CINVESTAV-IPN

Combinatorial Designs, Ideals and Quasi-Steiner Triple Systems

by

M. Sc. Javier Muñoz Bernabe

A Thesis Submitted
in Partial Fulfillment of the
Requirements for the Degree

Doctor in Mathematics

Advisor

Dr. Feliú D. Sagols Troncoso

Mexico, D.F

May, 2015

ABSTRACT

Combinatorial Designs, Ideals and Quasi-Steiner Triple Systems

by

M. Sc. Javier Muñoz Bernabe

In this work, we study the generation of Steiner triple systems, which are an important family of combinatorial designs. Combinatorial designs in general and Steiner triple systems, in particular, are useful in science and technology. A *Steiner triple system* (STS) of order v, briefly STS(v), is a set of 3-element subsets called *triples* of a v-set of points such that every pair of points occurs in exactly one triple. The work consists of two parts.

In the first part, we propose a method to generate combinatorial designs based on algebraic geometry techniques, and we consider particular combinatorial designs as points in the geometrical variety associated to a polynomial ideal. With this technique, we could construct ideals whose geometrical varieties are Steiner triple systems and also we were successful in producing Steiner triple systems satisfying additional restrictions, such as being anti-Pasch or Kirkman triple systems. Unfortunately, the computation of the geometric variety was only possible for systems with very small orders. First, we tried to construct a Gröbner basis and then to generate the points in the varieties by using genetic algorithms, but in all cases, our methods only worked for small orders.

The chromosomes of the genetic algorithms that we developed were precisely the points in the domain of the geometric varieties used, and the fitness function was

the number of polynomials in the ideal that a chromosome satisfied. The method worked fine when the fitness function was far from zero, but as it approached zero, it was increasingly difficult to find better chromosomes. After some adjustments, we found that by using only mutations (not crossovers) the behavior of the method was improved, and in particular, we found an appropriate mutation. Our operation was close to another reported by Hartley-Konstam [25] and then we found a hill-climbing algorithm by Stinson [40] that worked very similar to Hartley-Konstam's and our method but with a more efficient behavior. This fact discards the use of genetic algorithms to generate STSs; however, Hartley-Konstam's method was published in 1993 and Stinson's method in 1985. Eight years before!

We found that a formal analysis of Stinson's method is extremely difficult. The method is based on the extension of partial Steiner triple systems, and we found that by making a refinement of these designs that we called quasi-Steiner triple systems it was possible to produce a method with more operations than Stinson's method. On the other hand, the analysis on the correctness of this method is easier compared to Stinson's method.

In consequence, the second part of the work is devoted to study quasi-Steiner triple systems. We discovered a very rich structure in quasi-Steiner triple systems and some properties about them that we considered relevant. The study of quasi-Steiner triple systems are significant for either the theoretical and the practical points of view. Indeed finding STSs with additional properties may be simplified substantially by first finding a QSTS with the desired properties and then transforming it into an STS. For this purpose, we develop a method to transform a QSTS into an STS. We consider that another of the main contributions of this thesis is a method to transform a particular STS into non-isomorphic STSs.

Contents

Abstract ii
List of Illustrations vi
List of Tables vii

1 Introduction 1

2 Gröbner basis and combinatorial designs 10

3 Stable sets, ideals, stability ideal and Gröbner basis 14

4 Colorings Steiner triple systems and Kirkman triple systems 26

5 Parametric generation of STSs 32

6 Quasi-Steiner triple systems and basic operations 39

7 Graph decompositions of QSTSs and operations to reduce the level of QSTS 48

8 Quasi-Steiner triple systems of level two 61

9 Direct transformations among QSTSs 71

10 Conclusions 76

Bibliography **79**

Illustrations

7.1 A component of the decomposition $Q_{7,8}$ for the QSTS in Example 6.1. 48

7.2 Illustration of the proof of Theorem 7.3. 53

7.3 Blocking structure for the reducing method. 58

7.4 Operation to allow further reductions when a blocking structure appears. 60

8.1 Two climbing paths are contained into $Q_{2E,D}$. 66

8.2 Illustration of the proof of Theorem 8.7. 67

8.3 Fusion of two non-climbing paths to yield two climbing paths. 67

8.4 Separation of b and c in C. 69

Tables

6.1 Basic transformations. 44
6.2 Double permutation operation. 47

9.1 Transition matrix A(15). 75

Chapter 1

Introduction

Combinatorial designs are important for several reasons. Probably this is due to the fact that the design of experiments [43], which is formally part of statistics, is essential to perform experiments requiring balance among all the parameters involved. However, the applications of combinatorial designs go well beyond statistics. They are very important in the pharmaceutical industry [37], bio-statistics studies [21], the design of parallel RAID disk systems [28], the planning of sports tournaments [1], the design of failure resilient codes [23] and fiber-optic networks [16], and so on. In [11] appears a comprehensive survey of applications of combinatorial designs. Here we work with Steiner triple systems, which are a specific type of combinatorial design, but our ideas could be extended to other similar structures.

A *Steiner triple system* (STS) of order v, briefly STS(v), is a set of 3-element subsets called *triples* of a v-set of points such that every pair of points occurs in exactly one triple. Given an STS(v), standard counting arguments prove that each point must occur in exactly $r = \frac{v-1}{2}$ triples, and that the triple system consists of exactly $b = \frac{v(v-1)}{6}$ elements. Since both r and b are integers, we get necessary conditions for the existence of an STS(v), which in fact turn out to be sufficient.

Theorem 1.1 *For $v \geq 3$, an STS(v) exists if and only if either $v \equiv 1 \bmod 6$ or $v \equiv 3 \bmod 6$.*

For a survey of basic results on Steiner triple systems see [10].

A *partial Steiner triple system* (PSTS) of order v, briefly PSTS(v), is a set of 3-element subsets of a v-set of points such that every pair of points is contained into at most one triple. The size of a PSTS(v) is the number of triples it contains. It is easy to see that any PSTS(v) has size at most $\frac{v(v-1)}{6}$; and a PSTS(v) of size $\frac{v(v-1)}{6}$ is in fact an STS(v).

Several techniques have been used to generate Steiner triple systems. Among them, constructions based on groups and quasi-grous [29] are common, also exhaustive searches by computer and other heuristic searches [17]. Here we introduce a different method to generate combinatorial designs in general and to construct Steiner triple systems in particular. Our methods are based on algebraic geometry concepts and hill-climbing techniques.

Our first 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, we consider that algebraic geometry techniques that we use can be translated to other designs.

Our method to generate combinatorial designs by algebraic geometry techniques starts by encoding the restrictions of a particular combinatorial design class into a polynomial ideal I over an appropriate polynomial ring. By combinatorial design class we mean a whole family of combinatorial designs such as Steiner triple systems or Kirkman triple systems (see Chapter 4). The second step is to compute the Gröbner basis of I [2]. At this point, every particular combinatorial design in the class will be a point in the geometric variety of I and can be found from the Gröbner basis. When this basis is different from $\{1\}$, at least one instance of the combinatorial design class exist; otherwise, no instance exists and a formal proof of such fact could be

derived from the Gröbner basis. With this method we produced instances of several combinatorial design classes by placing the polynomials modeling the restrictions of each class. Among them were STSs, STSs anti-Pasch and Kirkman triple systems.

Computing the Gröbner basis of ideals generating a particular combinatorial design class is very important since it represents a synthetic form to encode every combinatorial design belonging to the class. So, to recover each one of this designs we only need to solve the polynomials in the Gröbner basis.

The ideals produced by our methods contain a huge number of polynomials and variables, and it represents a difficult problem because the software available to compute Gröbner basis only works with ideals involving at most 999 variables, see [5]. It only allowed us to generate Gröber basis for combinatorial designs of very small orders. For instance, to generate STSs of order 21 the polynomial ideal has 1330 variables, and no available software can manage this amount. To generate STSs of order 19 the polynomial ideal has 969 variables and contains 24226 polynomials; all the available software exhausted the computer memory after a few execution hours. So, we looked for alternatives where our ideals would be useful.

We found that genetic algorithms (GAs) could be used to look for points in the geometric variety. A set of triples (to be completed to an STS) could be codified as a chromosome represented by one characteristic vector and the fitness function could be the number of polynomials not satisfied by the chromosome. In this way, the objective was to find the best chromosome. That is, to find the chromosome minimizing the fitness function. For the basic nomenclature and definitions related to GAs we follow [24].

GAs are powerful tools. However, they proved to be inappropriate to generate STSs. There is a strong deficiency with the crossover operation because after applying

it the fitness of the resulting organism is sometimes significantly increased with respect to the parents' fitness; mainly when these are close to zero. Our genetic algorithm worked fast and fine when the fitness function of the population members was far from zero, but it became slow as the fitness approached to zero. Then we eliminated the crossover operation and thus a pure-mutative genetic algorithm [19] was used.

Our mutation operation looks randomly for two positions, one containing a zero and other containing a one and switch their values with a probability inversely proportional to the degree of unbalance of the resulting set. By *unbalance* of a set of triples we mean the standard deviation of the number of repetitions of the pairs in the triples.

With this mutation operation, we could construct combinatorial designs for several classes, but our polynomial ideals were non essential. For instance, to generate STSs it is possible to define a fitness function counting the missing pairs in each chromosome. The organisms themselves could be constructed without reference to any polynomial ideal. So, we finally developed our algorithms without using any polynomial ideal.

Looking into the literature for the construction of STSs by genetic algorithms we found a work by Hartley-Konstam [25]. The method in this paper is not purely-mutative, in fact it has two mutation operations described as follows.

Each chromosome is a bit string of length equal to the total number of triples over the set S of v elements. Each bit encodes whether or not the corresponding triple is in the potential Steiner triple system represented by the chromosome. Since the number of bits set to 1 in each chromosome corresponds to the number of triples in a solution the program keeps constant the number of bits set to 1 in each chromosome. The first mutation operator consists of choosing at random a bit to be flipped then some other bit set oppositely would be chosen at random to be flipped. Thus the

number of bits set to 1 in the chromosome is kept constant.

The second mutation operation by Hartley-Konstam is quite similar to ours. The idea is to remove from the chromosome a redundant triple. We mean, a triple containing a pair which is contained in another triple. And to add to the chromosome a triple that would contain pairs not contained in any other triple in the chromosome. From a performance point of view, Hartley-Konstam's method was equivalent to ours.

Then, trying to find similar methods not necessarily based on GAs we found another approach by D. Stinson [40]. This method was based on a hill-climbing heuristic which in each step used an operation that was very close to the second mutation operation used by Hartley-Konstam's. Stinson's called this operation SWITCH and it is described in Chapter 6.

Hill-climbing heuristics do not use big populations as it occurs in GAs. In fact, in hill-climbing heuristics only one organism is considered in each step and in consequence Stinson's method is much more efficient than both Hartley-Konstam's method and ours. From this, it immediately follows that hill-climbing heuristics are a better option to construct STSs than genetic algorithms, and it seems unfeasible that a genetic algorithm could improve Stinson's method.

We wondered why Stinson's method had such good performance. Stinson's only gave the brief algorithmic description of his method that we reproduced in Chapter 6, a justification in terms of intuitive ideas, the experimental results he obtained, and no more. We programed the method and in every run it always found an STS. We tried to construct a formal proof of the correctness of Stinson's method, but we found that it was difficult by using the elements in which Stinson based his development. He worked on partial Steiner triple systems (PSTSs), see Chapter 6, and we consider this as the source of the difficulties.

We then introduced a refinement of PSTSs that we called *quasi-Steiner triple systems* (QSTSs) and by using it we were able to understand better the behavior of Stinson's method. We also wondered whether a similar process was possible on triple systems with missing and repeated pairs, but with the same number of triples as an STS. We observed that with the introduction of this change several operations to increase or reduce the number of missing pairs were possible, and finally there appeared transformation methods and results applicable in a general context.

So, our second objective in this thesis is to study QSTSs. QSTSs of a specific order v contain the same number of triples than an STS of the same order v, but repeated and missing pairs are allowed. The number of missing pairs in a QSTS Q is named the *level* of Q. We focus our study on basic operations to transform QSTSs from one level to another being the most interesting the transformation from level two to level zero. This corresponds to the conversion of a QSTS into an Steiner triple system. In addition to the rich combinatorial structure of QSTSs, several properties of STSs can be derived from it. We remark that non-isomorphic QSTSs could be obtained from a single QSTS and this property is immediately valid in STSs.

We substitute PSTSs by quasi-Steiner triple systems. In a PSTS only information about missing pairs is provided, but in QSTSs information about repeated pairs is also given. This information allows us to identify patterns of triples to be changed in order to increase or reduce the level of the QSTS. In PSTSs these patterns are not visible just because they are at a coarser level than QSTSs. Probably that is the reason why Stinson did not present a formal proof on the correctness of his method in [40]. Our original purpose was to establish some operations similar to SWITCH to construct STSs from QSTSs, but we finally found combinatorial structures that we considered relevant and decided to study them in detail. The results of this study

are reported in Chapter 6.

Among these combinatorial structures are the *decomposition graphs*, see Chapter 7. The patterns referred in the previous paragraph are analyzed in Theorem 7.3. Decomposition graphs are also in STSs, but in this case their structure is just a family of cycles. For instance, a Pasch [33] inside an STS is a cycle of length four within a decomposition graph. By applying an operation named *swapping* on the connected components of decomposition graphs it is possible to eliminate or generate Pasches. Rather than studying the effect on Pasches, we focused our attention on the use of the swapping operation to convert an STS into non-isomorphic STSs.

Another interest on QSTSs is related to practical computational issues. Suppose, for instance, that we require some STS with certain hard to satisfy restrictions. However, there is no problem if we produce a QSTS Q at a small level $l > 0$ satisfying those restrictions. Then, finding Q could be less expensive because in general there are much more QSTSs of a given order v at level l than STSs of the same order.

Finally, the ideas in this work could be generalized to construct other combinatorial designs, as well as tools useful in their construction. An example is one-factorizations. A *one-factor* of a graph G is a set of edges that partitions the vertex set of G. A *one-factorization* of G is a set of one-factors that partitions the set of edges of G. Several elementary methods for the construction of Steiner triple systems use one-factorizations extensively, see [29] and [42]. They include Bose's and Skolem's constructions, see [29]. Now, we can define a *quasi one-factorization* of G as a set of one-factors $\{F_1, \ldots, F_n\}$ with as many elements as a one-factorization of G. The *level* of a quasi one-factorization is defined as the number of edges in G, which are not contained in any factor. Then we may look for local transformations to reduce the level. Strong related to one-factorizations are *room squares*. In [15] Dinitz and Stinson gave

the related basic definitions and present several hill-climbing methods for their construction. Furthermore, we can define the concept of "quasi room square" and apply the ideas in our work to generalize them. Dinitz and Stinson also use *strong starters*; these are initial configurations to build square rooms in which good performance for the hill-climbing heuristics is guarantied. We have evidence that some quasi-Steiner triple systems play an equivalent role to strong starters in our algorithms and we will concentrate only on quasi-Steiner triple systems.

The thesis is divided into two parts. The first part consists of Chapters 2, 3, 4, and 5. The second part consists of Chapters 6, 7, 8, and 9.

In Chapter 2 we introduce an ideal to generate stable or maximal independent sets based on the Motzkin-Strauss formula [34]. Then we describe a general ideal introduced by Lovász [32], which has been extensively used for the generation of stable sets in graphs. Both ideals are examples of *0-1 ideals*, a recently introduced class having combinatorial applications beyond stability (see [38]). These ideals are shown to be radical, and consequently we establish the equality of the two ideals. Also in this chapter we introduce basic properties of stability ideals. In Chapter 3 we determinate the stability ideal of the Johnson's graphs $J(n, 3, 2)$ and we use it to build MPTs; we explore difficulties to solve the equations involved, and we examinate potential means to generate MPTs with restrictions. In particular, a modification of the stability ideal of $J(n, 3, 2)$ is shown to generate anti-Pasch MPTs. Chapter 4 introduces two new ideals to generate MPTs that use colorings instead of stable sets. we also introduce an ideal to generate Kirkman triple systems that employs a mixture of techniques based on stable sets and colorings. Chapter 5 explores parametric generation of MPTs. This chapter ends the first part of the work.

The second part of this work starts in Chapter 6. Here we introduce the concept

of quasi-Steiner triple system as well as fundamental notation and results. We also introduce basic operations to either increment or decrement the level of QSTSs, we introduce a method to compute the change in the level and we develop a concrete example for one of the operations. Chapter 7 is devoted to decompositions of QSTSs, which are graphs representing dependence relations between the triples in the system; we give some elementary properties of decompositions as well as the concept of exchangeable path concept. At the middle of this chapter one of the main results, theorem 7.3, is stated. Then we present applications of the main theorem to reduce the level of QSTSs, and we prove general conditions to guaranty level reductions. Chapter 8 deals with combinatorial properties of QSTSs of level two and it introduces conditions to transform these systems into STSs. This chapter contains a theorem to transform QSTSs and STSs into non-isomorphic systems at the same level. In Chapter 9 we develop an algorithm to construct QSTSs pair-wise non-isomorphic. Finally, in Chapter 10 we present the conclusions of this work.

Chapter 2

Gröbner basis and combinatorial designs

This chapter contains a survey of some tools needed in the rest of the work.

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.

We use extensively graphs as well as basic related concepts. For all these elementary definitions. See [14], Chapter 1. All graphs considered here are finite and 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 [22].

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 $\{(x_0, \ldots, x_{n-1}) \mid$

$x_i = 1$ 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 $c(v) \neq c(w)$. 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 [12]) of $k[x_1, \ldots, x_n]$, the *ideal generated by* $f_1, \ldots, f_s$. One remarkable result, the *Hilbert Basis Theorem* (see [12]), establishes that every ideal $I \subset k[x_1, \ldots, x_n]$ has a finite generating set.

Let $I \subset k[\mathbf{x}]$ be an ideal. The *radical* of I is the set

$$\sqrt{I} = \{g \in k[\mathbf{x}] \mid g^m \in I \text{ for some } m \geq 1\}.$$

An ideal I is said to be a *radical ideal* if $\sqrt{I} = I$.

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 2.1 (Weak Hilbert Nullstellensatz (see [27])) *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 Chapter 5, 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 [18].

Chapter 3

Stable sets, ideals, stability ideal and Gröbner basis

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 [34]):

Theorem 3.1 *Let $G = (V, E)$ be a graph. Then*

$$1 - \frac{1}{\alpha(G)} \quad = \quad max \left\{ 2 \sum_{i,j \notin E} x_i x_j \Big| \sum_{i \in V(G)} x_i = 1, x_i \geq 0 \right\}. \tag{3.1}$$

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 (3.1), $\alpha(G)$ 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 $\alpha(G)$:

$$1 - \frac{1}{\alpha(G)} \quad = \quad \max \left\{ 2 \sum_{i,j \notin E} y_i^2 y_j^2 \Big| \sum_{i \in V(G)} y_i^2 = 1 \right\}. \tag{3.2}$$

Lagrange multipliers can be used for (3.2). Make the objective function's gradient equal to a multiplier λ times the restriction function's gradient to obtain the system

of equations:

$$\begin{aligned} 4y_i \sum_{j \in V(G) | i,j \notin E} y_j^2 &= 2\lambda y_i \text{ for each } i \in V(G), \\ \sum_{i \in V(G)} y_i^2 &= 1. \end{aligned} \tag{3.3}$$

This system has several solutions that do not maximize (3.2). Lovász [32] characterizes the set of maximum solutions for (3.1): 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 (3.2) such that $y_j \geq 0$ for every $j \in V(G)$. From (3.3), if $y_i \neq 0$ then

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

So, a solution of (3.3) is a maximum of the objective function in (3.2) if and only if $\lambda = 2\frac{\alpha(G)-1}{\alpha(G)}$. If we substitute this value in (3.3), 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 (3.3) into

$$\begin{aligned} z_i(z_i - 1) &= 0 \text{ for each } i \in V(G), \\ z_i(\sum_{j \in V(G) | i,j \notin E} z_j - \alpha(G) + 1) &= 0 \text{ for each } i \in V(G), \\ \sum_{i \in V(G)} z_i - \alpha(G) &= 0. \end{aligned} \tag{3.4}$$

This yields:

Proposition 3.2 *The graph G has stability number at least e if and only if the following zero-dimensional system of equations*

$$\begin{aligned} x_i^2 - x_i &= 0 \ \ for\ every\ node\ i \in V(G), \\ x_i(\sum_{j \in V(G) | i,j \notin E} x_j - e + 1) &= 0 \ \ for\ each\ i \in V(G), \\ \sum_{i=1}^{n} x_i - e &= 0, \end{aligned} \tag{3.5}$$

has a solution. The vector $\mathbf{x}$ *is a solution of (3.5) if and only if the support of* $\mathbf{x}$ *is a stable set.*

The ideal generated by the polynomials in (3.5) is the *Motzkin-Strauss ideal* of G, denoted by $MS(G)$.

A second approach was introduced by Lovász [32].

Proposition 3.3 (Lovász) *The graph G has stability number at least e if and only if the zero-dimensional system of equations*

$$\begin{aligned} x_i^2 - x_i &= 0 \ \ for\ every\ node\ i \in V(G), \\ x_i x_j &= 0 \ \ for\ every\ edge\ \{i,j\} \in E(G), \\ \sum_{i=1}^{n} x_i - e &= 0, \end{aligned} \tag{3.6}$$

has a solution. Vector $\mathbf{x}$ *is a solution of (3.6) 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 (3.6) is the *stability ideal* of G, denoted by $S(G)$. As Lovász [32] explains, solving (3.6) 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 $k[x_1, \ldots, x_n]$. 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. Consider 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.

Lemma 3.4 [4, pages 341-342, 8.2] *Let k a field and let I be a zero-dimensional ideal of $k[x_1, \ldots, x_n]$, and assume that for $1 \leq i \leq n$, I contains a polynomial $f_i \in k[x_i]$ with $\gcd(f_i, f_i') = 1$. Then I is an intersection of finitely many maximal ideals. In particular, I is then radical.*

Proposition 3.5 [2] *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 3.6 *Let k a field and I a 0-1 ideal in $k[x_1, \ldots, x_n]$ then I is a radical ideal.*

Proof: Let G be the reduced Gröbner basis for I. If $1 \in G$, by Theorem 2.1 $I = k[x_1, \ldots, x_n]$ and hence $I = \sqrt{I}$. Now we consider the case when I is zero-dimensional, since for each $i = 1, \ldots, n$, I contains the univariate polynomial $x_i^2 - x_i$ which satisfy that $\gcd(x_i^2 - x_i, 2x_i - 1)$=1, the result follows from Lemma 3.4. □

Theorem 3.7 (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 3.8 *For G a graph, $S(G) = MS(G)$.*

Proof: By Theorem 3.6 $S(G)$ and $MS(G)$ are both radical. By Propositions 3.2 and 3.3 these two ideals correspond to the same variety. Finally by Theorem 3.7, both ideals coincide. □

Note that Proposition 3.8 is valid for all field k.

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 [38].

In this chapter 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 [2] 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 $S(f, g) = \frac{\text{lcm}(in_\prec(f), in_\prec(g))}{in_\prec(g)} \cdot f - \frac{\text{lcm}(in_\prec(f), in_\prec(g))}{in_\prec(g)} \cdot g$. 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 $P_2(G)$:

$$P_1(G) = \{x_i^2 - x_i | i \in V(G)\} \bigcup \{x_i x_j | i, j \in E(G)\} \tag{3.7}$$

$$P_2(G) = \{\sum_{i \in V(G)} x_i - e\} \tag{3.8}$$

Proposition 3.9 *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 3.10 *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 [30].

Lemma 3.11 *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 the $S(G) = \langle P_1(G) \bigcup P_2(G) \rangle$, the number of S-polynomials calculated by Buchberger's algorithm increases exponentially. Proposition 3.12 explains this behavior.

Proposition 3.12 *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 3.5 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.

Maximum size stable sets in $J(n,3,2)$ correspond to MPT(n)s. In this chapter 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 3.13 *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 $E(J(n,3,2)) \subseteq \cup_{A\in\{4\text{-sets in }\Omega\}} E(K_A)$.

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

$$\begin{aligned} P_1(J(n,3,2)) &= \{x_A^2 - x_A | A \subseteq \{0,\ldots,n-1\} \text{ and } |A| = 3\} \bigcup \\ &\quad \{x_A x_B | A, B \subseteq \{0,\ldots,n-1\}, |A| = |B| = 3 \text{ and } |A \cup B| = 4\} \\ P_2(J(n,3,2)) &= \{\sum_{A \subseteq Triples(\{0,\ldots,n-1\})} x_A - e\}. \end{aligned} \tag{3.9}$$

The ideal generated by the polynomials in (3.9) is the *stability Steiner ideal* of order n. We have an algorithmic approach for its construction.

Algorithm 3.1 *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. $P \leftarrow P \cup \{x_{\{a[1],a[2],a[3]\}} x_{\{a[0],a[1],a[2]\}}\}$
12. $P \leftarrow P \cup \{x_{\{a[0],a[2],a[3]\}} x_{\{a[0],a[1],a[3]\}}\}$
13. $P \leftarrow P \cup \{x_{\{a[0],a[2],a[3]\}} x_{\{a[0],a[1],a[2]\}}\}$
14. $P \leftarrow P \cup \{x_{\{a[0],a[1],a[3]\}} x_{\{a[0],a[1],a[2]\}}\}$
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 [2]; 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 [6, 7]). 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 [6, 7].

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

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 too time-consuming. With the Sahuaro supercomputer in the Arizona State University in 2008 we made experiments for n

equals to 13, 15, and 19 obtaining results in 30 seconds, two minunts and three days, respectively. Being optimistic we consider that with this supercomputer and these heuristics, we may reach values of n as big as 21 after three or four weeks. 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 [41] used a similar development on polytopes in combinatorial optimization applications. At the moment, it is speculative that such structural results can be obtained.

Chapter 4

Colorings Steiner triple systems and Kirkman 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 the vertices in a colour class form a stable set. In this chapter, 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. Furthermore, we introduce an ideal based on a combination of stability and colorings for the generation of Kirkman triple systems (see [9]).

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.

Lemma 4.1 (Loera [31]**)** *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 $\mathbb{C}[x_1, \ldots, x_n]$*

$$x_i^{\lambda} - 1 = 0, \quad \textit{for every vertex } i \in V(G), \tag{4.1}$$

$$x_i^{\lambda-1} + x_i^{\lambda-2}x_j + \cdots + x_j^{\lambda-1} = 0, \quad \textit{for every edge } \{i, j\} \in E(G), \tag{4.2}$$

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 (4.1) and (4.2).

Note that the coloring ideal of λ and G is radical.

By (4.1) every vertex can take one of the λ possible colors. Let us examine (4.2) more thoroughly. Denote by $P_\lambda(x, y)$ the polynomial $x^{\lambda-1} + x^{\lambda-2}y + \cdots + y^{\lambda-1}$.

Lemma 4.2 *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

$$x^\lambda - y^\lambda = (x - y)P_\lambda(x, y). \tag{4.3}$$

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 (4.2) 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 4.3 *Let $n \equiv 1, 3 \pmod 6$ be a nonnegative integer. Let $\lambda = \frac{\binom{n}{2}}{3}$. The zero-dimensional system of equations*

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

has a solution if and only if $\{\{i,j,k\} \mid x_{\{i,j\}} = x_{\{j,k\}} = x_{\{k,i\}}\}$ *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 4.3 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 4.4 *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*

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

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

Proof: Analogous to the proof of Proposition 4.3. □

The ideal generated by the polynomials in the system of equations in Proposition 4.3 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 chapter. 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.

Proposition 4.5 *Let s be a positive integer and let $n = 6s+3$. The zero-dimensional system of equations*

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

has a solution if and only if $S = \{\{i,j,k\} \mid x_{\{i,j,k\}} = 1\}$ 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 4.3, 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 4.3 is the *Kirkman ideal* of order n.

In Proposition 4.5 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.

Chapter 5

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 points $(x_1, x_2, \ldots, x_\ell)$ given by

$$x_i = r_i(t_1, \ldots, t_m) \quad i = 1, \ldots, \ell \tag{5.1}$$

lie in 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 chapter 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).

$$\begin{aligned} x &= t \bmod 7 \\ y &= 1 + t \bmod 7 \\ z &= 3 + t \bmod 7 \end{aligned} \tag{5.2}$$

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 (5.2) 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 (5.2).

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 $n_1 < n$ and $\prod_{i=1}^{1} n_i = n(n-1)/6$. In other words, it is impossible to generalize (5.2) 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 5.1 *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*

$$\left.\begin{array}{r} Q(a_{\alpha_i}) \\ Q(b_{\beta_j}) \\ Q(c_{\delta_k}) \end{array}\right\} = 0, \quad \begin{array}{l} \text{for } i = 0, \ldots, l_1, \\ j = 0, \ldots, l_2 \text{ and } k = 0, \ldots, l_3 \end{array} \tag{5.3}$$

$$\left.\begin{array}{r} P(x(\mathbf{t}) - y(\mathbf{t})) \\ P(x(\mathbf{t}) - z(\mathbf{t})) \\ P(y(\mathbf{t}) - z(\mathbf{t})) \end{array}\right\} = 0, \quad \begin{array}{l} \text{for } \mathbf{t} \in \{0, \ldots, n_1 - 1\} \times \\ \ldots \times \{0, \ldots, n_\ell - 1\} \end{array} \tag{5.4}$$

$$\left.\begin{array}{l} P(x(\mathbf{t}_1)-x(\mathbf{t}_2))P(y(\mathbf{t}_1)-y(\mathbf{t}_2)) \\ P(x(\mathbf{t}_1)-y(\mathbf{t}_2))P(y(\mathbf{t}_1)-x(\mathbf{t}_2)) \\ P(x(\mathbf{t}_1)-x(\mathbf{t}_2))P(z(\mathbf{t}_1)-z(\mathbf{t}_2)) \\ P(x(\mathbf{t}_1)-z(\mathbf{t}_2))P(z(\mathbf{t}_1)-x(\mathbf{t}_2)) \\ P(z(\mathbf{t}_1)-z(\mathbf{t}_2))P(y(\mathbf{t}_1)-y(\mathbf{t}_2)) \\ P(z(\mathbf{t}_1)-y(\mathbf{t}_2))P(y(\mathbf{t}_1)-z(\mathbf{t}_2)) \end{array}\right\} = 0, \quad \begin{array}{c} \textit{for } \mathbf{t}_1,\mathbf{t}_2 \in \{0,\ldots,n_1-1\}\times \\ \ldots \times \{0,\ldots,n_\ell-1\}, \mathbf{t}_1 \neq \mathbf{t}_2 \end{array} \tag{5.5}$$

has a solution.

Proof: Assume that the system of equations is satisfied. Then by (5.3) 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 (5.4) 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 Chapter 4.) Finally, by (5.5) 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 5.1 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

$$\begin{aligned} \{\ & c_1^6-1, b_1-c_1, a_1-c_1, c_0^7-c_0, \\ & b_0^6+b_0^5c_0+b_0^4c_0^2+b_0^3c_0^3+b_0^2c_0^4+b_0c_0^5+c_0^6-1, \\ & a_0^5+a_0^4b_0+a_0^4c_0+a_0^3b_0^2+a_0^3b_0c_0+a_0^3c_0^2+a_0^2b_0^3+a_0^2b_0^2c_0+a_0^2b_0c_0^2+a_0^2c_0^3+a_0b_0^4+ \\ & a_0b_0^3c_0+a_0b_0^2c_0^2+a_0b_0c_0^3+a_0c_0^4+b_0^5+b_0^4c_0+b_0^3c_0^2+b_0^2c_0^3+b_0c_0^4+c_0^5\} \end{aligned}$$

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 (5.2).

Corollary 5.2 *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 $\mathbb{Z}/n\mathbb{Z}$

$$\begin{aligned} \phi(a+b) &= \phi(a)\phi(b) \\ \phi(a \cdot b) &= \phi(a)^b = \phi(b)^a \end{aligned} \tag{5.6}$$

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 $x(\mathbf{t}) = \sum_{j=1}^{l} a_{\alpha_j} \mathbf{t}^{\alpha_j}$ 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 (5.6); 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 5.3 *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*

$$Q_n(\hat{a}_{\alpha_i}) = Q_n(\hat{b}_{\beta_j}) = Q_n(\hat{c}_{\delta_k}) = 0, \quad \begin{array}{l} \textit{for } i = 0, \ldots, l_1, \\ j = 0, \ldots, l_2 \textit{ and} \\ k = 0, \ldots, l_3 \end{array} \tag{5.7}$$

$$\left.\begin{array}{r} P_n(\phi(x(\mathbf{t})), \phi(y(\mathbf{t}))) \\ P_n(\phi(x(\mathbf{t})), \phi(z(\mathbf{t}))) \\ P_n(\phi(y(\mathbf{t})), \phi(z(\mathbf{t}))) \end{array}\right\} = 0, \quad \begin{array}{l} \textit{for } \mathbf{t} \in \{0, \ldots, n_1 - 1\} \times \\ \ldots \times \{0, \ldots, n_\ell - 1\} \end{array} \tag{5.8}$$

$$\left.\begin{array}{r} P_n(\phi(x(\mathbf{t}_1)), \phi(x(\mathbf{t}_2)))P_n(\phi(y(\mathbf{t}_1)), \phi(y(\mathbf{t}_2))) \\ P_n(\phi(x(\mathbf{t}_1)), \phi(y(\mathbf{t}_2)))P_n(\phi(y(\mathbf{t}_1)), \phi(x(\mathbf{t}_2))) \\ P_n(\phi(x(\mathbf{t}_1)), \phi(x(\mathbf{t}_2)))P_n(\phi(z(\mathbf{t}_1)), \phi(z(\mathbf{t}_2))) \\ P_n(\phi(x(\mathbf{t}_1)), \phi(z(\mathbf{t}_2)))P_n(\phi(z(\mathbf{t}_1)), \phi(x(\mathbf{t}_2))) \\ P_n(\phi(z(\mathbf{t}_1)), \phi(z(\mathbf{t}_2)))P_n(\phi(y(\mathbf{t}_1)), \phi(y(\mathbf{t}_2))) \\ P_n(\phi(z(\mathbf{t}_1)), \phi(y(\mathbf{t}_2)))P_n(\phi(y(\mathbf{t}_1)), \phi(z(\mathbf{t}_2))) \end{array}\right\} = 0, \quad \begin{array}{l} \textit{for } \mathbf{t}_1, \mathbf{t}_2 \in \{0, \ldots, n_1 - 1\} \times \\ \ldots \times \{0, \ldots, n_\ell - 1\}, \mathbf{t}_1 \neq \mathbf{t}_2 \end{array} \tag{5.9}$$

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 (5.7) $\hat{a}_0 \ldots, \hat{a}_\ell$, $\hat{b}_0, \ldots, \hat{b}_\ell$, $\hat{c}_0, \ldots, \hat{c}_\ell$ 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 Chapter 4, and so, by Lemma 4.2 the arguments in the proof of Proposition 5.1 with respect to (5.4) and (5.5) are applicable to (5.8) and (5.9), 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 5.1 can be found faster in Macaulay 2 than the corresponding Gröbner basis for Proposition 5.3. 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 5.1 to Proposition 5.3 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 4.1 in the following way.

Lemma 5.4 *Let G be a graph on n vertices for some prime n, and let λ be a non-negative integer. Graph G is λ-colorable if and only if the following zero-dimensional system of equations in $\mathbb{Z}/n\mathbb{Z}[x_1, \ldots, x_n]$*

$$x_i(x_i - 1) \cdots (x_i - \lambda) = 0, \quad \textit{for every vertex } i \in V(G), \tag{5.10}$$

$$(x_i - x_j - 1) \cdots (x_i - x_j - \lambda) = 0, \quad \textit{for every edge } \{i, j\} \in E(G), \tag{5.11}$$

has a solution. □

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

Chapter 6

Quasi-Steiner triple systems and basic operations

The idea of defining Quasi-Steiner Triple Systems was suggested to us by a hill-climbing heuristic search proposed in 1985 by Stinson [40]. He transformed PSTSs by adding successively new triples until an STS was built. We wondered whether a similar process was possible on triple systems with missing and repeated pairs, but with the same number of triples as an STS. We observed that with this change, several operations to increase or reduce the number of missing pairs were possible. Finally, there appeared transformation methods and results applicable in a general context which we consider relevant.

The key element in Stinson's method is a randomized heuristic operation named *SWITCH* that will be explained now.

Let $(\mathcal{V}, \mathcal{B})$ be a PSTS(v). A point $x \in \mathcal{V}$ is *live* if $r_x < \frac{v-1}{2}$, where r_x is the number of blocks in $\mathcal{B}$ containing x. A pair of distinct points, $\{x, y\}$, is *live* if there is no block $B \in \mathcal{B}$ such that $\{x, y\} \subset B$.

Now, if $(\mathcal{V}, \mathcal{B})$ has size less than $\frac{v(v-1)}{6}$, then there must exist a live point, say x, and at least two points $y, z \in \mathcal{V}$ $(y \neq z)$, such that both $\{x, y\}$ and $\{x, z\}$ are live pairs. This is because $r_x \leq \frac{v-3}{2}$, and x has occurred in a block with at most $v - 3$ other points.

Algorithm 6.1 *SWITCH()*

Input: A PSTS(v) $\mathcal{B}$.

Output: The PSTS(v) $\mathcal{B}$ with a new triple added.

global NumBlocks

let x be any live point

let y, z be points such that both $\{x, y\}$ and $\{x, z\}$ are live pairs

if $\{y, z\}$ is a live pair **then**

$\mathcal{B} \leftarrow \mathcal{B} \cup \{\{x, y, z\}\}$

$NumBlocks \leftarrow NumBlocks + 1$

else

let $\{w, y, z\} \in \mathcal{B}$ be the block containing the pair $\{y, z\}$

$\mathcal{B} \leftarrow \mathcal{B} \cup \{\{x, y, z\}\} \setminus \{\{w, y, z\}\}$

Algorithm 6.2 *STINSON'S ALGORITHM(V)*

Input: A positive integer v.

Output: An STS(v).

global NumBlocks

$NumBlocks \leftarrow 0$

$\mathcal{V} \leftarrow \{1, \ldots, v\}$

$\mathcal{B} \leftarrow \emptyset$

while NumBlocks $< v(v-1)/6$

do $SWITCH$

output $(\mathcal{V}, \mathcal{B})$

The author of this method did not prove it works in general [40], and he accepted that it is possible to fail in finding an STS. He justifies the method experimentally.

We have implemented it and in every execution an STS was found in a reasonable short time.

We substitute PSTSs by Quasi-Steiner Triple Systems. In a PSTS only information about missing pairs is provided, but in QSTSs instead, information about repeated pairs is also given. This information allows to identify patterns of triples to be changed in order to increase or reduce the level of the QSTS. In PSTSs, these patterns are not visible just because they are at a coarser level than QSTSs. Probably that is the reason why Stinson did not present a formal proof of the correctness of his method in [40]. Our original purpose was to establish some operations similar to SWITCH to constructing STSs from QSTSs, but we finally found combinatorial structures we considered relevant and decided to study them in detail.

In this chapter we introduce five operations which are similar to SWITCH. These and other operations introduced in subsequent chapters are used by a method that will be referenced to as the *reduction method* whose purpose is to take as input a QSTS(v) Q of level greater than zero and produces a new QSTS(v) Q' with level lower than $l(Q)$. Due to the complexity of the reduction method we do not present here all the details, instead we explain the basic reduction transformations. The computer program implementing the complete algorithm may be requested from the authors.

In Example 6.1 a QSTS(13) is presented. The triples appear column-wise. There 10, 11 and 12 were replaced by A, B and C, respectively, to left aligned the triples as columns.

Example 6.1

```
0000001111122223333444567 8
1245792456A357957895689A8B
```

36CA8BB978C48CA6ABCB7ACB9C

Two triples in a QSTS(v) Q may have the same elements. So, we will consider that $Q = \{T_0, T_1, \ldots, T_{\frac{v(v-1)}{6}-1}\}$. The indexes will be used to avoid any confusion.

If several triples in Q contain $\{i, j\}$ then it is a *repeated pair* in Q. If no triple in Q contains $\{i, j\}$ then it is a *missing pair* in Q.

We define now three sets which are extensively used.

$$\begin{aligned} Ms(Q) &= \{\{i,j\} \mid \{i,j\} \nsubseteq T \text{ for all } T \in Q\} \\ Re(Q) &= \{\{i,j\} \mid \{i,j\} \text{ is a repeated pair in } Q\} \\ R_e^t(Q) &= \{(k, \{a,b\}) \mid T_k \in Q, \{a,b\} \subset T_k \text{ and } \{a,b\} \in Re(Q)\} \end{aligned}$$

Let a, b be two different elements in $\{0, \ldots, v-1\}$ we denote $r_{Q,a,b}$ the number of triples in Q containing $\{a, b\}$. The *level* of Q denoted $l(Q)$ is

$$l(Q) = |Ms(Q)|.$$

For the QSTS(13) Q in Example 6.1 we have

$$\begin{aligned} Ms(Q) &= \{\{6,9\},\{6,C\},\{7,B\}\}, \\ Re(Q) &= \{\{7,8\},\{8,B\},\{9,C\}\}, \\ R_e^t(Q) &= \{(4,\{7,8\}),(24,\{7,8\}),(17,\{8,B\}),(25,\{8,B\}),(18,\{9,C\}), \\ &\quad (22,\{9,C\})\}, \\ l(Q) &= 3. \end{aligned}$$

Lemma 6.2 *For all QSTS(v) Q*

$$l(Q) = |Ms(Q)| = |R_e^t(Q)| - |Re(Q)|.$$

Proof: The quantity $|R_e^t(Q)| - |Re(Q)|$ is the excess of pairs in Q. The meaning of "excess of pairs" is explained now. We know that a repeated pair $\{a, b\}$ in Q is in $r_{Q,a,b}$ triples in Q. Then, by definition, $r_{Q,a,b} - 1$ is the excess of the pair $\{a, b\}$ in Q. The "excess of pairs in Q" is the sum of the excess for all the repeated pairs in Q. Since Q has the same number of triples that any STS(v) every pair in excess in Q should replace a pair which becomes a missing pair in Q. The result follows. □

The maximum level of a QSTS(v) Q occurs when all the triples in Q are exactly the same, say $\{0, 1, 2\}$. It means that $\overline{Ms(Q)} = \{\{0, 1\}, \{1, 2\}, \{0, 2\}\}$ and $|Ms(Q)| = \frac{v(v-1)}{2} - 3$. Thus the level of a QSTS(v) is between zero and $\frac{v(v-1)}{2} - 3$. If a QSTS(v) has level zero then it is an STS(v).

Lemma 6.3 *No QSTS(v) has level one.*

Proof: Let us proceed by contradiction. Suppose that a QSTS(v) Q has level one. Then, there exists a pair $\{a, b\}$ and exactly two triples $B_1 = \{a, b, c\}$ and $B_2 = \{a, b, d\}$ in Q. Since no other pair of triples contains a repeated pair we have that for each element p in $\mathcal{A} = \{0, 1, \ldots, v-1\} - \{a, b, c, d\}$ there exists a unique element $p' \neq p$ such that $\{a, p, p'\} \in Q$. So, it is possible to establish a perfect matching in $K_{\mathcal{A}}$, the complete graph on the vertices of $\mathcal{A}$, but that is impossible because both v and $|\mathcal{A}|$ are odd. □

Each operation is specified as follows. We implicitly assume the existence of a QSTS(v) Q. Let $B_1, B_2, \ldots, B_k$ be a set of triples in Q for a positive integer k and let $B'_1, B'_2, \ldots, B'_k$ be a set of new triples which will replace $B_1, B_2, \ldots, B_k$ in Q to produce a new QSTS(v) Q'. Any possible transformation can be represented in this way, but we are only interested in those such that $l(Q') \leq l(Q)$. In general, we analyze the possibility that a proposed transformations and a specific QSTS satisfies

Name	Original triples	Transformed triples
Switch	$B_1 = \{a, b, c\}$	$B'_1 = \{d, e, f\}$
Repeated transposition	$B_1 = \{a, b, c\}$, $B_2 = \{a, b, d\}$	$B'_1 = \{a, c, d\}$, $B'_2 = \{b, c, d\}$
Diagonal permutation	$B_1 = \{a, b, c\}$, $B_2 = \{a, e, f\}$	$B'_1 = \{a, c, e\}$, $B'_2 = \{b, e, f\}$
Double permutation	$B_1 = \{a, b, c\}$, $B_2 = \{a, e, f\}$	$B'_1 = \{a, c, e\}$, $B'_2 = \{a, b, f\}$
Permutation with replacement	$B_1 = \{a, b, c\}$, $B_2 = \{c, d, e\}$	$B'_1 = \{b, c, f\}$, $B'_2 = \{a, c, d\}$

Table 6.1 : Basic transformations.

this condition by using the following.

Lemma 6.4 *The above described transformation yields a QSTS(v) Q' such that*

$$l(Q') = l(Q) - |\overline{Ms(Q')} - \overline{Ms(Q)}| + |\overline{Ms(Q)} - \overline{Ms(Q')}|. \tag{6.1}$$

Proof: The set $\overline{Ms(Q')} - \overline{Ms(Q)}$ contains pairs which were missing in Q but incorporated into Q' after the transformation. In other words, they are missing pairs in Q gained after the transformation into Q'. Similarly, the set $\overline{Ms(Q)} - \overline{Ms(Q')}$ contains pairs non-missing in Q but lost after the transformation. □

In Table 6.1 we introduce the basic operations used by the reduction method. In each case the original and transformed triples are provided.

In order to apply one of these operations it is necessary match two triples in Q with the triples in the "original triples" of the transformation. Then, such triples are

replaced in Q by the "transformed triples". In Example 6.5 we have a QSTS(13) and we apply a double permutation assigning $(a, b, c, e, f) = (5, 0, 8, B, C)$ to transform $B_1 = \{a, b, c\} = \{5, 0, 8\}$ and $B_2 = \{a, e, f\} = \{5, B, C\}$ into $B_1' = \{5, 8, B\}$ and $B_2' = \{5, 0, C\}$, respectively. The original Q has level three and the transformed Q' has level two. This fact is confirmed by using Equation 6.1 as shown in the following:

Example 6.5 *Original QSTS*(13) Q

```
00000001111222233334445567
12256783458569A468A79B6BB9
B3489ACC69A78BC579B8ACACCC
```

with $Ms(Q) = \{\{1, 2\}, \{1, 7\}, \{7, B\}, \{8, B\}\}$, $Re(Q) = \{\{B, C\}, \{0, 8\}, \{0, 2\}\}$ *and* $l(Q) = 4$.

Transformed QSTS(13) Q'

```
00050001111222233334445067
12286783458569A468A79B65B9
B34B9ACC69A78BC579B8ACACCC
```

with $Ms(Q') = \{\{1, 2\}, \{1, 7\}, \{7, B\}\}$, $Re(Q') = \{\{0, 2\}, \{0, C\}, \{B, C\}\}$ *and* $l(Q') = 3$.

$$
\begin{aligned}
l(Q') &= l(Q) - |\overline{Ms(Q')} - \overline{Ms(Q)}| + |\overline{Ms(Q)} - \overline{Ms(Q')}| \\
&= l(Q) - |\overline{\{\{1,2\},\{1,7\},\{7,B\}\}} - \overline{\{\{1,2\},\{1,7\},\{7,B\},\{8,B\}\}}| \\
&\quad + |\overline{\{\{1,2\},\{1,7\},\{7,B\},\{8,B\}\}} - \overline{\{\{1,2\},\{1,7\},\{7,B\}\}}| \\
&= 4 - |\{\{8,B\}\}| + |\emptyset| \\
&= 4 - 1 + 0 \\
&= 3
\end{aligned}
$$

The time to evaluate $l(Q')$ by Equation 6.1 can be reduced by employing an alternative method. In Table 6.2 there is one row for every pair x, y in which $x \neq y$ and $x, y \in B_1 \cup B_2$. In column "repetitions in Q" the number of repetitions of each pair are annotated and the analogous information for Q' appears in column "repetitions in Q'. As we have explained in the proof of Lemma 6.4 the set $\overline{Ms(Q')} - \overline{Ms(Q)}$ are the pairs gained after the transformation. A pair gained after the transformation is just a pair having a zero in column "repetitions in Q" of Table 6.2, and a number greater than zero in column "repetitions in Q'". So, $|\overline{Ms(Q')} - \overline{Ms(Q)}|$ is equal to the number of rows in Table 6.2 having this property. Analogously, $|\overline{Ms(Q)} - \overline{Ms(Q')}|$ is the number of rows in Table 6.2 having a zero in column "repetitions in Q'", but a number greater than zero in column "repetitions in Q". Obviously, it is not necessary to consider the pairs not changed by the transformation because for this entries the table will contain the same values for columns "repetitions in Q" and "repetitions in Q'".

In this way we are able to evaluate Expression 6.1. The number of entries in Table 6.2 with values zero in column "repetitions in Q" and a positive number in column "repetitions in Q'" is one, and so $|\overline{Ms(Q')} - \overline{Ms(Q)}| = 1$. Since no entry has

pair	repetitions in Q	repetitions in Q'
$\{a, b\} = \{5, 0\}$	1	1
$\{a, c\} = \{5, 8\}$	1	1
$\{b, c\} = \{0, 8\}$	2	1
$\{a, e\} = \{5, B\}$	1	1
$\{a, f\} = \{5, C\}$	1	1
$\{e, f\} = \{B, C\}$	3	2
$\{b, e\} = \{0, B\}$	1	1
$\{b, f\} = \{0, C\}$	1	2
$\{c, e\} = \{8, B\}$	0	1
$\{c, f\} = \{8, C\}$	1	1

Table 6.2 : Double permutation operation.

a zero in column "repetitions in Q'" $|\overline{Ms(Q)} - \overline{Ms(Q')}| = 0$.

The operations reported in Table 6.1 do not cover all the possibilities. In fact, we only considered the operations used by the reduction method. So, we exclusively use operations transforming two triples at most, and with exception of "switching" at most two modifications are allowed.

Chapter 7

Graph decompositions of QSTSs and operations to reduce the level of QSTS

For a QSTS(v) Q and two elements $a, b \in \{0, \ldots, v-1\}$ the *a-b-decomposition* of Q, denoted $Q_{a,b}$, is the graph with $V(Q_{a,b})$ equal to the subset of triples in Q having either a or b as members but not a and b together. Two vertices v_1 and v_2 in this graph are edges in $E(Q_{a,b})$ if and only if $v_1 = \{a, x, y\}$ and $v_2 = \{b, x, z\}$, with $x, y, z \in \{0, \ldots, n-1\}$ pair-wise different. In other words, two triples form an edge e in $Q_{a,b}$ if and only if the first one contains a, the second one contains b, and both triples contain a common element x; The elements a and b are the *axis* and x is the *pivot* of e.

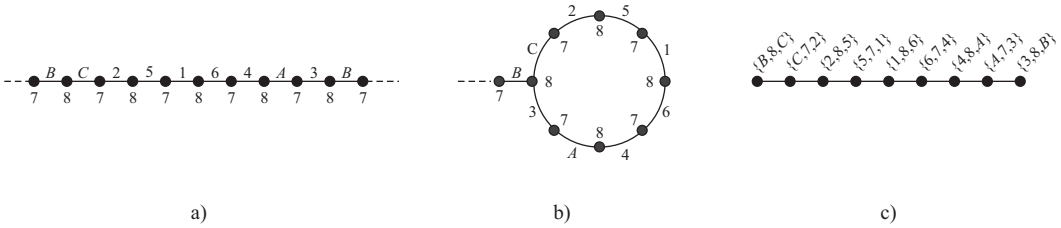

Figure 7.1 : A component of the decomposition $Q_{7,8}$ for the QSTS in Example 6.1.

In Figure 7.1(a) there is represented a component of the decomposition $Q_{7,8}$ of the QSTS(13) in Example 6.1. It corresponds to the path $\{B, 8, C\}$, $\{C, 7, 2\}$, $\{2, 8, 5\}$, $\{5, 7, 1\}$, $\{1, 8, 6\}$, $\{6, 7, 4\}$, $\{4, 8, A\}$, $\{A, 7, 3\}$,$\{3, 8, B\}$. Here, the lines and points are labeled by symbols in $\{0, \ldots, 9, A, B, C\}$, but the interpretation of the drawing

differs from the usual graph representation. For instance, the first vertex 8 in Figure 7.1(a) from left to right represents the triple $\{B, 8, C\}$ and the second vertex 7 the triple $\{C, 7, 2\}$. According to our definition, these triples form an edge in $Q_{7,8}$. In this representation the axis of the edges alternate along the path, and the pivots correspond to the labels of the lines joining vertices. In this drawing, we also see that the pair $\{B, 8\}$ is repeated; in fact, it belong to $\{B, 8, C\}$ and to $\{3, 8, B\}$. In consequence, Figure 7.1(b) is an alternative representation for our example. A dotted line in these drawings represents a missing pair. Thus, the dotted line incident to vertex 7 and line B indicates that the pair $\{7, B\}$ is missing.

We insist that the drawings in Figure 7.1 are different from the usual representation of graphs. In fact, in Figure 7.1(c) the same subgraph of $Q_{6,8}$ has been depicted in the usual graph representation. We rather use the representations in either Figure 7.1(a) or (b) because we consider them much more intuitive.

Lemma 7.1 *Let Q, a and b be as in the previous paragraphs. Then,*

1. *$Q_{a,b}$ is bipartite.*

2. *If Q is an STS then $Q_{a,b}$ is a set of cycles.*

Proof: The graph $Q_{a,b}$ is bipartite because each edge joins one triple containing a and another containing b.

To prove the second part consider that a vertex in $Q_{a,b}$ is a triple, say $\{c_1, a, c_2\}$, which is adjacent in $Q_{a,b}$ to $\{c_3, b, c_1\}$ and $\{c_2, b, c_4\}$ for some appropriate c_3 and c_4. No other possibility exists because every pair is contained into a single triple. It means that $Q_{a,b}$ is two-regular and in consequence, a cycle decomposition. □

Another basic result which will be useful in Chapter 8 and 9 is the following.

Proposition 7.2 *Let Q be a QSTS(v) and let a, b be two different elements in $\{0, \ldots, v-1\}$. Then*

1. *Each pivot i in $\{0, \ldots, v-1\}$ belongs to triples in at most one connected component of $Q_{a,b}$.*

2. *If Q is an STS then $Q_{a,b}$ has at most $v-2$ triples.*

Proof: For the first part, suppose, on the contrary, that some pivot c belongs to two different connected components C_1 and C_2 of $Q_{a,b}$. It means that there exists an edge in C_1, and another in C_2 both with pivot c, say $(\{p_1, b, c\}, \{c, a, p_1'\}) \in E(C_1)$, and $(\{p_2, b, c\}, \{c, a, p_2'\}) \in E(C_2)$. So, $(\{p_1, b, c\}, \{c, a, p_2'\})$ is an edge in $Q_{a,b}$ and $\{c, a, p_2'\} \in C_1$. Thus, $C_1 = C_2$ which is in contradiction to the election of C_1 and C_2.

For the second part, since Q is an STS the number of triples containing a is $\frac{v-1}{2}$ and the same amount of triples contain b. So, $v-3$ triples contain either a or b, but not a and b together. This is the number of vertices in $Q_{a,b}$. □

A QSTS(v) Q is *a-b-c-exchangeable* if and only if Q contains a repeated pair $\{a, b\}$ and a missing pair $\{a, c\}$; here a, b, c are distinct elements in $\{0, \ldots, v-1\}$. An *a-b-c-exchangeable path* is a path $P = \{a, b, p_1\}\{p_1, c, p_2\} \ldots \{p_{k-1}, \alpha, p_k\}$ of $Q_{b,c}$ in which α is either b or c depending upon the parity either even or odd of the length of P, respectively. If P is an *a-b-c*-exchangeable path the *b-c-swapping* of P is the path $sw_{b,c}(P) = \{a, c, p_1\}\{p_1, b, p_2\} \ldots \{p_{k-1}, \bar{\alpha}, p_k\}$ in which $\bar{\alpha}$ is b (resp. c) when $\alpha = c$ (resp. $\alpha = b$). I.e., all the triples in P swap the values of b and c. This is a useful transformation which under appropriate circumstances reduces the level of Q. In general, if T is a triple in $Q_{b,c}$ the *b-c-swapping* of T is the triple $T \Delta \{b, c\}$ where Δ represents the symmetric difference. If C is a subgraph of $Q_{b,c}$ the *b-c-swapping* of C denoted $sw_{b,c}(C)$ is the subgraph C' of $Q'_{b,c}$ induced by the vertices

$O = \{sw_{b,c}(T) \mid T \in V(C)\}$ and $Q' = (Q - V(C)) \cup O$. A *swapping cycle* is a cycle in a descomposition graph containing less than $v - 3$ vertices.

Theorem 7.3 *Let Q be a QSTS(v), let $P = \{a, b, p_1\}\{p_1, c, p_2\} \ldots \{p_{k-1}, \alpha, p_k\}$ be an a-b-c-exchangeable path such that the pairs $\{b, p_1\}$, $\{p_1, c\}$, $\{c, p_2\}, \ldots, \{\alpha, p_k\}$ are not repeated and not missing in Q, and $p_k \neq a$. Then, the QSTS $Q' = (Q - P) \cup sw_{b,c}(P)$ satisfies the following:*

1. Normal path. $l(Q') = l(Q)$, $r_{Q',a,b} = r_{Q,a,b} - 1$, $r_{Q',p_k,\overline{\alpha}} = r_{Q',p_k,\overline{\alpha}} + 1$, *and* $Ms(Q') = Ms(Q) \cup \{p_k, \alpha\} - \{a, c\}$.

2. Broken path. *If* $\{\bar{\alpha}, p_k\} \in Ms(Q)$ *then* $l(Q') = l(Q) - 1$, $r_{Q',a,b} = r_{Q,a,b} - 1$, *and* $Ms(Q') = Ms(Q) \cup \{p_k, \alpha\} - \{\bar{\alpha}, p_k\} - \{a, c\}$.

3. Left bifurcation. *If* $\{\alpha, p_k\} \in Re(Q)$ *then* $l(Q') = l(Q) - 1$, $r_{Q',a,b} = r_{Q,a,b} - 1$, $r_{Q',\overline{\alpha},p_k} = r_{Q,\overline{\alpha},p_k} + 1$, $r_{Q',\alpha,p_k} = r_{Q,\alpha,p_k} - 1$, *and* $Ms(Q') = Ms(Q) - \{a, c\}$.

4. Loop ending. *If* $\{\alpha, p_k\} = \{b, c\}$ *then* $l(Q') = l(Q) - 1$, $r_{Q',a,b} = r_{Q,a,b} - 1$, *and* $Ms(Q') = Ms(Q) - \{a, c\}$.

Proof: All the items in the proof use the following argument.

Since the triples $\{a, b, p_1\}$, $\{p_1, c, p_2\}, \ldots, \{p_{k-1}, \alpha, p_k\}$ are transformed, respectively, into $\{a, c, p_1\}$, $\{p_1, b, p_2\}, \ldots, \{p_{k-1}, \overline{\alpha}, p_k\}$ we have the following:

Fact 1. Before and after the transformation the pairs $\{b, p_1\}, \{p_1, c\}, \{c, p_2\}, \{p_2, b\}$, $\ldots$, $\{p_{k-1}, \alpha\}$ neither increase nor decrease their number of repetitions.

Fact 2. $r_{Q,a,b} = r_{Q',a,b} + 1$, because $\{a, b\} \subset \{a, b, p_1\} \in Q$ but $\{a, b\}$ does not belong to any triple in $sw_{b,c}(P)$.

Fact 3. $r_{Q,a,c} = r_{Q',a,c} - 1$, because $\{a, c\} \subset \{a, c, p_1\} \in sw_{b,c}(P)$, but $\{a, c\}$ does not belong a triple in Q.

Fact 4. $r_{Q,\alpha,p_k} = r_{Q',\alpha,p_k} + 1$ because $\{\alpha, p_k\} \subset \{p_{k-1}, \alpha, p_k\} \in Q$ but $\{\alpha, p_k\}$ does not belong to a triple in $sw_{b,c}(P)$.

Fact 5. $r_{Q,\overline{\alpha},p_k} = r_{Q',\overline{\alpha},p_k} - 1$ because $\{\overline{\alpha}, p_k\} \subset \{p_{k-1}, \overline{\alpha}, p_k\} \in sw_{b,c}(P)$, but $\{\overline{\alpha}, p_k\}$ does not belong to a triple in Q.

In Figure 7.2 these facts are illustrated.

Now these facts are applied to prove the theorem. Only the proof for the first item is developed; the other proofs are similar.

1. Normal path. We prove first that $Ms(Q') = Ms(Q) \cup \{p_k, \alpha\} - \{a, c\}$. Let $\{x, y\}$ be an element of $Ms(Q')$. The pair $\{x, y\} \neq \{a, c\}$ because from the definition of *a-b-c*-exchangeable path $\{a, c\}$ is a missing pair in Q, and from Fact three $\{a, c\}$ is not missing in Q'. The pair $\{x, y\}$ could be equal to $\{p_k, \alpha\}$ because from Fact four this pair is missing in Q'. Otherwise, $\{x, y\}$ must be a missing pair in Q because Facts one to five covers the changes in the number of repetitions for all the pairs contained into the original and transformed triples, and only Facts four and five deal with missing pairs in Q' but not in Q. In consequence, $Ms(Q') \subset Ms(Q) \cup \{p_k, \alpha\} - \{a, c\}$. The reciprocal contention is proved analogously. Since $\{p_k, \alpha\}$ is added and $\{a, c\}$ is deleted to $Ms(Q)$ to construct $Ms(Q')$ the cardinality of both sets is the same and $l(Q) = l(Q')$. Finally, $r_{Q',p_k,\bar{\alpha}} = r_{Q,p_k,\bar{\alpha}} + 1$ follows from Fact 5.

□

The items in this theorem are patterns which will be referred to by the names *normal path*, *broken path*, and so on. Patterns *broken path*, *left bifurcation* and *loop*

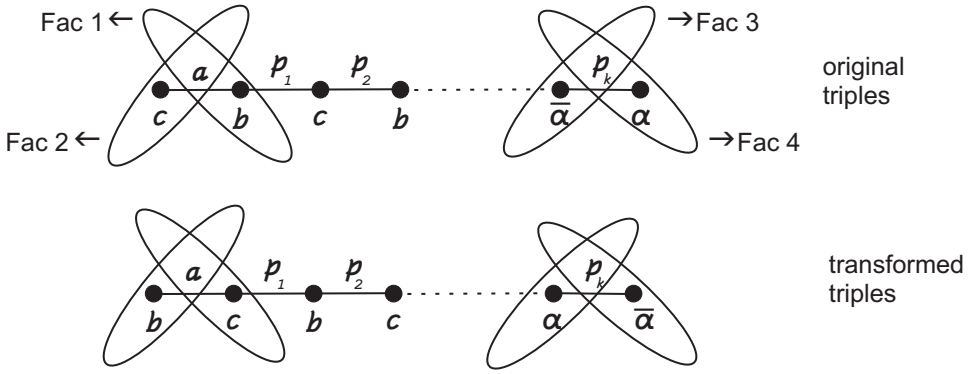

Figure 7.2 : Illustration of the proof of Theorem 7.3.

ending are named *reducing patters* because $sw_{b,c}(P)$ reduces the level of Q. The *normal path* pattern is not useful to reduce the level, but it is important too because it produces modifications in the sets $Re(Q)$ and $Ms(Q)$ without changing the level. A useful application of this will be discussed in Chapter 9.

In order to reduce the level of a QSTS Q by using exchangeable paths, we look for each a-b-c-exchangeable path P in Q and try to match each sub-path with one pattern in the theorem. If it contains one of the *reducing patterns* we apply the swapping operation on that sub-path. Otherwise, the path contains the pivot a twice and it is impossible to reduce it. It looks similar to the path depicted in Figure 7.1. A path as this is a *non-climbing* path. A *climbing path* is the opposite of a non-climbing path.

An additional reducing patter that we name *right bifurcation* is possible and it occurs when $\{\alpha, p_{k-1}\} \in Re(Q)$. However, this pattern is, in fact, a *left bifurcation* when P is a non-climbing path, and we traverse along P in the opposite direction. When all possible exchangeable paths in Q are non-climbing it is possible to transform just one triple in it to meet one of the reducing patters. This could be done in several

ways, but we only use the transformations in Table 6.1. Other transformations are possible but those in Table 6.1 were enough for the implementation of the reduction method.

For instance, the path depicted in Figure 7.1 is non-climbing. This path belongs to the decomposition $Q_{7,8}$ of a QSTS(v) Q. Now, we assume Q unrelated to the QSTS in Example 6.1. Suppose additionally that the pairs $\{0,8\}$, $\{0,6\}$ and $\{0,7\}$ belong to $Ms(Q)$. The switching operation in Table 6.1 transforming $\{4,6,7\}$ into $\{0,6,7\}$ will not change the level but broke the path. Because after the transformation no triple will contain the pair $\{8,0\}$. After this change, the path will meet the *broken path* pattern and the transformed path will be climbing.

Each of the transformations in Table 6.1, depending upon the number of repetitions of each pair, will make disappear some pairs, other pairs will increase the number of repetitions and a subset of triples will change. These simple modifications are enough to meet the reducing patters as it happened in the previous paragraph example. Let us analyze this with the double permutation operation.

We have explained how to calculate the change in the level of a QSTS(v) Q after a double permutation operation in Chapter 6. The pairs $\{b,c\}$ and $\{e,f\}$ reduce their number of repetitions while the same number is increased for $\{b,f\}$ and $\{c,e\}$. Going back to the decomposition component in Figure 7.1, a double permutation will be useful to meet the *broken path* pattern if we can find a couple of triples $\{a,b,c\}$ and $\{a,e,f\}$ such that the following conditions are hold.

1. A double permutation can be performed without changing the level of Q on $\{a,b,c\}$ and $\{a,e,f\}$.

2. $r_{Q,b,c} = 1$ (resp. $r_{Q,e,f} = 1$) and $\{b,c\}$ (resp. $\{e,f\}$) is one of the pairs $\{C,7\}$,

$\{2,8\}$, $\{5,7\}$, $\{1,8\}$, $\{6,7\}$, $\{4,8\}$, $\{A,7\}$, or $\{3,8\}$.

3. The transformation only changes the last triple in the sub-path to be swapped.

These conditions could be exhaustively analyzed by a computer program to find the right triples to be transformed. Of course, any pair (reduction pattern, basic operation) could be used. The important thing here is to find the right set of conditions to guaranty a level reduction. We do not include all possible combinations here, but they can be easily developed.

Another useful transformation is the redirection of a non-climbing path (to be explained now) to transform it into a climbing one. Again, the decomposition component in Figure 7.1 is used in the explanation. Suppose that there exists a transformation changing the triple $\{1,6,8\}$ into $\{0,1,8\}$ without changing neither the level nor a triple appearing from left to right before than $\{1,6,8\}$. After performing the transformation the final effect is to redirect the path starting at the changed triple. If the new path is climbing, then it will be possible to reduce the level of Q.

There is a big number of ways to compose the transformations in Table 6.1 to meet reducing patters in non-climbing paths. The *normal path* pattern is also useful in the opposite direction. I.e., it could be used to either reduce or increase the number of repetitions of pairs in order to perform a level reduction through the use of a transformation in Table 6.1.

Let us start with an example. From Table 6.1 it follows that repeated transposition changes two triples $\{a,b,c\}$ and $\{a,b,d\}$ into $\{c,d,a\}$ and $\{c,d,b\}$ respectively. This transformation reduces the level of the QSTS when the number of $\{a,b\}$ repetitions is greater than two and $\{c,d\} \in Ms(Q)$. Following the notation introduced for Theorem 7.3 a switching under a *normal path* P will add $\{p_k,\alpha\}$ to $Ms(Q)$ after

swapping P. So, if $\{p_k, \alpha\}$ is equal to $\{c, d\}$ then after the swapping of P, the repeated transposition of $\{a, b, c\}$ and $\{a, b, d\}$ will reduce the level of Q. In conclusion, the swapping of P by itself does not produce any reduction in the level of Q, but it prepares a successful reduction by applying a repeated transposition.

In some sense, the swapping operation on a *normal path* pattern works just as an additional basic transformation. In fact, a double permutation sometimes is equivalent to the swapping of a *normal path* pattern with just two triples. The difference is that the *normal path* pattern transforms an unspecified number of triples and the basic operations only work with at most two triples. The *normal path* pattern could also be used to either increase the number of repetitions of a pair or to change some elements in specific triples. Another practical application of the *normal path* pattern happens when two non-climbing paths meet at some triple: the swapping of a subpath starting in the initial triple of the path and ending in the meeting triple could be useful to meet one of the reducing patters in the second path.

Now, it should be clear that a basic transformations which does not change the level of Q could be used to prepare the system to allow a level reducing transformation. For instance, we have explained in a previous example that the switching transformation could be used to eliminate pairs in Q. If one of these pairs is $\{b, c\}$ then a repeated transposition on $\{a, b, c\}$ and $\{a, b, d\}$ will reduce the level provided that these triples are originally in Q.

For the practical implementation of the reducing method we started programing a subset of the basic operations and the analysis of *a*-*b*-*c*-decompositions to identify climbing-paths. Then, we executed the program for values of v as great as 500, in general it allowed us to reach QSTSs of levels lower bounded by 50. When it was not able to reduce more QSTSs our program looked for a new applicable transformation

to meet one of the reducing patters and incorporate it in the computer program. About 50 cases were found necessary, and we incorporate to our program all of them. Of course, several possibilities were left out because they were not required by any QSTS. However, we do not discard the possibility that some new cases be, in fact, necessary.

The running time complexity to transform a QSTS(v) into other with a lower level depends upon the way in which a non-climbing path is used, and the basic operation is applied. However, we consider that in general this is $O(v^5)$. The number of triples in Q is $b = \frac{v(v-1)}{6}$. Since at most we employed two triples to be changed in the basic transformations a $O(b^2)$ running time is required. Then, the maximum length of a non-climbing path is v because a repeated pivot originates either a *left bifurcation* or *right bifurcation* pattern, see Theorem 7.3, and so the final running time complexity is $O(b^2 \times v) = O(v^5)$.

Unfortunately, we cannot offer a full proof on the completeness of our reduction method, but we have identified some cases in which the reduction is guarantied.

Proposition 7.4 *Let Q be a QSTS(v) such that for a pair $\{a, b\}$ $r_{Q,a,b}$ is an odd integer greater than one, and one of the pairs either $\{a, c\}$ or $\{b, c\}$ is in $Ms(Q)$ for some $c \in \{0, \ldots, v-1\}$. Then, it is possible to reduce the level of Q.*

Proof: Without loss of generality, we assume $\{a, c\} \in Ms(Q)$. We start by constructing the path $P_1 = \{a, b, p_1\}, \{p_1, c, p_2\}, \ldots, \{p_{k-1}, \alpha, p_k\}$ as the one used in Theorem 7.3. If either one reducing pattern is met or $p_k = a$, we stop the construction. In the former case, the proposition is true by Theorem 7.3. In the latter; we start building a new path P_2 from the triple $\{a, b, q_1\}$ with q_1 different to both p_1 and p_{k-1}. Such q_1 exists because $r_{Q,a,b} > 2$. If P_2 is climbing, then we are done, in other

ways we proceed to build more paths similarly. Since $r_{Q,a,b}$ is odd, at some point we will construct a climbing path; otherwise, $r_{Q,a,b}$ would be even because each path has two ends. The proposition follows. □

Proposition 7.5 *Let Q be a QSTS(v) such that for a pair $\{a, b\}$ $r_{Q,a,b}$ is an even integer greater than two. If in addition Q contains a live point y then it is possible to reduce the level of Q.*

Proof: Since y is a live point there exist two elements x and z such that both $\{x, y\}$ and $\{y, z\}$ are in $Ms(Q)$. On the other hand, there exist a triple $\{a, b, c\} \in Q$ because $r_{Q,a,b} > 2$. If we change $\{a, b, c\}$ into $\{x, y, z\}$ to produce a new QSTS(v) Q' we have one of the following:

- $r_{Q,a,c} > 1$, $r_{Q,b,c} > 1$ or $\{x, z\} \in Ms(Q)$. Then, $l(Q') < l(Q)$ and the proposition follows.

- Both $r_{Q,a,c} = 0$ and $r_{Q,b,c} = 0$. Then, the transformation preserves the level, but now we apply Proposition 7.4 because Q, $\{a, b\}$, $r_{Q,a,b}$ and $\{b, c\}$ satisfy the hypothesis.

The proposition follows. □

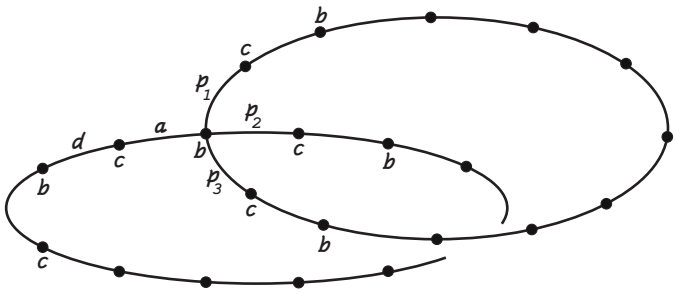

Figure 7.3 : Blocking structure for the reducing method.

In Proposition 7.4 a hypothesis is the existence of a pair either $\{a, c\}$ or $\{b, c\}$ in $Ms(Q)$. This pair is essential for the proof of this proposition. In Figure 7.3 a component of $Q_{b,c}$ is represented for some QSTS(v) in which $r_{Q,b,c} = 3$, but neither $\{a, c\}$ nor $\{b, c\}$ are missing pairs. Then three paths starting at triples $B_1 = \{a, b, p_1\}$, $B_2 = \{a, b, p_2\}$, and $B_3 = \{a, b, p_3\}$ can be build but all of them form cycles but no climbing path does exit. Instances of this structure appeared recurrently in QSTSs of level three when we ran our programs. In these structure the pair $\{a, b\}$ is contained into triples B_1, B_2, and B_3 but the pairs $\{a, c\}$ and $\{b, c\}$ are not missing for any value of c. In other words, for each element c different from a and b the components of the decompositions $Q_{a,c}$ and $Q_{b,c}$ containing B_1, B_2, and B_3 have a representation as the one in Figure 7.3. All these components act together as a blocking structure making difficult the application of any transformation to lower the level.

We conjecture that if the level of some QSTS Q cannot be reduced by our method then Q should contain the blocking structure just described. However, the following strategy has always solved the problem. We use the nomenclature introduced in the previous paragraph and consider that C is the component of $Q_{b,c}$ containing a as a pivot. First, we look at a value $c \notin \{a, b, p_1, p_2, p_3\}$, locate in Q the triple $B = \{a, c, d\}$, which surely exists because by hypothesis $\{a, c\} \notin Ms(Q)$. Then, we locate a value $e \notin \{a, b, c, d, p_1, p_2, p_3\}$ which surely exist when $v \geq 9$. We finally replace $\{a, c, d\}$ by $\{a, e, d\}$. The final effect is to break one cycle in C by eliminating the triple $\{a, c, d\}$. The cost of this operation is that the level of Q is increased by one. In Figure 7.4 is illustrated this transformation.

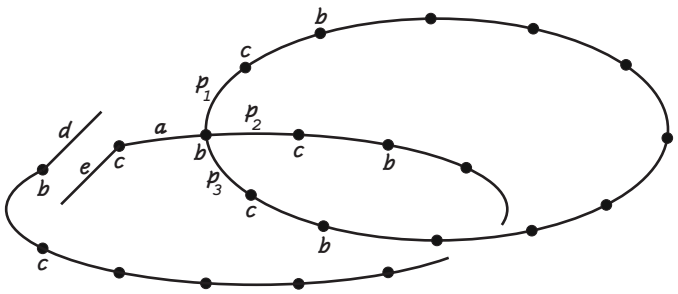

Figure 7.4 : Operation to allow further reductions when a blocking structure appears.

Chapter 8

Quasi-Steiner triple systems of level two

The work in the previous chapter in general can be applied to QSTSs of any level, and it is possible that even a basic operation in Table 6.1 transforms a QSTS of level two into an STS. However, QSTSs of level two have a special structure which is studied here. We start by giving general structural property of QSTSs.

Proposition 8.1 *Let Q be a QSTS(v), and let a be in $\{0,\ldots,v-1\}$. Then, the parity of the number n_o of elements $b \in \{0,\ldots,v-1\}-\{a\}$ such that $r_{Q,a,b} > 0$ and $r_{Q,a,b} \bmod 2 = 0$ is equal to the parity of the number n_2 of elements $d \in \{0,\ldots,v-1\}-\{a\}$ such that $r_{Q,a,d} = 0$.*

Proof: Let n_1 be the number of elements c such that $r_{Q,a,c} \bmod 2 = 1$. Now, N_0 and N_1 will represent

$$N_0 = \sum_{b \text{ such that } r_{Q,a,b}>0 \text{ and } r_{Q,a,b} \bmod 2=0} r_{Q,a,b}$$
$$N_1 = \sum_{b \text{ such that } r_{Q,a,b} \bmod 2=1} r_{Q,a,b}$$

The value of $parity(N_o)$ is zero because only even integers are added. Similarly, $parity(N_1) = parity(n_1)$ because n_1 is the number of terms added to compute N_1, and all these numbers are odd.

Besides, $parity(N_0+N_1)$ is zero because N_0+N_1 is the number of (not necessarily different) pairs having a in common, and contained into a triple in Q. On the other

hand, each block containing a has two of these pairs and so N_0+N_1 is even. It implies that $parity(N_1) = 0$ because $parity(N_o)$ is zero.

Since $v-1 = n_0+n_1+n_2$ we have that

$$0 = parity(v-1) = parity(n_o+n_1+n_2) = parity(n_o+n_2) \tag{8.1}$$

The last equality holds because $parity(n_1) = parity(N_1) = 0$. We finally have from expression 8.1

$$parity(n_0) = parity(n_2).$$

And the proposition follows. □

Proposition 8.2 *If Q is a QSTS(v) with level two, then there exist distinct elements a, b, a', $c \in \{0, \ldots, v-1\}$ such that one of the following conditions holds:*

1. *$Ms(Q) = \{\{a,c\},\{a',c\}\}$, $Re(Q) = \{\{a,b\},\{a',b\}\}$, and we call Q* non-transfer.
2. *$Ms(Q) = \{\{a,c\},\{a',b\}\}$, $Re(Q) = \{\{a,b\},\{a',c\}\}$, and we call Q* transfer.

Proof: Since Q has level two there exist two different missing pairs $\{x_1, y_1\}$ and $\{x_2, y_2\}$. In other words, the cardinality of the symmetric difference $\{x_1, y_1\}\Delta\{x_2, y_2\}$ is equal to either two or four. In the former case, we have a non-transfer QSTS, and in the last a transfer-QSTS. Now, we prove the equalities about $Re(Q)$.

In the case of a non-transfer QSTS, both $\{a, c\}$ and $\{a', c\}$ are missing pairs, and from Lemma 6.2 it follows that $|r_e^t(Q)| = 2$. In other words, two pairs $\{x_1, y_1\}$ and $\{x_2, y_2\}$, not necessarily different, must be contained into two triples.

Since a belongs to exactly one missing pair, Proposition 8.1 says that a must belong to an odd number of repeated pairs, and in fact this number should be one

because otherwise $l(Q)$ would be greater than two. For the same reason, a' should belong to a repeated pair. So, we have two possibilities: either $a = x_1$ and $a' = y_1$ or $a = x_1$ and $a' = x_2$.

The case $a = x_1$ and $a' = y_1$ is impossible, otherwise x_2 would belong to exactly one repeated pair but not belong to one missing pair contradicting Proposition 8.1. So, the only possibility is $a = x_1$ and $a' = x_2$. Now, we have two additional possibilities: either $y_1 \neq y_2$ or $y_1 = y_2$.

The case $y_1 \neq y_2$ is impossible because again y_1 will belong to a repeated pair but not to a missing pair. The conclusion is that $y_1 = y_2$. In the statement, we use b to denote this common element.

The proof for transfer QSTSs is analogous. □

The last proposition establishes possibilities for the sets $Ms(Q)$ and $Re(Q)$ when $l(Q) = 2$, but it does not present any evidence that such systems, in fact, exist.

Example 8.3 *For order $v = 15$ the QSTS(15) Q_1*

```
000000011111122222333334444555666789
123578b25789A458BD45678567C9C79BAAA
469ACED36BDCEA79CEBEADC8D9EBD8EEEBD
```

has level two, $Ms(Q_1) = \{\{6, C\}, \{A, C\}\}$, $Re(Q_1) = \{\{6, E\}, \{A, E\}\}$, and thus it is non-transfer. Analogously, the QSTS(15) Q_2

```
000000011111122222333334444555567789A
123456923469D346B8467867B67A8C8A9CB
7DC8EBACA58BE597EAE9BDADCD9CBECEDED
```

has also level two, $Ms(Q_2) = \{\{8, E\}, \{C, D\}\}$, $Re(Q_2) = \{\{8, D\}, \{C, E\}\}$, and is transfer.

When we talk about either transfer or non-transfer QSTSs, we implicitly assume they have level two.

We follow the variable names introduced in Proposition 8.2 and the nomenclature from Chapter 7. If Q is non-transfer then Q is a-b-c- and a'-b-c-exchangeable. However, if it is transfer then it is a-b-c-, a'-b-c-, b-a-a' and c-a-a'-exchangeable. So, in this sense, transfer QSTSs are "more" exchangeable that non transfer QSTSs. The adjective "transfer" is used here because either some path or cycle of $Q_{b,c}$ meets either a path or cycle in $Q_{a,a'}$.

Proposition 8.4 *Every non-transfer QSTS Q can be transformed into a transfer QSTS Q'.*

Proof: Let Q be a non-transfer QSTS, then $Ms(Q) = \{\{a, c\}, \{a', c\}\}$ and $Re(Q) = \{\{a, b\}, \{a', b\}\}$. Since $\{a, b\}$ is a repeated pair there exists a triple containing it, say $\{a, b, d\}$. If in this triple b is changed by c then $\{a, b, d\}$ is transformed into $\{a, c, d\}$ to produce a new Q' such that $l(Q') = l(Q)$, $Ms(Q) = \{\{b, d\}, \{a', c\}\}$ and $Re(Q) = \{\{c, d\}, \{a', b\}\}$ that is a transfer QSTS. □

So, without loss of generality we can always assume that we are working with transfer QSTSs.

Proposition 8.5 *If Q is an a-b-c-exchangeable QSTS(v) with level two and containing a climbing path, then Q can be transformed into an STS(v).*

Proof: It is immediate from the definition of climbing path, Proposition 6.3 and the fact that a QSTS(v) of level zero is an STS(v). □

Proposition 8.6 *Let Q be a transfer a-b-c-exchangeable QSTS(v) of level two. Then, $Q_{b,c}$ consists of a set of cycles and one of the following:*

1. *Two climbing paths.*

2. *Two non-climbing paths.*

Proof: Since Q is both transfer and a-b-c-exchangeable then $Ms(Q) = \{\{a, c\}, \{a', b\}\}$, and $Re(Q) = \{\{a, b\}, \{a', c\}\}$ for some appropriate a'. Since $\{a, b\}$ is repeated twice there are two different elements p_1 and p_2 such that both $\{a, b, p_1\}$ and $\{a, b, p_2\}$ are in Q.

If $Q_{b,c}$ contains a connected component C not containing neither p_1 nor p_2 as pivots, then C must be a cycle. The proof is similar to the second part of Lemma 7.1. If the connected component contains p_1 as a pivot, then we will try to build an a-b-c-exchangeable path P starting at $\{a, b, p_1\}$ until we are not able to continue. The next triple to be incorporated is the one containing $\{p_1, c\}$, say $\{p_1, c, p_2\}$ if it exists. And we continue adding triples $\{p_2, b, p_3\}$ and so on. We will stop at some point after a finite number of steps when some pair $\{p_k, \alpha\} \in Ms(Q)$ be reached with either $\alpha = b$ or $\alpha = c$ depending upon the parity of k. But we only have two possibilities for $\{p_k, \alpha\}$: either $\{a, c\}$ or $\{a', b\}$. For the first case we have a *normal path* pattern, which is not climbing and in the second one we have a *left bifurcation* which is climbing, see Theorem 7.3.

When P starts at $\{a, b, p_1\}$ and $\{p_k, \alpha\} = \{a, c\}$ then $\{p_{k-1}, \overline{\alpha}, p_k\} = \{p_{k-1}, b, a\}$ is the ending vertex of P. Then, other path P' starting at $\{a', c, p'_1\}$ and ending at $\{p'_{k'-1}, c, a'\}$ can be built. It means that two non climbing paths are in $Q_{b,c}$.

Otherwise, P starts at $\{a, b, p_1\}$ and ends at $\{p_{k-1}, c, a'\}$, and other path P' starting at $\{a, b, p_2\}$ and ending at $\{p'_{k'-1}, c, a'\}$ can be built. So, two climbing paths are in $Q_{b,c}$.

The proposition follows. □

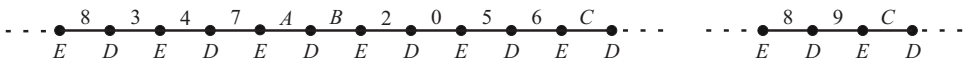

Figure 8.1 : Two climbing paths are contained into $Q_{2_{E,D}}$.

In Figure 8.1 we see that two climbing paths are contained into $Q_{2_{E,D}}$ for the QSTS Q_2 introduced after Proposition 8.2.

Of course, if in the last proposition the condition one holds, then we transform Q into an STS. Otherwise, since Q is transfer, it is also b-a-a'-exchangeable and we have the decompositions $Q_{b,c}$ and $Q_{a,a'}$ to look for a climbing path.

The following theorem will be used in practically all the remaining results in the paper.

Theorem 8.7 *Let Q be a QSTS(v) and let a, b be two different elements in $\{0, \ldots, v-1\}$. If $C_{a,b}$ is a connected component in $Q_{a,b}$ then the QSTS $Q' = (Q - C_{a,b}) \cup sw_{a,b}(C_{a,b})$ satisfies the following:*

1. *$l(Q) = l(Q')$.*

2. *If $C_{a,b}$ is a cycle then $Ms(Q) = Ms(Q')$.*

Proof: Consider the representation of graph decompositions introduced in Chapter 7. A single line labeled c in this representation joins two vertices a and b and represents the intersection of a set of triples $\{p_1, a, c\}, \ldots, \{p_{k_1}, a, c\}$ with a set of triples $\{c, b, q_1\}$, $\ldots$, $\{c, b, q_{k_2}\}$ for appropriate values $p_1, \ldots, p_{k_1}, q_1, \ldots, q_{k_2}$, $k_1 \geq 0$ and $k_2 \geq 0$, see Figure 8.2(a). The swapping operation $sw_{a,b}(C_{a,b})$ transform all these triples into $\{p_1, b, c\}, \ldots, \{p_{k_1}, b, c\}, \{c, a, q_1\}, \ldots, \{c, a, q_{k_2}\}$, see Figure 8.2(b).

In consequence, if $k_1 > 0$ and $k_2 > 0$ neither $\{a, c\}$ nor $\{c, b\}$ will be missing pairs in $Ms(Q')$ and no change in $l(Q')$ will occur with respect to $l(Q)$. Now, if $k_1 = 0$,

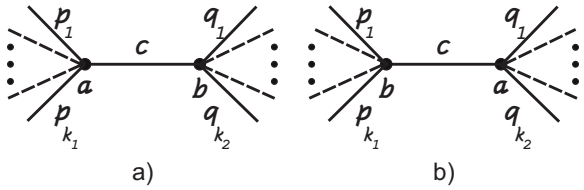

Figure 8.2 : Illustration of the proof of Theorem 8.7.

then k_2 should be greater than zero and so $\{a, c\}$ is in $Ms(Q)$ but it is not in $Ms(Q')$; $\{b, c\}$ is not in $Ms(Q)$ but it is in $Ms(Q')$. So, we are only replacing $\{a, c\}$ in $Ms(Q)$ by $\{b, c\}$ in $Ms(Q')$, but the cardinalities of both $Ms(Q)$ and $Ms(Q')$ are preserved. And thus, $l(Q) = l(Q')$.

Now, if $C_{a,b}$ is a cycle, then by the first sentence in the previous paragraph $Ms(Q)$ will be identical to $Ms(Q')$. □

We now address the level reduction of QSTSs of level two containing two non-climbing paths.

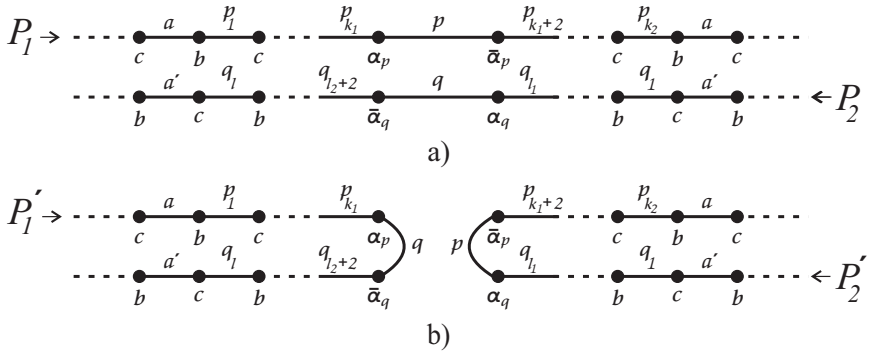

Figure 8.3 : Fusion of two non-climbing paths to yield two climbing paths.

Proposition 8.8 *Let Q be a transfer QSTS(v) of level two such that $Ms(Q) = \{\{a, c\}, \{a', b\}\}$, $Re(Q) = \{\{a, b\}, \{a', c\}\}$ and $Q_{b,c}$ contains two non climbing paths*

P_1 and P_2. If P_1 and P_2 contain pivots p and q, respectively, $\{p,q\} \not\subseteq \{a,a',b,c\}$, and b,c are in different connected components of $Q_{p,q}$ then $Q' = (Q - C_b) \cup sw_{p,q}(C_b)$ contains two climbing paths. Here, C_b represents the component of $Q_{p,q}$ containing b as a pivot.

Proof: From Proposition 8.6 we have that $P_1 = \{a,b,p_1\},\{p_1,c,p_2\},\ldots,\{p_{k_1},\alpha_p,p\}$, $\{p,\overline{\alpha_p},\ p_{k_1+2}\},\ \ldots,\{p_{k_2},b,a\}$ and $P_2 = \{a',c,q_1\},\{q_1,b,q_2\},\ \ldots,\ \{q_{l_1},\alpha_q,q\},\{q,\overline{\alpha_q},\ q_{l_1+2}\},\ldots,\{q_{l_2},c,\ a'\}$, see Figure 8.3(a).

Without losing generality, we will assume that $\alpha_p = \alpha_q = b$.

From all the triples in P_1 and P_2 only $\{p_{k_1},\alpha_p,p\}$ and $\{p_{l_1},\alpha_q,q\}$ will be changed into $\{p_{k_1},\alpha_p,q\}$ and $\{p_{l_1},\alpha_q,p\}$, respectively, after performing $sw_{p,q}(C_b)$. It is because all the pivots distinct from both a and a' in P_1 and P_2 are pairwise different. It follows from Proposition 7.2 because P_1 and P_2 are not connected in $Q_{b,c}$. Then, Theorem 8.7 guaranties that the swapping does not modify the missing pairs in Q and so the change maintains the level.

However, $sw_{p,q}(C_b)$ modifies P_1 and P_2 into transformed paths P_1' and P_2' as follows: $P_1' = \{a,b,p_1\},\{p_1,c,p_2\},\ldots,\{p_{k_1},\alpha_p,q\},\ \{q,\overline{\alpha_q},q_{l_1+2}\},\ldots,\{q_{l_2},c,a'\}$ and $P_2' = \{a',c,q_1\},\{q_1,b,q_2\},\ \ldots,\ \{q_{l_1},\alpha_q,p\},\ \{p,\overline{\alpha_p},p_{k_1+2}\},\ldots,\{p_{k_2},b,a\}$, see Figure 8.3(b).

In other words, we are transforming the paths in such a way that the ends of both P_1 and P_2 are now interchanged in P_1' and P_2'. But now these two paths are climbing. □

The hypothesis in Proposition 8.8 saying b,c are in different connected components of $Q_{p,q}$ is too restrictive for the application of Proposition 8.8. However, it is possible to use Theorem 8.7 in the following way.

Proposition 8.9 *Let Q, a, b, c, P_1, P_2, p, q be as in Proposition 8.8. Now, suppose*

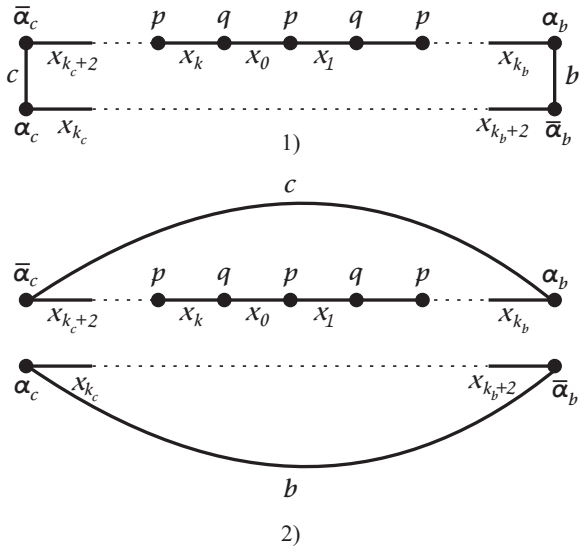

Figure 8.4 : Separation of b and c in C.

both b and c are in the same connected component C of $Q_{p,q}$. If the distance of a and b in C is even, then $Q' = (Q - P_1) \cup sw_{b,c}(P_1)$ satisfies all the hypothesis in Proposition 8.8.

Proof: The connected component C is a cycle because no repeated pair is contained into $Q_{p,q}$ and the proof of the second part of Lemma 7.1 can be directly applied to C. And thus, the distance between a, b can be taken from the cycle C, and without risk of confusion it will be either odd or even because C is bipartite by Lemma 7.1.

Assume that $C = \{x_0, p, x_1\}, \ldots, \{x_{k_b}, \alpha_b, b\}$, $\{b, \overline{\alpha_b}, x_{k_b+2}\}$, $\ldots, \{x_{k_c}, \alpha_c, c\}, \{c, \overline{\alpha_c}, x_{k_c+2}\}, \ldots \{x_k, q, x_0\}$, see Figure 8.4(1).

Without losing generality, we assume that $\alpha_b = p$. Now, as the distance in C between pivots b and c is even $\alpha_c = p$.

Since P_1 contains p as a pivot but not q, we have that the only triples in C, which change after applying $sw_{b,c}(P_1)$ are $\{x_{k_b}, \alpha_b, b\}$ and $\{x_{k_c}, \alpha_c, c\}$. The first one is trans-

formed into $\{x_{k_b}, \alpha_b, c\}$ and the second one into $\{x_{k_c}, \alpha_c, b\}$. But C itself is separated into two cycles: $C_1 = \{x_0, p, x_1\}, \ldots, \{x_{k_b}, \alpha_b, c\}, \{c, \overline{\alpha_c}, x_{k_c+2}\}, \ldots, \{x_k, q, x_0\}$, and $C_2 = \{b, \alpha_c, x_{k_c}\}, \{x_{k_c}, \overline{\alpha_c}, x_{k_c-1}\}, \ldots, \{x_{k_b+2}, \overline{\alpha_b}, b\}$. Then c is only contained into C_1 and b in C_2. See Figure 8.4(2). □

After $sw_{b,c}(P_1)$ the QSTS Q' in the last proposition has $Ms(Q') = \{\{a, b\}, \{a', c\}\}$, $Re(Q) = \{\{a, c\}, \{a', b\}\}$.

When both b and c are in the same component C of $Q_{p,q}$, but their distance is odd we have not found any useful transformation of Q to separate them. In practice, however, we have always found pivots p and q for which either Proposition 8.8 or Proposition 8.9 holds.

Chapter 9

Direct transformations among QSTSs

By using our reducing method it is possible to build random QSTSs just by making a random selection of the transformations to be applied. A similar method for STSs was also proposed by Stinson [40]. However, a full construction of a new QSTS is not necessary. Based on Theorem 8.7 it is possible to transform a QSTS(v) Q into another QSTS(v) Q' by changing at most v triples in such a way that Q is not necessarily isomorphic to Q'.

The transformation is described in the following algorithm.

Algorithm 9.1 *QSTSTRANSFORMATION(Q, v)*

Input: A QSTS(v) Q.

Output: A new QSTS(v) Q' such that $l(Q) = l(Q')$, and in general Q and Q' are not necessarily isomorphic.

let b, c *be two different elements in* $\{0, \ldots, v-1\}$.

let C *be a connected component of* $Q_{b,c}$ *containing less than* $v-3$ *triples in* Q.

$Q' \leftarrow (Q - C) \cup sw_{b,c}(C)$

The method works because it is precisely the statement of Theorem 8.7 and it is appropriate for any QSTS in general, and in particular, for any STS. When Q is an STS, the number of triples to be changed is at most $v-3$ because from Proposition 7.2 the maximum number of triples in C is this number. When the equality holds the

swapping operation on C only produces a permutation of b and c, and an isomorphic Q' is produced. When the number of triples in C is less than $v-3$ it is possible to have a non-isomorphic STS Q' as can be appreciated in the following:

Example 9.1 *One of the two canonical STS*(13) *in the minimum lexicographical isomorphic representation is:*

```
00000011111222223334445566
13579B3478A3456A6895797878
2468AC569BC789CBACBBACCAB9
```

If we name Q this STS then one of the cycles in $Q_{9,A}$ is $C = \{2,5,9\}$, $\{2,A,B\}$, $\{3,9,B\}$, $\{3,6,A\}$, $\{6,8,9\}$, $\{5,8,A\}$. Since $sw_{9,A}(C) = \{2,5,A\}$, $\{2,9,B\}$, $\{3,A,B\}$, $\{3,6,9\}$, $\{6,8,A\}$, $\{5,8,9\}$ the STS $Q' \leftarrow (Q-C) \cup sw_{9,A}(C)$ in the minimum lexicographical isomorphic representation is

```
00000011111222223334445566
13579B3478A3456968A5797878
2468AC569BC78ACB9CBBACC9BA
```

In fact, Q is isomorphous to the STS(13) *number 2: reported in Table 1.27 [33] and Q' to the STS*(13) *number 1: reported in the same table. So, Q and Q' are not isomorphic.*

We have made experiments for $v = 13$ and 15 with Algorithm 9.1, and reached all the non-isomorphic STSs of these orders. So, we believe that the following is true.

Conjecture 9.1 *Let Q be a QSTS(v). Then, every non-isomorphic QSTS Q' can be reached by a successive application of Algorithm 9.1.*

When Q is not an STS, the number of triples changed by Algorithm 9.1 is at most the number of triples in Q containing exactly one of b or c.

Given $v \equiv 1 \bmod 6$ or $v \equiv 3 \bmod 6$, the *swapping graph* of order v, denoted $\mathcal{S}(v)$ is the digraph having the isomorphism classes of the STSs of order v as set of vertices; two vertices a, b being joined by a directed edge if and only if the representative S_a of a can be transformed into one element from the class b by swapping a cycle in some decomposition graph of S_a. A random walk on $\mathcal{S}(v)$ will visit the isomorphism classes, and several questions arise. For instance:

1. What is the proportion of times that a certain class is visited by the random walk?

2. What classes can be reached from a starting vertex in $\mathcal{S}(v)$?

3. What is the expected number of steps to visit all the classes?

4. Is $\mathcal{S}(v)$ a connected graph?

5. Is there a particular class form which the other classes can be reached by random paths of a given bounded length?

A random walk on $\mathcal{S}(v)$ is, in fact, a Markov Chain [26] where the state space is the set of isomorphism classes $V(\mathcal{S}(v))$, and where the transition matrix $A(v)$ in the entry $A(v)[a, b]$ contains the number of different swapping cycles transforming a into b divided by the total number of swapping cycles. All the questions in the previous paragraph may be answered from the standard theory of Markov chains, and we rather prefer to omit the details. However, we have computed $A(15)$ and present it in Table 9.1. Since there are eighty isomorphism classes for the STSs of order 15 [26] we have represented each one as an integer number. The class i corresponds to the

isomorphism class whose representative is the lexicographical minimum element in the class and occupies the ith place in the representatives lexicographical order. Since $A(v)$ is a sparse matrix, we only present the non-zero entries.

For instance, the row "7: 6-0.107 51-0.107 59-0.107 61-0.321 69-0.321 73-0.036" means that in the seventh row $A(15)[7, 6] = 0.107$, $A(15)[7, 51] = 0.107$, $A(15)[7, 59] = 0.107$, $A(15)[7, 61] = 0.321$, $A(15)[7, 69] = 0.321$, and $A(15)[7, 73] = 0.036$, and all the other entries in the seventh row of $A(15)$ are zero.

Several interesting facts could be observed from this matrix. For example, the row 18 only contains a non-zero value in column 14. It means that for the 18th isomorphic class, any cycle swapping produces an STS in the 14th class. The representatives of these classes are:

```
Representative for the 14th isomorphism class of STSs of order 15
000000011111122222233334444555566666
13579bd3478bc3478bc789a789a789a789a
2468ace569ade65a9edbcdecbeddecbedbc

Representative for the 18th isomorphism class of STSs of order 15
000000011111122222233334444555566666
13579bd3478bc3478bc789a789a789a789a
2468ace569ade65a9edbcdecbeddebcedcb
```

The full list of isomorphic classes for orders 15 are available by requesting them to the authors. A direct analysis of $A(15)$ as an sparse matrices confirms that $\mathcal{S}(15)$ is a connected digraph.

1: 1-0.105 16-0.088 21-0.035 22-0.035 24-0.105 30-0.123 40-0.088 41-0.035 46-0.035 47-0.035 48-0.035 53-0.035 58-0.105 62-0.035 75-0.035 77-0.035 78-0.035	41: 1-0.032 2-0.065 3-0.097 17-0.065 20-0.129 23-0.032 41-0.065 43-0.129 44-0.032 46-0.032 59-0.032 69-0.032 74-0.097 75-0.129 79-0.032
2: 16-0.090 17-0.030 20-0.075 22-0.030 24-0.119 25-0.164 27-0.030 29-0.075 41-0.060 47-0.030 49-0.030 52-0.030 53-0.030 59-0.030 69-0.030 72-0.090 75-0.030 79-0.030	42: 4-0.082 5-0.082 6-0.197 23-0.262 25-0.066 31-0.066 32-0.082 40-0.066 77-0.098
3: 16-0.029 17-0.029 20-0.086 24-0.086 25-0.086 27-0.029 40-0.086 41-0.086 43-0.086 47-0.029 48-0.086 49-0.029 52-0.029 53-0.029 59-0.029 60-0.029 74-0.029 75-0.086 79-0.029	43: 3-0.103 17-0.103 23-0.034 24-0.034 25-0.034 27-0.103 30-0.138 41-0.138 46-0.034 48-0.034 52-0.034 59-0.034 69-0.103 74-0.034 75-0.034
4: 5-0.161 21-0.387 32-0.161 35-0.129 42-0.161	44: 6-0.250 17-0.250 20-0.083 40-0.083 41-0.083 46-0.083 69-0.083 79-0.083
5: 4-0.238 10-0.095 32-0.238 35-0.190 42-0.238	45: 10-0.032 21-0.129 29-0.387 35-0.387 56-0.032 77-0.032
6: 7-0.022 16-0.022 20-0.022 21-0.054 24-0.022 29-0.043 32-0.054 33-0.065 42-0.065 44-0.065 47-0.065 49-0.065 52-0.065 54-0.065 58-0.022 60-0.022 61-0.022 63-0.118 73-0.065 78-0.065	46: 1-0.143 41-0.143 43-0.143 44-0.143 46-0.143 75-0.286
7: 6-0.107 51-0.107 59-0.107 61-0.321 69-0.321 73-0.036	47: 1-0.026 2-0.026 3-0.026 6-0.077 16-0.026 17-0.077 20-0.026 22-0.077 23-0.077 25-0.026 28-0.077 30-0.026 50-0.154 52-0.077 59-0.077 69-0.051 74-0.026 75-0.026 77-0.026
8: 8-0.077 9-0.051 36-0.051 37-0.171 38-0.085 39-0.137 50-0.205 65-0.026 66-0.026 71-0.171	48: 1-0.026 3-0.077 16-0.026 17-0.051 23-0.090 24-0.026 29-0.026 30-0.026 40-0.026 43-0.026 50-0.026 52-0.026 53-0.064 60-0.064 61-0.090 69-0.141 74-0.090 75-0.026 77-0.077
9: 8-0.203 9-0.051 11-0.169 12-0.017 13-0.051 36-0.169 63-0.339	49: 2-0.056 3-0.056 6-0.168 17-0.140 23-0.168 26-0.019 27-0.056 50-0.168 60-0.056 69-0.056 71-0.056
10: 5-0.667 45-0.333	50: 8-0.063 16-0.021 21-0.042 22-0.053 25-0.042 30-0.021 33-0.053 40-0.021 47-0.126 48-0.021 49-0.063 52-0.053 54-0.168 55-0.053 60-0.021 63-0.063 70-0.116
11: 9-0.048 11-0.116 13-0.029 14-0.039 15-0.014 37-0.271 38-0.155 39-0.077 64-0.193 66-0.029 67-0.029	51: 7-0.056 51-0.168 57-0.168 60-0.140 61-0.140 62-0.140 63-0.056 64-0.019 71-0.056 76-0.056
12: 9-0.267 13-0.200 65-0.533	52: 2-0.023 3-0.023 6-0.070 17-0.070 22-0.058 25-0.023 30-0.023 33-0.070 43-0.023 47-0.070 48-0.023 50-0.058 52-0.116 54-0.058 55-0.140 60-0.023 61-0.023 62-0.023 71-0.058 74-0.023
13: 9-0.058 11-0.116 12-0.014 13-0.058 14-0.029 15-0.029 38-0.386 39-0.193 66-0.116	53: 1-0.041 2-0.041 3-0.041 17-0.082 20-0.122 21-0.041 24-0.041 26-0.041 48-0.102 60-0.102 62-0.163 69-0.102 72-0.041 75-0.041
14: 11-0.719 13-0.135 14-0.067 15-0.067 18-0.011	54: 6-0.054 16-0.036 21-0.045 22-0.152 28-0.054 29-0.036 33-0.080 37-0.098 50-0.143 52-0.045 55-0.045 56-0.054 61-0.018 64-0.098 70-0.045
15: 11-0.185 13-0.092 14-0.046 19-0.062 39-0.369 67-0.246	55: 21-0.050 31-0.020 32-0.059 33-0.050 35-0.020 37-0.050 38-0.059 50-0.050 52-0.119 54-0.050 55-0.059 58-0.020 64-0.030 66-0.059 69-0.020 70-0.198 73-0.089
16: 1-0.058 2-0.070 3-0.023 6-0.023 16-0.186 20-0.070 25-0.070 28-0.023 30-0.081 35-0.070 40-0.058 47-0.023 48-0.023 50-0.023 54-0.047 57-0.058 62-0.070 74-0.023	56: 32-0.122 33-0.204 38-0.204 45-0.020 54-0.245 70-0.204
17: 2-0.027 3-0.027 17-0.133 24-0.027 41-0.053 43-0.080 44-0.080 47-0.080 48-0.053 49-0.067 52-0.080 53-0.053 59-0.080 60-0.027 69-0.027 72-0.053 75-0.027 79-0.027	57: 16-0.126 29-0.151 31-0.025 35-0.126 51-0.151 57-0.202 58-0.101 63-0.050 64-0.050 68-0.017
18: 14-1.000	58: 1-0.079 6-0.026 21-0.026 29-0.079 31-0.066 32-0.026 35-0.171 40-0.079 55-0.026 57-0.053 58-0.184 59-0.026 60-0.079 70-0.026 73-0.026 74-0.026
19: 15-0.143 39-0.857	59: 2-0.038 3-0.038 7-0.038 17-0.115 20-0.038 23-0.154 27-0.154 40-0.038 41-0.038 43-0.038 47-0.115 58-0.038 69-0.038 74-0.115
20: 2-0.079 3-0.095 6-0.032 16-0.095 22-0.032 23-0.032 24-0.032 25-0.079 27-0.032 29-0.079 40-0.032 41-0.127 44-0.032 47-0.032 53-0.095 59-0.032 60-0.032 79-0.032	60: 3-0.023 6-0.023 17-0.023 20-0.023 22-0.023 24-0.023 27-0.023 29-0.070 48-0.058 49-0.023 50-0.023 51-0.058 52-0.023 53-0.058 58-0.070 60-0.070 61-0.058 62-0.058 69-0.198 70-0.023 74-0.023 79-0.023
21: 1-0.024 4-0.071 6-0.059 32-0.059 33-0.200 36-0.071 45-0.024 50-0.047 53-0.024 54-0.059 55-0.059 58-0.024 62-0.024 63-0.059 70-0.129 78-0.071	61: 6-0.028 7-0.083 23-0.181 26-0.083 27-0.028 30-0.028 31-0.083 32-0.028 48-0.097 51-0.069 52-0.028 54-0.028 60-0.069 62-0.069 74-0.097
22: 1-0.024 2-0.024 20-0.024 23-0.094 26-0.165 32-0.071 40-0.024 47-0.071 50-0.059 52-0.059 54-0.200 60-0.024 62-0.024 71-0.071 73-0.071	62: 1-0.034 16-0.102 21-0.034 22-0.034 33-0.034 35-0.102 51-0.085 52-0.034 53-0.136 60-0.085 61-0.085 62-0.102 74-0.102 75-0.034
23: 20-0.027 22-0.107 30-0.027 40-0.027 41-0.027 42-0.107 43-0.027 47-0.080 48-0.093 49-0.080 59-0.107 61-0.173 69-0.027 74-0.093	63: 6-0.168 9-0.038 21-0.076 32-0.076 36-0.038 37-0.076 38-0.076 50-0.092 51-0.031 57-0.031 63-0.069 64-0.092 68-0.046 71-0.092
24: 1-0.094 2-0.125 3-0.094 6-0.031 17-0.031 20-0.031 26-0.031 27-0.094 40-0.125 43-0.031 48-0.031 53-0.031 60-0.031 72-0.031 75-0.094 79-0.094	64: 11-0.093 33-0.093 38-0.093 51-0.012 54-0.205 55-0.056 57-0.037 63-0.112 64-0.093 70-0.149 71-0.037 73-0.019
25: 2-0.169 3-0.092 16-0.092 20-0.077 29-0.169 35-0.092 42-0.031 43-0.031 47-0.031 50-0.062 52-0.031 69-0.031 74-0.031 75-0.031 79-0.031	65: 8-0.207 12-0.069 36-0.207 39-0.207 66-0.310
26: 22-0.525 24-0.075 49-0.025 53-0.075 61-0.225 76-0.075	66: 8-0.044 11-0.044 13-0.044 36-0.044 37-0.089 38-0.089 39-0.089 55-0.356 65-0.067 67-0.133
27: 2-0.034 3-0.034 20-0.034 24-0.103 29-0.034 30-0.103 35-0.034 43-0.103 49-0.034 59-0.138 60-0.034 61-0.034 69-0.034 74-0.138 75-0.103	67: 11-0.061 15-0.041 37-0.122 38-0.122 39-0.061 66-0.184 70-0.408
28: 16-0.143 47-0.429 54-0.429	68: 36-0.297 57-0.079 63-0.356 68-0.030 78-0.238
29: 2-0.067 6-0.053 20-0.067 25-0.147 27-0.027 29-0.080 33-0.027 34-0.027 40-0.080 45-0.080 48-0.027 54-0.053 57-0.080 58-0.080 60-0.080 78-0.027	69: 2-0.025 7-0.074 17-0.025 23-0.025 25-0.025 27-0.025 30-0.025 40-0.074 41-0.025 43-0.074 44-0.025 47-0.049 48-0.136 49-0.025 53-0.062 55-0.025 59-0.025 60-0.210 75-0.025 79-0.025
30: 1-0.095 16-0.095 23-0.027 27-0.081 30-0.135 31-0.095 40-0.095 43-0.108 47-0.027 48-0.027 50-0.027 52-0.027 61-0.027 69-0.027 74-0.081 77-0.027	70: 21-0.097 33-0.088 35-0.035 38-0.044 39-0.053 50-0.097 54-0.044 55-0.177 56-0.044 58-0.018 60-0.018 64-0.071 67-0.044 70-0.142 73-0.027
31: 30-0.253 35-0.145 42-0.072 55-0.072 57-0.036 58-0.181 61-0.217 78-0.024	71: 8-0.129 22-0.155 37-0.129 49-0.052 51-0.052 52-0.129 63-0.155 64-0.052 71-0.129 76-0.017
32: 4-0.057 5-0.057 6-0.115 21-0.115 22-0.138 35-0.046 42-0.057 55-0.138 56-0.069 58-0.046 61-0.046 63-0.115	72: 2-0.308 17-0.205 24-0.103 53-0.103 75-0.103 79-0.154 80-0.026
33: 6-0.059 21-0.167 29-0.020 33-0.118 37-0.049 38-0.108 40-0.020 50-0.049 52-0.059 54-0.088 55-0.049 56-0.049 62-0.020 64-0.049 70-0.098	73: 6-0.178 7-0.020 22-0.178 37-0.178 55-0.267 58-0.059 64-0.030 70-0.089
34: 29-0.444 79-0.556	74: 3-0.029 16-0.029 23-0.101 25-0.029 27-0.116 30-0.087 41-0.087 43-0.029 47-0.029 48-0.101 52-0.029 58-0.029 59-0.087 60-0.029 61-0.101 62-0.087
35: 4-0.025 5-0.025 16-0.075 25-0.075 27-0.025 31-0.050 32-0.025 35-0.175 40-0.075 45-0.075 55-0.025 57-0.062 58-0.163 62-0.075 70-0.050	75: 1-0.032 2-0.032 3-0.097 17-0.032 24-0.097 25-0.032 27-0.097 41-0.129 43-0.032 46-0.065 47-0.032 48-0.032 53-0.032 62-0.032 69-0.032 72-0.032 75-0.065 79-0.097
36: 8-0.051 9-0.043 21-0.205 36-0.068 37-0.085 38-0.188 39-0.137 63-0.085 65-0.026 66-0.026 68-0.085	76: 26-0.429 51-0.429 71-0.143
37: 8-0.068 11-0.095 33-0.068 36-0.034 37-0.088 38-0.116 39-0.054 54-0.150 55-0.068 63-0.068 66-0.020 67-0.020 71-0.068 73-0.082	77: 1-0.129 30-0.129 42-0.194 45-0.032 47-0.129 48-0.387
38: 8-0.034 11-0.054 13-0.034 33-0.150 36-0.075 37-0.116 38-0.088 39-0.054 55-0.082 56-0.068 63-0.068 64-0.068 66-0.020 67-0.020 70-0.068	78: 1-0.107 6-0.321 21-0.321 29-0.107 31-0.036 68-0.107
39: 8-0.109 11-0.054 13-0.034 15-0.020 19-0.020 36-0.109 37-0.109 38-0.109 39-0.190 65-0.020 66-0.041 67-0.020 70-0.163	79: 2-0.047 3-0.047 17-0.047 20-0.047 24-0.141 25-0.047 34-0.059 40-0.047 41-0.047 44-0.047 60-0.047 69-0.047 72-0.071 75-0.141 79-0.118
40: 1-0.067 3-0.080 16-0.067 20-0.027 22-0.027 23-0.027 24-0.107 29-0.080 30-0.093 33-0.027 35-0.080 42-0.027 44-0.027 48-0.027 50-0.027 58-0.080 59-0.027 69-0.080 79-0.027	80: 72-1.000

Table 9.1 : Transition matrix A(15).

Chapter 10

Conclusions

When Hilbert submitted his famous finiteness theorem (see [12]) 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) [20]. 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 to make manipulation impractical from a computational point of view. The development of parallel algorithms to calculate

Gröbner basis efficiently are remarkable (see [3, 36]). 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 algebraic geometry and combinatorial design theory; this is one of the main contributions 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 [38].

Our interest in applying our polynomial ideals to generate STSs led us to understand that genetic algorithms are not appropriate tools because the existence of Stinson's method makes irrelevant to their use. This is a fact probably unknown in the context of genetic algorithms because, to the best of our knowledge, no other author has reported the connection between Stinson's method and genetic algorithms and the superiority of the first one.

Another contribution of our study is the introduction of QSTSs which by themselves are interesting combinatorial designs. They play an alternative role to STSs, mainly when looking for structures with restrictions difficult to find. That is, we have introduced operations to transform a QSTS of a given level into a new QSTS of a lower or greater level. Finally, all the properties of QSTS are inherited to STSs.

Finally, we developed a method to change an arbitrary STS(v) into non isomorphic STSs by replacing in each transformation at most $v - 3$ triples. This transformation is based on Theorem 7.3 which we consider one of the most important contributions in the thesis.

The study of QSTSs is not exhausted. We have found a set of transformations to generate STSs from an arbitrary QSTS. This transformations work well in practice, but a formal proof about their completeness is not given. However, we have proven here some general results about situations where level reductions of QSTSs are guarantied.

Another problem left open is the general transformation of a QSTS of level two into a QSTS, because we were not able not find a proof of a result similar to Proposition 8.9 when b and c are at an odd distance in C.

Bibliography

[1] Anderson, I. (1999) Balancing carry over effects in tournaments, in Combinatorial designs and their applications, Chapman & Hall/CRC Res. Notes Math., 403, Boca Raton, FL, 1-16.

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

[3] 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.

[4] T. Becker, V. Weispfenning and et al. *Gröbner Bases. A Computational Approach to Commutative Algebra,* Springer Graduate texts in Mathematics, Springer-Verlag, New York, 1993. p 341-342.

[5] M. Brickenstein, A. Dreyer, *PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials*,Journal of Symbolic Computation, vol 44, 9, pp. 1326 - 1345, 2009.

[6] 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.

[7] L. Caniglia, A. Galligo, and J. Heintz. *Equations for the projective closure and*

effective Nullstellensatz. Discrete Applied Math. **33** (1991), 11-23.

[8] C. W. Ahn, *Advances in Evolutionary Algorithms: Theory, Design and Practice*, Studies in Computational Intelligence (SCI) 18, pp. 7-22 (2006).

[9] 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.

[10] C. J. Colbourn and A. Rosa, *Triple systems*, Oxford University Press, Oxford, 1999.

[11] C. J. Colbourn and J. H. Dinitz and D. R. Stinson, *Applications of Combinatorial Designs to Communications, Cryptography, and Networking*, 1999.

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

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

[14] R. Diestel, *Graph Theory*, Springer Graduate texts in Mathematics, Springer, New York, 1997.

[15] J. H. Dinitz and D. R. Stinson, *Contemporary Design Theory A Coolection of Surveys*, John Wiley & Sons, USA and Canada, 1992.

[16] Ivan B. Djordjevic and Bane Vasic. *Novel Combinatorial Constructions of Optical Orthogonal Codes for Incoherent Optical CDMA Systems*, OURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 21, NO. 9, SEPTEMBER 2003.

[17] Donald L. Kreher and Douglas R. Stinson: *Combinatorial algorithms Generation, Enumeration and Search*

[18] 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.

[19] T. Eldos, *Mutative Genetic Algorithms*, Journal of Computations & Modelling,vol.3, no.2, 201 3,111-124.

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

[21] Glantz, Stanton A. (1992). Primer of biostatistics (3rd ed.). ISBN 0-07-023511-2.

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

[23] Gokhan Calis and O. Ozan Koyluoglu. *Repairable Block Failure Resilient Codes.* IEEE International Symposium on Information Theory, 2014.

[24] D. E. Goldberg, *Genetic Algorithms in Search, Optimization, and Machine Learning.* Addison-Wesley, Reading, MA, 1989.

[25] S. J. Hartley, A. H. Konstam, *Using Genetic Algorithms to Generate Steiner Triple Systems*, Proceedings of the 21st Annual ACM Computer Science Conference, (1993), 366-371, ACM.

[26] P. G. Hoel, S. C. Port and C. J. Stone, *Introduction to Stochastic Processes*, Boston: Houghton Mifflin, 1972.

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

[28] Kaushik Srinivasan, M.S. (CS), Disk recovery in double erasure RAID disk arrays, Computer Science and Engineering, Arizona State University, 2004.

[29] C. C. Lindner, C. A. Rodger, *Design Theory*, Chapman and Hall/CRC, 2008.

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

[31] 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.

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

[33] R. Mathon, A. Rosa, 2-(v, k, λ) Designs of small Order, in *Handbook of Combinatoria Designs*, C. J. Colbourn and J. H. Dinitz (Editors), 2nd ed., Chapman & Hall/CRC, Boca Raton, 2007, pp. 29.

[34] 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.

[35] J. Muñoz, F. Sagols, C. J. Colbourn, *Ideals, varieties, stability, colorings and combinatorial designs*, Morfismos, Vol. 17, No. 1, 2013, pp 41-65.

[36] 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.

[37] Ottoboni, M. Alice (1991). The dose makes the poison : a plain-language guide to toxicology (2nd ed.). New York, N.Y: Van Nostrand Reinhold. ISBN 0442006608.

[38] F. Sagols, J. Muñoz. *Structural properties and applications of binary ideals*. In process.

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

[40] D. R. Stinson: *Hill-Climbing Algorithms for the constructions of Combinatorial Designs* Annals of Discrete Mathematics 26 (1985) 321-334.

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

[42] W. D. Wallis, *One-Factorizations*, the Netherlands: Kluwer Academic Publishers, 1997.

[43] Zacks, S. (1996) "Adaptive Designs for Parametric Models". In: Ghosh, S. and Rao, C. R., (Eds) (1996). "Design and Analysis of Experiments," Handbook of Statistics, Volume 13. North-Holland. ISBN 0-444-82061-2. (pages 151-180).