Ideals, varieties, stability, colorings and combinatorial designs

Feliú Sagols[1] **Javier Muñoz**

Departamento de Matemáticas
Centro de Investigación y de Estudios Avanzados del IPN
Apartado Postal 14–740
07000 México City, D.F.
fsagols@math.cinvestav.mx jmunoz@math.cinvestav.mx

Charles J. Colbourn[2]

Department of Computer Science and Engineering
Arizona State University
Po Box 878809
Tempe, Arizona, U.S.A.
Charles.Colbourn@asu.edu

Abstract

A combinatorial design is equivalent to a stable set in a suitably chosen Johnson graph, whose vertices correspond to all k-sets that could be blocks of the design. In order to find maximum stable sets of a graph G, two ideals are associated with G, one constructed from the Motzkin-Strauss formula and one reported by Lovász in connection with the stability polytope. These ideals are shown to coincide and form the *stability ideal* of G. Graph stability ideals belong to a class of *0-1* ideals. These ideals are shown to be radical, and therefore have a strong structure.

Stability ideals of Johnson graphs provide an algebraic characterization that can be used to generate Steiner triple systems. Two different ideals for the generation of Steiner triple systems, and a third for Kirkman triple systems, are developed. The last of these combines stability and colorings.

1 Introduction

Our main objective is to establish links between design theory and algebraic geometry through the use of ideals and Gröbner bases. We concentrate on Steiner triple systems because they are simple designs with well known properties; however, the algebraic geometry techniques that we use can be easily translated to other designs.

[0] *Key words and phrases.* Computational Algebraic Geometry, Göbner basis, Combinatorial Designs, Steiner Triple Systems, 0-1 Ideals.

[1] Partially supported by SNI under contract number 7008.

[2] Partially supported by DOD grant N00014-08-1-1069.

Let us start defining the fundamental objects and concepts from design theory, graph theory and algebraic geometry with which we work. A *maximum packing by triples* (MPT or MPT(n)) of order $n > 0$ is maximum cardinality set of triples in $\{0, \ldots, n-1\}$ such that every pair $i, j \in \{0, \ldots, n-1\}$ is in at most one triple. MPTs exist for every $n \geq 3$. When $n \equiv 1, 3 \pmod 6$, an MPT(n) is a *Steiner triple system* (STS or STS(n)); in this case, every 2-subset of elements appears in exactly one triple.

All graphs considered here are simple. Let v, ℓ, and i be fixed positive integers, with $v \geq \ell \geq i$. Let Ω be a cardinality v set. Define a graph $J(v, \ell, i)$ as follows. The vertices of $J(v, \ell, i)$ are the ℓ-subsets of Ω, two ℓ-subsets being adjacent if their intersection has cardinality i. Therefore, $J(v, \ell, i)$ has $\binom{v}{\ell}$ vertices and it is a regular graph with valency $\binom{\ell}{i}\binom{v-\ell}{\ell-i}$. For $v \geq 2\ell$, graphs $J(v, \ell, \ell-1)$ are *Johnson* graphs [10].

One of the main methods that we use to characterize MPT(n)s consists of finding stable sets (or independent sets) in $J(n, 3, 2)$. A *stable set* S of a graph G is a subset of vertices in $V(G)$ containing no pair of adjacent vertices in G. The maximum size of a stable set in G is the *stability number* of G, denoted by $\alpha(G)$.

The *stability polytope* of a n-vertex graph G is the convex hull of $\{(x_0, \ldots, x_{n-1}) | x_i = 1$ or $x_i = 0$ and $\{i \in V(G) | x_i = 1\}$ is a stable set of $G\}$.

We also use vertex colorings. A λ *vertex coloring* (or coloring for short) of a graph G (where λ is a positive integer) is a function $c : V(G) \to \{1, \ldots, \lambda\}$ such that $(v, w) \in E(G)$ if and only if $c(v) \neq c(w)$. The minimum value of λ for which a λ coloring of G exists is the *chromatic number* of G, denoted by $\chi(G)$.

We introduce some algebraic structures. For k a field, $k[\mathbf{x}] = k[x_1, \ldots, x_n]$ is the *polynomial ring* in n variables. A subset $I \subset k[x_1, \ldots, x_n]$ is an *ideal* of $k[x_1, \ldots, x_n]$ if it satisfies $0 \in I$; if $f, g \in I$, then $f + g \in I$; and if $f \in I$ and $h \in k[x_1, \ldots, x_n]$ then $hf \in I$. When $f_1, \ldots, f_s$ are polynomials in $k[x_1, \ldots, x_n]$ we set

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \middle| h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}.$$

Then $\langle f_1, \ldots, f_s \rangle$ is an ideal (see [6]) of $k[x_1, \ldots, x_n]$, the *ideal generated by* $f_1, \ldots, f_s$. One remarkable result, the *Hilbert Basis Theorem* (see [6]), establishes that every ideal $I \subset k[x_1, \ldots, x_n]$ has a finite generating set.

The monomials in $k[\mathbf{x}]$ are denoted by $x^{\mathbf{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$; they are identified with lattice points $\mathbf{a} = (a_1, \ldots, a_n)$ in $\mathbb{N}^n$, where $\mathbb{N}$ is the set of nonnegative integers. A total order $\prec$ on $\mathbb{N}^n$ is a *term order* if the zero vector is the unique minimal element, and $\mathbf{a} \prec \mathbf{b}$ implies $\mathbf{a} + \mathbf{c} \prec \mathbf{b} + \mathbf{c}$ for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{N}^n$.

Given a term order $\prec$, every nonzero polynomial $f \in k[\mathbf{x}]$ has a unique initial monomial, denoted by $in_\prec(f)$. If I is an ideal in $k[\mathbf{x}]$, then its *initial ideal* is the monomial ideal $in_\prec(I) := \langle in_\prec(f) \;:\; f \in I \rangle$.

The monomials that do not lie in $in_\prec(I)$ are *standard monomials*. A finite subset $\mathcal{G} \subset I$ is a Gröbner basis for I with respect to $\prec$ if $in_\prec(I)$ is generated by $\{in_\prec(g) \;:\; g \in \mathcal{G}\}$. If no monomial in this set is redundant, the Gröbner basis is unique for I and $\prec$, provided that the coefficient of $in_\prec(g)$ in g is 1 for each $g \in \mathcal{G}$.

A finite subset $\mathcal{U} \subset I$ is a *universal Gröbner basis* if $\mathcal{U}$ is a Gröbner basis of I with respect to all term orders $\prec$ simultaneously.

A field k is *algebraically closed* if for every polynomial $f \in k[x]$ in one variable, the equation $f(x) = 0$ has a solution in k. Every field k is contained in a field $\bar{k}$ that is algebraically closed and such that every element of $\bar{k}$ is the root of a nonzero polynomial in one variable with coefficients in k. This field is unique up to isomorphism, and is the *algebraic closure* of k.

Given a subset $S \subseteq k[x_1, \ldots, x_n]$, the *variety* $V_{\bar{k}}(S)$ in $\bar{k}^n$ is

$$V_{\bar{k}}(I) = \{(a_1, \ldots, a_n) \in \bar{k}^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\}.$$

If $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$ then

$$V_{\bar{k}}(I) = \{(a_1, \ldots, a_n) \in \bar{k}^n \mid f_i(a_1, \ldots, a_n) = 0,\ 1 \leq i \leq s\} = V_{\bar{k}}(f_1, \ldots, f_s).$$

One of the most remarkable results in algebraic geometry is the following.

Theorem 1.1 (Weak Hilbert Nullstellensatz (see [11]**))** *Let I be an ideal contained in $k[x_1, \ldots, x_n]$. Then $V_{\bar{k}}(I) = \emptyset$ if and only if $I = k[x_1, \ldots, x_n]$*

We may use this theorem to demonstrate that some designs do not exist, by proving that they correspond to varieties of ideals whose reduced Gröbner basis is $\{1\}$, or equivalently that $I = k[x_1, \ldots, x_n]$ and, by the weak Hilbert Nullstellensatz, the variety is empty.

These are the fundamental objects employed, and more specific definitions are introduced as needed. With the exception of the ideals introduced in Section 7, we use the field of rational numbers. When an algebraic closed field is needed, the complex numbers are used instead. Computations for Gröbner basis ideals are done in Macaulay 2 [8].

The paper is organized as follows. In Section 2 an ideal to generate stable sets based on the Motzkin-Strauss formula [15] is first introduced. Then a general ideal introduced by Lovász [14], which has been extensively used for the generation of stable sets in graphs, is described. Both ideals are examples of *0-1 ideals*, a recently introduced class having combinatorial applications beyond stability (see [18]). These ideals are shown to be radical, and consequently the equality of the two ideals is established. Section 3 introduces basic properties of stability ideals. In Section 4 the stability ideal of $J(n, 3, 2)$ is determined and used to build MPTs; difficulties to solve the equations involved are explored, and potential means to generate MPTs with restrictions are examined. In particular a modification of the stability ideal of $J(n, 3, 2)$ is shown to generate anti-Pasch MPTs. Section 5 introduces two new ideals to generate MPTs that use colorings instead of stable sets. Section 6 introduces an ideal to generate Kirkman triple systems that employs a mixture of techniques based on stable sets and on colorings. Section 7 explores parametric generation of MPTs. Finally, in section 8 some concluding remarks are made.

2 Stable sets and ideals

Combinatorial and algebraic aspects of the stable set problem have been extensively studied. One of the most interesting connections is given by the Motzkin-Strauss explicit formula for $\alpha(G)$ (see [15]):

Theorem 2.1 *Let $G = (V, E)$ be a graph. Then*

$$1 - \frac{1}{\alpha(G)} \quad = \quad max \left\{ 2 \sum_{i,j \notin E} x_i x_j \middle| \sum_{i \in V(G)} x_i = 1, x_i \geq 0 \right\}. \tag{1}$$

The Motzkin-Strauss formula enables one to determine part of the structure of the stability polytope, and consequently to prove several results in extremal graph theory, including Turán's Theorem. In (1), $\alpha(G)$ is determined by an optimization problem which at first sight might be solved by Lagrange multipliers. Unfortunately the objective function reaches its maximum at the feasible region boundary and out of this region it is unbounded. We can circumvent this problem by squaring each variable to get a different version of the Motzkin-Strauss formula that still yields $\alpha(G)$:

$$1 - \frac{1}{\alpha(G)} \quad = \quad \max \left\{ 2 \sum_{i,j \notin E} y_i^2 y_j^2 \middle| \sum_{i \in V(G)} y_i^2 = 1 \right\}. \tag{2}$$

Lagrange multipliers can be used for (2). Make the objective function's gradient equal to a multiplier λ times the restriction function's gradient to obtain the system of equations:

$$\begin{aligned} 4y_i \sum_{j \in V(G) | i,j \notin E} y_j^2 &= 2\lambda y_i \text{ for each } i \in V(G), \qquad (3) \\ \sum_{i \in V(G)} y_i^2 &= 1. \end{aligned}$$

This system has several solutions that do not maximize (2). Lovász [14] characterizes the set of maximum solutions for (1): Any vector $\mathbf{x}$ maximizes the right hand side if and only if $\mathbf{x}$ has a stable set as support and if $x_i \neq 0$ for some $i \in V(G)$ then $x_i = 1/\alpha(G)$. Let $\mathbf{y}$ be an optimal solution to (2) such that $y_j \geq 0$ for every $j \in V(G)$. From (3), if $y_i \neq 0$ then

$$4\frac{\alpha(G) - 1}{\alpha(G)\sqrt{\alpha(G)}} = 4\frac{1}{\sqrt{\alpha(G)}} \frac{\alpha(G) - 1}{\alpha(G)} = 4y_i \sum_{j \in V(G) | i,j \notin E} y_j^2 = 2\lambda y_i = 2\lambda \frac{1}{\sqrt{\alpha(G)}}$$

So, a solution of (3) is a maximum of the objective function in (2) if and only if $\lambda = 2\frac{\alpha(G)-1}{\alpha(G)}$. If we substitute this value in (3), substitute $z_i = y_i^2 \alpha(G)$, and introduce the equations $z_i(z_i - 1) = 0$ to restrict the values of z_i to 0 or 1, then we transform (3) into

$$
\begin{aligned}
z_i(z_i-1) &= 0 \text{ for each } i \in V(G), \qquad (4)\\
z_i(\sum_{j\in V(G)|i,j\notin E} z_j - \alpha(G)+1) &= 0 \text{ for each } i \in V(G),\\
\sum_{i\in V(G)} z_i - \alpha(G) &= 0.
\end{aligned}
$$

This yields:

Proposition 2.2 *The graph G has stability number at least e if and only if the following zero-dimensional system of equations*

$$
\begin{aligned}
x_i^2 - x_i &= 0 \quad \textit{for every node } i \in V(G), \qquad (5)\\
x_i(\sum_{j\in V(G)|i,j\notin E} x_j - e + 1) &= 0 \quad \textit{for each } i \in V(G),\\
\sum_{i=1}^{n} x_i - e &= 0,
\end{aligned}
$$

has a solution. The vector $\mathbf{x}$ *is a solution of (5) if and only if the support of* $\mathbf{x}$ *is a stable set.*

The ideal generated by the polynomials in (5) is the *Motzkin-Strauss ideal* of G, denoted by $MS(G)$.

A second approach was introduced by Lovász [14].

Proposition 2.3 (Lovász) *The graph G has stability number at least e if and only if the zero-dimensional system of equations*

$$
\begin{aligned}
x_i^2 - x_i &= 0 \quad \textit{for every node } i \in V(G), \qquad (6)\\
x_i x_j &= 0 \quad \textit{for every edge } \{i,j\} \in E(G),\\
\sum_{i=1}^{n} x_i - e &= 0,
\end{aligned}
$$

has a solution. Vector $\mathbf{x}$ *is a solution of (6) if and only if the support of x is a stable set.*

Proof: If there exists some solution $\mathbf{x}$ to these equations, the identities $x_i^2 - x_i = 0$ ensure that all variables take values only in $\{0,1\}$. The set $S = \{i|x_i = 1\}$ is stable because equations $x_i x_j = 0$ guarantee that the end points of any edge in E(G) cannot belong simultaneously to S. Finally the cardinality of S is e by the last equation. ■

The ideal generated by the polynomials in (6) is the *stability ideal* of G, denoted by $S(G)$. As Lovász [14] explains, solving (6) appears to be hopeless but he uses $S(G)$ to write alternative proofs of several known restrictions on the stability polytope.

A quick comparison of $S(G)$ and $MS(G)$ demonstrates that the ideals are close; actually their generators only differ in the polynomials defined in terms of $E(G)$. However the generators of both ideals contain the polynomials $x_i^2 - x_i$ for $i \in V(G)$. This condition confers on them a strong structure that we can generalize by introducing a bigger class of ideals containing them.

Let I be an ideal in $k[x_1, x_2, \ldots, x_n]$. Then I is a *0-1 ideal* if $\{x_1^2 - x_1, x_2^2 - x_2, \ldots, x_n^2 - x_n\} \subset I$. Ideals $S(G)$ and $MS(G)$ are 0-1 ideals. Our objective now is to prove that 0-1 ideals are radical, with the consequence that the Motzkin-Strauss and stability ideals are the same for any graph G.

For a polynomial $f \in k[x_1, \ldots, x_n]$ write $f = p_1^{v_1} p_2^{v_2} \cdots p_m^{v_m}$ where the polynomials $p_1^{v_1} p_2^{v_2} \cdots p_m^{v_m}$ are irreducible. Polynomial $f^* = p_1 p_2 \cdots p_m$ is the *square free* part of f. Polynomial f is *square free* if and only if $f = f^*$.

If M is an additive group, for a natural number n and an element a of M, na denotes the n-ple sum $a + \cdots + a$ of a (the addition of a, n times). Under the notation, we define the characteristic of a ring k, denoted chart(k) as follows. Considerer the set $D = \{n \in \mathbb{N} | na = 0 \text{ for every } a \in k\}$. If D is empty, then the characteristic of k is defined to be zero, otherwise, the least number in D is defined to be the characteristic of k. The next result is due to A. Seidenberg.

Theorem 2.4 [17] *Let chart(k)=0 and let I be a zero-dimensional ideal of $k[x_1, \ldots, x_n]$. Assume that for each $i = 1, \ldots, n$, I contains a square free polynomial $g_i \in k[x_i]$. Then $I = \sqrt{I}$.*

Proposition 2.5 [1] *Let I be a zero-dimensional ideal and G be the reduced Gröbner basis for I with respect to the lex term order with $x_1 < x_2 < \cdots < x_n$. Then we can order $g_1, \ldots, g_t$ such that g_1 contains only the variable x_1, g_2 contains only the variables x_1 and x_2 and $lp(g_2)$ is a power of x_2, g_3 contains only the variables x_1, x_2 and x_3 and $lp(g_3)$ is a power of x_3, and so forth until g_n.*

Here $lp(g)$ stands for the *leader power* of the polynomial g.

Theorem 2.6 *Every 0-1 ideal I in $\mathbb{C}[x_1, \ldots, x_n]$ is a radical ideal.*

Proof: Let G be the reduced Gröbner basis for I. If $1 \in G$, by Theorem 1.1 $I = k[x_1, \ldots, x_n]$ and hence $I = \sqrt{I}$. Now we consider the case when I is zero-dimensional, since chart($\mathbb{C}$) = 0 and for each $i = 1, \ldots, n$, I contains the polynomial $x_i^2 - x_i$ which is square free, the result follows from Theorem 2.4. ■

Theorem 2.7 (Strong Hilbert Nullstellensatz) *$I(V_{\bar{k}}(I)) = \sqrt{I}$ for all ideals I of $k[x_1, \ldots, x_n]$.*

As a consequence, two ideals I and J correspond to the same variety ($V_{\bar{k}}(I) = V_{\bar{k}}(J)$) if and only if $\sqrt{I} = \sqrt{J}$.

Proposition 2.8 *For G a graph, $S(G) = MS(G)$.*

Proof: By Lemma 2.6 $S(G)$ and $MS(G)$ are both radical. By Propositions 2.2 and 2.3 these two ideals correspond to the same variety. Finally by Theorem 2.7, both ideals coincide. ■

This gives two names and two ways to designate the same ideal, so henceforth the terminology of *stability ideal* and $S(G)$ is used. All extremal graph theory results implied from the Motzkin-Strauss formula and those about the stability polytope can be established now from $S(G)$. This is one reason why $S(G)$ is important. The relevance of 0-1 ideals goes beyond stability. They help to solve problems like finding hamiltonian cycles in graphs and other combinatorial problems. A detailed presentation appears in [18].

3 Stability ideal and Gröbner basis

In this section we study basic properties of the stability ideal of a graph G from the point of view of its Gröbner basis. In an implicit way we use S-polynomials and Buchberger's algorithm for the calculation of reduced Gröbner basis; see [1] for details. The *S-polynomial* of two polynomials f and g in $k[x_1, \ldots, x_n]$, denoted $S(f, g)$, is the polynomial $S(f, g) = \frac{\mathrm{lcm}(in_{\prec}(f), in_{\prec}(g))}{in_{\prec}(g)} \cdot f - \frac{\mathrm{lcm}(in_{\prec}(f), in_{\prec}(g))}{in_{\prec}(g)} \cdot g$. The lcm is the least common multiple in relation to the monomial order $\prec$.

We separate the generators of $S(G)$ into sets of polynomials $P_1(G)$ and $P_2(G)$:

$$P_1(G) = \{x_i^2 - x_i | i \in V(G)\} \bigcup \{x_i x_j | i, j \in E(G)\} \tag{7}$$

$$P_2(G) = \{\sum_{i \in V(G)} x_i - e\} \tag{8}$$

Proposition 3.1 *Let G be a graph. Then $P_1(G)$ is the reduced Gröbner basis of $\langle P_1(G) \rangle$ with respect to any monomial order.*

Proof: Buchberger's algorithm starts with $P_1(G)$ as initial basis.

For every $i, j, k, \ell \in V(G)$ with $i \neq j$ and $k \neq \ell$, $S(x_i x_j, x_\ell x_k) = 0$. If $i \neq j$ then $S(x_i^2 - x_i, x_i x_j) = -x_i x_j$. If i, j and k are pairwise different $S(x_i^2 - x_i, x_j x_k) = -x_i x_j x_k$. Finally, if $i \neq j$ then $S(x_i^2 - x_i, x_j^2 - x_j) = -x_i(x_j^2 - x_j)$. No new polynomial should be added into the basis because any possible S-polynomial is zero or reduced to zero with respect to $P_1(G)$. We conclude that $P_1(G)$ is a reduced Gröbner basis. The monomial order is irrelevant. ■

Corollary 3.2 *For any G the set $P_1(G)$ is an universal Gröbner basis of $\langle P_1(G) \rangle$.*

This fact is a direct consequence of the following result [12].

Lemma 3.3 *Let $F = \{f_1, f_2, \ldots, f_k\}$ be a set of polynomials in $\boldsymbol{k}[x_1, \ldots, x_n]$such that polynomial f_i is a product of linear factors and for any permutation π of $\{1, \ldots, n\}$ we have $\pi(f_i(x_1, \ldots, x_n)) = f_i(x_{\pi(1)}, \ldots, x_{\pi(n)}) \in F$. If F is a Gröbner basis for the ideal $\langle F \rangle$ with respect to the lexicographic monomial order induced by $x_1 > x_2 > \cdots > x_n$ then F is a universal Gröbner basis for the ideal $\langle F \rangle$.*

The set of polynomials $P_1(G)$ is the reduced Gröbner basis of $\langle P_1(G) \rangle$ and $P_2(G)$ is the reduced Gröbner basis of $\langle P_2(G) \rangle$; actually both of them are universal, but when we try to calculate the Gröbner basis of $S(G) = \langle P_1(G) \bigcup P_2(G) \rangle$, the number of S-polynomials calculated by Buchberger's algorithm increases exponentially. Proposition 3.4 explains this behavior.

Proposition 3.4 *The Gröbner basis of $S(G)$ with respect to the term order $e < x_0 < x_1 < \cdots < x_{|V|-1}$ contains the polynomial $e(e-1)(e-2)\ldots(e-\alpha(G))$.*

Proof: By Proposition 2.5 there exists a polynomial g_1 in the reduced Gröbner basis of $S(G)$ such that g_1 is the generator of $S(G) \cap k[e]$. Since e represents the size of the stable set this variable can be assigned to one of the values $0, 1, \ldots, \alpha(G)$. Note that $g_1(i) = 0$ when $i \in \{0, 1, \ldots, \alpha(G)\}$ and $g_1(i) \neq 0$ when $i \notin \{0, 1, \ldots, \alpha(G)\}$. The polynomial $e(e-1)(e-2)\ldots(e-\alpha(G))$ has minimum degree and roots $0, 1, \ldots \ldots \alpha(G)$. Thus $g_1 = e(e-1)(e-2)\ldots(e-\alpha(G))$. ■

If we calculate a Gröbner basis for $S(G)$, in an implicit way we are calculating $\alpha(G)$: Look for the polynomial in the basis that only contains the variable e. This polynomial has degree $\alpha(G)+1$. Because the calculation of the stability number of a graph is NP-hard, unless $P = NP$, we cannot expect a polynomial time method to generate the Gröbner basis of $S(G)$. However we can use this ideal to do direct deductions related to stability.

4 Stability ideal for $J(n, 3, 2)$ and MPTs

Maximum size stable sets in $J(n, 3, 2)$ correspond to MPT(n)s. In this section we construct the generators of $S(J(n, 3, 2))$ and discuss some properties of this ideal and its Gröbner basis.

Let $n > 3$ be an integer, and let A be a 4-set contained in $\Omega = \{0, \ldots, n-1\}$. Any pair of triples in A is an edge in $J(n, 3, 2)$. In other words, the subgraph of $J(n, 3, 2)$ induced by the triples contained in A is isomorphic to K_4. We denote this subgraph by K_A.

Proposition 4.1 *Let n be a positive integer. The family $\{E(K_A)\}_{A \text{ is a 4-set in } \Omega}$ is a partition of $E(J(n, 3, 2))$.*

Proof: Let e be an arbitrary edge in $E(J(n, 3, 2))$, $e = (\{w_0, w_1, w_2\}, \{w_0, w_1, w_3\})$ for some w_0, w_1, w_2 and w_3 which are pairwise different elements in Ω. Then e belongs to $E(K_{\{w_0,w_1,w_2,w_3\}})$ and $E(J(n, 3, 2)) \subseteq \cup_{A \in \{\text{4-sets in } \Omega\}} E(K_A)$.

Let A be a 4-set contained in Ω and let e be an edge of K_A. There are two different triples A_1 and A_2 contained in A such that $e = (A_1, A_2)$. We have that $4 = |A_1 \cup A_2| =$

$|A_1| + |A_2| - |A_1 \cap A_2|$ and thus $|A_1 \cap A_2| = 2$ or equivalently $e \in E(J(n,3,2))$. Thus $E(K_A) \subseteq E(J(n,3,2))$.

Finally, let B_1 and B_2 be different 4-sets contained in Ω, then $E(K_{B_1}) \cap E(K_{B_2}) = \emptyset$. Suppose to the contrary that there is an edge e in the intersection of both sets. Let A_1 and A_2 be triples in Ω such that $e = (A_1, A_2)$, then $A_1 \cup A_2 = B_1$ given that $e \in E(K_{B_1})$, but $A_1 \cup A_2 = B_2$ because $e \in E(K_{B_2})$, but that is a contradiction. Thus $\{E(K_A)\}_{A \text{ is a 4-set in } \Omega}$ is a partition of $E(B(n))$. ■

We can use this proposition to construct the generators of $S(J(n,3,2))$.

Corollary 4.2 *Let $n \geq 4$ be a positive integer. Then*

$$\begin{aligned} P_1(J(n,3,2)) &= \{x_A^2 - x_A | A \subseteq \{0,\ldots,n-1\} \textit{ and } |A| = 3\} \bigcup \\ &\quad \{x_A x_B | A, B \subseteq \{0,\ldots,n-1\}, |A| = |B| = 3 \textit{ and } |A \cup B| = 4\} \\ P_2(J(n,3,2)) &= \{\sum_{A \subseteq Triples(\{0,\ldots,n-1\})} x_A - e\}. \end{aligned} \tag{9}$$

The ideal generated by the polynomials in (9) is the *stability Steiner ideal* of order n. We have an algorithmic approach for its construction.

Algorithm 4.1 *Construction of the generators of $S(J(n,3,2))$*

Input: An integer $n \geq 4$.

Output: The set P of polynomials generating $S(J(n,3,2))$.

Method:

1. $P \leftarrow \emptyset$
2. $f \leftarrow 0$
3. **for** $i \leftarrow 1$ **to** $\binom{n}{3}$
4. $\quad$ **a** $\leftarrow$ combination$(n,3,i)$
5. $\quad$ $P \leftarrow P \cup \{x^2_{\{a[0],a[1],a[2]\}} - x_{\{a[0],a[1],a[2]\}}\}$
6. $\quad$ $f \leftarrow f + x_{\{a[0],a[1],a[2]\}}$
7. **for** $i \leftarrow 1$ **to** $\binom{n}{4}$
8. $\quad$ **a** $\leftarrow$ combination$(n,4,i)$
9. $\quad$ $P \leftarrow P \cup \{x_{\{a[1],a[2],a[3]\}} x_{\{a[0],a[2],a[3]\}}\}$
10. $\quad$ $P \leftarrow P \cup \{x_{\{a[1],a[2],a[3]\}} x_{\{a[0],a[1],a[3]\}}\}$
11. $\quad$ $P \leftarrow P \cup \{x_{\{a[1],a[2],a[3]\}} x_{\{a[0],a[1],a[2]\}}\}$
12. $\quad$ $P \leftarrow P \cup \{x_{\{a[0],a[2],a[3]\}} x_{\{a[0],a[1],a[3]\}}\}$
13. $\quad$ $P \leftarrow P \cup \{x_{\{a[0],a[2],a[3]\}} x_{\{a[0],a[1],a[2]\}}\}$
14. $\quad$ $P \leftarrow P \cup \{x_{\{a[0],a[1],a[3]\}} x_{\{a[0],a[1],a[2]\}}\}$
15. $P \leftarrow \{f - e\}$
16. **return** P

Here "combination(n,k,i)" generates (in some order) the i-th k-set contained in Ω.

The complexity of Gröbner basis computation depends strongly on the term ordering. The best one is reported to be degree-reverse-lexicographical [1]; for this ordering, the computation of the Gröbner basis of the system of polynomial equations of degree d in n variables is polynomial in d^{n^2} if the number of solutions is finite (see [3, 4]). The time needed to compute an MPT(n) is therefore polynomial in 2^{n^2}. Indeed this suffices to find all possible MPT(n)s. However when n is small enough we can hope to do successful calculations to prove in "an automatic way" (through the Nullstelensatz Hilbert Theorem) conjectures about MPTs satisfying specific conditions.

We implemented this method in Macaulay 2. We adopted some heuristics, described next, that make the program faster, and use less memory, to allow the computation for larger values of n.

1. Substitute the variable e in the generating set of $S(J(n,3,2)$ by the constant value of $\alpha(J(n,3,2))$ in order to simplify computation. See [3, 4].

2. Always make the polynomials homogenous. Use reverse degree-reverse-lexicographical monomial order [1].

3. Restrict the MPTs to be generated. There is no lost of generality if we assume that the MPTs contain the triples $\{0,1,2\},\{0,3,4\},\{0,5,6\},\ldots,\{0,n-2,n-1\}$ and $\{1,3,5\}$ (assuming that n is odd). Of course, we are not working with $S(J(n,3,2))$ anymore, but we omit only systems isomorphic to those found. To enforce the presence of these triples, include in the generators the polynomials $x_{\{0,1,2\}}-1, x_{\{0,3,4\}}-1,\ldots,x_{\{1,3,5\}}-1$. Some further pruning can be done if we consider the combined presence of other triples, for example, the pair $\{2,3\}$ could belong without loss of generality only to the triple $\{2,3,6\}$ or to the triple $\{2,3,7\}$. To do this, adjoin to the generator set the polynomial $x_{\{2,3,6\}}+x_{\{2,3,7\}}-1$. We can continue with this process as desired to make the process faster and reduce the number of resulting MPTs. Taking this process to the extreme yields a full enumeration of the nonisomorphic MPTs.

4. Impose further restrictions when possible. For example, to build an anti-Pasch MPT (one not containing a copy of the MPT(6)), let $\mathbf{a}$ be an array containing a 6-subset of $\{0,\ldots,n-1\}$. Including $x_{\{a[3],a[4],a[5]\}}x_{\{a[1],a[2],a[5]\}}x_{\{a[0],a[2],a[4]\}}x_{\{a[0],a[1],a[3]\}}$ with the generators of $S(J(n,3,2))$ prevents the Pasch

$$\{a[3],a[4],a[5]\},\{a[1],a[2],a[5]\},\{a[0],a[2],a[4]\},\{a[0],a[1],a[3]\}$$

   from appearing in the MPTs. The other 23 monomials of this form must be included for the 6-set in $\mathbf{a}$. A total of $\binom{n}{6}24$ monomials must be included in order to ensure that the MPTs generated are anti-Pasch.

Despite these heuristics, computation is far too time-consuming. Being optimistic, with a supercomputer and these heuristics, we may reach values of n as big as 21. Bigger values appear to be hopeless at present.

This time consumed by this method is not very different from brute force algorithms. Why we would prefer to use the stability ideal and a program such as Macaulay 2? The answer is simple: Some conjecture is false when the number one enters the Gröbner basis. Macaulay 2 can in principle produce the sequence of calculations involved. The reductions and computations of S-polynomials involved is a formal deduction, while with brute force algorithms additional work is required to get a mathematical proof. On the other hand, when a conjecture is true, the Gröbner basis calculation provides a full description of the associated geometric variety. Moreover, the strong structure of the ideals, if understood well, may permit direct inferences without using the Buchberger algorithm. Sturmfels [19] used a similar development on polytopes in combinatorial optimization applications. At the moment, it is speculative that such structural results can be obtained.

5 Colorings and Steiner Triple Systems

Generation of MPTs from stability ideals is natural and could be extended to other designs. Now we turn to a different approach. Stability and colorings are closely related concepts because vertices in a colour class form a stable set. In this section we use colorings to construct STSs. First we introduce a well known ideal to find a λ coloring of a graph G provided that λ is known in advance. Then we use two variations of this ideal to construct STSs.

Lemma 5.1 (Loera [13]**)** *Let G be a graph on n vertices, and let λ be a nonnegative integer.The graph G is λ-colorable if and only if the zero-dimensional system of equations in $\mathbb{C}[x_1, \ldots, x_n]$*

$$x_i^\lambda - 1 = 0, \quad \textit{for every vertex } i \in V(G), \tag{10}$$

$$x_i^{\lambda-1} + x_i^{\lambda-2}x_j + \cdots + x_j^{\lambda-1} = 0, \quad \textit{for every edge } \{i,j\} \in E(G), \tag{11}$$

has a solution. Moreover, the number of solutions equals the number of distinct λ-colorings multiplied by $\lambda!$. ∎

The *coloring ideal* of λ and G is the ideal $I_\lambda(G)$ of $\mathbb{C}[x_1 \ldots, x_n]$ generated by the polynomials in (10) and (11).

Note that by Theorem 2.4, the coloring ideal of λ and G is radical.

By (10) every vertex can take one of λ possible colors. Let us examine (11) more thoroughly. Denote by $P_\lambda(x, y)$ the polynomial $x^{\lambda-1} + x^{\lambda-2}y + \cdots + y^{\lambda-1}$.

Lemma 5.2 *Let λ be a positive integer. If r_0 and r_1 are roots of unity of $x^\lambda - 1$ then $r_0 \neq r_1$ if and only if $P_\lambda(r_0, r_1) = 0$.*

Proof: We have that

$$x^\lambda - y^\lambda = (x - y)P_\lambda(x, y). \tag{12}$$

Since r_0 and r_1 are roots of unity $r_0^\lambda - r_1^\lambda = 1-1 = 0$. If $r_0 \neq r_1$ then $0 = (r_0-r_1)P_\lambda(r_0, r_1)$, since $r_0 - r_1 \neq 0$ we have that $P_\lambda(r_0, r_1) = 0$. On the other hand, if $r_0 = r_1$ then there exists an integer $j \in \{0, \ldots, \lambda - 1\}$ such that $r_0 = r_1 = e^{\frac{2\pi j}{\lambda}i}$, and so $P_\lambda(r_0, r_1) = \lambda(e^{\frac{2\pi j}{\lambda}i})^{\lambda-1} \neq 0$. The lemma follows. ∎

By (11) if $i, j \in E(G)$ then x_i should be different to x_j because otherwise $P_\lambda(x_i, x_j)$ would be nonzero. In other words, the color assigned to x_i should be different to the color assigned to x_j.

Proposition 5.3 *Let $n \equiv 1, 3 \pmod 6$ be a nonnegative integer. Let $\lambda = \frac{\binom{n}{2}}{3}$. The zero-dimensional system of equations*

$$\begin{aligned} x_{\{i,j\}}^{\lambda} - 1 &= 0, \text{ for every pair } (i,j) \in E(K_n) \\ P_\lambda(x_{\{i_1,j_1\}}, x_{\{i_2,j_2\}}) \cdot P_\lambda(x_{\{i_2,j_2\}}, x_{\{i_3,j_3\}}) \cdot & \\ P_\lambda(x_{\{i_3,j_3\}}, x_{\{i_1,j_1\}}) &= 0, \text{ for each 3-set } \{(i_1,j_1),(i_2,j_2),(i_3,j_3)\} \\ & \quad \text{not inducing a copy of } K_3 \text{ in } K_n \end{aligned}$$

has a solution if and only if $\{\{i,j,k\} | x_{\{i,j\}} = x_{\{j,k\}} = x_{\{k,i\}}\}$ is an STS.

Proof: Suppose that the system of equations has a solution. The value of $x_{\{i,j\}}$ is the color for the edge (i,j) in K_n. We are using as many colors as there are triples in a STS(n). If the coloring is not balanced, then some color is assigned to fewer than three edges and some color is assigned to more than 3 edges. In this way there exist edges $(i_1,j_1),(i_2,j_2),(i_3,j_3)$ and (i_4,j_4) for which $x_{\{i_1,j_1\}} = x_{\{i_2,j_2\}} = x_{\{i_3,j_3\}} = x_{\{i_4,j_4\}}$. Among these four edges, there are three which do not induce a copy of K_3 in K_n; we can assume that these edges are $(i_1,j_1),(i_2,j_2)$ and (i_3,j_3). By the properties of P_λ, $P_\lambda(x_{\{i_1,j_1\}}, x_{\{i_2,j_2\}})P_\lambda(x_{\{i_2,j_2\}}, x_{\{i_3,j_3\}})P_\lambda(x_{\{i_3,j_3\}}, x_{\{i_1,j_1\}}) \neq 0$ but this contradicts the existence of a solution to the system of equations. Thus three edges receiving the same color induce a copy of K_3 in K_n.

In the other direction, ordering the triples of an STS(n) as $\{i_0,j_0,k_0\}$, $\{i_1,j_1,k_1\}$, $\ldots$, $\{i_{\lambda-1},j_{\lambda-1},k_{\lambda-1}\}$, and for $l = 0,\ldots,\lambda-1$ we assign to $x_{\{i_l,j_l\}}$, $x_{\{j_l,k_l\}}$ and $x_{\{k_l,i_l\}}$ the l-th λ-root of unity then the system of equations is satisfied. ∎

The ideal generated by the polynomials in the system of equations in Proposition 5.3 is the *edge coloring Steiner ideal* of order n.

The stability Steiner ideal of order n associates the 3-sets in $\{0,\ldots,n-1\}$ to its variables; the edge coloring Steiner ideal associates the 2-sets. Does some ideal to generate STSs associate the variables to 1-sets? The answer is affirmative, but since in an STS(n) each vertex is assigned to $(n-1)/2$ triples, we need $(n-1)/2$ copies of each vertex. We denote by (i,j) the j-th copy of vertex i, $i = 0,\ldots,n-1$ and $j = 1,\ldots(n-1)/2$.

Proposition 5.4 *Let $n \equiv 1, 3 \pmod 6$ be a nonnegative integer. Let λ be equal to $\frac{\binom{n}{2}}{3}$. The zero-dimensional system of equations*

$$
\begin{aligned}
x_{(i,j)}^{\lambda} - 1 &= 0, \textit{ for every pair } (i,j) \textit{ with} \\
&\qquad i = 0, \ldots, n-1 \textit{ and } j = 1, \ldots, (n-1)/2 \\
P_\lambda(x_{(i_1,j_1)}, x_{(i_2,j_2)}) \cdot P_\lambda(x_{(i_2,j_2)}, x_{(i_3,j_3)}) \cdot & \\
P_\lambda(x_{(i_3,j_3)}, x_{(i_4,j_4)}) \cdot P_\lambda(x_{(i_1,j_1)}, x_{(i_3,j_3)}) \cdot & \\
P_\lambda(x_{(i_1,j_1)}, x_{(i_4,j_4)}) \cdot P_\lambda(x_{(i_2,j_2)}, x_{(i_4,j_4)}) &= 0, \textit{ for } i_1, i_2, i_3, i_4 \in \{0, \ldots, n-1\} \\
&\qquad \textit{distinct and} \\
&\qquad j_1, j_2, j_3, j_4 \in \{1, \ldots, (n-1)/2\} \\
P_\lambda(x_{(i,j_1)}, x_{(i,j_2)}) &= 0, \textit{ for } i \in \{0, \ldots, n-1\} \textit{ and} \\
&\qquad j_1, j_2 \in \{1, \ldots, (n-1)/2\},\ j_1 \neq j_2
\end{aligned}
$$

has a solution if and only if $\{\{i,j,k\} | x_{(i,l_1)} = x_{(j,l_2)} = x_{(k,l_3)}$ *for some* $l_1, l_2, l_3 \in \{0, \ldots, (n-1)/2\}\}$ *is an STS.*

Proof: Analogous to the proof of Proposition 5.3. ∎

The ideal generated by the polynomials in the system of equations in Proposition 5.3 is the *vertex coloring Steiner ideal* of order n.

The earlier comments for the stability Steiner ideal of order n are essentially the same for the ideals in this section. As long as the number of variables decreases the complexity of the polynomials involved increases. The final effect is that, as we expect, the practical limitations of these ideals are similar.

6 Ideals and Kirkman Triple Systems

In this section we introduce an ideal based on a combination of stability and colorings for the generation of Kirkman triple systems (see [5]).

Let s be a positive integer and let $n = 6s + 3$. A *Kirkman triple system* of order n is a Steiner triple system with parallelism, that is, one in which the set of $b = (2s+1)(3s+1)$ triples is partitioned into $3s + 1$ components such that each component is a subset of triples and each of the elements appears exactly once in each component.

Proposition 6.1 *Let s be a positive integer and let $n = 6s+3$. The zero-dimensional system of equations*

$$
\begin{aligned}
x_{\{i,j,k\}}^2 - x_{\{i,j,k\}} &= 0, \text{ \textit{when} } \{i,j,k\} \subset \{0,\ldots,n-1\},\\
x_{\{i,j,k\}}x_{\{j,k,l\}} &= 0, \text{ \textit{when} } \{i,j,k\},\{j,k,l\} \subset \{0,\ldots,n-1\}\\
& \quad \text{\textit{and} } i \neq l,\\
\sum_{\{i,j,k\}\subseteq\{0,\ldots,n-1\}} x_{\{i,j,k\}} - (2s+1)(3s+1) &= 0,\\
y_{\{i,j,k\}}^{3s+1} - 1 &= 0, \text{ \textit{when} } \{i,j,k\} \subset \{0,\ldots,n-1\},\\
x_{\{i,j,k\}}x_{\{k,l,m\}}P_{3s+1}(y_{\{i,j,k\}}, y_{\{k,l,m\}}) &= 0, \text{ \textit{for every unordered couple of different}}\\
& \quad \text{\textit{3-sets}} \{i,j,k\}, \text{ \textit{and} } \{k,l,m\} \text{ \textit{contained in}}\\
& \quad \{0,\ldots,n-1\}.
\end{aligned}
$$

has a solution if and only if $S = \{\{i,j,k\} | x_{\{i,j,k\}} = 1\}$ *is a Kirkman triple system.*

Proof: The first three equations in the system generate the stability Steiner ideal of order n, thus the set of triples S is an STS. A new variable $y_{\{i,j,k\}}$ is introduced for each vertex $\{i,j,k\}$ in $J(n,3,2)$. These variables are used for coloring the elements of S; by the fourth equation each triple receives one of $3s+1$ colors. When $x_{\{i,j,k\}} = 0$ the value of $y_{\{i,j,k\}}$ is immaterial. By the fifth equation, when $x_{\{i,j,k\}} = 1$ the color assigned to $y_{\{i,j,k\}}$ must be different from the one assigned to every other triple in S intersecting $\{i,j,k\}$.

Using the technique in the proof of Proposition 5.3, every color is associated to exactly $2s+1$ variables $y_{i,j,k}$. So S is a Kirkman triple system. ∎

The ideal generated by the polynomials in the system of equations in Proposition 5.3 is the *Kirkman ideal* of order n.

In Proposition 6.1 the fifth equation is equivalent to the conditional statement:

if $\{i,j,k\}$ and $\{k,\ell,m\}$ are in S **then**
Put $\{i,j,k\}$ and $\{k,\ell,m\}$ in different color classes.

Few elements in the ideal suffice for the construction of ideals related to design theory: stability, colorings, P_λ polynomials and the proper use of conditional polynomial constructions.

7 Parametric generation of STSs

Let $V = \mathbf{V}(f_1,\ldots,f_s) \subset k^\ell$ be a variety. Let $k(t_1,\ldots,t_m)$ represent the field of rational functions, that is, quotients between two polynomials in $k[t_1,\ldots,t_m]$. The *rational parametric representation* of V consists of rational functions $r_1,\ldots,r_\ell \in k(t_1,\ldots,t_m)$ such that the set of points $(x_1,x_2,\ldots,x_\ell)$ given by

$$x_i = r_i(t_1,\ldots,t_m) \quad i = 1,\ldots,\ell \tag{13}$$

is equal to V. When functions $r_1, \ldots, r_\ell$ are polynomials rather than rational functions this is a *parametric polynomial representation*. The original defining equations $f_1, \ldots, f_s$ form the *implicit parametric representation* of V.

It is well known that not every affine variety has a rational parametric representation; however the set of points described by a rational parametric representation is always an affine variety. In this section we consider the triples in a STS(n) as points in $\mathbb{R}^3$ (fixing elements in some particular order for each triple), and then we try to build a parametric polynomial representation for them. When successful, it is implicitly proved that the points produced from the triples in the STS form an affine variety.

For instance, for $n = 7$ the following parametric polynomial equations generate an STS(7).

$$\begin{aligned} x &= t \bmod 7 \\ y &= 1 + t \bmod 7 \\ z &= 3 + t \bmod 7 \end{aligned} \tag{14}$$

Taking $t = 0, \ldots, 6$ produces the STS

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

This is a parametric polynomial representation that works exactly as we want. The polynomials in (14) belong to $\mathbb{Z}/7\mathbb{Z}[x,y,z,t]$. However, we cannot generalize this directly because the quotient ring $\mathbb{Z}/n\mathbb{Z}$ is a field only when n is prime. This is a technical difficulty, addressed later. First let us generalize the parametric representation in (14).

Let $n \equiv 1, 3 \pmod 6$ be an integer and let $\ell, l_1, l_2, l_3, n_1, \ldots, n_\ell$ be nonnegative integers such that $n_i \leq n$ for $i = 1, \ldots, \ell$ and $\prod_{j=1}^{\ell} n_i = n(n-1)/6$ (the number of triples in an STS(n)). A *polynomial parametric Steiner representation* (PPSR) of order n, and parameters $\ell, l_1, l_2, l_3, n_1, \ldots, n_\ell$ is a triple $(\{\alpha_i\}_{i=0}^{l_1}, \{\beta_i\}_{i=0}^{l_2}, \{\delta_i\}_{i=0}^{l_3})$, such that the elements in each succession are pairwise different and belong to $(\mathbb{Z}^+ \bigcup \{0\})^\ell$. We denote a parametric representation like this as $\mathcal{P}(n, \ell, l_1, l_2, l_3, \{n_i\}_{i=1}^{\ell}, (\{\alpha_i\}_{i=0}^{l_1}, \{\beta_i\}_{i=0}^{l_2}, \{\delta_i\}_{i=0}^{l_3}))$. A PPSR is *feasible* if the system of equations

$$x(\mathbf{t}) = \sum_{i=0}^{l_1} a_{\alpha_i} \mathbf{t}^{\alpha_i} \quad y(\mathbf{t}) = \sum_{i=0}^{l_1} b_{\beta_i} \mathbf{t}^{\beta_i} \quad z(\mathbf{t}) = \sum_{i=0}^{l_1} c_{\delta_i} \mathbf{t}^{\delta_i}$$

in the variables $a_{\alpha_0}, \ldots, a_{\alpha_{l_1}}, b_{\beta_0}, \ldots b_{\beta_{l_2}}, c_{\delta_0}, \ldots, c_{\delta_{l_3}}$, (where $\mathbf{t} = (t_1, \ldots, t_l)$) has a solution such that the set $S = \{\{x(\mathbf{t}), y(\mathbf{t}), z(\mathbf{t})\} | \mathbf{t} \in \{0, \ldots, n_1 - 1\} \times \ldots \times \{0, \ldots, n_\ell - 1\}\}$ is an STS.

That $n_i \leq n$ for $i = 1, \ldots, \ell$ is necessary because the operations are on $\mathbb{Z}/n\mathbb{Z}$; but it imposes restrictions on the PPSRs dealt with. For example, only for $n = 7$ can we have a PPSR with $\ell = 1$. For any other value of n it is not possible to find an integer n_1 satisfying $n_1 \leq n$ and $\prod_{i=1}^{1} n_i = n(n-1)/6$. In other words, it is impossible to generalize (14) for $n > 7$ using only one parameter t.

The important fact concerning PPSRs is that their feasibility is decided by weak Hilbert Nullstelensatz Theorem.

Proposition 7.1 *Let $n \equiv 1, 3 \pmod 6$ be a prime. Let $\mathcal{P}(n, \ell, l_1, l_2, l_3, \{n_i\}_{i=1}^{\ell}, (\{\alpha_i\}_{i=0}^{l_1}, \{\beta_i\}_{i=0}^{l_2}, \{\delta_i\}_{i=0}^{l_3}))$ be a PPSR of order n. Let P and Q be the polynomials in $\mathbb{Z}/n\mathbb{Z}[a_{\alpha_0}, \ldots, a_{\alpha_{l_1}}, b_{\beta_0}, \ldots, b_{\beta_{l_2}}, c_{\delta_0}, \ldots, c_{\delta_{l_3}}]$, $P(u) = (u-1)(u-2)\cdots(u-n+1)$, $Q(u) = uP(u)$, $u \in \{0, \ldots, n-1\}$. Then $\mathcal{P}$ is feasible if and only if the zero-dimensional system of equations*

$$\left.\begin{array}{r} Q(a_{\alpha_i}) \\ Q(b_{\beta_j}) \\ Q(c_{\delta_k}) \end{array}\right\} = 0, \quad \begin{array}{l} \textit{for } i = 0, \ldots, l_1, \\ j = 0, \ldots, l_2 \textit{ and } k = 0, \ldots, l_3 \end{array} \tag{15}$$

$$\left.\begin{array}{r} P(x(\mathbf{t}) - y(\mathbf{t})) \\ P(x(\mathbf{t}) - z(\mathbf{t})) \\ P(y(\mathbf{t}) - z(\mathbf{t})) \end{array}\right\} = 0, \quad \begin{array}{l} \textit{for } \mathbf{t} \in \{0, \ldots, n_1 - 1\} \times \\ \ldots \times \{0, \ldots, n_\ell - 1\} \end{array} \tag{16}$$

$$\left.\begin{array}{r} P(x(\mathbf{t}_1) - x(\mathbf{t}_2))P(y(\mathbf{t}_1) - y(\mathbf{t}_2)) \\ P(x(\mathbf{t}_1) - y(\mathbf{t}_2))P(y(\mathbf{t}_1) - x(\mathbf{t}_2)) \\ P(x(\mathbf{t}_1) - x(\mathbf{t}_2))P(z(\mathbf{t}_1) - z(\mathbf{t}_2)) \\ P(x(\mathbf{t}_1) - z(\mathbf{t}_2))P(z(\mathbf{t}_1) - x(\mathbf{t}_2)) \\ P(z(\mathbf{t}_1) - z(\mathbf{t}_2))P(y(\mathbf{t}_1) - y(\mathbf{t}_2)) \\ P(z(\mathbf{t}_1) - y(\mathbf{t}_2))P(y(\mathbf{t}_1) - z(\mathbf{t}_2)) \end{array}\right\} = 0, \quad \begin{array}{l} \textit{for } \mathbf{t}_1, \mathbf{t}_2 \in \{0, \ldots, n_1 - 1\} \times \\ \ldots \times \{0, \ldots, n_\ell - 1\}, \mathbf{t}_1 \neq \mathbf{t}_2 \end{array} \tag{17}$$

$$\tag{18}$$

has a solution.

Proof: Assume that the system of equations is satisfied. Then by (15) the values of these coefficients should be in the set $\{0, 1, \ldots, n-1\}$ which corresponds to the roots of the polynomial $Q(t)$. Also (16) guarantees that the elements in each of the triples in S are distinct. (The polynomial P plays a similar role to that of the polynomials P_λ introduced in Section 5.) Finally, by (17) every pair of different vertices in $\{0, \ldots, n-1\}$ appears in exactly one of the triples and thus it is an STS. The converse is immediate. ∎

The ideal generated by the polynomials in Proposition 7.1 is the *parametric Steiner ideal* of $\mathcal{P}$.

Solutions to the polynomials in the parametric Steiner ideal of a PPSR can be found using Gröbner bases. For example, the Gröbner basis for the unique possible PPSR of order $n = 7$ and $\ell = l_1 = l_2 = l_3 = 1$ is

$$\begin{array}{l} \{\ c_1^6 - 1, b_1 - c_1, a_1 - c_1, c_0^7 - c_0, \\ \ \ b_0^6 + b_0^5 c_0 + b_0^4 c_0^2 + b_0^3 c_0^3 + b_0^2 c_0^4 + b_0 c_0^5 + c_0^6 - 1, \\ \ \ a_0^5 + a_0^4 b_0 + a_0^4 c_0 + a_0^3 b_0^2 + a_0^3 b_0 c_0 + a_0^3 c_0^2 + a_0^2 b_0^3 + a_0^2 b_0^2 c_0 + a_0^2 b_0 c_0^2 + a_0^2 c_0^3 + a_0 b_0^4 + a_0 b_0^3 c_0 + \\ \ \ a_0 b_0^2 c_0^2 + a_0 b_0 c_0^3 + a_0 c_0^4 + b_0^5 + b_0^4 c_0 + b_0^3 c_0^2 + b_0^2 c_0^3 + b_0 c_0^4 + c_0^5 \} \end{array}$$

A solution that makes all these polynomials zero is $a_0 = 0, b_0 = 1, c_0 = 3, a_1 = 1, b_1 = 1$, and $c_1 = 1$; it corresponds to the PPSR in (14).

Corollary 7.2 *A PPSR $\mathcal{P}$ is feasible if and only if the Gröbner basis of the parametric Steiner ideal of $\mathcal{P}$ does not contain 1.*

While these provide a relatively simple way to determine the feasibility of a PPSR, it is limited to prime orders. We can circumvent this limitation by working in the complex number field. We carry the operations from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{C}$ through the transformation $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, $\phi(k) = e^{\frac{2\pi k}{n} i}$. Two well known properties of ϕ are: For every a and b in $\mathbb{Z}/n\mathbb{Z}$

$$\begin{aligned} \phi(a+b) &= \phi(a)\phi(b) \\ \phi(a \cdot b) &= \phi(a)^b = \phi(b)^a \end{aligned} \tag{19}$$

Let $n \equiv 1, 3 \pmod 6$ be a prime. Let $\mathcal{P}(n, \ell, l_1, l_2, l_3, \{n_i\}_{i=1}^{\ell}, (\{\alpha_i\}_{i=0}^{l_1}, \{\beta_i\}_{i=0}^{l_2}, \{\delta_i\}_{i=0}^{l_3}))$ be a PPSR of order n. We extend the domain of ϕ to the polynomial $x(\mathbf{t}) = \sum_{j=1}^{l} a_{\alpha_j} \mathbf{t}^{\alpha_\mathbf{j}}$ as $\phi(\sum_{j=1}^{l} a_{\alpha_j} \mathbf{t}^{\alpha_j}) = \prod_{j=1}^{l} \phi(a_{\alpha_j})^{\mathbf{t}^{\alpha_j}} = \prod_{j=1}^{l} \hat{a}_{\alpha_j}^{\mathbf{t}^{\alpha_j}}$. This extension is compatible with (19); it takes a polynomial on the variables $a_{\alpha_0}, \ldots, a_{\alpha_{l_1}}$ and transforms it into a polynomial on the variables $\hat{a}_{\alpha_0}, \ldots, \hat{a}_{\alpha_{l_1}}$ (here $\hat{a}_{\alpha_j}$ stands for $\phi(a_{\alpha_j})$). For each $\mathbf{t} \in \{0, \ldots, n_1 - 1\} \times \ldots \times \{0, \ldots, n_\ell - 1\}$, $\phi(x(\mathbf{t})(a_{\alpha_0}, \ldots, a_{\alpha_{l_1}})) = \phi(x(\mathbf{t}))(\hat{a}_{\alpha_0}, \ldots, \hat{a}_{\alpha_{l_1}})$. Similar extensions are made to ϕ in order to be applied to the polynomials $y(\mathbf{t})$ and $z(\mathbf{t})$.

Proposition 7.3 *Let $n \equiv 1, 3 \pmod 6$ be a prime. Let $\mathcal{P}(n, \ell, l_1, l_2, l_3, \{n_i\}_{i=1}^{\ell}, (\{\alpha_i\}_{i=0}^{l_1}, \{\beta_i\}_{i=0}^{l_2}, \{\delta_i\}_{i=0}^{l_3}))$ be a PPSR of order n. Let P_n and Q_n be polynomials in $\mathbb{C}[\hat{a}_0, \ldots, \hat{a}_l, \hat{b}_0, \ldots, \hat{b}_l, \hat{c}_0, \ldots, \hat{c}_l]$, $P_n(u, v) = u^{n-1} + u^{n-2}v + \ldots + vw^{n-2} + w^{n-1}$, $Q_n(u) = u^n - 1$, $u, v \in \{0, \ldots, n-1\}$. Then $\mathcal{P}$ is feasible if the zero-dimensional system of equations*

$$Q_n(\hat{a}_{\alpha_i}) = Q_n(\hat{b}_{\beta_j}) = Q_n(\hat{c}_{\delta_k}) = 0, \quad \begin{array}{l} \textit{for } i = 0, \ldots, l_1, \\ j = 0, \ldots, l_2 \textit{ and } k = 0, \ldots, l_3 \end{array} \tag{20}$$

$$\left.\begin{array}{r} P_n(\phi(x(\mathbf{t})), \phi(y(\mathbf{t}))) \\ P_n(\phi(x(\mathbf{t})), \phi(z(\mathbf{t}))) \\ P_n(\phi(y(\mathbf{t})), \phi(z(\mathbf{t}))) \end{array}\right\} = 0, \quad \begin{array}{l} \textit{for } \mathbf{t} \in \{0, \ldots, n_1 - 1\} \times \\ \ldots \times \{0, \ldots, n_\ell - 1\} \end{array} \tag{21}$$

$$\left.\begin{array}{r} P_n(\phi(x(\mathbf{t}_1)), \phi(x(\mathbf{t}_2))) P_n(\phi(y(\mathbf{t}_1)), \phi(y(\mathbf{t}_2))) \\ P_n(\phi(x(\mathbf{t}_1)), \phi(y(\mathbf{t}_2))) P_n(\phi(y(\mathbf{t}_1)), \phi(x(\mathbf{t}_2))) \\ P_n(\phi(x(\mathbf{t}_1)), \phi(x(\mathbf{t}_2))) P_n(\phi(z(\mathbf{t}_1)), \phi(z(\mathbf{t}_2))) \\ P_n(\phi(x(\mathbf{t}_1)), \phi(z(\mathbf{t}_2))) P_n(\phi(z(\mathbf{t}_1)), \phi(x(\mathbf{t}_2))) \\ P_n(\phi(z(\mathbf{t}_1)), \phi(z(\mathbf{t}_2))) P_n(\phi(y(\mathbf{t}_1)), \phi(y(\mathbf{t}_2))) \\ P_n(\phi(z(\mathbf{t}_1)), \phi(y(\mathbf{t}_2))) P_n(\phi(y(\mathbf{t}_1)), \phi(z(\mathbf{t}_2))) \end{array}\right\} = 0, \quad \begin{array}{l} \textit{for } \mathbf{t}_1, \mathbf{t}_2 \in \{0, \ldots, n_1 - 1\} \times \\ \ldots \times \{0, \ldots, n_\ell - 1\}, \mathbf{t}_1 \neq \mathbf{t}_2 \end{array} \tag{22}$$

$$\tag{23}$$

has a solution in $\hat{a}_0, \ldots, \hat{a}_{l_1}, \hat{b}_0, \ldots, \hat{b}_{l_2}, \hat{c}_0, \ldots, \hat{c}_{l_3}$ if and only if $\mathcal{P}$ is feasible.

Proof: Assume that the system of equations has a solution. From (20) $\hat{a}_0 \ldots, \hat{a}_\ell$, $\hat{b}_0, \ldots, \hat{b}_\ell$, $\hat{c}_0, \ldots, \hat{c}_\ell$ could only be assigned to nth roots of unity. Since $\phi(x(\mathbf{t})), \phi(y(\mathbf{t}))$, and $\phi(z(\mathbf{t}))$ are expressed as products and integer powers of nth roots of unity, they evaluate to nth roots of unity too. The polynomial P_n is the polynomial P_λ, with $\lambda = n$, defined in Section 5, and so, by Lemma 5.2 the arguments in the proof of Proposition 7.1 with respect to (16) and (17) are applicable to (21) and (22), respectively. So $\hat{S} = \{\{\phi(x(\mathbf{t})), \phi(y(\mathbf{t})), \phi(z(\mathbf{t}))\} | \mathbf{t} \in \{0, \ldots, n_1 - 1\} \times \cdots \times \{0, \ldots, n_\ell - 1\}\}$ contains only triples of nth roots of unity and each pair of nth roots of unity is contained in exactly one triple. When we apply ϕ^{-1} to the elements in every triple in $\hat{S}$ we obtain an STS S. ∎

From a computational point of view, the Gröbner basis of the ideal in Proposition 7.1 can be found faster in Macaulay 2 than the corresponding Gröbner basis for Proposition 7.3. For $n = 7$ and $\ell = 1$ we required with the former approach 12 seconds, with the last one the system exhausted the memory.

Now we do the same type of transformation done from Proposition 7.1 to Proposition 7.3 in the opposite direction to get an ideal on $\mathbb{Z}/n\mathbb{Z}$ to obtain a λ-coloring of a graph G. We transform Lemma 5.1 in the following way.

Lemma 7.4 *Let G be a graph on n vertices for some prime n, and let λ be a nonnegative integer. Graph G is λ-colorable if and only if the following zero-dimensional system of equations in $\mathbb{Z}/n\mathbb{Z}[x_1, \ldots, x_n]$*

$$x_i(x_i - 1) \cdots (x_i - \lambda) = 0, \quad \textit{for every vertex } i \in V(G), \tag{24}$$

$$(x_i - x_j - 1) \cdots (x_i - x_j - \lambda) = 0, \quad \textit{for every edge } \{i, j\} \in E(G), \tag{25}$$

has a solution. ∎

This new ideal is useful only for prime values of n but the calculation of its Gröbner basis is more efficient.

8 Conclusions

When Hilbert submitted his famous finiteness theorem (see [6]) to the *Mathematische Annalen* in 1888, Gordan rejected the article. Gordan had earlier established the finiteness of generators for binary forms using a complex computational approach. He expected not only a finiteness existence proof, but also a more constructive approach. Gordan comment about Hilbert's work was "Das ist nicht Mathematik. Das ist Theologie" (This is not Mathematics. This is Theology) [9]. Encouraged by Gordan's opinion, Hilbert provided estimates of the maximum degree of the minimum set of generators. But in 1899 Gordan developed a constructive proof of the finiteness theorem, using what is now called the Gröbner basis to reduce to the more easily treated monomial case.

Gordan's tools were made more practical with the advent of modern computers. Despite this, implicit in the calculation of many Gröbner bases is the solution of NP-complete problems. Hence we cannot hope to solve every possible problem stated with Gröbner bases. Nevertheless, important problems in physics, robotics and engineering have been successfully solved with them.

Characterizations of combinatorial designs test these algebraic tools. We have examined how to represent the rich structure of designs into algebraic terms. We tested in Macaulay 2 that every ideal works as described. Unfortunately, the large dimensions of the systems of polynomials involved make manipulation impractical from a computational point of view. The development of parallel algorithms to calculate Gröbner basis efficiently are remarkable (see [2, 16]). Such advances may permit the direct calculation for the ideals introduced in this paper for small values of n. On the other hand, the increasing industrial interest in Gröbner basis will bring in the near future computer hardware especially designed to making fast the calculations involved. This progress will be important for design theory.

We opened unexplored connections between these algebraic geometry and combinatorial design theory; this is the main contribution of our work. From the algebraic geometry point of view the most interesting result from these connections is the discovery of 0-1 ideals whose structural properties and applications in combinatorics are explored in [18].

References

[1] W. Adams and P. Loustaunau: *An Introduction to Gröbner Bases*, American Mathematical Society, Providence, Rhode Island, 1994.

[2] I. A. Ajwa. *A case study of Grid Computing and computer algebra parallel Gröbner bases and Characteristic Sets*. The Journal of Supercomputing. Volume 41, Number 1. 2007.

[3] L. Caniglia, A. Galligo, and J. Heintz. *Some new affectivity bounds in computational geometry. Proceedings of AAECC-6*, Lect. Notes in Comp. Sci. 357 (1988), Springer Verlag, 131-152.

[4] L. Caniglia, A. Galligo, and J. Heintz. *Equations for the projective closure and effective Nullstellensatz*. Discrete Applied Math. **33** (1991), 11-23.

[5] C. J. Colbourn, "Triple Systems." ?II.2 in The Handbook of Combinatorial Designs, Second Edition (Ed. C. J. Colbourn and J. H. Dinitz). Boca Raton, FL: CRC Press, pp. 58–71, 2007.

[6] D. Cox, J. Little and D. O'Shea: *Ideals, Varieties and Algorithms,* Springer Undergraduate texts in Mathematics, Springer-Verlag, New York, 1992.

[7] D. Cox, J. Little and D. O'Shea: *Using Algebraic Geometry,* Springer Graduate texts in Mathematics, Springer-Verlag, New York, 2004.

[8] D. Eisenbud, D. R. Grayson, M. Stillman and B. Sturmfels (Eds). *Computations in Algebraic Geometry with Macaulay 2.* Algorithms and Computations in Mathematics Vol. 8. Springer-Verlag, New York, 2002.

[9] W. B. Ewald, ed., 1996. From Kant to Hilbert: A Source Book in the Foundations of Mathematics, 2 vols. Oxford Uni. Press.

[10] C. D. Godsil, G. Royle: *Algebraic Graph Theory.* Springer-Verlag, New York, 2001.

[11] T. W. Hungerford *Algebra.* Springer Graduate texts in Mathematics Springer-Verlag, New York, 1974.

[12] J. A. de Loera., Gröbner bases and graph colorings, Beiträge zur algebra und geometrie, **36** (1995), 89-86.

[13] J. A. de Loera, J. Lee, S. Margulies and S. Onn., *Expressing Combinatorial Optimization Problems by Systems of Polynomial Equations and the Nullstellensatz.* axXiv:0706.0578vl, 5 jun 2007.

[14] L. Lovász, *Stable sets and polynomials*, Discrete Mathematics, **124** (1994), 137-153.

[15] T. S. Motzkin and E. G. Strauss, *Maxima for graphs and a new proof of a theorem of Turán*, Canad. J. Math. **17**, 533-540, 1965.

[16] V. A. Mutyunin and E. V. Pankratiev. *Parallel Algorithms for Gröbner bases construction.* Journal of Mathematical Sciences, Springer New York. Volume 142, Number 4. 2007.

[17] A. Seidenberg, *Constructions in algebra*, Transactions American Mathematical Society **197** (1974), 272-313.

[18] F. Sagols, J. Muñoz. *Structural properties and applications of 0-1 ideals.* In process.

[19] B. Sturmfels: *Gröbner Bases and Convex Polytopes.* American Mathematical Society, Povidence, RI. 1995.