which are nonnegative on S. It may be of interest to the reader that the (non-polyhedral) case when $d = 1$ and $S = [0, 1] \subset \mathbb{R}$ is investigated in [2]. Here though, it is assumed that S is a finite set.

Lemma 2.5. *Let $f, g \in P_t^d(S)$, $g \not\equiv 0$, and suppose $\{\mathbf{x} \in S : f(\mathbf{x}) = 0\}$ is a proper subset of $\{\mathbf{x} \in S : g(\mathbf{x}) = 0\}$. Then f does not generate an extremal ray of $P_t^d(S)$.*

Proof: Choose $\epsilon > 0$ such that $f - \epsilon g \in P_t^d(S)$. Neither this polynomial, nor ϵg are identically zero by the condition given. Furthermore, ϵg is not in the ray generated by f. Thus by the definition in Section 1.2, f cannot generate an extremal ray since $f = (f - \epsilon g) + \epsilon g$. □

While characterizing the nonzero "maximally vanishing" polynomials in $P_t^d(S)$ is difficult in general, there is an easy solution in one variable. The following is a variant of Gale's evenness condition, which characterizes the facets of cyclic polytopes, [25].

Theorem 2.6. *Suppose $|S| \geq t + 1$ and let $f \in P_t^1(S)$ with $Z = \{x \in S : f(x) = 0\}$. Then f generates an extremal ray of $P_t^1(S)$ if and only if $|Z| = t$ and every two points of $S \setminus Z$ are separated by an even number of points of Z.*

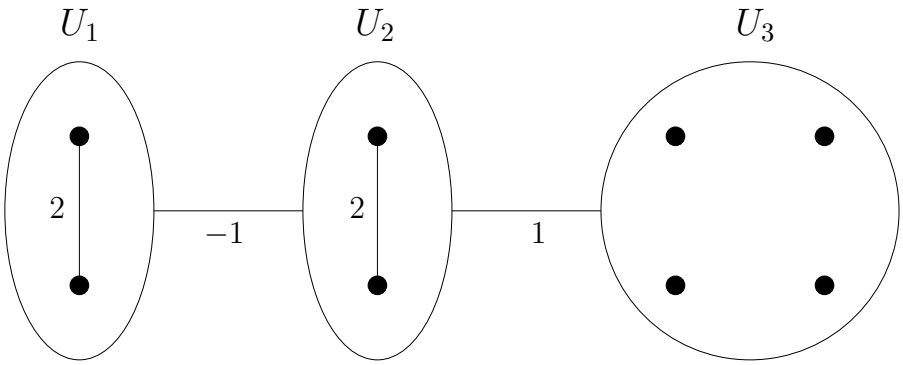


Figure 2.1: Edge weights for a facet of W_{23}^8.

Proof: By Lemma 2.5, any f generating an extremal ray must vanish maximally on S, so $|Z| = t$ and $f(x) = C\prod_{\zeta\in Z}(x-\zeta)$ for some $C \neq 0$. So in order for $f \geq 0$ on S, the evenness condition on Z must hold. Conversely, if $|Z| = t$ and $f(x) = C\prod_{\zeta\in Z}(x-\zeta) \in P_t^1(S)$ can be written as $f = g_1 + g_2$, where $g_1, g_2 \in P_t^1(S)$, then both g_1 and g_2 vanish on all of Z. As all degrees are $\leq t$, it follows that g_1 and g_2 are multiples of f. □

Vanishing subsets Z as in the theorem will be called *good*. It should be mentioned that a lower bound on the number of facets of W can be obtained by counting good subsets. In what follows, polynomials in the variables $x_1, \ldots, x_d$ which are nonnegative on $\mathbb{H}^d(k) \cap \{(x_1, \ldots, x_d) \leq \omega\}$ will often be identified with polynomials in $d-1$ variables, say $x_1, \ldots, x_{d-1}$, that are nonnegative on

$$\bigcup_{j\leq\omega_d} \mathbb{H}^{d-1}(k-j) \cap \{(x_1, \ldots, x_{d-1}) \leq (\omega_1, \ldots, \omega_{d-1})\}.$$

For instance, Theorems 2.3 and 2.6 applied to $S = \{\max(0, k-\omega_2), \ldots, \min(k, \omega_1)\}$ give a characterization of facets for W_Ω when $\Omega \in \mathbb{H}^2(V)$ is a bipartition of V. A concrete description of these facets appears in Section 3.2. The discussion of general facets will now be concluded with an example which does not arise from a bipartition.

Example 2.1. By implementing the algorithm in Section 1.2 on computer, 18 different facets (up to isomorphism) were generated for W_{23}^8. One of these is illustrated in

Figure 2.1. The supporting 2-vector $\mathbf{y}_f \in \mathbb{R}^{\binom{8}{2}}$ for this facet is formed from the edge weights in the diagram. An edge between the circled sets represents all edges between the two sets receiving the indicated weight. Otherwise, missing edges correspond to a weight of zero. Of the $\binom{8}{3} = 56$ possible 3-subsets of V, 36 have total inherited weight zero. The fact that $\mathbf{y}_f$ supports a facet means the characteristic vectors of these triangles span a subspace of $\mathbb{R}^{\binom{8}{2}}$ of dimension $\binom{8}{2} - 1 = 27$. This vector $\mathbf{y}_f$ is invariant under $\mathrm{stab}(\Omega) \cong \mathcal{S}_2 \times \mathcal{S}_2 \times \mathcal{S}_4$. A (three variable) polynomial class $[f] \in \Lambda_2$ for $\mathbf{y}_f$ is given by

$$f(x_1, x_2, x_3) = 2\binom{x_1}{2} + 2\binom{x_2}{2} - x_1x_2 + x_2x_3.$$

Reducing modulo the ideal $(x_1 + x_2 + x_3 - 3)$ allows for the simplification $[f] = [(1 - x_1)(2x_2 - x_1)]$. The relevant values of $f^*(x_1, x_2) = (1 - x_1)(2x_2 - x_1)$ are given in the table below.

f^*	0	1	2	x_2
0	0	2	4	
1	0	0	0	
2	2	0		
x_1				

2.3 The method of moments

Here, a generalization of the moment equations (1.1) will be proposed. Suppose $\Omega \in \mathbb{H}^d(V)$ is an invariant partition for $\mathbf{b}$, and let $|\Omega| = \omega$. Define W^*_Ω to be the $|\mathbb{H}^d(t)| \times |\mathbb{H}^d(k)|$ matrix indexed by the partitions of t and k, respectively, with

$$W^*_\Omega(\varphi, \psi) = \binom{\omega}{\psi}\binom{\psi}{\varphi}.$$

Then $W^*_\Omega = MD_k$, where $M = \left[\binom{\psi}{\varphi}\right]_{\varphi,\psi}$ has the same dimensions as W^*_Ω and $D_k = \mathrm{diag}\left(\binom{\omega}{\psi}\right)$ is a square diagonal matrix indexed over $\psi \in \mathbb{H}^d(k)$. Let $\mathbf{b}^*$ be the

$|\mathbb{H}^d(t)| \times 1$ vector indexed over $\mathbb{H}^d(t)$ and defined by

$$\mathbf{b}^*(\varphi) = \binom{\omega}{\varphi} b_\varphi,$$

where, as in Theorem 2.3, $b_\varphi = \mathbf{b}(T)$ for any T with $|T \cap \Omega| = \varphi$, and $b_\varphi = 0$ if no such T exists. Invariance under Ω allows for "averaging" Ω-equivalent entries of W and $\mathbf{b}$, as in the previous sections. It follows that $\mathbf{b} \in \mathcal{C}W$ if and only if $\mathbf{b}^* \in \mathcal{C}W^*_\Omega = \mathcal{C}(MD_k)$. And since D_k is diagonal with nonnegative entries, this latter condition is equivalent to $\mathbf{b}^* \in \mathcal{C}M$. A concrete restatement of this is now given.

Theorem 2.7. (Generalized Method of Moments) *With notation as above,* $\mathbf{b} \in \mathcal{C}W_\Omega$ *if and only if there exist nonnegative rational solutions* z_φ *to the equations*

$$\sum_{\psi \in \mathbb{H}^d(k), \psi \leq \omega} \binom{\psi}{\varphi} z_\varphi = \binom{\omega}{\varphi} b_\varphi, \quad \varphi \in \mathbb{H}^d(t).$$

The goal for the rest of this section will be to show that the system of equations in Theorem 2.7 reduces to the moment equations (1.1) when Ω is a bipartition and $\mathbf{b} = \lambda\mathbf{j}$. This will motivate the consideration of the condition $\mathbf{b} \in \mathcal{C}W^v_{tk}$ as a generalization of the method of moments.

Consider the bipartition $\Omega = (H, V \setminus H)$ with $|H| = w$ and $t \leq w \leq v - t$. Suppose that some collection of k-subsets from V has the property that every t-set T is contained in precisely b_h members of this collection, where $h = |T \cap H|$. (From now on, indexing over the ordered bipartitions of, say $s \in \mathbb{N}_0$, will be changed to simply indicate the first coordinate, from 0 to s.) Let z_j be the number of k-subsets in the collection that meet H in exactly j points. The following system of equations holds by the same double-counting proof as was mentioned before equations (1.1).

$$\sum_{j=0}^{k} \binom{j}{i} z_j = \binom{w}{i} \binom{k-i}{t-i}^{-1} \sum_{h=0}^{t} \binom{w-i}{h-i} \binom{v-w}{t-h} b_h, \quad i = 0, 1, \ldots, t. \tag{2.3}$$

Define the vector $\tilde{\mathbf{b}}$ indexed on $\{0, 1, \ldots, t\}$ by $\tilde{\mathbf{b}}(h) = b_h$. Note that when $\tilde{\mathbf{b}} = \lambda\mathbf{j}$, the equation above reduces to (1.1) via equation (1.4). Observe $\mathbf{b}^* = \operatorname{diag}\left(\binom{w}{i}\binom{v-w}{t-i}\right)\tilde{\mathbf{b}}$.

Define

$$N = \left[\binom{j}{i}\right]_{\substack{i\in\{0,1,\ldots,t\}\\ j\in\{0,1,\ldots,k\}}},$$

$$Q = \left[\binom{w-i}{h-i}\binom{v-w}{t-h}\right]_{\substack{i\in\{0,1,\ldots,t\}\\ h\in\{0,1,\ldots,t\}}},$$

and $D = \operatorname{diag}\left(\binom{w}{i}\binom{k-i}{t-i}^{-1}\right)$. Then the existence of nonnegative rational solutions z_j to the equations (2.3) is equivalent to $DQ\tilde{\mathbf{b}} \in \mathcal{C}N$.

For Ω a bipartition, the matrix M defined earlier is

$$M = \left[\binom{j}{i}\binom{k-j}{t-i}\right]_{\substack{i\in\{0,1,\ldots,t\}\\ j\in\{0,1,\ldots,k\}}}.$$

Write M_0 and N_0 for the square submatrices formed from the first $t+1$ columns (indexed by $\{0,1,\ldots,t\} \subset \{0,1,\ldots,k\}$) of M and N respectively. The inverse of M_0 is important for later work and will be calculated in Proposition 3.3. Some simple binomial identities prove that $[N_0^{-1}]_{ij} = (-1)^{i+j}\binom{j}{i}$. From this, computing $M_0N_0^{-1}$ is an easy application of Proposition 1.4.

Lemma 2.8. *With the matrices defined as above,* $[M_0N_0^{-1}]_{ij} = (-1)^{i+j}\binom{j}{i}\binom{k-j}{t-j}$.

The equivalence between the moment equations and the cone condition for W_Ω^* can now be established.

Theorem 2.9. $\mathbf{b}^* \in \mathcal{C}M$ *if and only if* $DQ\tilde{\mathbf{b}} \in \mathcal{C}N$.

Proof: It must be shown that the equations $M\mathbf{z} = \mathbf{b}^*$ and $N\mathbf{z} = DQ\tilde{\mathbf{b}}$ either both have or both do not have nonnegative solutions $\mathbf{z}$ for each choice of $\tilde{\mathbf{b}}$. By Lemma 2.8 and equation (1.4), it follows that $M = M_0N_0^{-1}N$. So, it suffices to prove $M_0N_0^{-1}DQ = \operatorname{diag}(\binom{w}{i}\binom{v-w}{t-i})$. Using Lemma 2.8 again gives

$$M_0N_0^{-1}D = \left[(-1)^{i+j}\binom{w}{j}\binom{j}{i}\right]_{\substack{i\in\{0,1,\ldots,t\}\\ j\in\{0,1,\ldots,t\}}}.$$

Now

$$\begin{aligned}(M_0N_0^{-1}DQ)_{ij} &= \sum_{\ell=i}^{j}(-1)^{i+\ell}\binom{w}{\ell}\binom{\ell}{i}\binom{w-\ell}{j-\ell}\binom{v-w}{t-j} \\ &= \binom{w}{i}\binom{v-w}{t-j}\sum_{\ell=i}^{j}(-1)^{i+\ell}\binom{w-i}{\ell-i}\binom{w-\ell}{j-\ell} \\ &= \binom{w}{i}\binom{v-w}{t-j}\binom{0}{j-i},\end{aligned}$$

by equations (1.3) and (1.5). It is evident that the off-diagonal entries of $M_0N_0^{-1}DQ$ vanish, and the proof is complete. □

Chapter 3

Bipartitions

In general, it is difficult to determine if an arbitrary vector $\mathbf{b} \in \mathbb{R}^{\binom{v}{t}}$ is contained in the cone $\mathcal{C}W^v_{tk}$. Dimensions alone often render this question impractical. However, most design-theoretic applications enjoy abundant symmetry, which is usually prudent to exploit. This chapter will explore, from the point of view of containment in $\mathcal{C}W$, certain structures in t-designs which are most naturally or easily handled by considering a bipartition of the points. There is no intent here to exhaust the possible application of bipartitions to the cone condition. It should also be noted that most inequalities presented here are already known for t-designs. Indeed, the main result of Section 2.3 is an equivalence between the cone condition for bipartitions and the well-studied method of moments, with which any of the results here have either already been proved, or can be proved. Regardless, there are various reasons for considering the cone in this context. It may be interesting to understand a description of the supporting vectors $\mathbf{y}_f$ and associated polynomials f which produce certain inequalities, for instance. And perhaps of most interest is the unification of many inequalities for designs, some of which require finer partitions and are presented later.

3.1 The Raghavarao-Wilson inequality

In [26], the moment equations (1.1) are used with the method of orthogonal projection to prove a family of inequalities concerning block density in t-designs. One result of particular interest is a generalization to t-designs of Raghavarao's upper bound [22]

on the cardinality of the intersection of n blocks in a 2-design. An interesting special case is that a $2s$-(v,k,λ) design with $v \geq k+s$ points having an n-fold repeated block must have at least $n\binom{v}{s}$ total blocks. This generalizes both Mann's inequality [17], in which $s=1$, and Wilson and Ray-Chaudhuri's extension [21] of Fisher's inequality, in which $n=1$. Note that by Proposition 1.1, this condition also holds for t-designs with $t \geq 2s$.

Here, another proof of the generalized Raghavarao inequality for t-designs is given using bipartitions and Theorem 2.3. Like Wilson's original proof, several binomial identities are needed in addition to a family of orthogonal polynomials. For $0 < s \leq k, w \leq v$, define

$$g = g_{s,k}^{w}(x) = \sum_{i=0}^{s} (-1)^{s-i} \frac{\binom{v-s}{i}\binom{w-1-i}{s-i}\binom{k-i}{s-i}}{\binom{s}{i}} \binom{x}{i}.$$

This is a multiple of a (terminating) hypergeometric series of type ${}_3F_2$ with unit argument. Alternate presentations of g arise from hypergeometric identities or facts related to orthogonal polynomials, as is mentioned in [26]. For instance, one has the relations

$$g_{s,k}^{w}(x) = g_{s,w-1}^{k+1}(x) = (-1)^s g_{s,k}^{v-w+1}(k-x) \tag{3.1}$$

and

$$g_{s,k}^{w}(w) = \binom{v}{s}^{-1}\binom{k}{s}\binom{v-w}{s}\sum_{i=0}^{s}\left[\binom{v}{i} - \binom{v}{i-1}\right]\frac{\binom{w}{i}\binom{v-k}{i}}{\binom{k}{i}\binom{v-w}{i}}. \tag{3.2}$$

The following result is equivalent to Corollary 1 of [26] upon application of Proposition 1.1 and equation (3.2).

Theorem 3.1. ([26]) *Let $t \geq 2s$, and suppose $v \geq k+s$. In a t-(v,k,λ) design with a collection $\mathcal{D}$ of n blocks containing w points in their intersection, $(s \leq w \leq v-s)$,*

$$\frac{n}{\lambda} \leq \binom{v}{t}\binom{v}{s}^{-1}\binom{k}{t}^{-1}\binom{k}{s}\binom{v-w}{s}(g_{s,k}^{w}(w))^{-1}. \tag{3.3}$$

Proof: Consider the bipartition $\Omega = (H, V \setminus H)$ of the pointset V, where H is the intersection in question. Then $|\Omega| = (w, v-w)$ and $(x, k-x)$ will be used as the

variables[1] for intersection of a k-set with Ω. The stated inequality will be shown to be equivalent to $\mathbf{y}_f \cdot \mathbf{b} \geq 0$ for $f(x) = (g^w_{s,k}(x))^2$, which is certainly nonnegative on $\{0, 1, \ldots, w\}$, and $\mathbf{b} = \lambda \mathbf{j} - \sum_{B \in \mathcal{D}} \mathbf{e}_B$. The result will then follow by an application of Theorems 2.3 and 2.4. Let $(a_0, \ldots, a_t)$ be such that

$$f(x) = \sum_{j=0}^{t} a_j \binom{x}{j} \binom{k-x}{t-j}$$

and let $F(x) = \sum_{j=0}^{t} a_j \binom{x}{j} \binom{v-x}{t-j}$. Then from $0 \leq \mathbf{y}_f \cdot \mathbf{b} = \lambda F(w) - n f(w)$, it is enough to show that

$$F(w) = g^w_{s,k}(w) \binom{v}{t} \binom{v}{s}^{-1} \binom{k}{t}^{-1} \binom{k}{s} \binom{v-w}{s}. \tag{3.4}$$

Now using equation (3.1),

$$\begin{aligned} f(x) &= (-1)^s g^w_{s,k}(x) g^{v-w+1}_{s,k}(k-x) \\ &= \sum_{r=0}^{t} (-1)^{s-r} \sum_{i} \frac{\binom{v-s}{i}\binom{v-s}{r-i}\binom{k-i}{s-i}\binom{k-r+i}{s-r+i}\binom{w-1-i}{s-i}\binom{v-w-r+i}{s-r+i}}{\binom{s}{i}\binom{s}{r-i}} \binom{x}{i}\binom{k-x}{r-i}, \end{aligned}$$

where the sum on i is from $\max\{0, r-s\}$ to $\min\{r, s\}$. It follows from equation (1.6) with $y = k - x$ that

$$a_j = \sum_{r=0}^{t} (-1)^{s-r} \sum_{i=\max\{0,r-s\}}^{\min\{r,s\}} \frac{\binom{v-s}{i}\binom{v-s}{r-i}\binom{k-i}{s-i}\binom{k-r+i}{s-r+i}\binom{w-1-i}{s-i}\binom{v-w-r+i}{s-r+i}\binom{j}{i}\binom{t-j}{r-i}}{\binom{s}{i}\binom{s}{r-i}\binom{k-r}{t-r}}. \tag{3.5}$$

One now has an expression for $F(x)$ in terms of these coefficients. Applying equation (1.3) and equation (1.6) with $y = v - x$ permits the simplification

$$F(w) = \binom{v-w}{s} \sum_{r=0}^{t} (-1)^{s-r} \frac{\binom{v-r}{t-r}}{\binom{k-r}{t-r}} \sum_{i=0}^{s} \frac{\binom{v-s}{i}\binom{v-s}{r-i}\binom{k-i}{s-i}\binom{k-r+i}{s-r+i}\binom{w-1-i}{s-i}\binom{w}{i}}{\binom{s}{i}}.$$

Changing back the indices of summation with $r = i + j$ and applying equation (1.3)

[1]For convenience, these and future variables will depart from the $x_1, x_2, \ldots$ used in Chapter 2.

again gives

$$F(w) = \frac{\binom{v-w}{s}}{\binom{v-t}{k-t}} \sum_{i,j=0}^{s} (-1)^{s-i-j} \frac{\binom{v-i-j}{k-i-j}\binom{v-s}{i}\binom{v-s}{j}\binom{k-i}{s-i}\binom{k-j}{s-j}\binom{w-1-i}{s-i}\binom{w}{i}}{\binom{s}{i}}.$$

The summation indexed by j is handled directly by Lemma 1.6. So one has

$$\begin{aligned} F(w) &= \frac{\binom{v-w}{s}\binom{v-s}{k-s}}{\binom{v-t}{k-t}} \sum_{i=0}^{s} (-1)^{s-i} \frac{\binom{v-s}{i}\binom{k-i}{s-i}\binom{w-1-i}{s-i}\binom{w}{i}}{\binom{s}{i}} \\ &= \binom{v}{t}\binom{k}{s}\binom{k}{t}^{-1}\binom{v}{s}^{-1}\binom{v-w}{s} g_{s,k}^{w}(w), \end{aligned}$$

as required, where two more applications of (1.3) have been used. □

It should be noted that Theorem 3.1 applied to the supplement of the given design produces a bound on the size of a union of n blocks, or the size of a set disjoint from each of n blocks (Corollaries 2 and 3 of [26].) When $w = k$ in the theorem, equation (3.2) recovers the generalization of Mann's inequality.

Corollary 3.2. ([26]) *Let $t \geq 2s$, and suppose $v \geq k + s$. In a t-(v, k, λ) design with an n-fold block,*

$$\frac{n}{\lambda} \leq \binom{v}{t}\binom{k}{t}^{-1}\binom{v}{s}^{-1}. \tag{3.6}$$

For equality to hold in (3.3), the given supporting vector $\mathbf{y}_f$ must annihilate all characteristic vectors of blocks $\mathbf{e}_B$ of the design which are not among the n given blocks. Lemma 2.2 then implies that there are at most s possible intersection sizes for a pair of different blocks, and these are the roots of $g_{s,k}^{w}(x)$. It is shown in [21] that *at least* $s + 1$ intersection sizes occur in any $2s$-design. Thus, the roots of $g_{s,k}^{w}$ being integral and distinct forms a surprisingly stringent necessary condition for the existence of designs meeting the bound with equality. This observation has essentially been used, for example, to disprove [20] the existence of any *tight* 6-designs. Better understanding the distribution of roots of these polynomials would appear to be a crucial step toward more sophisticated inequalities and nonexistence results for designs.

3.2 Enclosings of designs

An *enclosing* of a t-(w,k,λ') design $(U,\mathcal{B}')$ is a t-(v,k,λ) design $(V,\mathcal{B})$ such that $U \subseteq V$ and $\mathcal{B}'$ is a subcollection of $\mathcal{B}$. When $w = k$ and $\lambda' = n$, this is equivalent to the existence of an n-fold block in a t-(v,k,λ) design. Since this case is of particular interest, it will be considered in further detail here and in the next section. It should be noted that the inequalities in Theorem 3.1 and Corollary 3.2 apply to enclosings and n-fold blocks via the polynomials $g^k_{s,w}(x)$. The spirit of this section is that the facet-defining polynomials of Theorem 2.6 can be used to obtain sharper inequalities for enclosings. In fact, one obtains necessary and sufficient conditions for $\lambda\mathbf{j} - \lambda'\mathbf{e}_U$ to belong to $\mathcal{C}W$, since this vector is invariant under a bipartition. It is worth mentioning that improvements to Theorem 3.1, though sporadic and not in general optimal, can also be obtained in a similar manner.

In what follows, the cleaner case of t even will be assumed when necessary. Recall from Section 2.3 the $(t+1) \times (k+1)$ matrix

$$M = \left[\binom{j}{i} \binom{k-j}{t-i} \right]_{\substack{i \in \{0,1,\ldots,t\} \\ j \in \{0,1,\ldots,k\}}}.$$

By the discussion in Chapter 2, supporting vectors of $\mathcal{C}W_{(U,V\setminus U)}$ are of the form

$$\mathbf{y} = \sum_{i=0}^{t} a_i \sum_{|T \cap U| = i} \mathbf{e}_T,$$

where $\mathbf{a} = (a_0, a_1, \ldots, a_t) \neq \mathbf{0}$ is such that $\mathbf{a}M \geq \mathbf{0}$. The corresponding polynomial is

$$f(x) = \sum_{i=0}^{t} a_i \binom{x}{i} \binom{k-x}{t-i},$$

which supports a facet by Theorem 2.6 if and only if f vanishes on a good subset $Z \subset \{0,1,\ldots,k\}$ of size t, and has $f(r) > 0$ for any $r \in \{0,1,\ldots,k\} \setminus Z$. Let M_Z denote a square submatrix of M formed from the columns indexed by $Z^* = Z \cup \{r\}$, for some good Z and $r \notin Z$. (In many cases, $0 \notin Z$, and $r = 0$ is a nice choice for

the computations which follow.) Any $t+1$ columns of M are linearly independent, so the facets are simply described (up to a positive multiple) by the vector $(M_Z^{-1})_r$, i.e., the row of M_Z^{-1} indexed by r.

For interest, the task of computing these facets explicitly will now be briefly considered. Following the convention in Section 2.2, define $M_0 = M_{\{1,\ldots,t\}}$ (with "positive coordinate" taken arbitrarily to be $r = 0$).

Proposition 3.3.

$$(M_0)^{-1} = \left[(-1)^{i+j} \frac{k-t}{k-t+j-i} \binom{j}{i} \binom{k-i}{t-j}^{-1} \right]_{i,j \in \{0,1,\ldots,t\}}.$$

Proof: Both M_0 and the given matrix are upper triangular, so it suffices to consider inner products of row i of M_0 with column j of the asserted inverse when $i \le j$. For $i = j$, this is evidently equal to

$$\sum_{\ell=0}^{t} (-1)^{\ell+i} \binom{\ell}{i} \binom{i}{\ell} \binom{k-\ell}{t-i} \frac{k-t}{k-t-\ell+i} \binom{k-\ell}{t-j}^{-1} = (-1)^{2\ell} \frac{k-t}{k-t} = 1.$$

For $i < j$, the inner product is

$$\begin{aligned} & (k-t) \binom{j}{i} \binom{t-i}{t-j}^{-1} \sum_{\ell=i}^{j} (-1)^{\ell+j} \frac{1}{k-\ell-t+j} \binom{j-i}{\ell-i} \binom{k-\ell-t+j}{j-i} \\ = \; & \frac{k-t}{j-i} \binom{j}{i} \binom{t-i}{t-j}^{-1} \sum_{\ell=i}^{j} (-1)^{\ell+j} \binom{j-i}{\ell-i} \binom{k-\ell-t+j-1}{k-\ell-t+i} \\ = \; & \frac{k-t}{j-i} \binom{j}{i} \binom{t-i}{t-j}^{-1} \binom{k-t-1}{k-t} = 0, \end{aligned}$$

where equation (1.3) is used three times along with the summation identity (1.5). □

Now the matrix $(M_Z)^{-1}$ can, in principle, be computed for general Z by making use of the $(t+1) \times (t+1)$ *Vandermonde matrix* V_Z defined by $V_Z(i,j) = j^i$, where $i \in \{0,1,\ldots,t\}$ and $j \in Z^*$. Observe that $M_Z = EV_Z$, where E is defined by the polynomial equations

$$\binom{x}{i} \binom{k-x}{t-i} = \sum_{\ell=0}^{t} E_{i\ell} x^{\ell}.$$

Now

$$M_Z^{-1} = V_Z^{-1}E^{-1} = V_Z^{-1}V_{\{1,\ldots,t\}}M_0^{-1}.$$

By Proposition 3.3 and a known formula [15] for the inverse of a general Vandermonde matrix, the required row of M_Z^{-1} can be expressed concretely, if desired. All facets for a bipartition arise in this way.

Theorem 3.4. *Suppose $t \le |U| = w \le v$. Then $\lambda\mathbf{e}_V - \lambda'\mathbf{e}_U \in \mathcal{C}W_{tk}^v$ if and only if, for all good t-sets $Z \subset \{0,1,\ldots,k\}$ and some $r \notin Z$,*

$$\frac{\lambda'}{\lambda} \le \frac{\sum_{j=0}^t (M_Z^{-1})_{rj}\binom{w}{j}\binom{v-w}{t-j}}{(M_Z^{-1})_{rt}\binom{w}{t}}.$$

Proof: By Theorems 2.3 and 2.6, $\lambda\mathbf{e}_V - \lambda'\mathbf{e}_U \in \mathcal{C}W$ if and only if $\mathbf{y}_Z \cdot (\lambda\mathbf{e}_V - \lambda'\mathbf{e}_U) \ge 0$ for all good $Z \subset \{0,1,\ldots,k\}$, where $\mathbf{y}_Z = \sum_{i=0}^t (M_Z^{-1})_{ri} \sum_{|T\cap U|=i} \mathbf{e}_T$. The result follows upon observing that $\mathbf{y}_Z \cdot \mathbf{e}_U = (M_Z^{-1})_{rt}\binom{w}{t}$ and

$$\mathbf{y}_Z \cdot \mathbf{e}_V = \mathbf{y}_Z \cdot \mathbf{j} = \sum_j (M_Z^{-1})_{rj}\binom{w}{j}\binom{v-w}{t-j}.$$

□

Note that, for some constant C depending on the choice of $r \in \{0,1,\ldots,t\} \setminus Z$,

$$C\prod_{\zeta\in Z}(x-\zeta) = \sum_{j=0}^t (M_Z^{-1})_{rj}\binom{x}{j}\binom{k-x}{t-j}.$$

When some such r is understood, define

$$F_Z(x) = \sum_{j=0}^t (M_Z^{-1})_{rj}\binom{x}{j}\binom{v-x}{t-j}.$$

The following nonexistence result, first proved by Delsarte in [6], is a rather striking use of Theorem 3.4.

Example 3.1. There does not exist a 4-$(17,8,5)$ design. For these parameters, one has $f(x) = g_{2,k}^k(x)^2 \approx C(x-2.48)^2(x-4.52)^2$ for some constant C. Suppose there is an

n-fold block B, and consider the test of $\lambda\mathbf{j}-n\mathbf{e}_B \in \mathcal{C}W^v_{4k}$. From the supporting vector $\mathbf{y}_f$, the Wilson-Mann bound of $n/\lambda \leq 1/4$ results, which permits $n = 1$. Instead, consider the polynomial $(x-2)(x-3)(x-4)(x-5)$. The bound from $F_{\{2,3,4,5\}}(k)$ in Theorem 3.4 is $n/\lambda < 4/25$. This rules out even $n = 1$. In other words, a design with these parameters cannot exist.

In general, the upper bound on λ'/λ from Theorem 3.4 is obtained by minimizing a certain quantity with respect to Z. Some preliminary steps toward understanding the optimum such Z will now be presented.

Example 3.2. When $t = 2$, the only possible extremal polynomials (up to a positive multiple) are $x(k-x)$ or $(x-c)(x-c-1)$ for some $c = 0, \ldots, k-1$. The various cases for Z and corresponding facet weights a_0, a_1, a_2 are computed and presented in the table below.

Z	a_0	a_1	a_2
$\{k-1, k\}$	1	0	0
$\{0, k\}$	0	1	0
$\{0, 1\}$	0	0	1
$\{c, c+1\}$	$\frac{c+1}{k-c-1}$	-1	$\frac{k-c}{c}$

Note the last line in the table is for $1 \leq c \leq k-2$, and this case yields the only nontrivial family of facets for $\mathcal{C}W^v_{2k}$ that are invariant under a bipartition.

Corollary 3.5. *Suppose $t \leq |U| = w < v-1$. Then $\lambda\mathbf{j} - \lambda'\mathbf{e}_U \in \mathcal{C}W^v_{2k}$ if and only if*

$$\frac{\lambda'}{\lambda} \leq \frac{c(c+1)(v-w)(v-w-1)}{(k-c)(k-c-1)w(w-1)} - \frac{2c(v-w)}{(k-c)(w-1)} + 1,$$

where

$$c = \left\lfloor \frac{w(k-1)}{v-1} \right\rfloor.$$

Proof: Using the table above, a concrete restatement of Theorem 3.4 for $t = 2$ is

$$\frac{\lambda'}{\lambda} \leq \min_{c=1,\ldots,k-2} \frac{\frac{c+1}{k-c-1}\binom{v-w}{2} - w(v-w) + \frac{k-c}{c}\binom{w}{2}}{\frac{k-c}{c}\binom{w}{2}}. \tag{3.7}$$

(Note that the other three facets give no meaningful bound on λ'/λ.) Now, let $c \in (0, k-1)$ be a continuous parameter, and define $h(c)$ to be the rational function in c on the right side of (3.7). Using calculus and some factoring, the minimum of h on $(0, k-1)$ is seen to be achieved at

$$c_0 = \frac{(k-1)(v+w-1) - \sqrt{(k(v-w-1)+w)^2 - (v-1)^2}}{2(v-1)}.$$

The square root lies in the open interval with endpoints $k(v-w-1)+w \pm (v-1)$. After some simplification, it follows that $c_0 \in (\gamma - 1, \gamma)$, where $\gamma = \frac{w(k-1)}{v-1}$. Now the function h is strictly decreasing on $(0, c_0)$ and strictly increasing on $(c_0, k-1)$. Furthermore, a calculation shows $h(\gamma-1) = h(\gamma)$. So, the (1 or 2) integers in $(0, k-1)$ which minimize h must belong to the interval $[\gamma - 1, \gamma]$. Thus over integers, $h(c)$ is minimized at $c = \lfloor \gamma \rfloor$. □

Remarks: For $w = v - 1$, the inequality in (3.7) reduces to

$$\frac{\lambda'}{\lambda} \leq \min_{c=1,\ldots,k-2} 1 - \frac{2c}{(k-c)(v-2)} = 1 - \frac{k-2}{v-2}. \tag{3.9}$$

Enclosings with $w = v - 1$ are said to be *minimal*, and the smallest gap between λ' and λ is of interest. Some nice constructions of such enclosings for $t = 2$ and $k = 3$ are found in [13], along with an alternate proof of the bound in (3.9). Similar inequalities concerning enclosings of *group divisible designs* are considered (along with several constructions) in work in progress by Hurd, Purewal, and Sarvate, and these bounds can also be proved with a modification of Corollary 3.5.

It is interesting to note that γ above is the root of $g^k_{1,w}(x) = (v-1)x - w(k-1)$. Roughly speaking, a sharper inequality results because, in the cone of quadratics nonnegative on $\{0, 1, \ldots, k\}$, the polynomial $(x-\gamma)^2$ is closest to the extremal ray generated by $(x - \lfloor \gamma \rfloor)(x - \lfloor \gamma \rfloor - 1)$. In fact, it seems more generally that among *square* polynomials, the optimal bounds for enclosings arise from supporting vectors $\mathbf{y}_f$ of $\mathcal{C}W$ corresponding to $f(x) = (g^k_{s,w}(x))^2$. But curiously, Corollary 3.5 fails for $t \geq 4$ in the sense that it is *not* always the case that the minimizing good set Z of

Theorem 3.4 is obtained from the floor and ceiling of the roots of $g^k_{s,w}$; however, such sets appear to be "very close" to optimal. See Figure 3.1.

Example 3.3. Consider upper bounds on n/λ, where it is assumed that there exists an n-fold block in a 4-$(24, 12, \lambda)$ design. With $v = 24$,

$$g^{12}_{2,12}(x) = \frac{11}{2}(21x^2 - 241x + 660) \approx C(x - 4.51)(x - 6.96).$$

However, $F_{\{4,5,6,7\}}(w) \geq F_{\{4,5,7,8\}}(w)$.

When $k-t$ is small, the choices for Z are limited. In such cases, it may be possible to obtain, in closed form, a reasonable bound from Theorem 3.4. One such example is given next.

Corollary 3.6. *Let $t = 2s$. In a t-$(2t + 2, t + 1, \lambda)$ design with an n-fold block,*

$$n(t + 2) \leq 2\lambda.$$

Proof: This follows from Theorem 3.4 with $Z^* = \{0, 1, \ldots, t\}$, $w = k = t + 1$ and $\lambda' = n$. By Proposition 3.3 and equation (1.3), it follows that

$$(M_Z^{-1})_{0j} = (-1)^j \frac{1}{j+1}\binom{t+1}{j+1}^{-1} = (-1)^j \frac{1}{t+1}\binom{t}{j}^{-1}.$$

So

$$\begin{aligned} \frac{n}{\lambda} &\leq \frac{1}{\binom{t+1}{t}} \sum_{j=0}^{t} (-1)^j \binom{t}{j}^{-1} \binom{t+1}{j} \binom{t+1}{t-j} \\ &= \left(\frac{1}{t+1}\right) \frac{2(t+1)}{2t+2-t} = \frac{2}{t+2}, \end{aligned}$$

where equation (1.8) is invoked to simplify the sum. □

Remarks: This inequality is actually strict, because the associated supporting vector fails to annihilate t-sets fully contained in the specified block or its complement. Note that the Wilson-Mann inequality, Corollary 3.2, applied to a design with these

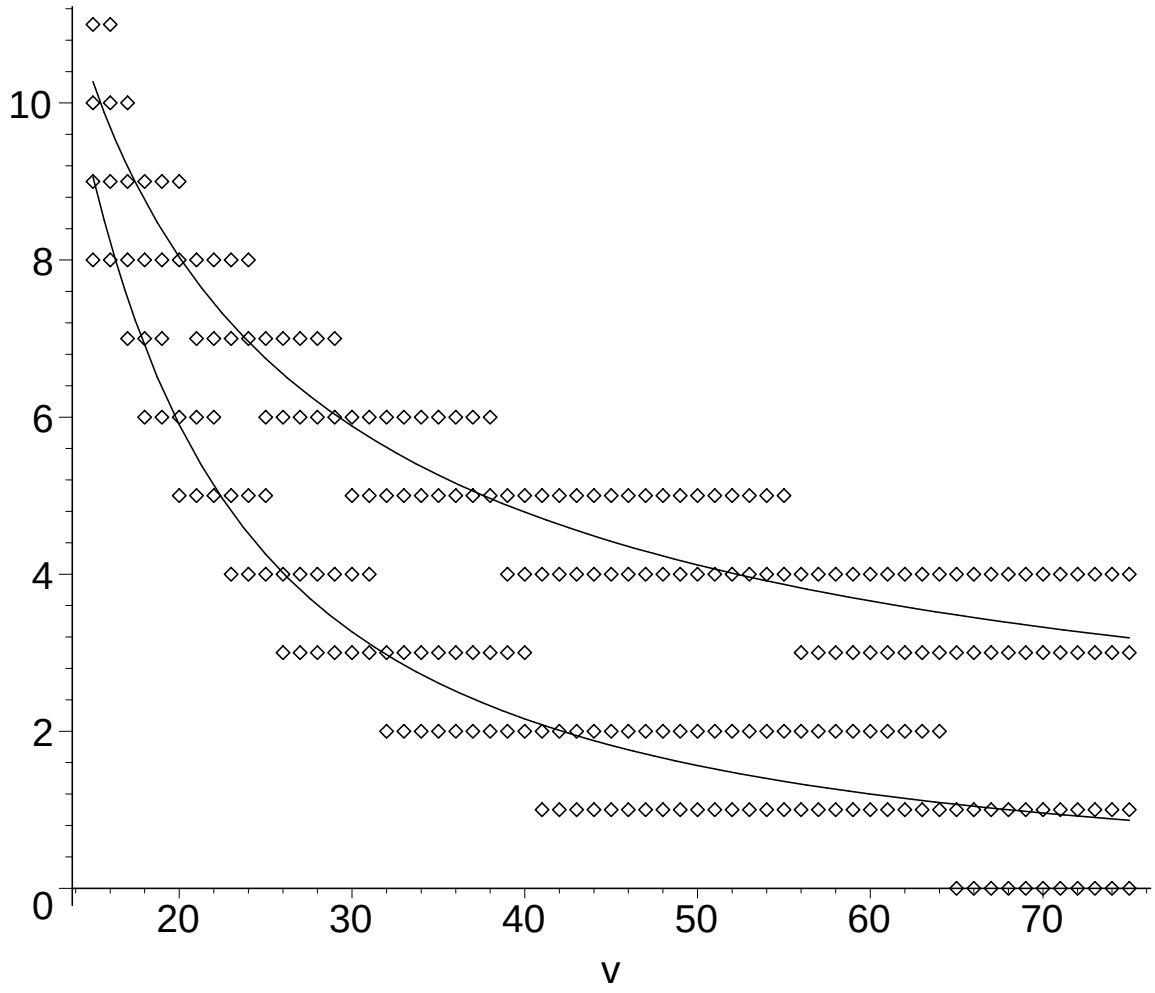


Figure 3.1: Optimal roots ($\diamond$) with roots of $g^k_{s,k}$ for $t = 4$, $k = 12$ and $15 \leq v \leq 75$.

parameters is the weaker statement

$$\frac{n}{\lambda} \leq \frac{\binom{2t+2}{t}}{(t+1)\binom{2t+2}{s}}.$$

It should be said, however, that Delsarte's inequalities [6] have been recently applied by Chan and Wilson to small $k-t$ and $n=1$ to obtain much stronger bounds than possible from Theorem 3.4.

3.3 Tables for n-fold blocks

Consider here the existence of an n-fold block in a t-(v,k,λ) design. For $t=2$, Corollary 3.5 provides, in closed form, the most strict upper bound on n/λ possible from the cone condition. However, the situation is less clear for $t>2$, as illustrated by Example 3.3. By automating Theorem 3.4 on computer, the best bound has been computed on n/λ in t-(v,k,λ) designs with an n-fold block for $t=4,6,8$, $t+1\leq k\leq 12$, and $2k\leq v\leq 24$. In the tables which follow, the entry "$\lambda_{\min}$" is the smallest positive integer λ satisfying the divisibility requirements of Proposition 1.1 for a given t,k,v. Any other such admissible λ must, of course, be a positive multiple of $\lambda_{\min}$. The column labeled "$n\leq$" gives the sharpest bound from Theorem 3.4 with $\lambda=\lambda_{\min}$, and the corresponding optimal vanishing set Z is included in the adjacent column. A missing parameter pair (v,k) within range indicates that the cone condition permits $n=\lambda$ in that case, thereby yielding no information. Note that for all t,k, this eventually occurs for sufficiently large v.

The smallest parameter pair $(v,k)=(2t+2,t+1)$ in each table corresponds to the case in Corollary 3.6. For other examples, the $t=4$ table says that every 4-$(23,11,12)$ design is simple, while the $t=6$ table asserts the nonexistence of 6-$(19,9,2)$ and 6-$(20,10,7)$ designs. The information in Examples 3.1 and 3.3 also appears in the $t=4$ table.

v	k	$\lambda_{\min}$	$n \leq$	Z	v	k	$\lambda_{\min}$	$n \leq$	Z
10	5	6	2	$1,2,3,4$	21	8	70	25.06	$1,2,3,4$
12	6	2	0.6	$1,2,3,4$	22	8	30	10.6	$1,2,3,4$
13	6	6	1.8	$1,2,3,4$	23	8	2	0.7143	$1,2,3,4$
14	6	15	5.4	$1,2,3,4$	24	8	5	1.857	$1,2,3,4$
15	6	5	2.6	$1,2,3,4$	18	9	14	1.6	$3,4,5,6$
16	6	6	5	$1,2,3,4$	19	9	21	3.143	$2,3,5,6$
14	7	20	3.6	$2,3,4,5$	20	9	168	29.71	$2,3,4,5$
15	7	5	1.8	$1,2,3,4$	21	9	14	2.429	$2,3,4,5$
16	7	20	6.8	$1,2,3,4$	22	9	252	46.23	$2,3,4,5$
17	7	2	0.6667	$1,2,3,4$	23	9	18	3.8	$2,3,4,5$
18	7	28	9.667	$1,2,3,4$	24	9	24	5.75	$1,2,4,5$
19	7	35	13.4	$1,2,3,4$	20	10	28	2.857	$3,4,5,6$
20	7	140	63.73	$1,2,3,4$	21	10	28	2.857	$3,4,5,6$
21	7	10	5.733	$1,2,3,4$	22	10	42	5	$3,4,5,6$
22	7	4	3	$1,2,3,4$	23	10	42	5.321	$2,3,5,6$
16	8	15	2.4	$2,3,4,5$	24	10	60	8.375	$2,3,5,6$
17	8	5	0.8	$2,3,4,5$	22	11	72	5.439	$3,4,6,7$
18	8	7	1.333	$2,3,4,5$	23	11	6	0.4786	$3,4,6,7$
19	8	105	28	$2,3,4,5$	24	11	120	11.17	$3,4,6,7$
20	8	70	22.05	$1,2,4,5$	24	12	15	0.9571	$4,5,7,8$

Table 3.1: $t = 4$.

v	k	$\lambda_{\min}$	$n \leq$	Z	v	k	$\lambda_{\min}$	$n \leq$	Z
14	7	4	1	$1,2,3,4,5,6$	23	9	20	6.5	$1,2,3,4,5,6$
16	8	15	3.429	$1,2,3,4,5,6$	24	9	24	10.25	$1,2,3,4,5,6$
17	8	5	1.143	$1,2,3,4,5,6$	20	10	7	0.7143	$2,3,4,5,6,7$
18	8	6	1.714	$1,2,3,4,5,6$	21	10	105	10.71	$2,3,4,5,6,7$
19	8	6	2.857	$1,2,3,4,5,6$	22	10	70	8.929	$2,3,4,5,6,7$
20	8	7	6.571	$1,2,3,4,5,6$	23	10	70	14.29	$2,3,4,5,6,7$
18	9	20	2.286	$2,3,4,5,6,7$	24	10	90	27.08	$1,2,3,4,5,6$
19	9	2	0.5714	$1,2,3,4,5,6$	22	11	168	10.71	$3,4,5,6,7,8$
20	9	28	7.571	$1,2,3,4,5,6$	23	11	14	1.611	$2,3,4,5,7,8$
21	9	35	9.286	$1,2,3,4,5,6$	24	11	252	29.76	$2,3,4,5,6,7$
22	9	280	78.04	$1,2,3,4,5,6$	24	12	42	2.381	$3,4,5,6,7,8$

Table 3.2: $t = 6$.

v	k	$\lambda_{\min}$	$n \leq$	Z
18	9	10	2	$1,2,3,4,5,6,7,8$
20	10	6	1.111	$1,2,3,4,5,6,7,8$
21	10	6	1.111	$1,2,3,4,5,6,7,8$
22	10	7	1.667	$1,2,3,4,5,6,7,8$
23	10	105	47.22	$1,2,3,4,5,6,7,8$
22	11	28	2.222	$2,3,4,5,6,7,8,9$
23	11	35	8.333	$1,2,3,4,5,6,7,8$
24	11	280	63.33	$1,2,3,4,5,6,7,8$
24	12	70	5	$2,3,4,5,6,7,8,9$

Table 3.3: $t = 8$.

Chapter 4

Finer Partitions

The goal of the last chapter was a fairly thorough investigation of facets and inequalities obtained from $\mathcal{C}W$ by using an automorphism that induces a bipartition of the points. Especially from the point of view of design configurations, this is a rather limited approach. Here, finer invariant partitions are considered. The primary focus will again be applications to t-designs. The first section shows how a classical result on the intersection size of two blocks (and its generalization due to Wilson) follows from partitions of size four. Still finer partitions are then used to study uniform intersection of three blocks in a 2-design.

4.1 The Connor-Wilson inequalities

Suppose in a t-(v, k, λ) design that two blocks B_1 and B_2 intersect in μ points. In [27], Wilson establishes conditions on μ generalizing Connor's inequalities [5], which give upper and lower bounds on μ for $t = 2$. Here, Wilson's result is reproduced with the cone condition. The t-vector under consideration is $\mathbf{b} = \lambda\mathbf{j} - \mathbf{e}_{B_1} - \mathbf{e}_{B_2}$, in which every entry is either $\lambda, \lambda-1$, or $\lambda-2$. Such $\mathbf{b}$ are clearly invariant under the partition

$$\Omega = (B_1 \setminus B_2, B_2 \setminus B_1, B_1 \cap B_2, V \setminus (B_1 \cup B_2)) .$$

It is required to consider polynomials $f(x_1, x_2, y)$ in three variables which are non-negative on $0 \leq x_1, x_2 \leq k - \mu$, $0 \leq y \leq \mu$, and $x_1 + x_2 + y \leq k$.

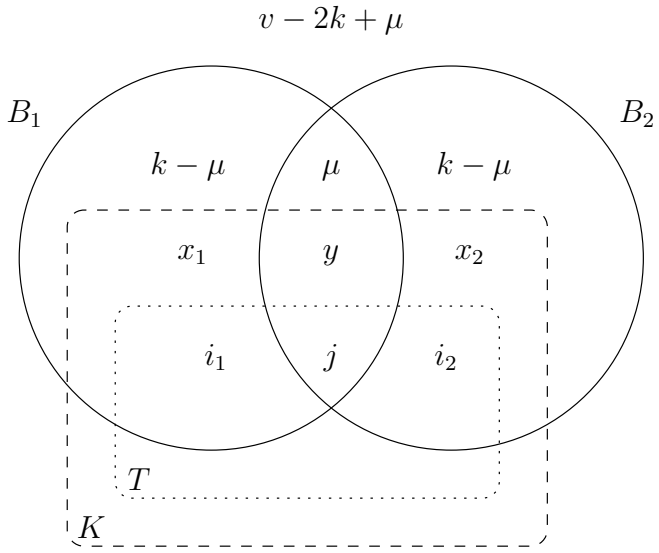


Figure 4.1: Cardinalities for a typical k-set K and t-set T meeting B_1, B_2.

The polynomials from Chapter 3 will play an important role once again. To simplify notation, define $g_s(x) = g^k_{s,k}(x)$.

Theorem 4.1. ([27]) *Let $t \geq 2s$, and suppose $v \geq k + s$. In a t-(v, k, λ) design with two blocks intersecting in μ points,*

$$\binom{k}{s}\binom{v-k}{s} \pm g_s(\mu) \leq \lambda \binom{v}{t}\binom{v}{s}^{-1}\binom{k}{t}^{-1}\binom{k}{s}\binom{v-k}{s}. \tag{4.1}$$

Proof: Theorem 2.3 is used with the partition described above and the (nonnegative) polynomials $f(x_1, x_2, y) = [g_s(x_1 + y) \pm g_s(x_2 + y)]^2$. For $\{p, q\} \subset \{1, 2\}$, define the weights $a_{pq}(i_1, i_2, j)$ by

$$g_s(x_p + y)g_s(x_q + y) = \sum_{0 \leq i_1 + i_2 + j \leq t} a_{pq}(i_1, i_2, j)\binom{x_1}{i_1}\binom{x_2}{i_2}\binom{y}{j}\binom{k - x_1 - x_2 - y}{t - i_1 - i_2 - j}.$$

It is immediate that $a_{12}(i_1, i_2, j) = a_{12}(i_2, i_1, j)$ and $a_{11}(i_1, i_2, j) = a_{11}(i_1, i_2', j)$ for any i_2, i_2', and similarly for a_{22} with i_1, i_1'. Define

$$a(i_1, i_2, j) = a_{11}(i_1, i_2, j) + a_{22}(i_1, i_2, j) \pm 2a_{12}(i_1, i_2, j).$$

The condition $\mathbf{y}_f \cdot \mathbf{b} \geq 0$ is seen to be equivalent to

$$\left[\sum_{i_1+j=t, i_2=0} + \sum_{i_2+j=t, i_1=0}\right] A(i_1, i_2, j) \leq \lambda \sum_{0 \leq i_1+i_2+j \leq t} A(i_1, i_2, j), \tag{4.2}$$

where

$$A(i_1, i_2, j) = a(i_1, i_2, j)\binom{k-\mu}{i_1}\binom{k-\mu}{i_2}\binom{\mu}{j}\binom{v-2k+\mu}{t-i_1-i_2-j}.$$

It remains to simplify the sums on the left and right sides of this inequality, which will be denoted by Σ^L and Σ^R, respectively. Define Σ^L_{pq} and Σ^R_{pq} to be these sums with "a_{pq}" taking the place of "a," so that $\Sigma^L = \Sigma^L_{11} + \Sigma^L_{22} \pm 2\Sigma^L_{12}$, and similarly for Σ^R. It is a straightforward observation that

$$\Sigma^L_{11} = \Sigma^L_{22} = (g_s(k))^2 + (g_s(\mu))^2 \text{ and } \Sigma^L_{12} = 2g_s(k)g_s(\mu).$$

And computing as in the proof of Theorem 3.1 yields

$$\Sigma^R_{11} = \Sigma^R_{22} = \binom{v}{t}\binom{v}{s}^{-1}\binom{k}{t}^{-1}(g_s(k))^2, \quad \Sigma^R_{12} = \binom{v}{t}\binom{v}{s}^{-1}\binom{k}{t}^{-1} g_s(k)g_s(\mu).$$

The inequality (4.2) can now be rewritten as

$$2(g_s(k) \pm g_s(\mu))^2 \leq \lambda\binom{v}{t}\binom{v}{s}^{-1}\binom{k}{t}^{-1} 2g_s(k)(g_s(k) \pm g_s(\mu)).$$

Canceling $2(g_s(k) \pm g_s(\mu))$, which is evidently positive if the inequality holds, and using the ${}_2F_1$ identity $g_s(k) = \binom{k}{s}\binom{v-k}{s}$ completes the proof. □

Remarks: The case $\mu = k$ of the above reduces to the case $n = 2$ of Corollary 3.2. In general, however, Theorem 4.1 is a more stringent condition on μ than Theorem 3.1 is on w for $n = 2$. When $t = 2$, Theorem 4.1 reduces (after some arithmetic) to Connor's inequalities for a pair of blocks:

$$k - \lambda\left(\frac{v-k}{k-1}\right) \leq \mu \leq \frac{2k(k-1)}{v-1} - k + \lambda\left(\frac{v-k}{k-1}\right). \tag{4.3}$$

The left inequality results from the polynomial with the "$-$" sign and the right

inequality arises from the polynomial with the "+" sign.

It is of interest when equality occurs in the bounds of this section. By Lemma 2.2, this happens for bounds corresponding to f if and only if for every block B distinct from B_1 and B_2 with $|B \cap \Omega| = (x_1, x_2, y, k - x_1 - x_2 - y)$, it is the case that $f(x_1, x_2, y) = 0$. So the lower bound of (4.3) is met with equality if and only if $g_1(x_1 + y) - g_1(x_2 + y) = 0$ for every block B meeting the partition as above. Since g_1 is linear, this is simply equivalent to $x_1 = x_2$. Therefore, equality results in the lower bound of Connor's inequalities for $\mu = |B_1 \cap B_2|$ if and only if every other block meets the given pair of blocks in the same number of points. In this case, there are only two possible intersection sizes in the 2-design for a disjoint pair of blocks. This observation was first made by Majindar [16]. Similarly, equality occurs in the upper bound of (4.3) if and only if $g_1(x_1+y)+g_1(x_2+y) = 0$, or $|B\cap B_1|+|B\cap B_2| = 2k(k-1)/(v-1)$ for all B distinct from B_1 and B_2. The following gives a flavor of the conditions for equality when $t > 2$.

Proposition 4.2. *When $t = 4$, equality occurs in the "−" bound of Theorem 4.1 if and only if, for every block B distinct from B_1 and B_2, either*

(i) $|B \cap B_1| = |B \cap B_2|$ *or*

(ii) $|B \cap B_1| + |B \cap B_2| = 1 + \frac{2(k-1)(k-2)}{v-3}$.

Proof: This follows from the remarks above with the factorization

$$g_2(x_1 + y) - g_2(x_2 + y) = \frac{1}{4}(v - 2)(x_1 - x_2)\left(x_1 + x_2 + 2y - 1 - \frac{2(k-1)(k-2)}{v-3}\right).$$

(By comparison, the polynomial $g_2(x_1 + y) + g_2(x_2 + y)$ does not split in $\mathbb{R}[x_1, x_2, y]$.)

□

With only a minor modification to the proof of Theorem 4.1, a generalization to blocks with higher multiplicity follows.

Theorem 4.3. *Let $t \geq 2s$ and suppose $v \geq k + s$. Suppose in a t-(v, k, λ) design that*

an n-fold block B_1 meets the (different) block B_2 in μ points. Then

$$n\binom{k}{s}\binom{v-k}{s} \pm g_s(\mu) \leq \lambda\binom{v}{t}\binom{v}{s}^{-1}\binom{k}{t}^{-1}\binom{k}{s}\binom{v-k}{s}. \tag{4.4}$$

Note that this result can be applied to the intersection of an n_1-fold block with a distinct n_2-fold block upon multiplication by n_2. Undoubtedly, inequalities concerning the still more general $\mathbf{b} = \lambda\mathbf{j} - n_1\mathbf{e}_{W_1} - n_2\mathbf{e}_{W_2}$ for $s \leq |W_1|, |W_2| \leq v - s$ can be established by merging the proofs of Theorems 3.1 and 4.1.

4.2 Examples from linear programming

The polynomials used to establish Theorem 4.1 are squares; hence they do not define facets of $\mathcal{C}W$. As before, tighter inequalities arise from facets, but at the expense of losing a concise closed form. Rather than looking for the best extremal polynomials in several variables, the approach will be to find optimal facets of $\mathcal{C}W$ using linear programming. Computational restrictions will force this discussion to the case $t = 2$.

First, consider bounds on the intersection μ of two blocks B_1, B_2 in a 2-(v, k, λ) design. The vector $\mathbf{b} = \lambda\mathbf{j} - \mathbf{e}_{B_1} - \mathbf{e}_{B_2}$ is invariant under the partition Ω of size four described in the last section. The further symmetry between $B_1 \setminus B_2$ and $B_2 \setminus B_1$ allows a reduction to the seven orbits of pairs, or edges, described below.

edge orbit for $\{x, y\}$	$x \in$	$y \in$	number of edges
E_1	$(B_1 \cup B_2)^c$	$(B_1 \cup B_2)^c$	$\binom{v-2k+\mu}{2}$
E_2	$B_1 \triangle B_2$	$(B_1 \cup B_2)^c$	$2(k-\mu)(v-2k+\mu)$
E_3	$B_1 \cap B_2$	$(B_1 \cup B_2)^c$	$\mu(v-2k+\mu)$
E_4	$B_1 \setminus B_2$	$B_2 \setminus B_1$	$(k-\mu)^2$
E_5	$B_i \setminus B_j$	$B_i \setminus B_j$	$2\binom{k-\mu}{2}$
E_6	$B_1 \cap B_2$	$B_1 \triangle B_2$	$2\mu(k-\mu)$
E_7	$B_1 \cap B_2$	$B_1 \cap B_2$	$\binom{\mu}{2}$

It is a linear programming problem to determine edge weights $a_1, \ldots, a_7$ so that the 2-vector $\mathbf{y} = \sum_{i=1}^{7} a_i \sum_{T \in E_i} \mathbf{e}_T$ minimizes the quantity $\mathbf{y} \cdot \mathbf{b}$ subject to some normalization (say $a_1 = 1$) and the constraints $\mathbf{y} \cdot \mathbf{e}_K \geq 0$ for all k-sets K. If this minimum is negative for some v, k, λ, μ, it follows that any 2-(v, k, λ) design cannot have two blocks with intersection μ. The table below summarizes the results of implementing this on computer for various small parameters. The columns labeled "Connor" and "L.P." give intervals for allowable μ from Connor's inequalities and the linear programming bound, respectively. By Theorem 4.1, the latter range on is always contained in the former.

v	k	λ	Connor	L.P.	v	k	λ	Connor	L.P.
6	3	2	$[0,2]$	$[1,2]$	22	8	4	$[0,5]$	$[0,4]$
8	4	3	$[0,3]$	$[0,3]$	29	8	2	$\{2\}$	$\{2\}$
9	4	3	$[0,4]$	$[0,3]$	36	8	2	$[0,3]$	$[1,2]$
10	4	2	$[0,2]$	$[1,2]$	18	9	8	$[0,8]$	$[1,8]$
10	5	4	$[0,4]$	$[1,4]$	19	9	4	$\{4\}$	$\{4\}$
11	5	2	$\{2\}$	$\{2\}$	21	9	6	$[0,7]$	$[0,6]$
15	5	2	$[0,2]$	$[1,2]$	25	9	3	$\{3\}$	$\{3\}$
12	6	5	$[0,5]$	$[0,5]$	27	9	4	$[0,5]$	$[0,5]$
13	6	5	$[0,6]$	$[0,5]$	33	9	3	$[0,4]$	$[0,3]$
16	6	2	$\{2\}$	$\{2\}$	20	10	9	$[0,9]$	$[0,9]$
16	6	3	$[0,4]$	$[0,4]$	21	10	9	$[0,10]$	$[0,9]$
21	6	2	$[0,3]$	$[1,2]$	25	10	3	$\emptyset$	$\emptyset$
21	6	3	$[0,6]$	$[0,4]$	25	10	6	$[0,7]$	$[0,7]$
14	7	6	$[0,6]$	$[1,6]$	28	10	5	$[0,6]$	$[0,6]$
15	7	3	$\{3\}$	$\{3\}$	31	10	3	$\{3\}$	$\{3\}$
21	7	3	$[0,4]$	$[0,3]$	22	11	10	$[0,10]$	$[1,10]$
22	7	2	$\{2\}$	$\{2\}$	23	11	5	$\{5\}$	$\{5\}$
28	7	2	$[0,3]$	$[1,2]$	33	11	5	$[0,6]$	$[0,6]$
29	7	3	$[0,7]$	$[0,5]$	24	12	11	$[0,11]$	$[0,11]$
35	7	3	$[0,7]$	$[0,6]$	25	12	11	$[0,12]$	$[0,11]$
16	8	7	$[0,7]$	$[0,7]$	34	12	2	$\emptyset$	$\emptyset$
17	8	7	$[0,8]$	$[0,7]$	34	12	4	$\{4\}$	$\{4\}$

Table 4.1: Comparison of Connor's inequalities and the cone condition.

Example 4.1. In a 2-$(22, 8, 4)$ design, for which existence remains open, Connor's inequalities state that two blocks can meet in 0 through 5 points. With $\mu = 5$, the

minimum L.P. bound $\mathbf{y} \cdot \mathbf{b} = -\frac{28}{15}$ is achieved with

$$(a_1, \ldots, a_7) = \left(1, -\frac{1}{3}, -\frac{7}{5}, \frac{1}{5}, \frac{1}{5}, 1, \frac{11}{3}\right).$$

Thus two blocks of such a design cannot meet in more than 4 points.

The analogous linear programming problem for three blocks intersecting uniformly in a 2-design has also been implemented. There are 13 variables and many more constraints. While small values of v and k permit fairly quick solutions, there is currently no interesting information to report on μ and ν.

A set of v/k blocks which partitions the points of a 2-(v, k, λ) design is called a *parallel class*. A block B' is *transverse* to a parallel class $\{B_1, \ldots, B_{v/k}\}$ if $|B' \cap B_i| \leq 1$ for all i. This chapter is concluded with an elementary result on parallel classes in 2-designs.

Proposition 4.4. *Suppose a* 2-(v, k, λ) *design with* $v \geq (k+1)\binom{k-1}{2} + k$ *contains a parallel class* P. *Then some block is transverse to* P.

Proof: Suppose no block is transverse to P. The vector $\mathbf{b} = \lambda\mathbf{j} - \sum_{B \in P} \mathbf{e}_B$ is invariant under the partition defined by P. It is necessary that $\mathbf{b} \in \mathcal{C}W$, where $W = W_{tk}^v | \mathcal{K}$ is the restriction of W_{tk}^v to columns indexed by k-sets not transverse to P. Define the 2-vector $\mathbf{y}$ by

$$\mathbf{y}(T) = \begin{cases} \binom{k}{2} - 1 & \text{if } T \text{ is a pair within some } B \in P, \\ -1 & \text{otherwise.} \end{cases}$$

At least one pair of points in every $K \in \mathcal{K}$ is contained in some $B \in P$, so $\mathbf{y}W \geq \mathbf{0}$. Let $p = |P| = v/k$. Then $\mathbf{y} \cdot \mathbf{b} \geq 0$ implies

$$1 > 1 - \frac{1}{\lambda} \geq \frac{k^2\binom{p}{2}}{\left(\binom{k}{2} - 1\right)\binom{k}{2}p} = \frac{k(p-1)}{(k+1)\binom{k-1}{2}},$$

from which the result follows. □

It should be remarked that the proof above essentially just relies on counting pairs within and across blocks of P. Nonetheless, this is another simple example which can be formulated in terms of the cone condition.

4.3 Pairwise intersection of several blocks

In principle, the same approach as in Section 4.1 can be applied to the pairwise intersection sizes among n blocks.

Theorem 4.5. ([27]) *Let $t \geq 2s$ and $v \geq k+s$. Suppose $B_1, \ldots, B_n$ are blocks in a t-(v,k,λ) design with $|B_i \cap B_j| = \mu_{ij}$ for all i, j. Define the $n \times n$ matrix $G = [g_s(\mu_{ij})]_{ij}$. Then*

$$\det(\lambda\gamma G - G^2) \geq 0,$$

where $\gamma = \binom{v}{t}\binom{v}{s}^{-1}\binom{k}{t}^{-1}\binom{k}{s}\binom{v-k}{s}$.

Proof outline: It is enough to show that $\lambda\gamma G - G^2$ is positive semidefinite. Consider the partition Ω of V into 2^n subsets defined by intersection with either B_i or B_i^c for all i, and with associated variables $\{x_S : S \in \Omega\}$. Let $X_i = \sum_{S \subset B_i} x_S$ and $\mathbf{X} = (X_1, \ldots, X_n)$. Define the vector of polynomials

$$\mathbf{g}(\mathbf{X}) = (g_s(X_1), \ldots, g_s(X_n)).$$

For $\mathbf{u} \in \mathbb{R}^n$, consider the nonnegative polynomial $f(\mathbf{X}) = (\mathbf{u} \cdot \mathbf{g}(\mathbf{X}))^2$. With similar computations and notation as in Theorem 4.1, one has $\mathbf{y}_f \cdot (\lambda \mathbf{j} - \sum \mathbf{e}_{B_i}) \geq 0$ equivalent to

$$\mathbf{u}^\top [\Sigma_{ij}^L] \mathbf{u} \leq \lambda \mathbf{u}^\top [\Sigma_{ij}^R] \mathbf{u},$$

where $\Sigma_{ij}^L = \sum_{m=1}^n g_s(\mu_{im}) g_s(\mu_{mj})$ and $\Sigma_{ij}^R = \gamma g_s(\mu_{ij})$. Since $\Sigma_{ij}^L = G_{ij}^2$, it follows that $\mathbf{u}^\top(\lambda\gamma G - G^2)\mathbf{u} \geq 0$. Since $\mathbf{u}$ was arbitrary, this shows that the given matrix is positive semidefinite. □

Remark: The statement $\det(\lambda\gamma I - G) \geq 0$ is proved in [27] and follows from Theorem 4.5 if it is known that G has positive determinant.

Example 4.2. Consider 2-$(56, 12, 3)$ designs, for which existence is known, and suppose some three blocks meet pairwise in $\mu = 4$ points. The above determinant inequality for $n = 3$ fails, so this block intersection pattern is not allowed. Connor's inequalities (4.3) for two blocks permit $\mu = 4$, however.

Some concluding remarks should be made at this point. It is unfortunate that the bound in Theorem 4.5 is independent of the threewise intersection numbers $\nu_{hij} = |B_h \cap B_i \cap B_j|$. If the variable z represents the threewise intersection, the polynomial $(g_s(z))^2$ yields an upper bound on ν_{hij}; however, this inequality is implied by the case $n = 3$ of Theorem 3.1. One important possible continuation of this work is an exploration of other polynomials which produce meaningful statements depending on m-wise intersections for $2 \leq m \leq n$. Additionally, it would be desirable to find a theoretical link between the method of orthogonal projection used in [27] and the cone condition.

Chapter 5

Other Structures and Incidence Matrices

Thus far, inequalities concerning configurations in t-designs have been established from a convex cone condition. An initial observation is that the structure of other combinatorial objects, such as tBDs with different block sizes, Room squares, orthogonal arrays, and codes, to name only a few, might be analyzed by modifying the setup in Chapter 1. The purpose of this chapter is a very brief look at two well-studied generalizations of t-designs and their connection with more general incidence matrices. This will motivate an application to orthogonal arrays in the next chapter. It is also hoped that the discussion which follows is a first step towards unifying the cone condition with Delsarte's inequalities.

5.1 Hypergraph designs and tBDs

A *t-uniform hypergraph* is a pair (X, E), where X is a set of points (here, a finite set) and E is a set of t-subsets of X called *edges*. Suppose $\mathcal{H}$ is a finite set of t-uniform hypergraphs whose points belong to some underlying universe V. The incidence matrix $W = W_{\mathcal{H}}^{V}$ has rows indexed by all t-subsets of V and columns indexed by all members of $\mathcal{H}$, and is defined as in [29] by

$$W(T, H) = \begin{cases} 1 & \text{if } T \text{ is an edge of } H \in \mathcal{H}, \\ 0 & \text{otherwise.} \end{cases}$$

As usual, let $|V| = v$. If $|X| = k$, the *complete* t-uniform hypergraph on X has as edges all $\binom{k}{t}$ t-subsets of X. When $\mathcal{H}$ is the set of all $\binom{v}{k}$ complete t-uniform hypergraphs on some k points of V, the matrix $W_{\mathcal{H}}^V$ coincides with W_{tk}^v introduced earlier. It is then natural to say that nonnegative integral solutions $\mathbf{d}$ of $W_{\mathcal{H}}^V \mathbf{d} = \lambda \mathbf{j}$ correspond to *hypergraph designs*. Usually, a graph or collection of graphs is specified up to isomorphism, and $\mathcal{H}$ consists of all possible embeddings into the points of V.

Example 5.1. A k-cycle system of index λ on a v-set V of points is a collection $\mathcal{B}$ of cycles of length k in V, such that every pair of points is an edge of exactly λ members of $\mathcal{B}$. Let W' be the incidence matrix of 2-subsets of V with k-cycles in V. Then W' is a $\binom{v}{2} \times \binom{v}{k}(k-1)!$ matrix. By "averaging" k-cycles over a k-subset of V, it follows that $\mathcal{C}W_{2k}^v \subset \mathcal{C}W'$. This containment of cones is proper, since there certainly exist supporting vectors of $\mathcal{C}W_{2k}^v$ which have negative inherited weight on some k-cycle. Suppose $\mathbf{e}_C$ is a 2-vector with entries in $\{0,1\}$ encoding the k edges of some generic k-cycle C in V. Then, for instance, the condition $\lambda \mathbf{j} - n\mathbf{e}_C \in \mathcal{C}W'$ generates a family of inequalities on the existence of an n-fold cycle in a cycle system with the given parameters. An automorphism group under which this vector is invariant is isomorphic to $\mathbb{Z}_k \times \mathcal{S}_{v-k}$.

Example 5.2. The collection of complete t-uniform hypergraphs on $k_1 < k_2 < \ldots$ points gives rise to a tBD with block sizes $k_1, k_2, \ldots$. The corresponding matrix is a compound $W = \left[W_{tk_1}^v | W_{tk_2}^v | \cdots\right]$ of the matrices from Section 1.1. As before, define $\mathbf{e}_K$ to be the $\{0,1\}$-vector for incidence of t-subsets with the k-subset K. Note that for $t \leq l < k$,

$$\mathbf{e}_K = \frac{1}{\binom{k-t}{l-t}} \sum_{L \subset K, |L|=l} \mathbf{e}_L.$$

It follows that $\mathcal{C}W_{tk_1}^v \subset \mathcal{C}W_{tk_2}^v \subset \ldots$ and so $\mathcal{C}W = \cup_j \mathcal{C}W_{tk_j}^v = \mathcal{C}W_{tk_1}^v$.

A *generalized incomplete t-wise balanced design* (or GItBD) with index λ and *hole* H of *strength* m is a triple $(V, H, \mathcal{B})$ such that $H \subset V$ and $\mathcal{B}$ is a collection of blocks of V with the property that every t-subset T occurs in exactly λ blocks if $|T \cap H| < t - m$, and exactly 0 blocks otherwise. A GItBD is called *proper* if all block sizes are strictly

between t and v. The case $m = 0$ is the well-studied *incomplete* tBD (ItBD) with hole H.

Theorem 5.1. *Suppose $t - m$ is even. In a GItBD $(V, H, \mathcal{B})$ with $|V| = v$, $|H| = h \geq t$, and hole strength m, it is necessary that $v \geq 2h + m + 1$. Equality holds if and only if every block $B \in \mathcal{B}$ satisfies $|B \setminus H| \leq t$.*

Proof: Define the t-vector $\mathbf{b}$ by

$$\mathbf{b}(T) = \begin{cases} 1 & \text{if } |T \cap H| < t - m, \\ 0 & \text{otherwise.} \end{cases}$$

By the remarks in Example 5.2, it is required that $\mathbf{b} \in \mathcal{C}W^v_{t,t+1}$. Clearly, $\mathbf{b}$ is invariant under the bipartition $(H, V \setminus H)$. Define the polynomial $f(x) = (-1)^t \binom{x-1}{t}$, so that $f(x) \geq 0$ for $0 \leq x < t$. The alternate expression

$$f(x) = (t+1) \sum_{j=0}^{t} (-1)^j \binom{t}{j}^{-1} \binom{x}{j} \binom{t+1-x}{t-j}$$

is implicit from the matrix M_0^{-1} of Proposition 3.3. By Theorem 2.3, $\mathbf{y}_f \cdot \mathbf{b} \geq 0$, or

$$\begin{aligned} 0 &\leq \sum_{j=0}^{t-m-1} \binom{t}{j}^{-1} \binom{h}{j} \binom{v-h}{t-j} \\ &= \frac{t+1}{v-t} \left[\binom{v-h}{t+1} - (-1)^{t-m} \binom{h}{t-m} \binom{v-h}{m+1} \binom{t+1}{m+1}^{-1} \right], \end{aligned}$$

where the closed form arises from identity (1.8). Using equation (1.3), this is equivalent to

$$\binom{v-h-m-1}{t-m} \geq \binom{h}{t-m},$$

or $v \geq 2h + m + 1$. For equality to occur, no $B \in \mathcal{B}$ can contain a $(t+1)$-set X disjoint from H; for otherwise $\mathbf{y}_f \cdot \mathbf{b} \geq \mathbf{y}_f \cdot \mathbf{e}_X = f(0) > 0$. In other words, it must be that $m < |B \setminus H| \leq t$ for all blocks B. □

Remarks: The case $m = 0$ was recently proved in [14], and an argument similar to

the one given here is presented in [29]. Either proof can be modified for $m > 0$. Note that the condition on equality, also discussed in [29] for $m = 0$, implies that all block sizes are between $t+1$ and $2t-m+1$. It is curious that the inequality in Theorem 5.1 is the same constraint as on an ItBD with $v+m$ points and hole size $h+m$, yet there appears to be no easy combinatorial equivalence between these objects and GItBDs with v points, hole size h, and hole strength m.

5.2 Poset t-designs

The notation and terminology here essentially follows that in [7]. Let $(\mathcal{P}, \preceq)$ be a semilattice with rank function $\rho : \mathcal{P} \to \{0, 1, \ldots, k\}$. Define $\mathcal{P}^i$ to be the ith *fiber* of $\mathcal{P}$, namely the set

$$\mathcal{P}^i = \{x \in \mathcal{P} : \rho(x) = i\}$$

of elements of rank i. Suppose $z \in \mathcal{P}^j$ and $x \in X$. If the quantities

$$\alpha_{ij} = |\{y \in \mathcal{P}^i : z \preceq y \preceq x\} \quad \text{and} \quad \beta_{ij} = |\{y \in \mathcal{P}^i : z \preceq y\}|$$

are constants independent of x and z, it is said that $(\mathcal{P}, \preceq)$ is a *regular* semilattice.

Define the incidence matrix $W = W_t$, whose rows and columns are indexed by $\mathcal{P}^t$ and $\mathcal{P}^k$, respectively, by

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

Now let $(\mathcal{P}, \preceq)$ be a regular semilattice with $X = \mathcal{P}^k$. The vector $\mathbf{d} \in \mathbb{N}_0^{|X|}$ is a (poset) *t-design of index λ* in $(\mathcal{P}, \preceq)$ if $W_t\mathbf{d} = \lambda\mathbf{j}$. This definition is extended beyond regular semilattices to more general "Q-posets" for association schemes in the recent paper [18].

Example 5.3. The classical t-designs introduced earlier are poset t-designs in the truncated boolean lattice $(\mathcal{P}, \preceq)$, where $\mathcal{P} = \{S \subseteq V : |S| \leq k\}$ and $\preceq$ is the usual set inclusion $\subseteq$. The associated rank function is of course $\rho(S) = |S|$. In [18], it is

mentioned that both *resolutions* of t-designs and so-called *mixed* t-designs [19] can be formulated as poset designs in the product of two truncated boolean lattices, each with incidence matrix W defined by the associated Kronecker product of incidence matrices.

The related lattice of subspaces of the vector space $\mathrm{GF}(q)^n$ with rank defined by dimension gives rise to *q-analogs* of classical t-designs; see [6] and [7].

The Hamming lattice and orthogonal arrays

The remainder of this section, as well as the next chapter, will focus on t-designs in a different poset. The *Hamming lattice* $(\mathcal{P}, \preceq)$ on a vertex set U (with $|U| = n$) has $\mathcal{P}$ given by the words of length k over the alphabet $U \cup \{*\}$. For $x, y \in \mathcal{P}$, define $x \preceq y$ if and only if $y_i = *$ implies $x_i = *$ and $x_i \neq *$ implies $x_i = y_i$, for each i. The rank function for this poset is $\rho(x) = |\{i : x_i \neq *\}|$. The top fiber $X = \mathcal{P}^k$ consists of words with no occurrence of $*$. The incidence matrix $W = W_t$ for this poset has dimensions $\binom{k}{t} n^t \times n^k$. A poset t-design in this lattice is known as an *orthogonal array* of *strength* t and *index* λ, which will be denoted here by $\mathrm{OA}_\lambda(t, k, n)$. Concretely, an $\mathrm{OA}_\lambda(t, k, n)$ is a $\lambda n^t \times k$ array (say A) with entries from U, such that in any selection of t columns, each of the n^t ordered t-tuples of vertices occurs in exactly λ rows. Unless otherwise noted, only orthogonal arrays of index unity will be considered in what follows. The subscript $\lambda = 1$ is usually omitted from the notation in this case. There is a standard finite field construction for orthogonal arrays of arbitrarily high strength.

Theorem 5.2. ([3]) *Let q be a prime power and suppose $1 \leq t < q$. Let $K = \mathrm{GF}(q) = \{e_1, \ldots, e_q\}$ and $\mathcal{F} = \{f_1, \ldots, f_{q^t}\}$ denote the set of all polynomials of degree $\leq t - 1$ in $K[x]$. Then the matrix A defined by*

$$A_{ij} = f_i(e_j)$$

is an $OA(t, q, q)$.

Proof: It suffices to prove that any $q^t \times t$ submatrix of A has no two distinct rows, say i, i', that are identical. This holds because $f_{i'} - f_i$ is a nonzero polynomial of degree at most $t-1$, so it can have at most $t-1$ zeros in K. □

Equations (1.1) have an analog for orthogonal arrays.

Proposition 5.3. *Suppose A is an $OA_\lambda(t,k,n)$ on the points U. Let $H \subset U$ with $|H| = m$. If there are z_j rows which contain exactly j points of H, then*

$$\sum_{j=0}^{k} \binom{j}{i} z_j = \lambda \binom{k}{i} m^i n^{t-i}, \quad i = 0, \ldots, t. \tag{5.1}$$

Proof: The ith equation is a consequence of counting in two ways all ordered pairs (I, R), where I is an ordered i-tuple of points from H contained in row R of the OA. A detailed argument for $t = 2$ can be found in [11]. □

It will now be shown that Proposition 5.3 follows from the condition $W\mathbf{d} = \lambda\mathbf{j}$. This is similar to the argument in Section 2.3. Consider block matrices from W, $\mathbf{d}$, and $\lambda\mathbf{j}$ with indexing according to the number of points of H in words of the tth and kth fibers of the Hamming lattice. The situation is summarized in Figure 5.1. There are $\binom{j}{i}\binom{k-j}{t-i}$ members of the tth fiber with i points from H which are dominated by a given word in the kth fiber with j points from H. Also, there are $\binom{k}{t}\binom{t}{i} m^i (n-m)^{t-i}$

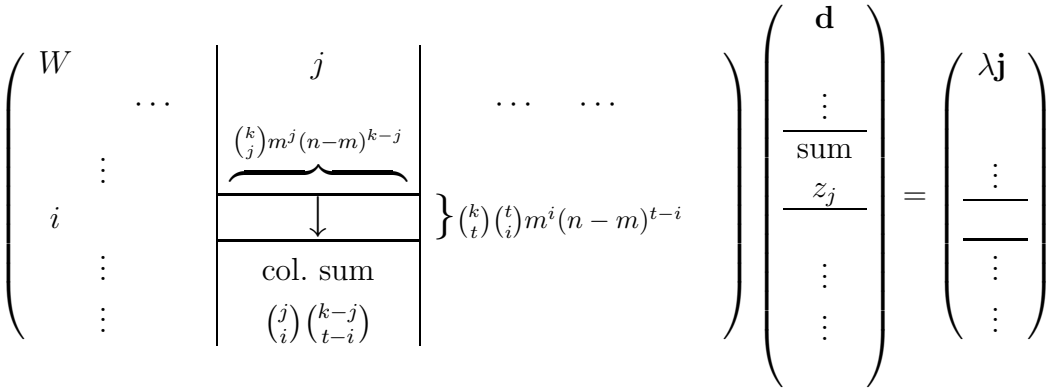


Figure 5.1: Block matrix diagram for $W\mathbf{d} = \lambda\mathbf{j}$ indexed by intersection with H.

total members of the tth fiber with i points from H. So with z_j as before,

$$\sum_{j=0}^{k} \binom{j}{i}\binom{k-j}{t-i} z_j = \lambda \binom{k}{t}\binom{t}{i} m^i (n-m)^{t-i}, \quad i = 0, \ldots, t. \tag{5.2}$$

Let $\mathbf{r}_1, \mathbf{r}_2 \in \mathbb{R}^{t+1}$ be vectors whose ith coordinates are given by the right side of equations (5.1) and (5.2), respectively. To show the two conditions on the z_j are equivalent amounts to a calculation similar to that in Theorem 2.9. One has, by Lemma 2.8,

$$\begin{aligned} M_0 N_0^{-1} \mathbf{r}_1 &= \lambda \sum_{j=0}^{t} (-1)^{i+j} \binom{j}{i}\binom{k-j}{t-j}\binom{k}{j} m^j n^{t-j} \\ &= \lambda \binom{k}{t}\binom{t}{i} \sum_{j=0}^{t-i} (-1)^j \binom{t-i}{j} m^{i+j} n^{t-i-j} \\ &= \lambda \binom{k}{t}\binom{t}{t} m^i (n-m)^{t-i} = \mathbf{r}_2, \end{aligned}$$

where the second line follows from two applications of (1.3) and a shifting of the index of summation.

For convenience, the application to follow in the next chapter will make use of the "moment equations" (5.1) rather than their counterparts (5.2) from the cone condition $\lambda \mathbf{j} \in \mathcal{C}W$.

Chapter 6

An Application: t-Point Based Sampling

This chapter is essentially a reproduction of the paper [8].

6.1 Background

While many decision problems have no known fast deterministic algorithm, it is often the case that they can be settled using randomized algorithms. A survey of such algorithms and their applications can be found in [12]. One standard randomized algorithm is the *Monte Carlo* algorithm, in which an answer is always returned for any instance I; however, the answer may be incorrect with some probability. Here, we will consider *yes-biased* Monte Carlo algorithms having *error probability* ϵ, which satisfy the following conditions:

1. If I is a no-instance, then the algorithm answers "no."

2. If I is a yes-instance, then the probability that the algorithm answers "yes" is at least $1 - \epsilon$.

Therefore, any "yes" answer from such an algorithm is guaranteed to be correct. A *no-biased* algorithm is defined similarly, but there is no loss of generality in considering only yes-biased Monte Carlo algorithms.

Let U be some finite universe with $|U| = n$. A yes-biased Monte Carlo algorithm can be viewed as a two-stage procedure, in which a random "sample point" r in U is

first chosen, and then given as input to some deterministic algorithm. If the answer returned is "yes," then r is said to *witness* the decision. The collection of all witnesses in U is sometimes called the set of *good* points. Primality testing is one important example mentioned in [10]. A yes-biased Monte Carlo algorithm to decide if a positive integer n is composite amounts to running a test on a single randomly selected integer a between 1 and $n-1$. These a are the candidates for witnessing the compositeness of n.

Despite the fact that Monte Carlo algorithms can give wrong answers, the error probability can be made as small as desired by repeated application of the algorithm. Running a yes-biased Monte Carlo algorithm k times independently in succession, and returning "yes" if at least one "yes" answer occurs among the k trials, reduces the error probability to ϵ^k. In the case of primality testing above, the error probability for a single test is $\epsilon \leq 1/2$, but in some cases this probability can be larger. In many common applications, the deterministic portion of a Monte Carlo algorithm is fast enough to allow for repeated trials. Unfortunately, it may be more difficult to guarantee true randomness (independence) of the chosen sample points. The work which follows here will explore the trade-off between error bounds and the cost of random bit generation from a combinatorial viewpoint.

Many researchers have attempted to construct pseudo-random number generators for which provable bounds can be obtained on the probability that none of k successive values is a witness. One simple and effective method known as *two-point sampling* was developed in [4] by Chor and Goldreich. Their idea is to generate only 2 independent sample points (requiring $2 \log n$ random bits), but to then generate a total of k sample points deterministically from the chosen pair. The specific construction given in [4] is to first choose a random linear function $f(i) = ai + b$ over $U = \mathbf{Z}_p$, p prime, and then to compute the k residues $f(0), f(1), \ldots, f(k)$. If ϵ is the error probability (that is, the proportion of elements in U which are not witnesses), it is proven that the probability that none of $f(0), f(1), \ldots, f(k)$ is a witness is at most

$$\frac{\epsilon}{k(1-\epsilon)}.$$

In the context of random pattern testing of VLSI chips, Spencer [23] developed a pseudo-random generator, also based on two-point sampling. The corresponding worst-case error bound for k sample points is roughly equal to

$$\frac{1}{1+k(1-\epsilon)}.$$

In [11], both of these methods was generalized and improved by pointing out a connection with orthogonal arrays. The approach is to use an $\mathrm{OA}(2,k,n)$ with two specified columns, and to generate k pseudo-random points by identifying the unique row indexed (in the specified columns) by an initial chosen pair of points. By using Proposition 5.3 for $t=2$, that paper establishes the upper error bound

$$\frac{\epsilon}{1+(k-1)(1-\epsilon)},$$

which is shown to be stronger than each of the two bounds above. Additionally, the bound is proved to be optimal (for OAs of strength 2) by using maximal arcs in projective planes.

While two-point based sampling aims to ensure pairwise independence of the generated points, it may be desirable in some applications to have t-wise independence for larger t, [4]. Also, it may be feasible to construct more than $2\log n$ initial random bits for the reward of a smaller error bound, closer to the ideal ϵ^k. These two possibilities motivate us to study t-point based sampling using orthogonal arrays of higher strength $t \geq 2$. The sampling method is analogous to that in [11] mentioned above, but it remains to calculate a generalized error bound and analyze its behavior.

6.2 Calculation of the error bound

Let A be an $\mathrm{OA}(t,k,n)$ with $t=2s$ an even positive integer. Suppose there is a set G of the points, which we call *good*. Let $|G|=m$ and $\epsilon = 1-m/n$. For $x=0,\ldots,m$, let $\omega(x)$ denote the number of rows of A which include exactly x points of G. We desire an upper bound on the probability that a randomly chosen row contains no

good points. This will be called the *error* and denoted by E. We have $E = n^{-t}\omega(0)$, because there are $\omega(0)$ rows avoiding all good points, and n^t total rows. Consider the polynomials

$$p(x) = \sum_{i=0}^{s} (-1)^i \binom{k-1-i}{s-i} (1-\epsilon)^{s-i} \binom{x-1}{i}.$$

An alternative expression is

$$p(x) = \sum_{j=0}^{s} (-1)^j \binom{x}{j} g(j),$$

where

$$g(j) = \sum_{i=j}^{s} \binom{k-1-i}{s-i} (1-\epsilon)^{s-i}.$$

By equation (1.7), the square of $p(x)$ can be written as

$$(p(x))^2 = \sum_{r=0}^{t} (-1)^r \sum_{j=0}^{r} g(j)g(r-j) \sum_{h=j}^{r} \binom{h}{j} \binom{j}{r-h} \binom{x}{h}.$$

Now from the inequality

$$\sum_{x=1}^{k} (p(x))^2 \omega(x) \geq 0,$$

it follows that

$$\sum_{r=0}^{t} (-1)^r \sum_{j=0}^{r} g(j)g(r-j) \sum_{h=j}^{r} \binom{h}{j} \binom{j}{r-h} \sum_{x=1}^{k} \binom{x}{h} \omega(x) \geq 0.$$

By Proposition 5.3, the sum on x is $n^t \binom{k}{h} (1-\epsilon)^h$ when $h > 0$. If $h = 0$, the entire sum vanishes except when $r = j = h = 0$, in which case the sum is $(n^t - \omega(0)) \cdot (g(0))^2$. (Note the sum omits $x = 0$.) Therefore,

$$n^t \sum_{r=0}^{t} (-1)^r \sum_{j=0}^{r} g(j)g(r-j) \sum_{h=j}^{r} \binom{h}{j} \binom{j}{r-h} \binom{k}{h} (1-\epsilon)^h \geq \omega(0) \cdot (g(0))^2,$$

and so

$$E \;\leq\; (g(0))^{-2}\sum_{r=0}^{t}(-1)^r\sum_{j=0}^{r}g(j)g(r-j)\sum_{h=j}^{r}\binom{h}{j}\binom{j}{r-h}\binom{k}{h}(1-\epsilon)^h.$$

Changing the order of summation and using equation (1.3) gives

$$\begin{aligned}
E &\leq (g(0))^{-2}\sum_{j=0}^{t}\binom{k}{j}g(j)\sum_{h=j}^{t}(1-\epsilon)^h\binom{k-j}{h-j}\sum_{r=h}^{h+j}(-1)^r\binom{j}{r-h}g(r-j)\\
&= (g(0))^{-2}\sum_{j=0}^{s}\binom{k}{j}g(j)\sum_{h=j}^{s+j}(-1)^h(1-\epsilon)^h\binom{k-j}{h-j}\sum_{r=0}^{j}(-1)^r\binom{j}{r}g(r+h-j)\\
&= (g(0))^{-2}\sum_{j=0}^{s}(-1)^j\binom{k}{j}g(j)(1-\epsilon)^j\\
&\quad\times\sum_{h=0}^{s}(-1)^h(1-\epsilon)^h\binom{k-j}{h}\sum_{r=0}^{j}(-1)^r\binom{j}{r}g(r+h), \qquad (6.1)
\end{aligned}$$

where we have shifted the indexing of the sums on r and on h, while using that $g(j)$ vanishes for $j > s$. We now show that all terms of the outer sum vanish, except when $j = 0$.

Lemma 6.1.

$$\sum_{h=0}^{s}(-1)^h(1-\epsilon)^h\binom{k-j}{h}\sum_{r=0}^{j}(-1)^r\binom{j}{r}g(r+h) = \begin{cases}\epsilon^s & \text{if } j=0,\\ 0 & \text{otherwise.}\end{cases}$$

Proof: Let S denote the required sum. To start, we expand the powers of $(1-\epsilon)$ and change the order and indices of summation.

$$\begin{aligned}
S &= \sum_{r=0}^{j}(-1)^r\binom{j}{r}\sum_{h=0}^{s}(-1)^h\binom{k-j}{h}\sum_{i=r+h}^{s}\binom{k-1-i}{s-i}(1-\epsilon)^{s-i+h}\\
&= \sum_{r=0}^{j}(-1)^r\binom{j}{r}\sum_{h=0}^{s}(-1)^h\binom{k-j}{h}\sum_{i=r}^{s-h}\binom{k-1-i-h}{s-i-h}\sum_{\ell=0}^{s-i}(-1)^\ell\binom{s-i}{\ell}\epsilon^\ell\\
&= \sum_{r=0}^{j}(-1)^r\binom{j}{r}\sum_{\ell=0}^{s-r}(-1)^\ell\epsilon^\ell\sum_{i=r}^{s}\binom{s-i}{\ell}\sum_{h=0}^{s-i}(-1)^h\binom{k-1-i-h}{s-i-h}\binom{k-j}{h}.
\end{aligned}$$

Applying identity (1.5) to the innermost sum on h, and then using equation (1.3) gives

$$\begin{aligned} S &= \sum_{r=0}^{j}(-1)^r\binom{j}{r}\sum_{\ell=0}^{s-r}(-1)^\ell\epsilon^\ell\sum_{i=r}^{s}(-1)^{s-i}\binom{s-i}{\ell}\binom{s-j}{s-i} \\ &= \sum_{r=0}^{j}(-1)^r\binom{j}{r}\sum_{\ell=0}^{s-r}(-1)^\ell\epsilon^\ell\binom{s-j}{\ell}\sum_{i=j}^{s}(-1)^{s-\ell-i}\binom{s-j-\ell}{i-j}. \end{aligned}$$

The alternating inner sum of binomial coefficients reveals that only the terms with $j+\ell = s$ are nonzero. So

$$S = \sum_{r=0}^{j}(-1)^r\binom{j}{r}\binom{s-j}{s-j}\epsilon^{s-j} = \begin{cases} \epsilon^s & \text{if } j = 0, \\ 0 & \text{otherwise,} \end{cases}$$

where the last equality follows from another alternating sum. □

A simplified error bound of $E \leq \epsilon^s/g(0)$ now follows from (6.1) and Lemma 6.1. It should be noted that this reduces to the Gopalakrishnan-Stinson bound in [11] when $s = 1$, as in this case our polynomial $p(x)$ agrees with their quadratic used with the moment equations.

Theorem 6.2. *Let $t = 2s$. The error probability of the t-point based sampling technique for a universe of n points, using an $OA(t, k, n)$, is at most*

$$\frac{\epsilon^s}{\sum_{i=0}^{s}\binom{k-1-i}{s-i}(1-\epsilon)^{s-i}}.$$

While our discussion thus far only applies to OA of even strength, a small improvement in the error bound can be obtained by using $2s+1$ independent sample points and an $\mathrm{OA}(2s, k-1, n)$.

Corollary 6.3. *Suppose $t = 2s+1$. The error probability of the t-point based sampling technique for a universe of n points, is at most*

$$\frac{\epsilon^{s+1}}{\sum_{i=0}^{s}\binom{k-2-i}{s-i}(1-\epsilon)^{s-i}}.$$

6.3 Analysis and comparison of error bounds

Weaker bounds from the generalized Chebyshev inequality

Chor and Goldreich mention in [4] that their result can be generalized to larger t by application of the generalized Chebyshev inequality, which in their context is the statement that

$$\text{Prob}[|X-\mu| \geq \rho] \leq \frac{\text{Exp}[|X-\mu|^t]}{\rho^t},$$

where $t > 0$ and X is a random variable with mean μ. Suppose that in the t-point based sampling method we pick points v_i for $i = 1, \ldots, k$. Define the indicator random variables

$$X_i = \begin{cases} 1 & \text{if } v_i \in S, \\ 0 & \text{otherwise.} \end{cases}$$

Then with $X = \frac{1}{k}\sum_i X_i$ and $\rho = \mu = 1-\epsilon$, the generalized Chebyshev inequality with exponent t leads to an upper bound on $E = \text{Prob}[X = 0]$. When $t = 2$, the authors prove the bound $E \leq (1-\rho)/k\rho$ (stated in section 2), with the classical Chebyshev inequality. However, it appears a mistake occurs in their assertion (without proof) that the inequality with the tth moments of X yields $E \leq (1+1/k)((1-\rho)/k\rho)^{\lfloor t/2 \rfloor}$. Here, we compute the error bound directly for $t = 4$ using the generalized Chebyshev inequality and refute their claim.

$$\begin{aligned} E &\leq \frac{\text{Exp}[|X-\rho|^4]}{\rho^4} \\ &= \frac{1}{k^4\rho^4} \sum_{i_1,i_2,i_3,i_4} \text{Exp}\left[\prod_{j=1}^{4}(X_{i_j}-\rho)\right] \\ &= \frac{1}{k^4\rho^4}\left(k\text{Exp}[(X_1-\rho)^4] + 6\binom{k}{2}\text{Exp}[(X_1-\rho)^2]\cdot\text{Exp}[(X_2-\rho)^2]\right), \end{aligned}$$

where we have used that the X_i are 4-wise independent and identically distributed with mean ρ. The required moments can be explicitly calculated to give the bound

$$E \leq \frac{(1-\rho)(1+3(k-2)\rho(1-\rho))}{k^3\rho^3},$$

which is easily shown to exceed the claimed bound of $(1 + 1/k)((1 - \rho)/k\rho)^2$.

In any case, the bound from Theorem 6.2 is always sharper than that given by the generalized Chebyshev inequality. However, it appears these are close for large k and small ϵ.

Comparison of the bounds for different values of t

For analysis in this section, define $C(s, k)$ to be the upper error bound given by Theorem 6.2. Similar consideration can be given to the bound for odd t from Corollary 6.3. A first observation is that this bound is (asymptotically in k) on the order of the sth power of the bound in [11] which uses strength-two OAs. We compute

$$\lim_{k\to\infty} \frac{C(s,k)}{(C(1,k))^s} = \lim_{k\to\infty} \frac{(1+(k-1)(1-\epsilon))^s}{\sum_{i=0}^{s} \binom{k-1-i}{s-i}(1-\epsilon)^{s-i}} = \lim_{k\to\infty} \frac{(1-\epsilon)^s k^s + \dots}{(1-\epsilon)^s k^s/s! + \dots} = s!.$$

In light of this fact, there at first appears to be no advantage of $2s$-point based sampling over s independent trials of two-point based sampling. Indeed, the limit above even approaches $s!$ from *above*, so for small values of k the error may be much less when repeated two-point based sampling is used. However, some practical reasons support using t-point based sampling for larger t. For instance, a fair comparison of sampling errors ought to take into account the sk tests that must be run when s independent trials of the two-point method are used. Allowing sk tests for one application of $2s$-point based sampling using an $\mathrm{OA}(2s, sk, n)$, we have by a similar calculation as above that the quotient of errors can be made arbitrarily small by increasing s. The graphs in Figure 6.1 illustrate this behavior as s and k vary.

Proposition 6.4.

$$\lim_{k\to\infty} \frac{C(s,sk)}{(C(1,k))^s} = \frac{s!}{s^s}.$$

Since we have worked under the assumption that $t \log n$ independent random bits can be generated in the first place, it is of interest to compare $C(s, k)$ with ϵ^{2s}. There always exists k_0 (depending on s and ϵ) such that $k > k_0$ implies $C(s, k) < \epsilon^{2s}$. When $\epsilon \geq .5$, we have $k_0 \leq 2s + 1$; however $k \geq 2s + 1$ is necessary for the mere existence

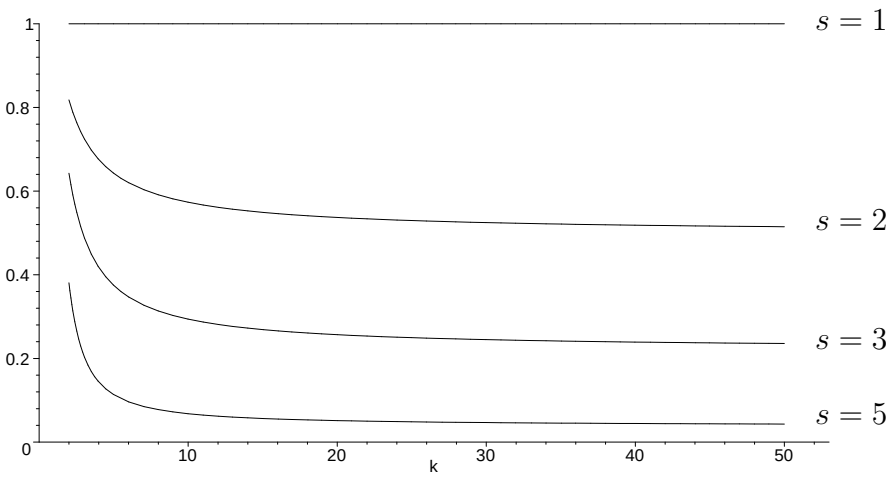


Figure 6.1: Plots of $C(s, sk)/C(1, k)^s$ for $\epsilon = .5$.

of an OA with k columns and strength $2s$. When $\epsilon < .5$, it may be required to take larger k. Luckily, it appears that this k_0 grows at most linearly in s for a fixed ϵ. The table below gives some values of k_0 for certain s and ϵ.

s	1	2	3	4	5
$\epsilon = .1$	11.00	16.11	21.09	26.00	30.86
$\epsilon = .2$	6.00	9.09	12.11	15.09	18.05
$\epsilon = .3$	4.33	6.78	9.19	11.57	13.94
$\epsilon = .4$	3.50	5.65	7.79	9.91	12.02
$\epsilon = .5$	3.00	5.00	7.00	9.00	11.00

We conclude with a remark about independence. The main strength of sampling using OAs is that it bypasses the need for selecting a full $k \log n$ independent random bits. But for some applications, expending the cost of $t \log n$ random bits may be worthwhile if t-wise independence is desired over pairwise independence. It is straightforward from the definition that sampling from the rows of an OA of strength t ensures t-wise independence.

Bibliography

[1] W. N. Bailey, *Generalized Hypergeometric Series*, Cambridge University Press, Cambridge, 1935.

[2] G. P. Barker and A. Thompson, Cones of polynomials, *Portugaliae Math.* **44** (1987), 183–197.

[3] K. A. Bush, Orthogonal arrays of index unity, *Ann. Math. Stat.* **23** (1952), 426–434.

[4] B. Chor and O. Goldreich, On the power of two-point based sampling, *Journal of Complexity* **5** (1989), 96–106.

[5] W. S. Connor, Jr., On the structure of balanced incomplete block designs, *Ann. Math. Statist.* **23** (1952), 57–71.

[6] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* No. 10 (1973).

[7] P. Delsarte, Association schemes and t-designs in regular semilattices, *J. Combin. Theory, Ser. A* **19** (1976), 230–243.

[8] P. Dukes and A. C. H. Ling, A combinatorial error bound for t-point based sampling, submitted for publication to *Theoretical Computer Science, Ser. A*.

[9] M. Gasca and T. Sauer, Polynomial interpolation in several variables, *Adv. Comput. Math.* **12** (2000), 377–410.

[10] K. Gopalakrishnan and D. R. Stinson, Derandomization, in: *The CRC Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, eds.) CRC Press, Inc., 1996, 467–473.

[11] K. Gopalakrishnan and D. R. Stinson, A simple analysis of the error probability of two-point based sampling, *Inform. Process. Lett.* **60** (1996), 91–96.

[12] R. Gupta, S. A. Smolka, and S. Bhaskar, On randomization in sequential and distributed algorithms, *ACM Computing Surveys* **26** (1994), 7–86.

[13] S. P. Hurd, P. Munson and D. G. Sarvate, Minimal enclosings of triple systems I: adding one point, *Ars Combin.*, to appear.

[14] D. L. Kreher and R. S. Rees, A hole-size bound for incomplete t-wise balanced designs, *J. Combin. Des.* **9** (2001), 269–284.

[15] N. Macon and A. Spitzbart, Inverses of Vandermonde matrices, *American Math. Monthly* **65** (1958), 95–100.

[16] K. N. Majindar, On the parameters and intersection of blocks of balanced incomplete block designs, *Ann. Math. Statist.* **33** (1962), 1200–1205.

[17] H. B. Mann, A note on balanced incomplete block designs, *Ann. Math. Statist.* **40** (1969), 679–680.

[18] W. J. Martin, Designs in product association schemes, *Des. Codes Cryptogr.* **16** (1999), 271–289.

[19] W. J. Martin, Mixed block designs, *J. Combin. Des.* **6** (1998), 151–163.

[20] C. Peterson, On tight 6-designs, *Osaka J. Math.* **14** (1977), 417–435.

[21] D. K. Ray-Chaudhuri and R. M. Wilson, On t designs, *Osaka J. Math.* **12** (1975), 737–744.

[22] D. Raghavarao, A note on the block structure of BIB designs, *Calcutta Statist. Assoc. Bull.* **12** (1963), 60–62.

[23] T. H. Spencer, Provably good pattern generation for a random pattern test, *Algorithmica* **11** (1994), 429–442.

[24] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.

[25] R. Webster, *Convexity*, Oxford University Press, New York, 1994.

[26] R. M. Wilson, Inequalities for t designs, *J. Combin. Theory Ser. A* **34** (1983), 313–324.

[27] R. M. Wilson, On the theory of t designs, in *Enumeration and Design* (Waterloo, Ont., 1982), 19–49, Academic Press, Toronto, 1984.

[28] R. M. Wilson, Signed hypergraph designs and diagonal forms for some incidence matrices, *Des. Codes Cryptog.* **17** (1999), 289–297.

[29] R. M. Wilson, Some applications of incidence matrices of t-subsets and hypergraphs, *Discrete Math.*, to appear.