J. Algebra Comb. Discrete Appl.
7(2) • 161–181

Received: 21 January 2019
Accepted: 4 December 2019

Journal of Algebra Combinatorics Discrete Structures and Applications

Some bounds arising from a polynomial ideal associated to any t-design*

Research Article

William J. Martin, Douglas R. Stinson

Abstract: We consider ordered pairs $(X, \mathcal{B})$ where X is a finite set of size v and $\mathcal{B}$ is some collection of k-element subsets of X such that every t-element subset of X is contained in exactly λ "blocks" $B \in \mathcal{B}$ for some fixed λ. We represent each block B by a zero-one vector $\mathbf{c}_B$ of length v and explore the ideal $\mathcal{I}(\mathcal{B})$ of polynomials in v variables with complex coefficients which vanish on the set $\{\mathbf{c}_B \mid B \in \mathcal{B}\}$. After setting up the basic theory, we investigate two parameters related to this ideal: $\gamma_1(\mathcal{B})$ is the smallest degree of a non-trivial polynomial in the ideal $\mathcal{I}(\mathcal{B})$ and $\gamma_2(\mathcal{B})$ is the smallest integer s such that $\mathcal{I}(\mathcal{B})$ is generated by a set of polynomials of degree at most s. We first prove the general bounds $t/2 < \gamma_1(\mathcal{B}) \leq \gamma_2(\mathcal{B}) \leq k$. Examining important families of examples, we find that, for symmetric 2-designs and Steiner systems, we have $\gamma_2(\mathcal{B}) \leq t$. But we expect $\gamma_2(\mathcal{B})$ to be closer to k for less structured designs and we indicate this by constructing infinitely many triple systems satisfying $\gamma_2(\mathcal{B}) = k$.

2010 MSC: 05B05, 05E30, 13F20

Keywords: Design, Steiner system, Polynomial ideal, Bounds

1. Introduction

Let X be a finite set of size v and consider a k-uniform hypergraph $(X, \mathcal{B})$ with vertex set X and block (hyperedge) set $\mathcal{B}$. We aim to study polynomial functions on X which vanish on each element of $\mathcal{B}$ so that $\mathcal{B}$ may be viewed as the variety of some naturally defined ideal of polynomials in v variables. In order to do so, we identify each block $B \in \mathcal{B}$ with a 01-vector $\mathbf{c}_B$, with entries indexed by the elements

* *The first author's research is supported by a grant from the US National Science Foundation. The second author's research is supported by NSERC discovery grant RGPIN-03882.*

William J. Martin (Corresponding Author); Department of Mathematical Sciences and Department of Computer Science, Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609, USA (email: martin@wpi.edu).

Douglas R. Stinson; David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada (email: dstinson@uwaterloo.ca).

of X, whose i^{th} entry is equal to one if $i \in B$ and equal to zero otherwise. In other words, $\mathbf{c}_B$ is the B^{th} column of the point-block incidence matrix, A, of the hypergraph. In this paper we work in characteristic zero and consider the polynomial ring $\mathcal{R} = \mathbb{C}[x_1, \ldots, x_v]$. The *evaluation map*

$$\varepsilon : \mathcal{R} \to \mathbb{C}^{\mathcal{B}}$$

given by $\varepsilon(f)(B) = f(\mathbf{c}_B)$ is a ring homomorphism and its kernel is the ideal of all polynomials in v variables which evaluate to zero on each block of the hypergraph. Denoting this kernel by I, we see that I is the ideal of the finite variety $\{\mathbf{c}_B \mid B \in \mathcal{B}\}$ and we write $\mathsf{I} = \mathcal{I}(\mathcal{B})$. Our goal in this paper is to explore connections between this ideal I and the hypergraph $(X, \mathcal{B})$. Our primary question involves the identification of good generating sets $\mathcal{G}$ for I based on the combinatorial structure of the design $(X, \mathcal{B})$. We are not concerned here with the actual size of the generating set; in fact, we prefer a set of polynomials preserved by the automorphism group of the design. By "good" here, we mean principally that polynomials in the generating set are all of low degree. But we also seek polynomials that shed light on properties of the design.

1.1. Background and related work

Algebraic geometry has a long history in the theory of error-correcting codes. We also have a theory of spherical codes and designs that involves the evaluation of multivariate polynomials at finite sets of points on the unit sphere. Möller [20] constructs good quadrature rules for spherical integration by choosing zero sets of well-chosen families of polynomials. Conder and Godsil [5] studied the symmetric group as a polynomial space. The standard module of the Johnson association scheme $J(v, k)$ can be identified with polynomials of degree at most k in v variables in such a way that the polynomials of a given maximum degree j correspond to a sum of eigenspaces $V_0 + V_1 + \cdots + V_j$. This approach, which is implicit in [8] is worked out in more detail in a later paper of Delsarte [9] (see also [3]). These phenomena motivated Martin and Steele [17] to consider the ideal of polynomials that vanish on the shortest vectors of certain lattices. In work in progress, Martin [18] extends this to attach an ideal to any cometric association scheme by viewing the columns of the Q-polynomial generator E_1 in the Bose-Mesner algebra as a finite variety. Several important examples are connected to combinatorial t-designs and – when disentangled from the language of association schemes – the problem of determining generating sets for the ideals of those association schemes reduces to the problem we address here.

The "polynomial method" in combinatorics [24] is a powerful tool for deriving bounds on the size of combinatorial objects and for proving non-existence of extremal objects. In particular, a recent breakthrough by Croot, Lev and Pach [7] (see also [11]) has stimulated interest in collections of multivariate polynomials that vanish on some configuration in a finite vector space. Here, we work in characteristic zero and are interested in how the ideal we obtain is related to the structure of the design. By contrast, the authors of [7, 11] work over fields of positive characteristic. To see the connection, we note that, since our zero set lies in $\mathbb{Z}^v$, the polynomial generators $g \in \mathcal{G}$ may always be chosen from $\mathbb{Z}[\mathbf{x}]$. So application of the reduction $\mathbb{Z} \to \mathbb{Z}_p$ maps the ideal $\langle \mathcal{G} \rangle \subseteq \mathbb{Z}[\mathbf{x}]$ into the ideal of the same finite variety considered modulo p. It will be an interesting follow-up task to determine when the image under this map is the full ideal in positive characteristic.

We have recently learned of previous Gröbner basis approaches to algebraic aliasing in the statistical design of experiments. Once a useful basis is chosen for the space of polynomial functions on the elements of the design, higher order effects can be mapped to more elementary interactions between factors. For a recent survey, see [19], with the caveat that the terminology used there differs from the terminology in this paper.

1.2. The trivial ideal

We pause to introduce our notation for the standard operations of elementary algebraic geometry. (See, e.g., [10, Chapter 15] for a basic introduction.) For a set $\mathcal{S} \subseteq \mathbb{C}^v$, we let $\mathcal{I}(\mathcal{S})$ denote the ideal of all polynomials in $\mathbb{C}[\mathbf{x}] := \mathbb{C}[x_1, \ldots, x_v]$ that vanish at each point in $\mathcal{S}$. And if $\mathcal{G}$ is any set of

polynomials in $\mathbb{C}[x_1,\ldots,x_v]$, we denote by $\mathcal{Z}(\mathcal{G})$ the zero set of $\mathcal{G}$, the collection of all points $\mathbf{c}$ in $\mathbb{C}^v$ which satisfy $f(\mathbf{c})=0$ for all $f\in\mathcal{G}$. Note that, when $\mathcal{S}$ is finite, we have $\mathcal{Z}(\mathcal{I}(\mathcal{S}))=\mathcal{S}$. In the opposite direction, for any ideal J of polynomials, the Nullstellensatz (see, e.g., [13, p21], [6, p179]) informs us that $\mathcal{I}(\mathcal{Z}(\mathsf{J}))=\mathrm{Rad}(\mathsf{J})$, where $\mathrm{Rad}(\mathsf{J})$ denotes the *radical* of ideal J, the ideal of all polynomials g such that $g^n\in\mathsf{J}$ for some positive integer n. A *radical ideal* is an ideal which is already closed under this process: $\mathrm{Rad}(\mathsf{J})=\mathsf{J}$.

Our first example to consider is the *complete uniform hypergraph* $(X,\mathcal{K}_k^v)$.

Lemma 1.1. *Let X be a finite set of size $v\geq k$ and let $\mathcal{K}_k^v=\binom{X}{k}$ consist of all k-subsets of X. Let*

$$\mathcal{G}_0=\{x_1+\cdots+x_v-k\}\cup\{x_i^2-x_i\mid 1\leq i\leq v\}. \tag{1}$$

Then $\mathcal{I}(\mathcal{K}_k^v)=\langle\mathcal{G}_0\rangle$ and $\mathcal{Z}(\langle\mathcal{G}_0\rangle)=\{\mathbf{c}_B\mid B\in\mathcal{K}_k^v\}$.

Proof. One easily checks that each $\mathbf{c}_B$ is a common zero of the polynomials in $\mathcal{G}_0$. Conversely, any point in $\mathbb{C}^v$ which is a zero of each polynomial in $\mathcal{G}_0$ must be a 01-vector with exactly k ones. In order to verify that $\mathcal{G}_0$ generates the full ideal, we check that the Zariski tangent space at each point is full-dimensional. Let $B\subset X$ be a k-set; evaluating the gradient ∇f of $f(\mathbf{x})=x_j^2-x_j$ at $\mathbf{c}_B$ we obtain $\pm\mathbf{e}_j$ where $\mathbf{e}_j$ is the standard basis vector with a one in position j and all other entries zero. So the Jacobian of the set $\mathcal{G}_0$ of $v+1$ polynomials in v variables evaluated at $\mathbf{c}_B$ takes the form

$$\mathrm{Jac}(\mathcal{G}_0,\mathbf{c}_B)=\left[\left.\frac{\partial f_i}{\partial x_h}\right|_{\mathbf{c}_B}\right]_{h,i}=\begin{bmatrix}1&\pm1&0&\cdots&0\\1&0&\pm1&\cdots&0\\\vdots&&&\ddots&\\1&0&0&\cdots&\pm1\end{bmatrix}$$

which clearly has column rank equal to v. This guarantees that each $\mathbf{c}_B$ is a simple zero of $\langle\mathcal{G}_0\rangle$ and so the ideal is indeed radical. It now follows from the Nullstellensatz that

$$\mathcal{I}(\{\mathbf{c}_B\mid B\in\mathcal{K}_k^v\})=\mathcal{I}(\mathcal{Z}(\langle\mathcal{G}_0\rangle))=\mathrm{Rad}(\langle\mathcal{G}_0\rangle)=\langle\mathcal{G}_0\rangle.$$

See Section 3 for details of these last calculations. □

2. Two parameters

In this paper, once we fix v and k, every ideal will contain the ideal we have just considered. We call this the *trivial ideal* and denote

$$\mathcal{T}=\langle\mathcal{G}_0\rangle=\left\langle x_1+\cdots+x_v-k,\quad x_1^2-x_1,\ldots,x_v^2-x_v\right\rangle. \tag{2}$$

For any k-uniform hypergraph $(X,\mathcal{B})$ on v points, the ideal $\mathcal{I}(\mathcal{B}):=\mathcal{I}(\{\mathbf{c}_B\mid B\in\mathcal{B}\})$ will contain $\mathcal{T}$ and a polynomial $f\in\mathcal{I}(\mathcal{B})$ will be called *non-trivial* if $f\notin\mathcal{T}$ and *trivial* otherwise.

To each $C\subseteq\{1,2,\ldots,v\}$ we associate the monomial $x^C=\prod_{j\in C}x_j$ and note that, for a block $B\in\mathcal{B}$, the value of x^C at point $\mathbf{c}_B$ is one if $C\subseteq B$ and zero otherwise. A k-uniform hypergraph $(X,\mathcal{B})$ is a t-(v,k,λ) *design* (or a block design of *strength* t) if, for every t-element subset $T\subseteq X$ of points, there are exactly λ blocks $B\in\mathcal{B}$ with $T\subseteq B$ (so $\sum_{B\in\mathcal{B}}f(\mathbf{c}_B)=\lambda$ whenever $f(\mathbf{x})=x^T$ for some t-set $T\subseteq X$). Every t-(v,k,λ) design is an s-(v,k,λ_s) design for each $s\leq t$ where $\lambda_s\binom{k-s}{t-s}=\lambda\binom{v-s}{t-s}$.

The following characterization of t-designs is well-known (see, for example, Godsil [14, Cor. 14.6.3]).

Lemma 2.1 (Cf. Delsarte [9, Theorem 7])**.** *Let X be a set of size v and let $(X,\mathcal{B})$ be a k-uniform hypergraph defined on X with corresponding vectors $\mathbf{c}_B$ ($B\in\mathcal{B}$) as defined above. Then $(X,\mathcal{B})$ is a t-design on X if and only if the average over $\mathcal{B}$ of any polynomial $f(\mathbf{x})$ in v variables of total degree at most t is equal to the average of $f(\mathbf{x})$ over the complete uniform hypergraph $\mathcal{K}_k^v$ defined on X.*

Proof. Let $C \subseteq X$ with $|C| = s \leq t$. Exactly $\binom{v-s}{k-s}$ elements of $\mathcal{K}_k^v$ contain C so the average value of $f(\mathbf{x}) = x^C$ over $\{\mathbf{c}_B \mid B \in \mathcal{K}_k^v\}$ is

$$\binom{v-s}{k-s} \Big/ \binom{v}{k} = \frac{k(k-1)\cdots(k-s+1)}{v(v-1)\cdots(v-s+1)} = \frac{\lambda_s}{\lambda_0}$$

which is exactly the average of $f(\mathbf{x})$ over the block set $\mathcal{B}$. So the result holds for monomials. But every polynomial in v variables of total degree at most t is a linear combination of such monomials, so the result holds for these as well by linearity. □

Given $(X, \mathcal{B})$, we seek combinatorially meaningful generating sets for $\mathcal{I}(\mathcal{B})$. Two polynomials $f(\mathbf{x})$ and $g(\mathbf{x})$ have the same value at every point $\mathbf{c}_B$, $B \in \mathcal{B}$ if and only if their difference belongs to the ideal $\mathcal{I}(\mathcal{B})$. For example, $f(\mathbf{x}) = x_j^2$ and $g(\mathbf{x}) = x_j$ take the same value on every 01-vector so $x_j^2 - x_j$ belongs to the ideal of any design. We say $f(\mathbf{x})$ is a *multilinear polynomial* in v variables if f is linear in each x_i: i.e., each monomial with non-zero coefficient in f is a product of distinct indeterminates. Modulo the trivial ideal $\mathcal{T}$, each polynomial in $\mathbb{C}[x_1, \ldots, x_v]$ is equivalent to some (not necessarily unique) multilinear polynomial with zero constant term. With a preference for polynomials of smallest possible degree, we define two fundamental parameters.

Definition 2.2. *Let $(X, \mathcal{B})$ be a non-empty, non-complete k-uniform hypergraph on vertex set $X = \{1, \ldots, v\}$ with corresponding ring of polynomials $\mathcal{R} = \mathbb{C}[x_1, \ldots, x_v]$. Let $\mathcal{I}(\mathcal{B})$ and $\mathcal{T}$ be defined as above. Define*

$$\gamma_1(\mathcal{B}) = \min\{\deg f \mid f \in \mathcal{I}(\mathcal{B}),\ f \notin \mathcal{T}\}$$

and

$$\gamma_2(\mathcal{B}) = \min\{\max\{\deg f : f \in \mathcal{G}\} \mid \mathcal{G} \subseteq \mathcal{R},\ \langle \mathcal{G} \rangle = \mathcal{I}(\mathcal{B})\}.$$

So $\gamma_1(\mathcal{B})$ is the smallest possible degree of a non-trivial polynomial that vanishes on each block and $\gamma_2(\mathcal{B})$ is the smallest integer s such that $\mathcal{I}(\mathcal{B})$ admits a generating set all polynomials of which have degree at most s. Obviously, $\gamma_1(\mathcal{B}) \leq \gamma_2(\mathcal{B})$; designs satisfying equality here are particularly interesting.

Theorem 2.3. *If $(X, \mathcal{B})$ is a t-design ($t \geq 2$) and $f \in \mathcal{I}(\mathcal{B})$ is non-trivial, then $\deg f > t/2$. So, for any non-trivial t-design $(X, \mathcal{B})$, $\gamma_1(\mathcal{B}) \geq (t+1)/2$.*

Proof. Suppose $F \in \mathcal{I}(\mathcal{B})$ has degree at most $t/2$. Write $F(\mathbf{x}) = f(\mathbf{x}) + ig(\mathbf{x})$ where $f, g \in \mathbb{R}[\mathbf{x}]$ each have degree at most $t/2$. Since the entries of each $\mathbf{c}_B$ are real, it is clear that $f, g \in \mathcal{I}(\mathcal{B})$. Then $f^2 \in \mathcal{I}(\mathcal{B})$ is a non-negative polynomial of degree at most t. By Lemma 2.1, its average over $\mathcal{B}$ is zero hence its average over $\mathcal{K}_k^v$ is also zero. Since f^2 is everywhere non-negative, it must evaluate to zero on the incidence vector $\mathbf{c}_B$ of every k-set B. So it belongs to the ideal $\mathcal{I}(\mathcal{K}_k^v)$. Since this ideal is radical and contains f^2, it also contains f. By Lemma 1.1, f must be trivial. The same argument applies to g and, hence, to F. □

Remark 2.4. *The same sort of reasoning used in this proof shows that $\mathcal{I}(\mathcal{B})$ admits a vector space basis, even a generating set, of polynomials with integer coefficients. Let F be a polynomial which vanishes on $\mathcal{B}$ and let $\{\zeta_1 \ldots, \zeta_m\} \subseteq \mathbb{C}$ be a basis for the subspace of $\mathbb{C}$, as a vector space over $\mathbb{Q}$, that contains all the coefficients of F. Then there exist unique polynomials $F_1, \ldots, F_m$ in $\mathbb{Q}[\mathbf{x}]$ with $F = \sum_h \zeta_h F_h$. Since each $\mathbf{c}_B$ is a vector with integer entries, the fact that F evaluates to zero at $\mathbf{c}_B$ implies that each F_h also vanishes at that point. So, scaling appropriately, we may assume each generator belongs to $\mathbb{Z}[\mathbf{x}]$.*

A standard result in the theory of designs (see; Cameron [4] and Delsarte [8, Theorem 5.21]) is the fact that a t-design with s distinct block intersection sizes satisfies $t \leq 2s$. We now show that Theorem 2.3 implies a stronger result, which we believe is new.

Let $C \subseteq X$ with characteristic vector $\mathbf{c}$ and suppose $\{|C \cap B| : B \in \mathcal{B}\} = \{i_1, \ldots, i_s\}$. Then every $\mathbf{c}_B$ for $B \in \mathcal{B}$ is a zero of the degree s *zonal polynomial*

$$F(\mathbf{x}) = (\mathbf{c} \cdot \mathbf{x} - i_1) \cdots (\mathbf{c} \cdot \mathbf{x} - i_s).$$

Of course, if $|C|$ is sufficiently small, this polynomial belongs to the trivial ideal.

Corollary 2.5. *Let $(X, \mathcal{B})$ be a t-design and let $C_1, \ldots, C_\ell \subseteq X$ and $\{i_{1,1}, \ldots, i_{1,s_1},\ i_{2,1}, \ldots,\ i_{\ell,s_\ell}\}$ be a multiset of integers such that, for every $B \in \mathcal{B}$ there exist $1 \le h \le \ell$ and $1 \le j \le s_h$ with $|B \cap C_h| = i_{h,j}$. If there exists some k-set $S \notin \mathcal{B}$ with $|S \cap C_h| \notin \{i_{h,1}, \ldots, i_{h,s_h}\}$ for all $h = 1, \ldots, \ell$, then $\gamma_1(\mathcal{B}) \le s_1 + \cdots + s_\ell$ hence $s_1 + \cdots + s_\ell > t/2$.*

Proof. For $Y \subseteq X$, define 01-vector $\boldsymbol{\chi}_Y$ by $(\boldsymbol{\chi}_Y)_a = 1$ if $a \in Y$ and $(\boldsymbol{\chi}_S)_a = 0$ otherwise. E.g., $\boldsymbol{\chi}_B = \mathbf{c}_B$ when B is a block. Consider the product of ℓ zonal polynomials

$$F(\mathbf{x}) = \prod_{h=1}^{\ell} \prod_{j=1}^{s_h} \left(\boldsymbol{\chi}_{C_h} \cdot \mathbf{x} - i_{h,j}\right).$$

By hypothesis, $F(\mathbf{c}_B) = 0$ for every $B \in \mathcal{B}$. Since $F(\boldsymbol{\chi}_S) \neq 0$, F is non-trivial. So, by Theorem 2.3, $\deg F > t/2$. □

Lemma 2.6. *Let $(X, \mathcal{B})$ be a t-(v, k, λ) design. Let s denote the smallest integer such that $\binom{v}{s} > |\mathcal{B}|$. Then $\gamma_1(\mathcal{B}) \le s$.*

Proof. The vector space of functions on $\mathcal{K}_k^v$ representable by multilinear polynomials in $\mathcal{R}$ with zero constant term and total degree at most s has dimension $\binom{v}{s}$. For the chosen value of s, there exists a non-zero multilinear polynomial $f(\mathbf{x}) \in \mathcal{R}$, of total degree at most s, which vanishes on each element of $\mathcal{B}$. (We have $|\mathcal{B}|$ equations and $\binom{v}{s}$ unknowns.) Being multilinear with zero constant term, $f(\mathbf{x})$ is non-trivial with degree at most s. □

We finish this section with two instructive examples.

Example 2.7. *Let us construct the ideal of the Fano plane. Let $X = \mathbb{Z}_7$ and take*

$$\mathcal{B} = \{\{0,1,3\}, \{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,0\}, \{5,6,1\}, \{6,0,2\}\}.$$

Starting from $\mathcal{G}_0$, let us build up a meaningful generating set for $\mathcal{I}(\mathcal{B})$. The unique triple in $\mathcal{B}$ containing both 0 and 1 also contains 3; this combinatorial condition may be encoded as $x_0x_1 - x_0x_1x_3 \in \mathcal{I}(\mathcal{B})$. Alternatively, including the quadratic polynomial $x_0x_1 - x_0x_3$ in a generating set $\mathcal{G}$ for our ideal also guarantees that any vector $\mathbf{c} \in \mathcal{Z}(\langle \mathcal{G} \rangle)$ with $\mathbf{c}_0 = 1$ and $\mathbf{c}_1 = 1$ must have $\mathbf{c}_3 = 1$ as well. Up to sign, there are $\binom{7}{2}$ quadratic generators of this form and these, together with those in $\mathcal{G}_0$, generate the full ideal.

Example 2.8. *With $X = \{1, \ldots, 9\}$ and $\mathcal{B} = \{\{1,2,3\}, \{4,5,6\}, \{7,8,9\}\}$, a 1-design, we find generating set*

$$\mathcal{G} = \mathcal{G}_0 \cup \{x_1 - x_2,\ x_1 - x_3,\ \ x_4 - x_5,\ x_4 - x_6,\ \ x_7 - x_8,\ x_7 - x_9\}.$$

While we will not see further examples where the ideal is generated by $\mathcal{G}_0$ and linear polynomials, we will see that the difference of two monomials appears again as a useful tool.

3. Radical ideals

In this section, we deal with a technicality which arises as we compute ideals of finite sets. We show here that every ideal containing the trivial ideal is radical, thereby eliminating any further need to check this property.

Given a finite set $\mathcal{S}$ of points in $\mathbb{C}^v$, it is often easy to come up with polynomials that vanish at each of those points and, with a bit of work, we might find a generating set $\mathcal{G}$ for some ideal $\mathsf{J} = \langle \mathcal{G} \rangle$ whose zero set is exactly $\mathcal{S}$: $\mathcal{Z}(\langle \mathcal{G} \rangle) = \mathcal{S}$. Hilbert's Nullstellensatz then tells us that

$$\mathcal{I}(\mathcal{S}) = \mathcal{I}(\mathcal{Z}(\mathsf{J})) = \mathrm{Rad}(\mathsf{J}), \tag{3}$$

the *radical* of of ideal J given by

$$\mathrm{Rad}(\mathsf{J}) = \{ f \in \mathcal{R} \mid (\exists n \in \mathbb{N})\, (f^n \in \mathsf{J}) \}.$$

The ideal J is a *radical ideal* if $\mathrm{Rad}(\mathsf{J}) = \mathsf{J}$. Our goal then is achieved in three steps: given a finite set of points $\mathcal{S}$, find a nice set $\mathcal{G}$ of small-degree polynomials that vanish on $\mathcal{S}$; verify that $\mathcal{Z}(\mathcal{G}) = \mathcal{S}$ and nothing more; verify also that $\langle \mathcal{G} \rangle$ is a radical ideal. In this section, we discuss ways to achieve this last step.

If J is an ideal in $\mathbb{C}[x_1, \ldots, x_v]$ with finite zero set $\mathcal{Z}(\mathsf{J}) = \mathcal{S}$, then $\mathbb{C}[\mathbf{x}]/\mathsf{J}$ is a finite-dimensional complex vector space and its dimension is equal to the sum of the multiplicities of all the zeros of $\mathcal{I}$, $\dim \mathbb{C}[\mathbf{x}]/\mathsf{J} = \sum_{\mathbf{c} \in \mathcal{S}} \mathrm{mult}(\mathbf{c})$. The *coordinate ring* of a variety $\mathcal{S} \subseteq \mathbb{C}^v$ is defined as the quotient ring $\mathbb{C}[\mathbf{x}]/\mathcal{I}(\mathcal{S})$ and this is naturally identified with the ring of "polynomial functions" on the set $\mathcal{S}$. If J is an ideal in $\mathbb{C}[\mathbf{x}]$ with finite zero set $\mathcal{Z}(\mathsf{J}) = \mathcal{S}$, then it is well-known (e.g., Section 5.3, Proposition 7 in [6]) that

$$\sum_{\mathbf{c} \in \mathcal{S}} \mathrm{mult}(\mathbf{c}) = \dim \mathbb{C}[\mathbf{x}]/\mathsf{J} \geq \dim \mathbb{C}[\mathbf{x}]/\,\mathrm{Rad}(\mathsf{J}) = |\mathcal{S}| \tag{4}$$

where $\mathrm{mult}(\mathbf{c})$ is the multiplicity of point $\mathbf{c}$ as a zero of J. This proves

Proposition 3.1. *With notation as above:*

(i) If $\mathcal{S} \subseteq \mathcal{Z}(\mathsf{J})$, then $\dim \mathbb{C}[\mathbf{x}]/\mathsf{J} \geq |\mathcal{S}|$;

(ii) If J is a radical ideal and $\mathcal{Z}(\mathsf{J}) = \mathcal{S}$ is finite, then $\mathsf{J} = \mathcal{I}(\mathcal{S})$;

(iii) If J is an ideal in $\mathbb{C}[\mathbf{x}]$ with finite zero set $\mathcal{Z}(\mathsf{J}) \supseteq \mathcal{S}$ and the coordinate ring $\mathbb{C}[\mathbf{x}]/\mathsf{J}$ has dimension equal to $|\mathcal{S}|$, then the ideal J is radical, $\mathcal{Z}(\mathsf{J}) = \mathcal{S}$, each point of $\mathcal{S}$ is a smooth point (multiplicity one), and $\mathcal{I}(\mathcal{S}) = \mathsf{J}$. ■

Let $\mathcal{G} = \{f_1, \ldots, f_\ell\}$ be a generating set for ideal $\mathsf{J} \subseteq \mathbb{C}[x_1, \ldots, x_v]$. The *Jacobian* of the system $\{f_1(\mathbf{x}) = 0, \ldots, f_\ell(\mathbf{x}) = 0\}$ of polynomial equations evaluated at point $\mathbf{c} \in \mathbb{C}^v$ is the $v \times \ell$ matrix $\mathrm{Jac}(\mathcal{G}, \mathbf{c})$ with (i,j)-entry equal to $\left.\frac{\partial f_j}{\partial x_i}\right|_{\mathbf{c}}$, the partial derivative $\partial f_j/\partial x_i$ evaluated at point $\mathbf{c}$. Since we are dealing only with zero-dimensional varieties in this paper, we say the point $\mathbf{c}$ is *smooth* if $\mathrm{Jac}(\mathcal{G}, \mathbf{c})$ has column rank v, so that the Zariski tangent space is zero-dimensional. A smooth point has multiplicity one. So another way to show that the ideal J is radical is to check that, at each point $\mathbf{c}$ of its zero set, the Jacobian $\mathrm{Jac}(\mathcal{G}, \mathbf{c})$ has full row rank where $\mathcal{G}$ is some generating set for J.

Proposition 3.2. *Let $\mathcal{G} \subseteq \mathbb{C}[\mathbf{x}]$ be any set of polynomials such that $\mathcal{G}_0 \subseteq \mathcal{G}$ (cf. Equation (1)). Then $\langle \mathcal{G} \rangle$ is a radical ideal.*

Proof. In the proof of Lemma 1.1, we proved that the Jacobian $\mathrm{Jac}(\mathcal{G}_0, \mathbf{c}_B)$ of $\mathcal{G}_0$ has column rank equal to v at any characteristic vector $\mathbf{c}_B$ of any k-set B. Since $\mathrm{Jac}(\mathcal{G}_0, \mathbf{c}_B)$ is a submatrix of $\mathrm{Jac}(\mathcal{G}, \mathbf{c}_B)$, this latter Jacobian also has full row rank and each point of the finite variety $\mathcal{Z}(\mathcal{G})$ is smooth. □

We note here that this approach also provides another proof of the fundamental bound of Ray-Chaudhuri and Wilson.

Lemma 3.3. *Let $S \subseteq \{1, \ldots, v\}$ and $t \geq |S|$. If I is an ideal containing $\mathcal{T}$, then in the quotient ring $\mathbb{C}[\mathbf{x}]/\mathsf{I}$, the coset $x^S + \mathsf{I}$ is expressible as a linear combination of cosets $x^T + \mathsf{I}$ where $|T| = t$.*

Proof. Assume $t = |S| + 1$. Since $1 + \mathsf{I} = \frac{1}{k}\sum_j x_j + \mathsf{I}$ we have

$$x^S + \mathsf{I} = \prod_{s\in S} x_s + \mathsf{I} = \frac{1}{k}\sum_j x_j \prod_{s\in S} x_s + \mathsf{I} = \left(\frac{t-1}{k}x^S + \mathsf{I}\right) + \left(\sum_{\substack{S\subseteq T\\ |T|=t}} x^T\right) + \mathsf{I}$$

and we may solve for $x^S + \mathsf{I}$. □

Theorem 3.4. *If $(X, \mathcal{B})$ is a $2s$-(v, k, λ) design, then $|\mathcal{B}| \geq \binom{v}{s}$.*

Proof. Since the coordinate ring $\mathbb{C}[\mathbf{x}]/\mathcal{I}(\mathcal{B})$ has dimension $|\mathcal{B}|$ and the monomials $\{x^C : |C| = s\}$ represent linearly independent cosets in this quotient ring, we have $|\mathcal{B}| \geq \binom{v}{s}$. □

This language differs from that employed by Ray-Chaudhuri and Wilson. Consider the $\binom{v}{s} \times |\mathcal{B}|$ matrix $A^{(s)}$ with rows indexed by all $C \subseteq X$ with $|C| = s$, with columns indexed by the set $\mathcal{B}$ of blocks of a t-(v, k, λ) design, and (C, B)-entry equal to one if $C \subseteq B$ and equal to zero otherwise. The proof of Theorem 1 in [21] establishes that the columns $\mathbf{c}_B$ of $A^{(s)}$ span the space $\mathbb{R}^{\binom{v}{s}}$. The celebrated bound follows immediately for even t and, for odd t, one obtains $|\mathcal{B}| \geq 2\binom{v}{s}$ whenever $\mathcal{B}$ is the block set of a t-(v, k, λ) design with $t = 2s+1$ by applying this idea to both the derived design and the residual design. As we will use the fact later, we record it here as a lemma.

Lemma 3.5. *Let $(X, \mathcal{B})$ be a t-(v, k, λ) design with $t \geq 2s$ and consider the incidence matrix $A^{(s)}$ of s-subsets of X versus blocks as defined in the previous paragraph. Then the column rank of $A^{(s)}$ is exactly $\binom{v}{s}$.* ■

4. Steiner systems and partial designs

For a subset $C \subseteq X$ and $f \in \mathcal{R}$, define $f(C)$ in the obvious way, by setting $x_i = 1$ if $i \in C$ and $x_i = 0$ if $i \notin C$ $(1 \leq i \leq v)$, and then evaluating $f(\chi_C)$ where $\chi_C = (x_1, \ldots, x_v)$.

We want to construct small-degree generating sets $\mathcal{G}$ for the ideal $\mathsf{I} = \mathcal{I}(\mathcal{B})$ where $\mathcal{B}$ is the block set of our design $(X, \mathcal{B})$. We assume throughout that $\mathcal{G}$ contains $\mathcal{G}_0$ so that $\langle\mathcal{G}\rangle$ contains the trivial ideal $\mathcal{T}$. Every zero of this latter ideal is a 01-vector with exactly k ones. As we choose the remaining generators, we need only search for multilinear polynomials: each monomial $x_1^{e_1}\cdots x_v^{e_v}$ appearing in $f(\mathbf{x})$ has all $e_i \in \{0, 1\}$. It is clear that the automorphism group of a design $(X, \mathcal{B})$ acts on the ideal $\mathcal{I}(\mathcal{B})$ by permuting indeterminates; rather than minimizing $|\mathcal{G}|$, we typically show a preference for sets of generators invariant under this action.

Recall, for a subset $C \subseteq X$, we have $x^C = \prod_{i\in C} x_i$. Next define, for an integer $j \leq |C|$, the polynomial

$$x^{C,j} = \sum_{J\subseteq C, |J|=j} x^J.$$

(This is a certain symmetric function — the elementary symmetric polynomial of degree j — in the variables $\{x_i \mid i \in C\}$.) For example, $x^{C,|C|} = x^C$. Since the trivial ideal contains $\left(x^{X,1} - k\right)^j$ for all j it

also contains $x^{X,j} - \binom{k}{j}$ for $1 \le j \le k$. For example, modulo $\langle \mathcal{G}_0 \rangle$,

$$\begin{aligned}\left(x^{X,1} - k\right)^2 &= \sum_{i=1}^{v} x_i^2 + 2\left(\sum_{i<j} x_i x_j\right) - 2k\left(\sum_{i=1}^{v} x_i\right) + k^2 \\ &\equiv \left(\sum_{i=1}^{v} x_i - k\right) + 2\left(\sum_{i<j} x_i x_j - \binom{k}{2}\right) - 2k\left(\sum_{i=1}^{v} x_i - k\right) \\ &\equiv \left(x^{X,1} - k\right) + 2\left(x^{X,2} - \binom{k}{2}\right) - 2k\left(x^{X,1} - k\right).\end{aligned}$$

Lemma 4.1. *Suppose that $B \subseteq X$, $|B| = k$ and $J \subseteq B$. Denote $j = |J|$. Define*

$$g_{B,J}(\mathbf{x}) = x^{B,j} - \binom{k}{j} x^J \ . \tag{5}$$

Then, for every $C \subseteq X$, we have that $g_{B,J}(C) \neq 0$ if and only if $j \le |C \cap B| < k$.

Proof. If $|C \cap B| < j$, then every monomial appearing in $g_{B,J}(\mathbf{x})$ evaluates to 0 on χ_C. If $|C \cap B| = k$, then all the monomials in $g_{B,J}(\mathbf{x})$ take nonzero values on χ_C, and $g_{B,J}(C) = \binom{k}{j}(1) - (1)\binom{k}{j} = 0$. If $j \le |C \cap B| < k$, then some proper subset of the monomials occurring in $g_{B,J}(\mathbf{x})$ take nonzero value, and $g_{B,J}(C)$ cannot equal 0. □

Theorem 4.2. *For any k-uniform hypergraph $(X, \mathcal{B})$, $\gamma_2(\mathcal{B}) \le k$.*

Proof. In addition to our generators $\mathcal{G}_0$ for $\mathcal{T}$ given in (1), we will include one generator $g_Y(\mathbf{x})$ for each set Y of $k-1$ points. For $Y \subseteq X$ with $|Y| = k-1$, define

$$J = \{j \in X : Y \cup \{j\} \in \mathcal{B}\}.$$

Suppose $J = \{j_1, \ldots, j_\ell\}$ (possibly the empty set). Then consider the polynomial

$$g_Y(\mathbf{x}) = x^Y (x^{J,1} - 1), \tag{6}$$

noting that $g_Y(\mathbf{x}) = -x^Y$ whenever Y is contained in no block of the hypergraph.

Let I be the ideal generated by

$$\mathcal{G} = \mathcal{G}_0 \cup \{g_Y(\mathbf{x}) : |Y| = k-1\}.$$

It follows from Proposition 3.2 that I is a radical ideal. In order to prove that $\mathsf{I} = \mathcal{I}(\mathcal{B})$ (and hence that $\gamma_2(\mathcal{B}) \le k$), we must verify

- $f(B) = 0$ for every $f \in \mathcal{G}$ and every $B \in \mathcal{B}$;
- for any k-set $C \notin \mathcal{B}$, there is some Y with $g_Y(C) \neq 0$.

Suppose that $B \in \mathcal{B}$; then it is easy to verify from (6) that $g_Y(B) = 0$ for any $(k-1)$-subset Y. Now suppose that $C \subseteq X$, $|C| = k$, $C \notin \mathcal{B}$. Let $Y \subseteq C$, $|Y| = k-1$. If Y is contained in no blocks, then $g_Y(C) = -1$ since $g_Y(\mathbf{x}) = -x^Y$. On the other hand, if Y is contained in at least one block, then $g_Y(C) = -1$ from (6). We then have that I is a radical ideal with $\mathcal{Z}(\mathsf{I}) = \mathcal{B}$; by Proposition 3.1*(ii)* we are done. □

A Steiner system is a t-(v, k, λ) design with $\lambda = 1$. The question of existence of non-trivial Steiner systems with $t > 5$ has been recently resolved in spectacular fashion by Keevash [16].

Theorem 4.3. *Let $(X, \mathcal{B})$ be any t-$(v, k, 1)$ design. For a block $B \in \mathcal{B}$ and any t-element subset T contained in B, define (as in (5))*

$$g_{B,T}(\mathbf{x}) = x^{B,t} - \binom{k}{t} x^T.$$

Then

(i) *$\mathcal{I}(\mathcal{B})$ is generated by $\mathcal{G}_0 \cup \{g_{B,T}(\mathbf{x}) : B \in \mathcal{B}, T \subseteq B, |T| = t\}$;*

(ii) *$\gamma_2(\mathcal{B}) \leq t$.*

Proof. In view of Theorem 4.2, we can assume that $t < k$. Consider the generating set

$$\mathcal{G} = \mathcal{G}_0 \cup \{g_{B,T}(\mathbf{x}) : B \in \mathcal{B}, T \subseteq B, |T| = t\}.$$

From Lemma 4.1, if $B \in \mathcal{B}$ then $g_{B,T}(B) = 0$ for each t-subset T of B, while if $B' \in \mathcal{B}$, $B' \neq B$, then $|B' \cap B| \leq t - 1$ and it follows that $g_{B',T}(B) = 0$ for any t-subset T of B'.

Now suppose that $|C| = k$, $C \notin \mathcal{B}$, and choose $T \subseteq C$, $|T| = t$. There is a block $B \in \mathcal{B}$ with $T \subseteq B$. Then $g_{B,T}(C) \neq 0$ from Lemma 4.1 because $t \leq |B \cap C| \leq k - 1$.

So $\mathcal{Z}(\mathcal{G}) = \{\mathbf{c}_B \mid B \in \mathcal{B}\}$. By Proposition 3.2, $\langle \mathcal{G} \rangle$ is a radical ideal. So Equation (3) gives $\mathcal{I}(\mathcal{B}) = \langle \mathcal{G} \rangle$ and the result follows. □

Remark 4.4. *Let B be a block of the t-$(v, k, 1)$ design $(X, \mathcal{B})$ and let T and T' be two t-element subsets of B. Then it is easy to see that $\mathcal{I}(\mathcal{B})$ contains $x^T - x^{T'}$. Since each of the generators $g_{B,T}$ in the above theorem is expressible as a sum of polynomials of this form, we have a perhaps simpler set of generators $\mathcal{G}_0 \cup \left\{x^T - x^{T'} \mid T, T' \subseteq B \in \mathcal{B},\ |T| = |T'| = t\right\}$ for the ideal.*

Question: Do the cosets $\left\{x^{B,t} + \mathcal{I}(\mathcal{B}) \mid B \in \mathcal{B}\right\}$ form a basis for the coordinate ring $\mathbb{C}[\mathbf{x}]/\mathcal{I}(\mathcal{B})$ in this case?

Next, we describe a couple of variations of Theorem 4.3. A *partial* t-$(v, k, 1)$-design is a k-uniform hypergraph in which any t-subset occurs in *at most* one block. A partial t-$(v, k, 1)$-design, $(X, \mathcal{B})$, is *maximal* if there does not exist a k-subset $C \subseteq X$, $C \notin \mathcal{B}$ such that $(X, \mathcal{B} \cup \{C\})$ is a partial t-$(v, k, 1)$-design.

Corollary 4.5. *For any maximal partial t-$(v, k, 1)$-design $(X, \mathcal{B})$, $\gamma_2(\mathcal{B}) \leq t$.*

Proof. As we employ the same generating set as in the proof of Theorem 4.3, we need only check that $\mathcal{Z}(\langle \mathcal{G} \rangle) = \mathcal{B}$. As before, we have that $g_{B,T}(B') = 0$ for all blocks $B, B' \in \mathcal{B}$ and all t-subsets T of B. Now suppose that $|C| = k$, $C \notin \mathcal{B}$. Because $(X, \mathcal{B})$ is a maximal partial t-$(v, k, 1)$-design, it is possible to choose $T \subseteq C$, $|T| = t$ such that there is a block $B \in \mathcal{B}$ with $T \subseteq B$. Then $g_{B,T}(C) \neq 0$ as before. □

By a slight extension of our construction, we do not require the partial t-$(v, k, 1)$-design to be maximal.

Theorem 4.6. *For any partial t-$(v, k, 1)$-design $(X, \mathcal{B})$, $\gamma_2(\mathcal{B}) \leq t$.*

Proof. If $(X, \mathcal{B})$ is maximal, then Corollary 4.5 yields the desired result, so assume $(X, \mathcal{B})$ is not maximal. Let

$$\mathbf{T} = \{T \subseteq X \ : \ |T| = t, (\forall B \in \mathcal{B})(T \not\subseteq B)\}.$$

Now consider the generating set

$$\mathcal{G} = \mathcal{G}_0 \cup \{g_{B,T}(\mathbf{x}) : B \in \mathcal{B}, T \subseteq B, |T| = t\} \cup \{x^T : T \in \mathbf{T}\}.$$

Since x^T evaluates to zero on every block, we still have $\mathcal{B} \subseteq \mathcal{Z}(\langle\mathcal{G}\rangle)$. But if C is a k-set not belonging to $\mathcal{B}$, either $\mathcal{B} \cup \{C\}$ is again a partial t-design or some t-subset T of C is contained in some block B. In the latter case, $g_{B,T}(C) \neq 0$ as above; in the former case, every t-subset of C belongs to $\mathbf{T}$ so we can take any t-subset $T \subseteq C$ and, with $f(\mathbf{x}) = x^T \in \mathcal{G}$, we have $f(C) \neq 0$. So $\mathcal{Z}(\langle\mathcal{G}\rangle) = \mathcal{B}$ and the rest of the proof follows just as before. □

This result gives us another upper bound on γ_2 for general t-designs.

Corollary 4.7. *Let $(X, \mathcal{B})$ be a t-(v, k, λ) design with $|B \cap B'| < s$ for every pair B, B' of distinct blocks. Then $\gamma_2(\mathcal{B}) \leq s$.* ■

5. Symmetric balanced incomplete block designs

A 2-(v, k, λ) design is traditionally called a *balanced incomplete block design* (BIBD) [23, Chapter 1]. Fisher's inequality states that, for any such 2-design, we have $|\mathcal{B}| \geq |X|$ since, for $t \geq 2$, the point-block incidence matrix A has rank v. A 2-design with equally many blocks and points is called a *symmetric 2-design*. While Theorem 2.3 implies here that $\gamma_1(\mathcal{B}) > 1$, we may use the invertibility of A to obtain more information in this case. If $f(\mathbf{x}) = w_0 + \sum_{i=1}^{v} w_i x_i \in \mathcal{I}(\mathcal{B})$ then $\mathbf{w} = (w_1, \ldots, w_v)$ satisfies $\mathbf{w}^\top A = -w_0\mathbf{1}$ and $\mathbf{w} + \frac{w_0}{k}\mathbf{1}$ lies in the left nullspace of A. So $\mathbf{w}$ is a scalar multiple of $\mathbf{1}$ and f is trivial. The quadratic case is more interesting. Let $\mathbf{r}_i$ denote row i of matrix A. For any two distinct points $i, j \in X$, the entrywise product $\mathbf{r}_i \circ \mathbf{r}_j$ is expressible as a linear combination of the rows of A. Say

$$\mathbf{r}_i \circ \mathbf{r}_j = \sum_{h=1}^{v} w_h \mathbf{r}_h \ .$$

Then the polynomial $f(\mathbf{x})$ given by

$$f(\mathbf{x}) = x_i x_j - \sum_{h=1}^{v} w_h x_h$$

is easily seen to belong to $\mathcal{I}(\mathcal{B})$: for a block B indexing column ℓ of matrix A, we have $f(\mathbf{c}_B) = A_{i\ell}A_{j\ell} - \sum_{h=1}^{v} w_h A_{h\ell} = 0$. In fact, we may determine the coefficients w_h explicitly to obtain a nice generating set for our ideal.

Theorem 5.1. *Let $(X, \mathcal{B})$ be any non-trivial symmetric 2-(v, k, λ) design. For each pair i, j of distinct points from X define*

$$f_{i,j}(\mathbf{x}) = (k - \lambda)x_i x_j - \sum_{i,j \in B \in \mathcal{B}} x^{B,1} + \lambda^2.$$

Then

(i) *$\mathcal{I}(\mathcal{B})$ is generated by $\mathcal{G}_0 \cup \{f_{i,j} \mid i, j \in X\}$;*

(ii) *$\gamma_1(\mathcal{B}) = \gamma_2(\mathcal{B}) = 2$;*

(iii) *the coordinate ring $\mathbb{C}[\mathbf{x}]/\mathcal{I}(\mathcal{B})$ admits a basis consisting of cosets $\{x_i + \mathcal{I}(\mathcal{B}) \mid 1 \leq i \leq v\}$.*

Proof. Assume $(X, \mathcal{B})$ is a 2-design with $|\mathcal{B}| = v$ and incidence matrix A. As $AA^\top = (k-\lambda)I + \lambda J$, we see that the inverse of our incidence matrix is

$$A^{-1} = \frac{1}{k-\lambda}\left(A^\top - \frac{\lambda}{k}J\right).$$

Letting $\mathbf{r}_i$ denote the i^{th} row of A ($i \in X$), observe that $\mathbf{r}_i \circ \mathbf{r}_j$ is a 01-vector of length v with λ entries equal to one. So $\mathbf{r}_i \circ \mathbf{r}_j = \mathbf{w}^\top A$ gives

$$\mathbf{w}^\top = (\mathbf{r}_i \circ \mathbf{r}_j)\, A^{-1} = \frac{1}{k-\lambda}\sum_{i,j\in B} \mathbf{c}_B^\top - \frac{\lambda^2}{k(k-\lambda)}\mathbf{1}^\top$$

with entries

$$w_h = \frac{-\lambda^2}{k(k-\lambda)} + \frac{1}{k-\lambda}\,|\{B \in \mathcal{B} \mid h,i,j \in B\}|\,;$$

that is, $\mathcal{I}(\mathcal{B})$ contains the quadratic polynomial

$$x_i x_j + \frac{1}{k-\lambda}\sum_{i,j\in B} x^{B,1} - \frac{\lambda^2}{k(k-\lambda)}x^{X,1}.$$

As $x^{X,1}$ takes value k on each $\mathbf{c}_B$, this shows that ideal I contains $f_{i,j}(\mathbf{x})$ for every pair i,j of distinct points.

Set $\mathcal{G} = \mathcal{G}_0 \cup \{f_{i,j} \mid i,j \in X\}$ and consider $\mathsf{I} = \langle \mathcal{G} \rangle$. The dimension of the quotient ring $\mathbb{C}[\mathbf{x}]/\mathsf{I}$ is v since every monomial of degree two is congruent, modulo $\langle \mathcal{G} \rangle$, to some polynomial of degree one[1]. Since we have $\dim \mathbb{C}[\mathbf{x}]/\mathsf{I} = |\mathcal{B}|$, we use Proposition 3.1*(iii)* to see that $\mathcal{Z}(\mathsf{I}) = \mathcal{B}$ and each zero has multiplicity one. It then follows that $\mathsf{I} = \mathcal{I}(\mathcal{B})$ and the cosets of the form $x_i x_j + \mathcal{I}(\mathcal{B})$ $(i \neq j)$ form a basis as claimed. □

Example 5.2. *Consider the case where $(X, \mathcal{B})$ is a symmetric 2-$(v,k,2)$ design. Let $X = \{i : 1 \le i \le v\}$ be the set of points and let $\mathcal{B} = \{B_r : 1 \le r \le v\}$ be the set of blocks in the design. Let i,j be any two distinct points. There are two blocks that contain i and j, say B_r and B_s. Note that $B_r \cap B_s = \{i,j\}$. Denote the symmetric difference by*

$$Z_{i,j} = B_r \cup B_s \setminus \{i,j\}$$

and define

$$f_{i,j}(\mathbf{x}) = (k-2)x_i x_j + 4 - 2(x_i + x_j) - \sum_{h \in Z_{i,j}} x_h.$$

Then $\mathcal{I}(\mathcal{B})$ is generated by $x^{X,1} - k$, $x_i(x_i - 1)$ $(1 \le i \le v)$ and the polynomials $f_{i,j}(\mathbf{x})$.

Theorem 5.3. *Suppose that $(X, \mathcal{B})$ consists of the points and e-dimensional subspaces of $\mathrm{PG}(d,q)$, where $1 \le e < d$. Let $\mathcal{L}$ denote the set of all lines (1-dimensional subspaces) of $\mathrm{PG}(d,q)$. For every line L in $\mathcal{L}$ and every 2-element subset $J \subseteq L$ define $g_{L,J}(\mathbf{x}) = x^{L,2} - \binom{q+1}{2}x^J$. Then*

(i) *$\mathcal{I}(\mathcal{B})$ is generated by $\mathcal{G} := \mathcal{G}_0 \cup \{g_{L,J} \mid L \in \mathcal{L}, J \subseteq L, |J| = 2\}$;*

(ii) *$\gamma_1(\mathcal{B}) = \gamma_2(\mathcal{B}) = 2$;*

[1] *We choose some monomial ordering for the ring $\mathbb{C}[\mathbf{x}]$ which refines the partial order by total degree.*

(iii) *the coordinate ring* $\mathbb{C}[\mathbf{x}]/\mathcal{I}(\mathcal{B})$ *admits a basis consisting of cosets* $\{x_i + \mathcal{I}(\mathcal{B}) \mid 1 \le i \le v\}$.

Proof. Here we have $v = (q^{d+1}-1)/(q-1)$ and $k = (q^{e+1}-1)/(q-1)$. Every line of $\mathrm{PG}(d,q)$ contains $q+1$ points. Suppose B is an e-dimensional subspace of $\mathrm{PG}(d,q)$ and L is a line. Then $|L \cap B| \in \{0, 1, q+1\}$. In each case, $g_{L,J}(B) = 0$ for any 2-element $J \subseteq L$ by Lemma 4.1.

A subset of points of $\mathrm{PG}(d,q)$ that intersects any line in $0, 1$ or $q+1$ points is necessarily a subspace of $\mathrm{PG}(d,q)$. Suppose that $|C| = k$ but C is not an e-dimensional subspace of $\mathrm{PG}(d,q)$. Then there exists a line L such that $|L \cap C| \notin 0, 1, q+1$. In this case, $g_{L,J}(C) \neq 0$ by Lemma 4.1.

We have shown that the ideal generated by $\mathcal{G}$ is a radical ideal with zero set $\mathcal{B}$, so we are done by Proposition 3.1*(ii)*. □

Remark 5.4. *Clearly we can build a much smaller generating set than our choice of* $\mathcal{G}$ *by selecting just one pair* J *of points in each line. We instead prefer here to choose a set* $\mathcal{G}$ *of polynomials which is invariant under the automorphism group of the design.*

6. Triple systems

Identifying each square-free monomial x^C with the set C, the multilinear polynomials with real coefficients are in bijective correspondence with the real-valued functions on the Boolean lattice. For multilinear f write

$$c(f) = (f_D : D \subseteq \{1, \ldots, v\}) \qquad \text{where} \qquad f(\mathbf{x}) = \sum_D f_D x^D.$$

Suppose that $C \subseteq X$ and $0 \le s \le |C|$. The *s-incidence vector* of C, denoted $\delta = \delta^s(C)$, is the vector of length $w = \sum_{i=0}^{s} \binom{v}{i}$, whose coordinates correspond to the subsets of X of cardinality at most s, defined by

$$\delta_J = \begin{cases} 1 & \text{if } J \subseteq C \\ 0 & \text{otherwise,} \end{cases}$$

where $|J| \le s$.

Now suppose that f is a multilinear polynomial in $x_1, \ldots, x_v$ of degree at most s. The vector of coefficients of f, denoted $c = c(f)$, is also a w-dimensional vector whose coordinates correspond to the subsets of X of cardinality at most s.

The following lemma is obvious.

Lemma 6.1. *If* f *is a polynomial of degree at most* s *and* $C \subseteq X$*, then* $f(C) = \delta \cdot c$*, where* $\delta = \delta^s(C)$ *and* $c = c(f)$. ■

Example 6.2. *Suppose that* $X = \{1, 2, 3, 4, 5\}$*,* $C = \{1, 2, 3\}$ *and* $s = 2$*. Let*

$$f = 1 + x_1 + 2x_2 - 3x_3 + 4x_4 - x_1x_2 + +3x_1x_5 + 2x_2x_3 - 3x_3x_5.$$

Then

$$c(f) = (1, 1, 2, -3, 4, 0, -1, 0, 0, 3, 2, 0, 0, 0, -3, 0)$$

and

$$\delta^s(C) = (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0).$$

It is easy to verify that $f(C) = 1 + 1 + 2 - 3 - 1 + 2 = 2$.

Theorem 6.3. *Suppose that* $(X, \mathcal{B})$ *is a* 2-$(v, 3, 2)$ *design such that*

$$\{\{1,2,3\},\{1,4,5\},\{2,4,6\},\{3,5,6\},\{1,2,4\},\{1,3,5\},\{2,3,6\}\} \subseteq \mathcal{B},$$

but

$$\{4,5,6\} \notin \mathcal{B}.$$

Then $\gamma_2(\mathcal{B}) = 3$.

Proof. By Theorems 2.3 and 4.2, we have $2 \leq \gamma_2(\mathcal{B}) \leq 3$. We now show $\gamma_2(\mathcal{B}) > 2$. Denote $B_1 = \{1,2,3\}$, $B_2 = \{1,4,5\}$, $B_3 = \{2,4,6\}$, $B_4 = \{3,5,6\}$, $B_5 = \{1,2,4\}$, $B_6 = \{1,3,5\}$, $B_7 = \{2,3,6\}$ and $C = \{4,5,6\}$. For $s = 2$, it is easy to verify that

$$\delta^s(B_1) + \delta^s(B_2) + \delta^s(B_3) + \delta^s(B_4) = \delta^s(B_5) + \delta^s(B_6) + \delta^s(B_7) + \delta^s(C). \tag{7}$$

For any $f \in \mathcal{I}(\mathcal{B})$, we have that $f(B_1) = f(B_2) = \cdots = f(B_7) = 0$. It then follows from (7) and Lemma 6.1 that $f(C) = 0$. However, since $C \notin \mathcal{B}$, it must be the case that $f(C) \neq 0$ for some $f \in \mathcal{I}(\mathcal{B})$. This contradiction establishes the desired result. □

Note that this linearization technique may be applied more generally. If we can find $C \notin \mathcal{B}$ such that $\delta^s(C)$ is a linear combination of the w-dimensional vectors $\{\delta^s(B) \mid B \in \mathcal{B}\}$, then $\gamma_2(\mathcal{B}) > s$.

We now show one way to construct examples of 2-$(v, 3, 2)$ designs that satisfy the hypotheses of Theorem 6.3. Our construction works for any $v \equiv 1, 3 \pmod 6$, $v \geq 15$.

Suppose we have a 2-$(v, 3, 2)$ design that satisfies the hypotheses of Theorem 6.3. We first observe that

$$\{\{1,2,3\},\{1,4,5\},\{2,4,6\},\{3,5,6\}\} \tag{8}$$

is a set of four blocks that forms a so-called *quadrilateral* (or *Pasch configuration*). As well,

$$\{\{1,2,4\},\{1,3,5\},\{2,3,6\}\} \tag{9}$$

is a set of three blocks that is not contained in a quadrilateral (because $\{4,5,6\}$ is not a block).

We require two ingredients:

1. The unique 2-$(7, 3, 1)$ design is isomorphic to point-line structure of PG$(2, 2)$ and it contains a quadrilateral (in fact, it contains exactly seven distinct quadrilaterals). Therefore the points of this design can be relabelled so it contains the four blocks in (8). Now, from the Doyen-Wilson Theorem, we can embed this 2-$(7, 3, 1)$ design in a 2-$(v, 3, 1)$ design for any $v \equiv 1, 3 \pmod 6$, $v \geq 15$.
2. It is shown in [22, Theorem 3.1] that the maximum number of quadrilaterals in a 2-$(v, 3, 1)$ design is $v(v-1)(v-3)/24$, and this maximum is attained if an only if the design is isomorphic to the point-line structure of the projective geometry PG$(n, 2)$ for some integer $n \geq 2$. Take any 2-$(v, 3, 1)$ design that is not isomorphic to the projective geometry PG$(n, 2)$ (this can be done provided $v \equiv 1, 3 \pmod 6$, $v \geq 9$. It is easy to see that design must contain three non-collinear points that are not contained in a quadrilateral. By relabelling points in the design, we can assume that the three non-collinear points are denoted $1, 2$ and 3, and they are contained in the three blocks in (9). Moreover, $\{4,5,6\}$ is not a block in this design because the three points $1, 2, 3$ are not contained in a quadrilateral.

Now we take the union of the blocks in the two 2-$(v, 3, 1)$ designs constructed above. The result is a 2-$(v, 3, 2)$ design that contains the seven blocks in (8) and (9). We have already noted that $\{4,5,6\}$ is not a block in the second design. It is also not a block in the first design because the pairs $\{4,5\}$, $\{4,6\}$ and $\{5,6\}$ occur in three different blocks in this design.

As a consequence of this discussion and Theorem 6.3, the following result is immediate.

Theorem 6.4. *Suppose* $v \equiv 1, 3 \pmod 6$, $v \geq 15$. *Then there exists a* 2-$(v, 3, 2)$ *design* $(X, \mathcal{B})$ *such that* $\gamma_2(\mathcal{B}) = 3$. ■

We now give a more general version of this construction, starting from an arbitrary trade. We recall some definitions from [12]. A *trade* is a set $\mathbf{T}$ of two (finite) subsets of blocks of size three, say $\mathbf{T} = \{T_1, T_2\}$ that satisfies the following properties:

1. each T_ℓ $(\ell = 1, 2)$ is a partial Steiner triple system (i.e., no pair of points occurs in more than one block)
2. $T_1 \cap T_2 = \emptyset$
3. the set of pairs contained in the blocks in T_1 is identical to the set of pairs contained in the blocks in T_2.

As an example, if

$$T_1 = \{\{1, 2, 3\}, \{1, 4, 5\}, \{2, 4, 6\}, \{3, 5, 6\}\}$$

and

$$T_2 = \{\{1, 2, 4\}, \{1, 3, 5\}, \{2, 3, 6\}, \{4, 5, 6\}\},$$

then $\mathbf{T} = \{T_1, T_2\}$ is a trade.

The *volume* of a trade $\mathbf{T} = \{T_1, T_2\}$, which is denoted $vol(\mathbf{T})$, is the number of blocks in T_1 (or, equivalently, the number of blocks in T_2). The *foundation* of $\mathbf{T}$, denoted $found(\mathbf{T})$, is the set of points covered by the blocks in T_1 (or, equivalently, the set of points covered by the blocks in T_2).

In the above example, $vol(\mathbf{T}) = 4$ and $found(\mathbf{T}) = \{1, 2, 3, 4, 5, 6\}$.

The following lemma is easy to prove.

Lemma 6.5. $\mathbf{T} = \{T_1, T_2\}$ *is a trade. Then*

$$\sum_{B \in T_1} \delta^2(B) = \sum_{B \in T_2} \delta^2(B).$$

Proof. The definition of a trade $\mathbf{T} = \{T_1, T_2\}$ ensures that T_1 and T_2 cover the same set of pairs. So we just need to prove that T_1 and T_2 contain the same points with the same multiplicities. Suppose $i \in found(\mathbf{T})$. Let

$$N_\ell = \{j : \{i, j\} \text{ is contained in a block in } T_1\}.$$

Then it is easy to see that i is contained in $|N_\ell|/2$ blocks in each of T_1 and T_2. □

The following is a slight generalization of Theorem 6.3. We omit the proof, which makes use of Lemma 6.5, since it is essentially the same.

Theorem 6.6. *Let* $\mathbf{T} = \{T_1, T_2\}$ *be a trade. Suppose* $B = \{h, i, j\} \in T_2$. *Suppose that* $(X, \mathcal{B})$ *is* 2-$(v, 3, 2)$ *design such that* $T_1 \cup (T_2 \setminus \{B\}) \subseteq \mathcal{B}$ *and* $B \notin \mathcal{B}$. *Then* $\gamma_2(\mathcal{B}) = 3$. ■

Theorem 6.7. *Suppose that* $\mathbf{T} = \{T_1, T_2\}$ *is a trade, where* $|found(\mathbf{T})| = n$. *Let* $B \in T_1$. *Suppose* $v \equiv 1, 3 \pmod 6$, $v \geq 2n + 3$. *Then there exists a* 2-$(v, 3, 2)$ *containing all the blocks in* $T_1 \cup (T_2 \setminus \{B\})$, *such that* $\gamma_2(\mathcal{B}) = 3$.

Proof. T_1 is a partial Steiner triple system on n points. The famous result of Bryant and Horsley [2] shows that T_1 can be embedded in a 2-$(v, 3, 1)$ design for any $v \equiv 1, 3 \pmod 6$, $v \geq 2n + 1$.

Suppose $B = \{h, i, j\}$ and let $B^* = \{i, j, \ell\}$, where $\ell \notin \mathit{found}(\mathbf{T})$. Define $T_2^* = (T_2 \setminus \{B\}) \cup \{B^*\}$. T_2^* is a partial Steiner triple system on $n+1$ points, so (again, from [2]) it can be embedded in a 2-$(v, 3, 1)$ design for any $v \equiv 1, 3 \pmod 6$, $v \geq 2(n+1)+1$. So for $v \equiv 1, 3 \pmod 6$, $v \geq 2n+3$, we have two 2-$(v, 3, 1)$ designs (which we can assume are defined on the same set of points), say $(Y, \mathcal{B}_1)$ and $(Y, \mathcal{B}_2)$, such that $T_1 \subseteq \mathcal{B}_1$ and $T_2^* \subseteq \mathcal{B}_2$. Then $(Y, \mathcal{B}_1 \cup \mathcal{B}_2)$ is a 2-$(v, 3, 2)$ design that contains all the blocks in $T_1 \cup (T_2 \setminus \{B\})$.

We claim that B is not a block in $\mathcal{B}_1 \cup \mathcal{B}_2$. First, there is a unique block $B' \in \mathcal{B}_1$ that contains the pair $\{i, j\}$, and this block B' is one of the blocks in T_1. Because $B' \in T_1$ and $B \in T_2$, it follows that $B' \neq B$. Therefore $B \notin \mathcal{B}_1$. To see that $B \notin \mathcal{B}_2$, we observe that the unique block in $\mathcal{B}_2$ that contains the pair $\{i, j\}$ is $B^* \neq B$.

Thus we have shown that $(Y, \mathcal{B}_1 \cup \mathcal{B}_2)$ satisfies the hypotheses of Theorem 6.6, and the proof is complete. □

7. Strength greater than two

We finish by addressing the ideals of non-trivial t-(v, k, λ) designs with $t > 2$. For Steiner systems (where $\lambda = 1$), we have

$$\frac{t+1}{2} \leq \gamma_1(\mathcal{B}) \leq \gamma_2(\mathcal{B}) \leq t$$

using Theorem 2.3 and Theorem 4.3. When $\lambda > 1$, the lower bound still holds and we may apply Lemma 2.6: since the number of blocks is

$$|\mathcal{B}| = \lambda \binom{v}{t} \binom{k}{t}^{-1},$$

we find $\gamma_1(\mathcal{B}) \leq s$ whenever $\binom{v}{s}\binom{k}{t} > \lambda\binom{v}{t}$. We also have Corollary 4.7 which tells us that $\gamma_2(\mathcal{B}) \leq m+1$ when m is the maximum size of the intersection of two distinct blocks.

Let $(X, \mathcal{B})$ be a t-(v, k, λ) design. For $i \in X$, the *derived design* of $(X, \mathcal{B})$ with respect to i is the ordered pair $(\dot{X}, \dot{\mathcal{B}})$ where $\dot{X} = X \setminus \{i\}$ and

$$\dot{\mathcal{B}} = \{B \setminus \{i\} \mid i \in B \in \mathcal{B}\}.$$

The *residual design* of $(X, \mathcal{B})$ with respect to i has vertex set $\dot{X}$ and block set $\{B \in \mathcal{B} \mid i \notin B\}$. If $(X, \mathcal{B})$ is a t-design, then both its derived design and its residual design are $(t-1)$-designs.

Lemma 7.1. *Let $(X, \mathcal{B})$ be a non-trivial t-design with $i \in X$. With notation as above $\gamma_h(\dot{\mathcal{B}}) \leq \gamma_h(\mathcal{B})$ for $h = 1, 2$. The same inequalities hold for the residual design.*

Proof. We handle the case of the derived design; the computations for the residual design are similar. To simplify the notation, we take $i = 1$. Let $\mathsf{I} = \mathcal{I}(\mathcal{B})$ and define ideal J as the image of I under the ring homomorphism $\varphi : \mathbb{C}[x_1, \ldots, x_v] \to \mathbb{C}[x_2, \ldots, x_v]$ mapping x_1 to 1 and mapping each x_j to itself for $j = 2, \ldots, v$. For $g \in \mathsf{I}$ write $\dot{g} := \varphi(g) \in \mathsf{J}$. For any $(k-1)$-set $C \subseteq \{2, \ldots, v\}$, we have $\dot{g}(C) = g(C \cup \{1\})$ and so, for $C \in \dot{\mathcal{B}}$ we have $\dot{g}(C) = 0$ for all $\dot{g} \in \mathsf{J}$ and, for $C \notin \dot{\mathcal{B}}$, there exists $\dot{g} \in \mathsf{J}$ for which $\dot{g}(C) \neq 0$. It follows that, if $\mathcal{G}$ is a generating set for I, then $\varphi(\mathcal{G})$ is a generating set for J. This shows $\gamma_2(\dot{\mathcal{B}}) \leq \gamma_2(\mathcal{B})$. Next, if g is a non-trivial polynomial in I of smallest degree, then $\dot{g}$ has degree no larger than the degree of g and is also non-trivial since φ maps trivial ideal to trivial ideal. □

We illustrate this and other results in this paper by recording, in the following table, the exact value of these parameters for the Witt designs and the t-designs appearing as their derived designs. Up to isomorphism, there are unique block designs with parameters 5-$(24, 8, 1)$, 4-$(23, 7, 1)$, 3-$(22, 6, 1)$, 5-$(12, 6, 1)$, 4-$(11, 5, 1)$ and 3-$(10, 4, 1)$. One accessible source of information on the Witt designs is the note [1] by Andries Brouwer.

t-(v,k,λ)	$\gamma_1(\mathcal{B})$	$\gamma_2(\mathcal{B})$	Notes
5-$(24,8,1)$	3	3	Theorems 2.3, 7.2
4-$(23,7,1)$	3	3	Theorem 7.3
3-$(22,6,1)$	2	2	Theorem 7.4
2-$(21,5,1)$	2	2	Theorem 5.3
5-$(12,6,1)$	3	3	discussion below
4-$(11,5,1)$	3	3	Lemma 7.1
3-$(10,4,1)$	2	2	discussion below
2-$(9,3,1)$	2	2	Theorems 2.3, 4.3

In the large Witt design, with parameters 5-$(24,8,1)$, blocks intersect in 0, 2 or 4 points. So we might start with the zonal polynomials

$$(\mathbf{c}_B \cdot \mathbf{x})(\mathbf{c}_B \cdot \mathbf{x} - 2)(\mathbf{c}_B \cdot \mathbf{x} - 4)(\mathbf{c}_B \cdot \mathbf{x} - 8)$$

where $B \in \mathcal{B}$. We know that the blocks of this design are the supports of the minimum weight codewords in the extended binary Golay code. We may then use the fact that this is a self-dual code to show that these, together with the generators of $\mathcal{T}$, generate our ideal. But we can do better.

Theorem 7.2. *Let $(X,\mathcal{B})$ be the 5-$(24,8,1)$ design. For a block $B \in \mathcal{B}$ and points $i,j \in B$, define*

$$f_{B,i,j}(\mathbf{x}) = (x_i - x_j)(\mathbf{c}_B \cdot \mathbf{x} - 2)(\mathbf{c}_B \cdot \mathbf{x} - 4).$$

Then

(i) *$\mathcal{I}(\mathcal{B})$ is generated by $\mathcal{G}_0 \cup \{f_{B,i,j} \mid i,j \in B \in \mathcal{B}\}$;*

(ii) $\gamma_1(\mathcal{B}) = \gamma_2(\mathcal{B}) = 3$.

Proof. We know $\gamma_1(\mathcal{B}) \geq 3$ by Theorem 2.3.

For any block $B \in \mathcal{B}$, the number m_i of blocks $B' \in \mathcal{B}$ with $|B \cap B'| = i$ is given by

i	8	7	6	5	4	3	2	1	0
m_i	1	0	0	0	280	0	448	0	30

So the zonal polynomial (cf. Corollary 2.5) $\prod_{i=8,4,2,0}(\mathbf{c}_B \cdot \mathbf{x} - i)$ belongs to $\mathcal{I}(\mathcal{B})$ and the quadratic polynomial $(\mathbf{c}_B \cdot \mathbf{x} - 2)(\mathbf{c}_B \cdot \mathbf{x} - 4)$ vanishes on every block except B itself and those blocks disjoint from B. But if i and j both belong to block B, the linear function $x_i - x_j$ vanishes on $\mathbf{c}_B$ and on $\mathbf{c}_{B'}$ for any block B' disjoint from B. To show that the polynomials $f_{B,i,j}$ — as B ranges over the blocks and i, j range over the elements of B — together with the polynomials in the trivial ideal, generate our ideal, we employ two basic facts about the extended binary Golay code G_{24}. The blocks in $\mathcal{B}$ are precisely the supports of minimum weight codewords in this code. This is a self-dual code, so a binary tuple $c \in \mathbb{F}_2^{24}$ satisfies $c \in \mathsf{G}_{24}$ if and only if the mod 2 dot product $c \cdot c'$ is zero for every $c' \in \mathsf{G}_{24}$. Since G_{24} is generated by its weight eight codewords, we may say $c \in \mathsf{G}_{24}$ if and only if its inner product with these 759 codewords is zero mod two. Since we only want to recover the codewords of weight eight, we may omit integer inner product six.

Let $\mathsf{I} = \langle \mathcal{G}_0 \cup \{f_{B,i,j} \mid i,j \in B \in \mathcal{B}\}\rangle$ and observe that any element of $\mathcal{Z}(\mathsf{I})$ has exactly eight entries equal to one and sixteen entries equal to zero. For $c \in \mathbb{F}_2^{24}$, let $\mathbf{c} \in \mathbb{R}^{24}$ be the corresponding 01-vector with real entries: $\mathbf{c}_j = 1$ if $c_j = 1$ and $\mathbf{c}_j = 0$ if $c_j = 0$. Assuming $\mathbf{c} \in \mathcal{Z}(\mathsf{I})$, we have $f_{B,i,j}(\mathbf{c}) = 0$ for each $B \in \mathcal{B}$ and each $i,j \in B$ which implies that either $\mathbf{c}_B \cdot \mathbf{c} \in \{2,4\}$ or $c_i = 1 \Leftrightarrow c_j = 1$ for all $i,j \in B$. This latter alternative clearly means that either $\mathbf{c} = \mathbf{c}_B$ or $\mathbf{c} \cdot \mathbf{c}_B = 0$. For the corresponding binary vectors, this implies $c \cdot c' = 0$ for each $c' \in \mathsf{G}_{24}$ with Hamming weight eight. As outlined above, this gives $c \in \mathsf{G}_{24}$ and, in turn, $\mathbf{c} = \mathbf{c}_{B'}$ for some $B' \in \mathcal{B}$. By Propositions 3.2 and 3.1*(ii)*, we have $\mathsf{I} = \mathcal{I}(\mathcal{B})$. □

Theorem 7.3. *Let $(X, \mathcal{B})$ be the 4-$(23, 7, 1)$ design. For three distinct points i, j and k, let $\mathcal{C}_{i,j,k} = \{C = B \setminus \{i,j,k\} \mid \{i,j,k\} \subseteq B \in \mathcal{B}\}$ and define*

$$h_{i,j,k}(\mathbf{x}) = 3 + 12x_ix_jx_k - 3(x_ix_j + x_ix_k + x_jx_k) - \sum_{C \in \mathcal{C}_{i,j,k}} x^{C,2} .$$

Then

(i) *$\mathcal{I}(\mathcal{B})$ is generated by $\mathcal{G}_0 \cup \{h_{i,j,k} \mid i,j,k\}$;*

(ii) *$\gamma_1(\mathcal{B}) = \gamma_2(\mathcal{B}) = 3$;*

(iii) *the coordinate ring $\mathbb{C}[\mathbf{x}]/\mathcal{I}(\mathcal{B})$ admits a basis consisting of those $\binom{23}{2}$ cosets $x_ix_j + \mathcal{I}(\mathcal{B})$ represented by multilinear monomials of degree two.*

Proof. Denote by B_1, B_2, B_3, B_4, B_5 the five blocks containing $T := \{i,j,k\}$ and set $C_\ell = B_\ell \setminus T$. We know that two distinct blocks of our Witt design intersect in either three points or one point. We now show that $h_{i,j,k}(B) = 0$ for each $B \in \mathcal{B}$. To illustrate the simple arithmetic involved, we write

$$h_{i,j,k}(\mathbf{x}) = 3 + 12(x_ix_jx_k) - 3(x_ix_j + x_ix_k + x_jx_k) - (x^{C_1,2}) - (x^{C_2,2}) - (x^{C_3,2}) - (x^{C_4,2}) - (x^{C_5,2})$$

where $B_\ell = C_\ell \cup T$ and we retain most of the parentheses here in our evaluation.

case (1) $T \subseteq B$. Here, we have $B = B_\ell$ for some $\ell \in \{1, \ldots, 5\}$ and

$$h_{i,j,k}(B) = 3 + 12(1) - 3(1+1+1) - (1+1+1+1+1+1) - (0) - (0) - (0) - (0) = 0.$$

case (2) $|T \cap B| = 2$. Here we must have $|B \cap B_\ell| = 3$ for all ℓ and, as B never contains two points from the same "sub-block" $C_\ell = B_\ell \setminus T$, we have

$$h_{i,j,k}(B) = 3 + 12(0) - 3(1) - (0) - (0) - (0) - (0) - (0) = 0.$$

case (3) $|T \cap B| = 1$. In this case, as there are five blocks containing T and $|B| = 7$, we must have $|B \cap B_\ell| = 3$ for exactly three values of ℓ and, as B contains two points from the same sub-block $C_\ell = B_\ell \setminus T$ in each of these three cases, we have

$$h_{i,j,k}(B) = 3 + 12(0) - 3(0) - (1) - (1) - (1) - (0) - (0) = 0.$$

case (3) $T \cap B = \emptyset$. In this case, as there are five blocks containing T and $|B| = 7$, we must have $|B \cap C_\ell| = 3$ for some unique sub-block $C_\ell = B_\ell \setminus T$ and B must contain a unique point from each of the other four. In this case, we have

$$h_{i,j,k}(B) = 3 + 12(0) - 3(0) - (1+1+1) - (0) - (0) - (0) - (0) = 0.$$

On the other hand, if S is a 7-set of points which is not a block, then $h_{i,j,k}(S) \neq 0$ for any $\{i,j,k\} \subseteq S$. For if $T := \{i,j,k\}$ is contained in S and $h_{i,j,k}(S) = 0$, then we have

$$0 = h_{i,j,k}(S) = 3 + 12(1) - 3(1+1+1) - \binom{m_1}{2} - \binom{m_2}{2} - \binom{m_3}{2} - \binom{m_4}{2} - \binom{m_5}{2}$$

where $m_\ell = |S \cap C_\ell|$. But $m_1 + \cdots + m_5 = 4$ and we see that the only arrangement that achieves the stated equality is where some $m_\ell = 4$. But then $S = B_\ell$ and we are done. So, if

$$\mathsf{I} = \langle \mathcal{G}_0 \cup \{h_{i,j,k} \mid i,j,k\} \rangle$$

we have shown $\mathcal{Z}(\mathsf{I}) = \{\mathbf{c}_B \mid B \in \mathcal{B}\}$. By Proposition 3.2, I is a radical ideal. so Proposition 3.1*(ii)* gives us $\mathsf{I} = \mathcal{I}(\mathcal{B})$. This proves that $\gamma_2(\mathcal{B}) = 3$ and, by Theorem 2.3, $\gamma_1(\mathcal{B}) = 3$ as well.

By Lemma 3.3, each coset $x_i + \mathsf{I}$ can be expressed as a linear combination of cosets $x_ix_j + \mathsf{I}$. Since the number of blocks of the design is $\binom{23}{2}$, we see that the cosets $\{x_ix_j + \mathsf{I} \mid i,j\}$ form a vector space basis for $\mathbb{C}[\mathbf{x}]/\mathsf{I}$. □

Next, if $(X, \mathcal{B})$ denotes the Witt design on 22 points, Lemma 7.1 tells us $2 \leq \gamma_1(\mathcal{B}) \leq \gamma_2(\mathcal{B}) \leq 3$. We now show that both values are equal to two.

Theorem 7.4. *Let $(X, \mathcal{B})$ be the 3-$(22, 6, 1)$ design. For two distinct points i, j and a block B containing them, say $B = \{i, j, r, s, t, u\}$, define*

$$h_{i,j,B}(\mathbf{x}) = (x_i - x_j)(x_r + x_s + x_t + x_u - 1).$$

Then

(i) *$\mathcal{I}(\mathcal{B})$ is generated by $\mathcal{G}_0 \cup \{h_{i,j,B} \mid i \neq j,\ i, j \in B,\ B \in \mathcal{B}\}$;*

(ii) *$\gamma_1(\mathcal{B}) = \gamma_2(\mathcal{B}) = 2$;*

(iii) *the coordinate ring $\mathbb{C}[\mathbf{x}]/\mathcal{I}(\mathcal{B})$ admits a basis consisting of the 77 cosets $x^{B,2} + \mathcal{I}(\mathcal{B})$ obtained as B ranges over the blocks of the design.*

Proof. By Theorem 2.3, we have $\gamma_1(\mathcal{B}) \geq 2$. Consider $B \in \mathcal{B}$ and two distinct points $i, j \in B$. Write $B = \{i, j, r, s, t, u\}$. Since any two blocks of this design intersect in zero or two points, any block B' that contains exactly one of i, j contains exactly one element from $\{r, s, t, u\}$. So $h_{i,j,B}(B') = 0$. The same holds if $|B' \cap \{i, j\}|$ is even. On the other hand, let C be a 6-element subset of X and choose three distinct points $i, t, u \in C$. There is a unique block B containing these three points, say $B = \{i, j, r, s, t, u\}$. If all three polynomials $h_{i,j,B}(\mathbf{x})$, $h_{i,r,B}(\mathbf{x})$, $h_{i,s,B}(\mathbf{x})$ vanish on C, then we must have $C = B$. This finishes the proof that $\mathcal{Z}(\mathcal{G}) = \{\mathbf{c}_B \mid B \in \mathcal{B}\}$ and, as $\mathcal{G}_0 \subseteq \mathcal{G}$, the ideal $\langle \mathcal{G} \rangle$ is radical, proving **(i)** and **(ii)**.

To show that the functions on $\mathcal{B}$ represented by the polynomials $\{x^{B,2} \mid B \in \mathcal{B}\}$ are linearly independent, consider the 77×77 matrix M with (B, B')-entry equal to the value the polynomial $x^{B',2}$ takes at the point $\mathbf{c}_B$. Then $M - I$ is the adjacency matrix of a well-known[2] strongly regular graph with eigenvalues 60, 5 and -3. It follows that M is invertible and the 77 cosets $\{x^{B,2} + \mathcal{I}(\mathcal{B}) \mid B \in \mathcal{B}\}$ are linearly independent in the coordinate ring. □

For the small Witt designs, we do not have a computer-free proof of our claims. Let us instead describe some generators for the ideals.

First consider the unique Witt design on twelve points. Let $(X, \mathcal{B})$ be the 5-$(12, 6, 1)$ design. For three distinct points i, j and k, let $C = X \setminus \{i, j, k\}$. The twelve blocks containing i, j and k yield a 2-$(9, 3, 1)$ design

$$(C, \mathcal{B}'), \qquad \mathcal{B}' = \{B \setminus \{i, j, k\} \mid i, j, k \in B \in \mathcal{B}\}$$

on the point set C and the four parallel classes of this affine plane may be oriented in a total of sixteen ways (each resulting in a 4-set of directed triples of blocks). We find that certain orientations yield polynomials of degree three which, together with those polynomials in $\mathcal{G}_0$, generate the ideal $\mathcal{I}(\mathcal{B})$. This shows $\gamma_1(\mathcal{B}) = \gamma_2(\mathcal{B}) = 3$.

To be precise, let M_{12} be the subgroup of S_{12} generated by

$$\{(1\ 4)(3\ 10)(5\ 11)(6\ 12),\ \ (1\ 8\ 9)(2\ 3\ 4)(5\ 12\ 11)(6\ 10\ 7)\}$$

and consider the 132 6-sets in the orbit containing $\{1, 2, 3, 4, 5, 9\}$. Since M_{12} is 5-transitive, this is a 5-$(12, 6, 1)$ design. Two parallel lines in the derived design consisting of all blocks containing points 1, 2 and 3 are $\{4, 5, 9\}$ and $\{8, 10, 11\}$. With a computer, one easily verifies that the polynomial

$$\begin{aligned} F(\mathbf{x}) \ = \ & x_1x_4(x_{10} - x_{11}) + x_1x_5(x_{11} - x_8) + x_1x_9(x_8 - x_{10}) + \\ & x_2x_9(x_{10} - x_{11}) + x_2x_4(x_{11} - x_8) + x_2x_5(x_8 - x_{10}) + \\ & x_3x_5(x_{10} - x_{11}) + x_3x_9(x_{11} - x_8) + x_3x_4(x_8 - x_{10}) \end{aligned}$$

[2] *See, for example,* https://www.win.tue.nl/~aeb/graphs/srg/srgtab51-100.html

vanishes on each block of the design. It follows that any image

$$[1^\pi, 2^\pi, 3^\pi], [4^\pi, 5^\pi, 9^\pi], [10^\pi, 11^\pi, 8^\pi]$$

of the three triples of indices under any $\pi \in \mathsf{M}_{12}$ yields another polynomial in the ideal. It requires a bit more computation, using the SINGULAR computer algebra system [15], to check that the ideal $\mathcal{I}(\mathcal{B})$ is generated by these polynomials together with those in $\mathcal{G}_0$. The relative orderings within the three triples above is important and we do not have an intrinsic description of the permissible orderings that yield vanishing polynomials.

If we take the above computation as correct, we may determine γ_1 and γ_2 for the Witt design on eleven points. If $(X, \mathcal{B})$ now denotes a 4-$(11, 5, 1)$ design, we may use Theorem 2.3 to see that $\gamma_1(\mathcal{B}) \geq 3$. By Lemma 7.1, we have equality, and $\gamma_2(\mathcal{B}) = 3$ as well.

Without proof, we note that if $(X, \mathcal{B})$ is the unique 3-$(10, 4, 1)$ design [23, Fig. 9.1], we find $\gamma_1(\mathcal{B}) = \gamma_2(\mathcal{B}) = 2$. In addition to the generators of the trivial ideal, we build certain quadratic generators from any pair B_1, B_2 of disjoint blocks. In order to explain these generators, we first describe the design.

For the construction in [23], we take $X = \mathbb{F}_3^2 \cup \{\infty\}$ with the numbering

0	1	2	3	4	5	6	7	8	9
∞	(0,0)	(1,0)	(2,0)	(0,1)	(1,1)	(2,1)	(0,2)	(1,2)	(2,2)

and blocks $\{0\} \cup \ell$ where ℓ is a line of $AG(2, 3)$ and the following eighteen symmetric differences of orthogonal lines:

$$\begin{array}{cccccccccc} 1245, & 1278, & 1269, & 1346, & 1379, & 1358, & 2356, & 2389, & 2347, \\ 4578, & 4679, & 5689, & 1567, & 2468, & 3459, & 1489, & 2579, & 3678. \end{array}$$

For any pair $B_1, B_2 \in \mathcal{B}$ with $B_1 \cap B_2 = \emptyset$, the number $m_{i,j}$ of blocks $B \in \mathcal{B}$ with $|B \cap B_1| = i$ and $|B \cap B_2| = j$ is given in the following table:

$i \backslash j$	0	1	2	3	4
0	0	0	2	0	1
1	0	0	8	0	0
2	2	8	8	0	0
3	0	0	0	0	0
4	1	0	0	0	0

For each $i \in B_1$, the two blocks meeting B_1 only in this point partition B_2 into two sets of size two by their intersections. We select one of these two to determine two neighbours of i along an octagon as in Figure 1. Once B_1 and B_2 have been selected and this choice of a pair of neighbours has been made, this determines a quadratic generator for our ideal. We illustrate this with $B_1 = \{0, 1, 2, 3\}$ and $B_2 = \{4, 5, 7, 8\}$. The resulting polynomial is

$$g(\mathbf{x}) = x_0x_5 - x_5x_1 + x_1x_7 - x_7x_3 + x_3x_8 - x_8x_2 + x_2x_4 - x_4x_0.$$

We leave it to the reader to check that the way in which any block intersects this configuration guarantees that $g(\mathbf{c}_B) = 0$ for any $B \in \mathcal{B}$. In fact, just five of these polynomials are needed — along with $\mathcal{G}_0$ — to generate the ideal.

8. Conclusion

We have introduced an algebraic approach to the study of t-designs which builds on existing machinery tied to the space of polynomial functions on blocks. For a design $(X, \mathcal{B})$, we introduced the ideal

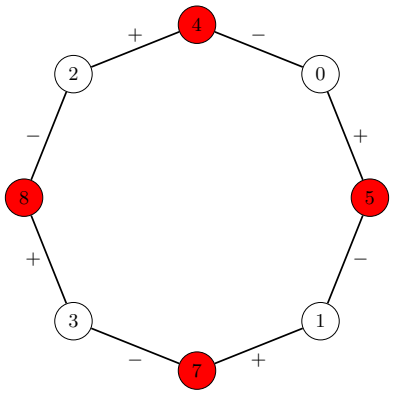

Figure 1. Two disjoint blocks $\{0,1,2,3\}$ and $\{4,5,7,8\}$ and the quadratic polynomial obtained from the pair

$\mathcal{I}(\mathcal{B})$ and proposed two parameters $\gamma_1(\mathcal{B})$ and $\gamma_2(\mathcal{B})$ which we claim capture essential information in the case of designs where the number of blocks achieves, or is close to, the bound of Ray-Chaudhuri and Wilson. We prove, among other things, that

$$\frac{t+1}{2} \le \gamma_1(\mathcal{B}) \le \gamma_2(\mathcal{B}) \le k$$

with the upper bound of k replaced by t in the case of Steiner systems or partial Steiner systems. We determine the exact value of these parameters for symmetric 2-designs and the Witt designs. By constructing many triple systems with $\gamma_2(\mathcal{B}) = k$, we indicate that $\gamma_2(\mathcal{B})$ can be larger than t. While we expect the value to be more typically close to k, we leave this as an open problem.

One may also investigate the ideal vanishing on the codewords of an error-correcting code. In order to compute γ_1 and γ_2 in such a situation, we have some degree of freedom as these parameters are invariant under affine transformations (provided one is careful with the definition of the trivial ideal). Representing the codewords of a binary linear $[n,k,d]$ code C by ± 1 vectors in $\mathbb{R}^n$, we see that each dual codeword $c = [c_1, \ldots, c_n]$ corresponds to an element $f_c(\mathbf{x}) = -1 + \prod_j x_j^{c_j}$ in the ideal of our code. In the linear case, $\gamma_1(C)$ is the minimum distance of $C^\perp$ and $\gamma_2(C)$ seems tied to the smallest g such that $C^\perp$ is generated by its codewords of weight g or less. So it seems interesting to classify those codes C for which $\gamma_1(C) = \gamma_2(C)$ as these seem related to tight designs.

Acknowledgment: The authors thank Padraig Ó Catháin, Bill Kantor and Brian Kodalen for useful comments on the work presented here. We are grateful to the referee for several improvements to the manuscript.

References

[1] A. E. Brouwer, The Witt designs, Golay codes and Mathieu groups, *Unpublished notes*, https://www.win.tue.nl/~aeb/2WF02/Witt.pdf.

[2] D. Bryant, D. Horsley, A proof of Lindner's conjecture on embeddings of partial Steiner triple systems. J. Combin. Des. 17 (2009) 63–89.

[3] A. R. Calderbank, P. Delsarte, Extending the t–design concept, Trans. Amer. Math. Soc. 338 (1993) 941–952.

[4] P. J. Cameron, Near–regularity conditions for designs, Geom. Dedicata 2 (1973) 213–223.
[5] M. Conder, C. D. Godsil, The symmetric group as a polynomial space, Combinatorial and Graph-Theoretical Problems in Linear Algebra (R.A. Brualdi, S. Friedland and V. Klee, eds.) IMA Vol. Math. Appl. 50 (1993) 219–227.
[6] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra (4th ed.), Springer-Verlag Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2015.
[7] E. Croot, V. F. Lev, P. P. Pach, Progression–free sets in $\mathbb{Z}_4^n$ are exponentially small, Ann. of Math. 185 (2017) 331–337.
[8] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Reports Suppl. No. 10, 1973.
[9] P. Delsarte, Hahn polynomials, discrete harmonics, and t-designs, SIAM J. Appl. Math. 34(1) (1978) 157–166.
[10] D. S. Dummit, R. M. Foote, Abstract Algebra (3rd ed.), John Wiley and Sons, Hoboken, 2004.
[11] J. S. Ellenberg, D. Gijswijt, On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression, Ann. of Math. 185 (2017) 339–343.
[12] A. D. Forbes, M. J. Grannell, T. S. Griggs, Configurations and trades in Steiner triple systems, Australas. J. Combin. 29 (2004) 75–84.
[13] W. Fulton, Algebraic Curves: An Introduction to Algebraic Geometry, Advanced Book Classics, Addison-Wesley, Reading, Mass., 1989.
[14] C. D. Godsil, Algebraic Combinatorics, Chapman and Hall, New York, 1993.
[15] G.-M. Greuel, G. Pfister, H. Schönemann, SINGULAR 3.0.2. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern, 2005.
[16] P. Keevash, The existence of designs, Preprint v.3, (2019) arXiv:1401.3665.
[17] W. J. Martin, C. L. Steele, On the ideal of the shortest vectors in the Leech lattice and other lattices, J. Algebraic Combin. 41(3) (2015) 707–726.
[18] W. J. Martin, An ideal associated to any cometric association scheme, In preparation.
[19] H. Maruri–Aguilar, H. P. Wynn, Algebraic Method in Experimental Design, pp. 415–454. In: Handbook of Design and Analysis of Experiments (1st Ed.) Chapman & Hall/CRC Handbooks of Modern Statistical Methods, Boca Raton, 2015.
[20] H. M. Möller, On the construction of cubature formulae with few nodes using Groebner bases, pp. 177–192 in: Numerical integration (Halifax, N.S., 1986) NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 203, Reidel, Dordrecht, 1987.
[21] D. K. Ray-Chaudhuri, R. M. Wilson, On t-designs, Osaka J. Math. 12(3) (1975) 737–744.
[22] D. R. Stinson, Y. J. Wei, Some results on quadrilaterals in Steiner triple systems, Discrete Math. 105(1–3) (1992) 207–219.
[23] D. R. Stinson, Combinatorial Designs: Constructions and Analysis, Springer, New York, 2004.
[24] T. Tao, Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory. EMS Surv. Math. Sci. 1 (2014) 1–46.