Convex Algebraic Geometry Approaches to Graph Coloring and Stable Set Problems

by

Julián Ariel Romero Barbosa

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2021

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner: **Jesús De Loera**
Professor, Dept. of Mathematics,
University of California, Davis

Supervisor: **Levent Tunçel**
Professor, Dept. of Combinatorics and Optimization
University of Waterloo

Internal Members: **Bertrand Guenin**
Professor, Dept. of Combinatorics and Optimization
University of Waterloo

Jochen Koenemann
Professor, Dept. of Combinatorics and Optimization
University of Waterloo

Internal-External Member: **Rafael Oliveira**
Professor, David R. Cheriton School of Computer Science
University of Waterloo

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

The objective of a combinatorial optimization problem is to find an element that maximizes a given function defined over a large and possibly high-dimensional finite set. It is often the case that the set is so large that solving the problem by inspecting all the elements is intractable. One approach to circumvent this issue is by exploiting the combinatorial structure of the set (and possibly the function) and *reformulate* the problem into a familiar set-up where known techniques can be used to attack the problem.

Some common solution methods for combinatorial optimization problems involve formulations that make use of Systems of Linear Equations, Linear Programs (LPs), Semidefinite Programs (SDPs), and more generally, Conic and Semi-algebraic Programs. Although, generality often implies flexibility and power in the formulations, in practice, an increase in sophistication usually implies a higher running time of the algorithms used to solve the problem. Despite this, for some combinatorial problems, it is hard to rule out the applicability of one formulation over the other.

One example of this is the *Stable Set Problem*. A celebrated result of Lovász's states that it is possible to solve (to arbitrary accuracy) in polynomial time the Stable Set Problem for *perfect graphs*. This is achieved by showing that the *Stable Set Polytope* of a perfect graph is the projection of a slice of a Positive Semidefinite Cone of not too large dimension. Thus, the Stable Set Problem can be solved with the use of a reasonably sized SDP. However, it is unknown whether one can solve the same problem using a reasonably sized LP. In fact, even for simple classes of perfect graphs, such as Bipartite Graphs, we do not know the right order of magnitude of the minimum size LP formulation of the problem.

Another example is Graph Coloring. In 2008 Jesús De Loera, Jon Lee, Susan Margulies and Peter Malkin proposed a technique to solve several combinatorial problems, including Graph Coloring Problems, using Systems of Linear Equations. These systems are obtained by reformulating the decision version of the combinatorial problem with a system of polynomial equations. By a theorem of Hilbert, known as *Hilbert's Nullstellensatz*, the infeasibility of this polynomial system can be determined by solving a (usually large) system of linear equations. The size of this system is an exponential function of a parameter d that we call the *degree* of the Nullstellensatz Certificate.

Computational experiments of De Loera *et al.* showed that the Nullstellensatz method had potential applications for detecting non-3-colorability of graphs. Even for known hard instances of graph coloring with up to two thousand vertices and tens of thousands of

edges the method was useful. Moreover, all of these graphs had very small Nullstellensatz Certificates. Although, the existence of hard non-3-colorable graph examples for the Nullstellensatz approach are known, determining what combinatorial properties makes the Nullstellensatz approach effective (or ineffective) is wide open.

The objective of this thesis is to amplify our understanding on the power and limitations of these methods, all of these falling into the umbrella of Convex Algebraic Geometry approaches, for combinatorial problems. We do this by studying the behavior of these approaches for Graph Coloring and Stable Set Problems.

First, we study the Nullstellensatz approach for graphs having large girth and chromatic number. We show that that every non-k-colorable graph with girth g needs a Nullstellensatz Certificate of degree $\Omega(g)$ to detect its non-k-colorability. It is our general belief that the power of the Nullstellensatz method is tied with the interplay between local and global features of the encoding polynomial system. If a graph is locally k-colorable, but globally non-k-colorable, we suspect that it will be hard for the Nullstellensatz to detect the non-k-colorability of the graph. Our results point towards that direction.

Finally, we study the Stable Set Problem for d-regular Bipartite Graphs having no C_4, i.e., having no cycle of length four. In 2017 Manuel Aprile *et al.* showed that the Stable Set Polytope of the incidence graph G_{d-1} of a Finite Projective Plane of order $d-1$ (hence, d-regular) does not admit an LP formulation with fewer than $\frac{\ln(d)}{d}|E(G_{d-1})|$ facets. Although, we did not manage to improve this lower bound for general d-regular graphs, we show that any 4-regular bipartite graph G having no C_4 does not admit an LP formulation with fewer than $|E(G)|$ facets. In addition, we obtain computational results showing the $|E(G)|$ lower bound also holds for the Finite Projective Plane G_4, a 5-regular graph. It is our belief that Aprile *et al.* bounds can be improved considerably.

Acknowledgements

I would like to thank my supervisor Levent Tunçel. Ultimately, this thesis is a product of his invaluable teachings, counseling and guidance. Since day one, Levent has been supportive of my idea of balancing academia with industry. I thank him for allowing me to explore and venture myself into different work environments during my PhD studies.

In addition, I would like to thank the committee members for their valuable comments and questions. Several of the open questions presented in the thesis are a product of valuable discussions with them.

It goes without saying that emotional support was one, if not the most important factor that helped me continue working during these years, especially during rough times. This support was mostly coming from my lovely wife Diana, my mother Clara, my father Jairo, my sisters Coco and Rosy and lately from my daughter Juliana. Diana, we made it! Thank you for coming to Canada with me, your happiness and constant support made this ride the best!

Finally, I would like to thank my friends at C&O, I had great times with them. Thanks Alan, Nanis and Lucho for Friday's tacos!

The material in this thesis is based upon research supported in part by NSERC Discovery Grants, Tutte Scholarship, U.S. Office of Naval Research under award numbers: N00014-15-1-2171 and N00014-18-1-2078. This financial support is gratefully acknowledged.

Dedication

This is dedicated to the loving memory of my father, Jairo and to the new joy of my life, my daughter Juliana.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Given a finite set X, a *combinatorial problem* aims to find an element $x \in X$ having certain *attributes*. Usually, it is the case that the set X is extremely large and solving the problem by inspecting the set is impossible. Different techniques are thus required to solve the desired problem. For instance, one could look for special properties of the set X, such as symmetry, in order to reduce the number of inspections needed. We could also *reformulate* the problem into a form for which well known techniques can be applied.

Some common reformulations make use of *Systems of Linear Equations*, *Linear Programs* (LP), *Positive Semidefinite Programs* (SDP) and more generally, *Conic Programs* over convex cones with a *polynomial time separation oracle* [GLS93a]. The broad idea is to map the set X into a convex set S and find the desired element $x \in X$ by optimizing a suitable linear function over S. The attractiveness of these methods is that polynomial time algorithms can be used to solve the optimization problem, provided that the reformulation is *compact*. Interestingly, several combinatorial problems admit different reformulations and it is not always clear which reformulation is best for the problem.

Take for instance the **Stable Set Problem**. In this problem we are given a graph $G = (V, E)$ and a positive integer $k \geqslant 1$. The goal is to find a subset of vertices $S \subseteq V$ of size k such that no two vertices in S are adjacent. We can formulate the stable set problem in many different ways, but let us focus on the following three well known formulations (and corresponding relaxations) of the problem.

Polynomial Formulation
Find $x \in \mathbb{C}^V$ such that:

$$\begin{aligned} x_u x_v &= 0, \quad \forall uv \in E, \\ x_u^2 - x_u &= 0, \quad \forall u \in V, \\ x(V) := \sum_{u \in V} x_v &= k. \end{aligned} \tag{1.0.1}$$

Integer Programming Formulation
Find $x \in \mathbb{Z}^V$ such that:

$$\begin{aligned} x(V) &= k, \\ x_u + x_v &\leqslant 1, \quad \forall uv \in E, \\ 1 \geqslant x_u &\geqslant 0, \quad \forall u \in V \end{aligned} \tag{1.0.2}$$

Lovász Theta Integer Formulation
Find $X \in \{0,1\}^{V \times V}$ positive semidefinite such that:

$$\begin{aligned} \sum\nolimits_{u,v \in V} X_{uv} &= k^2, \\ \sum\nolimits_{u \in V} X_{uu} &= k, \\ X_{uv} &= 0, \quad \forall uv \in E. \end{aligned} \tag{1.0.3}$$

Each of these formulations already describe **NP**-hard problems and as with the Stable Set Problem for general graphs, we may have no hope in finding an efficient formulation from each of these. Nevertheless, each formulation has its own strengths and it may become not apparent to rule out their efficiency for some specific families of graphs. Let us dive a little deeper into each of these three formulations.

1.1 Polynomial Representations and Systems of Linear Equations

The formulation (1.0.1) models the Stable Set problem using a system of polynomial equations. Despite the fact that solving systems of polynomial equations lies in the class of **NP**-hard problems [GKP10], a celebrated theorem of Hilbert [Hil93] allows us to further reformulate the problem using *systems of linear equations*. More concretely, given a set of multivariate polynomials $p_1, p_2, \ldots, p_m$ over the complex numbers with n variables, *Hilbert's Nullstellensatz* states that

$$\begin{array}{c} p_1(x) = \cdots = p_m(x) = 0 \\ \text{has no solution } x \in \mathbb{C}^n, \end{array} \iff \begin{array}{c} r_1(x)p_1(x) + \cdots + r_m(x)p_m(x) = 1 \\ \text{for some polynomials } r_1, \ldots, r_m. \end{array} \tag{1.1.1}$$

The polynomials $r_1, r_2, \ldots, r_m$ on the right hand side of (1.1.1) provide a certificate for the non-solubility of the system. Such certificate is called a *Nullstellesatz Certificate* and its degree is the maximum degree of the polynomials r_i with $i \in \{1, 2, \ldots, m\}$. Determining the existence of a Nullstellensatz Certificate of a given degree can be done using a *system of linear equations*. Indeed, if we fix the degree of the polynomials $r_1, \ldots, r_m$, then the equation

$$r_1(x)p_1(x) + \cdots + r_m(x)p_m(x) = 1 \tag{NCERT}$$

becomes nothing but a system of linear equations, where the variables are the coefficients of the polynomials r_i with $i \in \{1, 2, \ldots, m\}$. For example, if $G = (V, E)$ is a triangle and we let $k = 2$, then (1.0.1) has a Nullstellensatz Certificate of degree one given by

$$\begin{aligned} -\frac{1}{2}(x_1 + x_2 + x_3 + 1)(x_1 + x_2 + x_3 - 2) + \frac{1}{2}(x_1^2 - x_1) + \ldots \\ \cdots + \frac{1}{2}(x_2^2 - x_2) + \frac{1}{2}(x_3^2 - x_3) = 1 - x_1x_2 - x_1x_3 - x_2x_3. \end{aligned} \tag{1.1.2}$$

Such certificate can be easily found by solving a linear system of size 7×7. In general, finding a Nullstellensatz Certificate of degree d on n variables usually involves a system of size $\binom{n+d}{n}$ which grows exponentially when d is linear in n. De Loera *et al.* [DLLMM08] showed that when the system (1.0.1) has no solution, a Nullstellensatz certificate of degree $\alpha(G)$ is needed, where $\alpha(G)$ denotes the size of the largest stable set of G. In particular, this method is not useful for graphs where $\alpha(G)$ is large.

However, the method is practical when certificates of low degree exist. This, as one can often use finite field computations to solve the linear systems faster [DLLMM08]. For instance, it is a result of Bayer [Bay82] that one can cast a k-colorability problem on a graph $G = (V, E)$ using the following system of polynomial equations

$$\begin{aligned} p_u(x) &:= x_u^k - 1 = 0, && \forall u \in V, \\ q_{uv}(x) &:= x_u^{k-1} + x_u^{k-2}x_v + \cdots + x_ux_v^{k-2} + x_v^{k-1} = 0, && \forall \{u, v\} \in E. \end{aligned} \tag{BCOL$_k$}$$

Indeed, the first set of polynomials assigns a k-root of the unity to each variable x_u with $u \in V$, and the second set of polynomials guarantees that $x_u \neq x_v$ for all $\{u, v\} \in E$. This last condition is easily seen from the equation

$$0 = p_u(x) - p_v(x) = (x_u - x_v) \cdot q_{uv}(x).$$

De Loera *et al.* [DLLMM08] carried out several computational experiments for the Nullstellensatz approach over known hard instances of 3-coloring problems. Surprisingly, the

approach detected the non-3-colorability of various graphs with up to a thousand vertices. No graph needing a certificate of degree larger than *four* was encountered by their experiments. In fact, the existence of non-k-colorable graphs needing large certificates was not settled until recently by Lauria and Nordström [LN17]:

Theorem 1.1.1 ([LN17] (restated))**.** *For any integer $k \geqslant 3$ there is an efficiently constructible family of graphs $\{G_n\}_{n\in\mathbb{N}}$ with $O(k^4 n)$ vertices of degree $O(k^2)$ that do not possess k-colourings, but for which the corresponding system of polynomial equations (BCOL_k) require degree $\Omega(n)$ Nullstellensatz Certificates.*

We should point out that the proof of the above theorem uses a nifty reduction to a well-known system of polynomial equations arising from the Pingeonhole Principle, where bounds of Mikša and Nordström [MN15] apply. However, this approach does not give much insight into which *combinatorial properties* of a graph G are required to obtain very high degree Nullstellensatz certificates.

In the author's master thesis [Rom16], which was done completely independently of [LN17], it was found some partial evidence that non-3-colorable graphs with large enough girth, i.e., the length of the shortest cycle in the graph, may need large Nullstellensatz certificates. Using some techniques introduced by Aleknovich and Razborov in [AR03], we were able to prove the following result.

Theorem 1.1.2 (New)**.** *Let $G = (V, E)$ be a graph with chromatic number $\chi(G) = k + 1$ and girth $g > 2k$. Suppose that $d + k - 1 < \frac{g}{4k}$, then G has no degree-d Nullstellensatz Certificate for its non-k-colorability.*

1.2 Polyhedral Representations

Formulation (1.0.2) models the Stable Set problem for a graph $G = (V, E)$ using an Integer Programming problem. In fact, the set described by the second and third constrains in (1.0.2) is known as the Stable Set Polytope of G, denoted by $STAB(G)$. This polytope is precisely the convex hull of all characteristic vectors of stable sets of the graph G. Its linear relaxation is the Fractional Stable Set Polytope

$$FRAC(G) := \{x \in \mathbb{R}^V : \ 1 \geqslant x_u \geqslant 0, \ \forall u \in V; \ x_u + x_v \leqslant 1, \ \forall uv \in E\}. \tag{1.2.1}$$

It is a well known result that $FRAC(G) = \mathrm{STAB}(G)$ if and only if G is a bipartite graph. Thus, the Stable Set Problem can be solved in polynomial time for bipartite graphs by

means of solving an LP with $|V| + |E|$ constraints. The same follows for every graph G where we are able to describe $\text{STAB}(G)$ using a polynomial number of inequalities. This of course is not always the case. For instance, Chvátal [Chv73] proved that for every maximal clique $C \subseteq V$ the inequality $\sum_{v \in C} x_v \leqslant 1$ is facet defining, whence $\text{STAB}(G)$ may have an exponential number of facets. Notice this fact *does not* imply that the Stable Set problem cannot be solved in polynomial time. For example, it may be the case that $\text{STAB}(G)$ can be obtained as an affine image of a polyhedron with polynomial number of facets (see *t-perfect graphs* in [Lov94]). Is it the case that we can always find such affine image for every Stable Set polytope?

The above problem was stated in a seminal paper due to Yannakakis [Yan91]. In this paper, Yannakakis, among other important discoveries, introduced the concept of *Linear Extended Formulations*. Formally, a *linear extension* of a polytope $P \subseteq \mathbb{R}^m$ is a polyhedron $Q \subseteq \mathbb{R}^d$ and an affine map $\phi : \mathbb{R}^d \to \mathbb{R}^n$ such that $\phi(Q) = P$. The *size* of the extension is the number of facets of the polyhedron Q. The *extension complexity* of P, denoted by $\text{xc}(P)$, is the size of an extension of P of minimum size.

Interestingly, Yannankakis' question was just settled a few years ago by Fiorini et al. [FMP+15]. Not only they proved the existence of a family of graphs H_n on n vertices for which $\text{xc}(\text{STAB}(H_n)) \geqslant 1.5^{O(\sqrt{n})}$ (see also [KW15] for a short proof of this), but they showed that many well known polytopes such that the Traveling Salesman, Cut and Correlation polytopes do not admit a small extended formulations.

Probably one of the most interesting topics in the area is that of understanding the power and limitations of LPs. For instance, even though we can solve the *Weighted Matching Problem* on graphs in polynomial time, it is a result of [Rot14] the existence of a family of graphs on n vertices whose *Matching Polytope* has a extension complexity of $2^{\Omega(n)}$. In the same spirit, there is a beautiful problem regarding the extension complexity of the Stable Set polytope of *Perfect Graphs*. Recall that a graph $G = (V, E)$ is *perfect* if for every induced subgraph H of G one has that $\chi(H) = \omega(H)$, where $\omega(H)$ denotes the size of the largest clique of H and $\chi(H)$ denotes its chromatic number. Perfect graphs, among other things, is a class of graphs for which hard combinatorial optimization problems like coloring and the stable set problem are polynomial-time solvable. It is a result of Yannakakis [Yan91] that if G is perfect, then $\text{xc}(\text{STAB}(G)) \leqslant n^{O(\log n)}$. It is an open question to determine if Yannakakis' result is tight.

Question 1.2.1. Determine the existence of a family of perfect graphs G_n on n vertices for which $\text{xc}(\text{STAB}(G_n))$ is superpolynomial in n.

To the best of our knowledge, the best approximation to the question above is a result due to Mika Göös [GÏ5]. This result states the existence of graphs G for which the clique relaxation $\{x \in [0,1]^V : x(C) \leqslant 1, \forall C \subseteq V \text{ clique of } G\}$ of $\text{STAB}(G)$ has extension complexity bounded above by $2^{\Omega(\log^{1.128} n)}$. The second best approximation we know of is precisely coming from bipartite graphs. In [AFF+17], the authors exhibit a family of bipartite graphs on n vertices whose stable set polytope has extension complexity of $\Omega(n \log n)$. They also showed that the extension complexity of the stable set polytope of any bipartite graph on n vertices is at most $O(n^2/\log n)$. This shows an improvement on the upper bound $|V| + |E|$ obtained from the Fractional Stable Set polytope formulation, in the case when $|E|$ is quadratic on $|V|$.

In this thesis, we dive deeper into this problem. Although we were not able to find an improvement to the results in [AFF+17], we proved that for d-regular graphs with d small tighter bounds are possible to be obtained. In particular we show the following.

Theorem 1.2.2 (New)**.** *Let G be a 4-regular bipartite graph with no C_4. Then,*

$$\text{xc}(\text{STAB}(G)) \geqslant |E|.$$

A family of dense, regular bipartite graphs having no C_4 are the incidence graphs G_q of *Finite Projective Planes* $PG(2,q)$ of order $q = p^k$ for some prime p. These graphs are $q+1$-regular, with $|V(G_q)| = 2(q^2+q+1)$ vertices. Using computational tools, we obtained the following result.

Theorem 1.2.3 (New)**.** *We have that* $\text{xc}(\text{STAB}(G_4)) \geqslant |E(G_4)| = 105$.

1.3 Spectrahedral Representations

Finally, formulation (1.0.3) is inspired by the well known Lovász Theta relaxation for the stability number $\alpha(G)$ of G. The *Theta value* of a graph G is defined as

$$\vartheta(G) := \sup\left\{\sum\nolimits_{u,v\in V} X_{uv} : \sum\nolimits_{u\in V} X_{uu} = 1,\ X_{uv} = 0, \forall uv \in E,\ X \succeq 0\right\} \tag{1.3.1}$$

where by $X \succeq 0$ means that X is a $|V| \times |V|$ symmetric positive definite matrix. A result of Lovász [Lov79] states that for every graph G the following inequalities hold,

$$\alpha(G) \leqslant \vartheta(G) \leqslant \omega(G). \tag{1.3.2}$$

Moreover, Lovász proved that when G is perfect, $\text{STAB}(G)$ is an affine image of the feasible set described in (1.3.1). This result provided the first (and only, to the best of our knowledge) polynomial time algorithm to solve hard optimization problems such as the Stable Set Problem, the Maximum Clique Problem and the Coloring Problem for perfect graphs. This, as the feasible region of (1.3.1), called the *Lovász Theta Body*, admits a polynomial time separation oracle.

The Lovász Theta Body is one of the first examples of a Positive Semidefinite Extended Formulation. Let us denote by $\mathbb{S}^n$ and $\mathbb{S}^n_+$ the sets of $n \times n$ symmetric and symmetric positive semidefinite matrices respectively. Let $P \subseteq \mathbb{R}^n$ be a polytope and let $Q \subseteq \mathbb{S}^d_+$ be a *spectrahedron*, i.e. an affine slice of the cone $\mathbb{S}^d_+$. We say that Q is a *Positive Semidefinite Extended Formulation* of P (of size d) if there exists an affine map $\phi : \mathbb{S}^d \to \mathbb{R}^n$ from the such that $\phi(Q) = P$. The semidefinite extension complexity of P, denoted by $\text{xc}_{SDP}(P)$, is the smallest size of a semidefinite extension of the polytope P. We can restate Lovász's result as follows.

Theorem 1.3.1 ([Lov79])**.** *Let $G = (V, E)$ be perfect graph. Then, $\text{xc}_{SDP}(\text{STAB}(G)) \leqslant n$.*

One way to obtain extended formulations of polytopes is by means of *hierarchies*. Given polytopes $P, Q \subseteq \mathbb{R}^n$ with $P \subset Q$, one aims to define an operator $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ satisfying

$$P \subseteq \cdots \subsetneq \varphi^\ell(Q) \subsetneq \cdots \subsetneq \varphi^2(Q) \subsetneq \varphi(Q) \subsetneq Q.$$

The operator φ is often constructed using non-linear inequalities satisfied by P, which are then "linearized" in a higher dimensional space, what we call a *lift*. Then, one *projects* back the result into the original space, hopefully obtaining a tighter relaxation.

One example of this is the hierarchies obtained via the *Lovász-Schrijver (SDP) Operator* LS_+, first introduced by Lovász and Schrijver in [LS91]. They proved that when applied to the fractional stable set polytope of a graph G, the resulting convex set already satisfied the clique constraints and many other well known constraints of $\text{STAB}(G)$, such as the odd wheel, hole and anti-hole constraints. Thus, after just one iteration the LS_+ operator already defines a semidefinite extended formulation of $\text{STAB}(G)$ of size $O(n)$ for Perfect Graphs and other families of graphs (see [LS91],[BENT14],[BENT17]).

Although this thesis does not study this hierarchy in detail, we should point out that there are a number of exciting open problems in the theory of spectrahedral relaxations that are related to our work and viewpoint (see Chapter 4). We hope to extend our studies to these problems in the near future.

1.4 Organization of the thesis

We have structured the thesis into three main chapters, each containing its own introduction, background and preliminaries. Although, our presentation and notation is unified, there is very little dependency between Chapters 2 and 3. Hence, the reader is free to read these independently without diminishing the global understanding and ideas of the thesis.

In Chapter 2 we introduce the Nullstellensatz Method and show how Systems of Linear Equations can be used to solve Combinatorial Optimization Problems such as Graph Coloring. Next, we introduce Razborov's technique to obtain lower bounds using properties of the principal ideal of polynomial sub-systems. Then, we introduce the concept of *essential graph* of a monomial and study the properties of the principal ideals generated by these sub-graphs. Finally, we put these pieces together and prove our main result on lower bounds for graphs with large girth.

In Chapter 3 we study polyhedral extended formulations of polytopes. We give a broad overview of the current known results for the extension complexity of the stable set polytope of perfect graphs and general techniques used to obtain these. Next, we specify our study to the regular bipartite case and we proof the main results of the chapter. Namely, we show lower bounds for the extension complexity of 4-regular bipartite graph with no C_4 and some computational result concerning the incidence graph of the projective plane of order 4.

Finally, in Chapter 4 we give a broad look to the results found in the thesis and discuss some open problems and future work. Furthermore, we include some open problems regarding the semidefinite extension complexity of the stable set polytope of graphs.

Chapter 2

Systems of Linear Equations: Graph Coloring, Nullstellensatz and Girth

2.1 Introduction

The use of algebraic geometry methods in combinatorial optimization has increased in popularity over the last couple of decades. The ability to reformulate hard optimization problems using simple multivariate polynomial formulations can be quite appealing. Specially, because these formulations can often be *relaxed* to obtain computationally tractable approximations to the hard optimization problem. Popular examples of this are hierarchy based approaches such as the Sherali-Adams, Lovász-Schrijver and Sum of Squares, or Lasserre relaxations for optimization problems (see [CT12]), where *Linear Programming* and *Semidefinite Programming* problems are used as building blocks to construct tighter and tighter relaxations to the optimization problem.

Another polynomial approach for combinatorial problems, implicit in the work of Beame *et al.* [BIK+94] and later proposed by De Loera *et al.* [DLLMM08] and Margulies [Mar08a], uses Hilbert's Nullstellensatz to create a hierarchy of relaxations based on *Systems of Linear Equations*. More concretely, one first formulates (the decision version of) a combinatorial problem using a system of polynomial equations

$$f_1(x) = f_2(x) = \cdots = f_m(x) = 0, \tag{2.1.1}$$

for polynomials $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ on $n \geqslant 1$ variables over some field $\mathbb{K}$. This is done in a way that the system (2.1.1) has a solution over the algebraic closure $\overline{\mathbb{K}}$ if and only if the combinatorial problem has a solution. By Hilbert's Nullstellensatz (see [CLO07]), if the problem does not have a solution then there exist polynomials $r_1, \ldots, r_m \in \mathbb{K}[x_1, \ldots, x_n]$, which we call *Nullstellensatz Certificates*, such that

$$r_1(x)f_1(x) + \cdots + r_m(x)f_m(x) = 1. \tag{2.1.2}$$

Although the Nullstellensatz has been used to obtain interesting results in combinatorics (see Alon [Alo99]), a crucial observation made by De Loera et al. is that the existence Nullstellensatz Certificates $r_1, \ldots, r_m$ of degree at most d, can be determined using a **system of linear equations** over $\mathbb{K}$. This allows us to use a hierarchy of systems of linear equations to solve the combinatorial problem. For general systems of polynomial equations, the maximum degree of the Nullstellensatz Certificates can be exponential in n and m. However, for systems based on combinatorial problems with a special structure, the maximum degree of the certificates can be small, which makes the method computationally attractive, as solving systems of linear equations is usually significantly faster than solving linear or semidefinite programs of comparable size.

In a series of papers, De Loera *et al.* [DLLMM08, DLHMO10, DLLMM15] studied the Nullstellensatz approach for several combinatorial problems, with special attention given to *Graph Coloring*. Recall that for a graph $G = (V, E)$ and an integer $k \geqslant 2$, the graph G is *k-colorable* if it is possible to assign k colors to its vertices in a way that no pair of adjacent vertices have the same color. The polynomial formulation they used for the k-coloring problem, due to Bayer [Bay82], is given by the system

$$\begin{aligned} p_u(x) &:= x_u^k - 1 = 0, && \forall u \in V, \\ q_{uv}(x) &:= \frac{x_u^k - x_v^k}{x_u - x_v} = 0, && \forall \{u, v\} \in E. \end{aligned} \tag{BCOL$_k$}$$

The computational experiments of De Loera *et al.* showed the potential applications of the Nullstellensatz method in detecting non-3-colorability of graphs. They were able to solve known hard instances, such as the Mizuno and Nishihara [MN08] families, of non-3-colorable graphs with up to a thousand of vertices over $\mathbb{F}_2$. In fact, no graph needing a Nullstellensatz certificate of degree larger than *four* was encountered at the time. This was quite surprising, given the fact that unless $\mathbf{P} = \mathbf{NP}$, families of graphs needing large Nullstellesatz Certificates should exists.

The problem of finding non-k-colorable graphs needing large certificates was settled until recently by Lauria and Nordström [LN17]. Their proof consisted of a nifty *Polynomial Calculus* (PC) reduction from the Functional Pigeonhole Principle (FPHP) to Graph Coloring. Since lower bounds for the degrees of PC proofs for special instances of FPHP had already been shown in [MN15], the result follows for k-colorability as well, implying the need of large Nullstellensatz Certificates for those instances. The graphs found in [LN17] yield asymptotically tight results in the sense that these graphs need certificates whose degrees share the same order of magnitude as the number vertices in the graph times k.

Despite these results, it is still wide open to determine the *combinatorial properties* that non-k-colorable graphs require to have small (or large) Nullstellensatz Certificates. For instance, De Loera et al. [DLHMO10] fully characterized all non-3-colorable graphs having a Nullstellensatz certificate of degree one over $\mathbb{F}_2$. However, it is still an open question to characterize all non-3-colorable graphs needing certificate of degree at most four over $\mathbb{F}_2$. The only related result we know is due to Li, Lowenstein and Omar [LLO15], who showed that no 4-critical graph with at most 12 vertices has a Nullstellensatz Certificate larger than four over $\mathbb{F}_2$.

In order to understand this problem further, it is natural to study families of graphs that are hard for coloring problems, such as the instances studied in [MN08] among others. One novel example of these are graphs with large *girth*, the length of the shortest cycle in the graph. A classical result of Erdös [Erd59] establishes the existence of graphs having arbitrarily large girth and chromatic number. These graphs look locally like trees, thus it is "easy" to color them locally, however a global understanding of the graph is needed in order to determine their chromatic number.

Explicit examples of graphs with large girth and chromatic number can be found in [Lov68, LPS88] and more recently in [AKR+16]. Most of the known explicit examples of k-colorable graphs having large girth are also fairly large in size. In fact, if we denote by $n(g,k)$ the number vertices of the smallest graph having chromatic number k and girth g, it is known that (see [EG18] for lower bound and [Mar08b] for upper bound)

$$\frac{2(k-2)^{(g-1)/2}-2}{k-3} \leqslant n(g,k) \leqslant 9gk^{6g+1}. \tag{2.1.3}$$

In particular, the size of these graphs are exponential in their girth. In this chapter, we show how to exploit the local behavior of this family of graphs to prove that non-k-colorable graphs with large girth also need large Nullstellensatz Certificates. More concretely, we show the following.

Theorem 2.1.1. *Let $G = (V, E)$ be a graph with chromatic number $\chi(G) = k + 1$ and girth $g > 2k$. Then, for every non-negative integer d satisfying*

$$d + k - 1 < \frac{g}{4k}, \tag{2.1.4}$$

G has no Nullstellensatz Certificates of degree at most d for the system (BCOL_k).

We follow a similar approach to the work of Razborov [Raz98], Aleknovich and Razborov [AR03] (later expanded in [MN15]) for boolean systems. A key idea is to understand the principal ideal of subsystems of (BCOL_k) corresponding to local subgraphs. Since these local subgraphs will be essentially trees for a graph with large girth, one can never find a Nullstellensatz Certificate of a given degree using these subsystems. This can be witnessed by what we call a *Dual Nullstellensatz Certificate* of the subsystem, which is constructed using information of the *standard monomials* of the subsystem. These "local" dual certificates are then patched to create a "global" dual certificate for the whole system, thus proving that the system does not admit a Nullstellensatz Certificate of certain degree.

We should point out that, while being partly inspired by the work in [AR03] and [MN15], our work does not seem to be a direct consequence of these studies. Besides them being applicable for Boolean systems only, one key component in their result requires the polynomial-variable incidence graph (or a clustering of it, as shown in [MN15]) of the system of polynomial equations to be a "good enough" expander. However, large girth alone does not seem to imply good expansion properties of the polynomial-variable incidence graph (or a clustering of this) for Bayer's polynomial system. Still, if these properties were to carry out, we would need to adjust the proofs in [MN15] to apply for more general set of systems of polynomial equations or use a different encoding for the graph coloring problem using Boolean systems, such as the one used in [LN17].

Instead, we found that understanding the structure of the principal ideal of local subsystems, as it is done in [Raz98] for systems arising from the *Pigeonhole Principle*, was critical and it allowed us to further understand the behavior of the Nullstellensatz and Polynomial Calculus proof systems for graph coloring in general.

2.2 Notation and Preliminaries

For a positive integer n, let $[n]$ be the set $\{1, \ldots, n\}$. Let $\mathbb{K}$ be an algebraically closed field and let $\mathbb{K}[x_1, \ldots, x_n]$ be the ring of polynomials with coefficients in $\mathbb{K}$. Monomials

in $\mathbb{K}[x_1, \ldots, x_n]$ are denoted using multi-index notation $x^{\boldsymbol{\alpha}} := x_1^{\boldsymbol{\alpha}_1} \cdots x_n^{\boldsymbol{\alpha}_n}$ where $\boldsymbol{\alpha} := (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n)$ is a non-negative integer vector. The degree of the monomial $x^{\boldsymbol{\alpha}}$ is defined as

$$|\boldsymbol{\alpha}| := \boldsymbol{\alpha}_1 + \cdots + \boldsymbol{\alpha}_n$$

and the support of $\boldsymbol{\alpha}$, denoted by $\text{supp}(\boldsymbol{\alpha})$, is the set of indices $i \in [n]$ such that $\boldsymbol{\alpha}_i > 0$. For a non-negative integer d, the set $\mathbb{K}[x_1, \ldots, x_n]_{\leqslant d}$ denotes the vector space of polynomials of degree at most d, i.e., the set of polynomials $f \in \mathbb{K}[x_1, \ldots, x_n]$ that can be written as

$$f(x) = \sum_{|\boldsymbol{\alpha}| \leqslant d} f_{\boldsymbol{\alpha}} x^{\boldsymbol{\alpha}} \tag{2.2.1}$$

for some scalars $f_{\boldsymbol{\alpha}} \in \mathbb{K}$. The support of f, denoted by $\text{supp}(f)$ is the set of multi-indices $\boldsymbol{\alpha}$ such that $f_{\boldsymbol{\alpha}} \neq 0$.

Division algorithms over $\mathbb{K}[x_1, \ldots, x_n]$ are possible once a *monomial ordering* has been established. Some commonly used monomial orderings are

1. The *Lexicographic Order* (LEX). For any pair of monomials $x^{\boldsymbol{\alpha}}$ and $x^{\boldsymbol{\beta}}$ we write $x^{\boldsymbol{\alpha}} \preceq_{LEX} x^{\boldsymbol{\beta}}$ if there exists a positive integer $i \in [n]$ such that $\boldsymbol{\alpha}_j = \boldsymbol{\beta}_j$ for all $j < i$ and $\boldsymbol{\alpha}_i < \boldsymbol{\beta}_i$.

2. The *Graded Lexicographic Order* (GLEX). For any pair of monomials $x^{\boldsymbol{\alpha}}$ and $x^{\boldsymbol{\beta}}$ we write $x^{\boldsymbol{\alpha}} \preceq_{GLEX} x^{\boldsymbol{\beta}}$ if either $|\boldsymbol{\alpha}| < |\boldsymbol{\beta}|$, or $|\boldsymbol{\alpha}| = |\boldsymbol{\beta}|$ and $x^{\boldsymbol{\alpha}} \preceq_{LEX} x^{\boldsymbol{\beta}}$.

Unless stated otherwise, in this chapter we will use the graded lexicographic order (GLEX) and we set $\preceq := \preceq_{GLEX}$. For a given polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$, its *leading monomial*, denoted by $LM(f)$, is the largest (in GLEX order) monomial in the support of f.

Given a finite set of polynomials $F := \{f_1, \ldots, f_m\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$, the *ideal* generated by F is the set

$$\langle F \rangle := \{r_1 f_1 + \cdots + r_m f_m : r_i \in \mathbb{K}[x_1, \ldots, x_n]\}. \tag{2.2.2}$$

The *variety* defined by F, denoted by $\mathcal{V}(F)$, is the set of solutions to the system

$$f_1(x) = f_2(x) = \cdots = f_m(x) = 0. \tag{2.2.3}$$

The following notion will be used quite often in this chapter.

Definition 2.2.1. Let $\mathcal{I}$ of $\mathbb{K}[x_1, \ldots, x_n]$ be an ideal. We denote by $LM(\mathcal{I})$ the set of all leading monomials of polynomials in $\mathcal{I}$. If $x^{\boldsymbol{\alpha}} \in LM(\mathcal{I})$, then we say that the monomial $x^{\boldsymbol{\alpha}}$ is **reducible modulo** the ideal $\mathcal{I}$, otherwise we say that the monomial is **irreducible modulo** $\mathcal{I}$.

Recall that a *Gröbner basis* of $\mathcal{I}$ is a set of polynomials $\{g_1, \ldots, g_r\}$ such that $\mathcal{I} = \langle g_1, \ldots, g_r \rangle$ and

$$\langle LM(\mathcal{I}) \rangle = \langle LM(g_1), \ldots, LM(g_r) \rangle.$$

In particular, a monomial $x^{\boldsymbol{\alpha}}$ is reducible modulo the ideal $\mathcal{I}$ if and only if $x^{\boldsymbol{\alpha}}$ is divisible by $LM(g_i)$ for some $i \in [r]$. The following notion is also key in this chapter.

Definition 2.2.2. Let $\mathcal{I}$ be an ideal and let $f \in \mathbb{K}[x_1, \ldots, x_n]$ be any polynomial. Let $g_1, \ldots, g_r$ be a Gröbner Basis of $\mathcal{I}$. The *reduction* (or, *normal form*) of f modulo $\mathcal{I}$ is the remainder of the division of f by the basis $g_1, \ldots, g_r$, i.e., it is the unique polynomial $\phi_{\mathcal{I}}(f) \in \mathbb{K}[x_1, \ldots, x_n]$ such that

1. $f = g + \phi_{\mathcal{I}}(f)$ for some $g \in \mathcal{I}$, and
2. no monomial in $\phi_{\mathcal{I}}(f)$ is reducible modulo $\mathcal{I}$.

Hilbert's Nullstellensatz [Hil93, Tao07, CLO07], in its most basic form, is the statement that $\mathcal{V}(F) = \emptyset$ if and only if $1 \in \langle F \rangle$. In other words, the system (2.2.3) has no solution if and only if

$$r_1(x) f_1(x) + \cdots + r_m(x) f_m(x) = 1 \tag{2.2.4}$$

for some polynomials $r_1, \ldots, r_m \in \mathbb{K}[x_1, \ldots, x_n]$. We say that the polynomials $r_1, \ldots, r_m$ in (2.2.4) are a *Nullstellensatz Certificate* of degree d if each polynomial r_i has degree at most d. A crucial observation is that Nullstellensatz Certificates of degree d can be found by solving a system of linear equations as easily seen from (2.2.4). Indeed, such system is found by considering each r_i in (2.2.4) with variable coefficients and then equating the resulting polynomial with the constant polynomial 1. Let us denote this system of equations by

$$A_{F,d} y = b_{F,d}. \tag{2.2.5}$$

It is a result of Kollar [Kol88] that if the system (2.2.3) is infeasible, then there exists a Nullstellensatz Certificate of degree $d_K := \max(3, d_{\max})^{\min(n,m)}$ where $d_{\max}$ is the largest

degree of the polynomials in F. However, in order for the algorithm to detect feasibility, a system of size

$$\Theta\left(\frac{4^{d_K}}{d_k^{1/2}}\right)$$

should be solved. Since d_k is exponential in n, the system ends up being doubly exponential in the number of variables. There are some cases where such size can be reduced. For instance, if the polynomials in F have no common root at infinity, a theorem of Lazard [Laz77] allows us to reduce Kollar's bound to $d_L := n \cdot (d_{\max} - 1)$. Thus, feasibility can be checked by solving a linear system of size singly exponential in the number of variables.

2.2.1 Graph Coloring and Subgraph Ideals

Let $G = (V, E)$ be a graph with vertex set $V = [n]$ for some $n \in \mathbb{Z}_+$. All graphs in this thesis are simple, finite and undirected. A graph is said to be k-colorable if there exists a map $\kappa : V \to [k]$ such that $\kappa(u) \neq \kappa(v)$ for all edges $uv \in E$. The minimum $k \in \mathbb{Z}_+$ for which G is k-colorable is called the *chromatic number* of G and we denote this number by $\chi(G)$. The *girth* of G is the length of the shortest cycle in G.

Let $\mathbb{K}$ be a field of characteristic not dividing k. For a vertex $u \in V$ and edge $vw \in E$, let $p_u(x)$ and $q_{vw}(x)$ be the polynomials defined in Bayer's formulation:

$$\begin{aligned} p_u(x) &:= x_u^k - 1 = 0, && \forall u \in V, \\ q_{uv}(x) &:= \frac{x_u^k - x_v^k}{x_u - x_v} = 0, && \forall \{u, v\} \in E. \end{aligned} \tag{BCOL$_k$}$$

Notice that the graph G is k-colorable if and only if (BCOL$_k$) has a solution: the first set of polynomial equations tells us that we aim to color the graph with k-roots of the unity and the second set of polynomial equations encode the fact that no pair of adjacent vertices can be assigned the same k-th root of the unity. Indeed, if $x_u = x_v = \zeta$ for some root of the unity $\zeta \in \mathbb{K}$ then

$$q_{uv}(x)|_{x_u = x_v = \zeta} = x_u^{k-1} + x_u^{k-2} x_v + \cdots + x_u x_v^{k-2} + x_v^{k-1}|_{x_u = x_v = \zeta} = k \cdot \zeta^{k-1} \neq 0, \tag{2.2.6}$$

as the characteristic of $\mathbb{K}$ does not divide k. Let $\mathcal{I}_{V,k}$ be the ideal generated by the polynomials p_u with $u \in V$. Consider the quotient ring $R_{V,k} := \mathbb{K}[x_u : u \in V]/\mathcal{I}_{V,k}$, i.e.,the

set of all congruent classes of polynomials modulo the ideal $\mathcal{I}_{V,k}$. Then, every polynomial f is congruent with the polynomial

$$f(x) \equiv \sum_{\boldsymbol{\alpha} \in \mathbb{Z}_k^V} c_{\boldsymbol{\alpha}} x^{\boldsymbol{\alpha}} \qquad \mod \mathcal{I}_{V,k},$$

for some $c_{\boldsymbol{\alpha}} \in \mathbb{K}$ and $\boldsymbol{\alpha} \in \mathbb{Z}_k^V$, where $\mathbb{Z}_k$ is the set of integers modulo k. Such a representation exhibits the fact that $R_{V,k}$ is a finite dimensional vector space, which is isomorphic to the space of functions $\boldsymbol{\alpha} \mapsto c_{\boldsymbol{\alpha}}$ mapping $\mathbb{Z}_k^V$ to $\mathbb{K}$.

Given a subset of edges $F \subseteq E$, we let $\mathcal{I}_F$ be the ideal of $R_{V,k}$ generated by the polynomials q_{uv} with $uv \in F$. Since the polynomials $x_u^k - 1$ are square free, the ideal $\mathcal{I}_F$ is radical (see [CLO05, Proposition 2.7]). Thus, we have that $f \in \mathcal{I}_F$ if and only if $f(a) = 0$ for every valid k-coloring $a = (a_w)_{w \in V(F)}$ of the graph induced by F, that is $a_w^k = 1$ for all $w \in V(F)$ and $a_v \neq a_w$ for all $vw \in F$.

Clearly, the existence of a Nullstellensatz Certificate of degree d for (BCOL_k) guarantees the existence of polynomials r_{uv} for $uv \in E$ of degree at most d such that

$$\sum_{uv \in E} r_{uv}(x) q_{uv}(x) \equiv 1 \mod \mathcal{I}_{V,k}. \tag{2.2.7}$$

Therefore, in order to find lower bounds for Nullstellensatz Certificates, it is enough to show that there are no polynomials r_{uv} of degree at most d in $R_{V,k}$ satisfying (2.2.7). This in turn can be certified using the following lemma. In the lemma, $e_u \in \mathbb{Z}_k^V$ with $u \in V$ denote the standard vectors of $\mathbb{Z}_k^V$.

Lemma 2.2.3. *Let $G = (V, E)$ be a graph. Suppose there exists some vector $\lambda = (\lambda_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha} \in \mathbb{Z}_k^V, |\boldsymbol{\alpha}| \leqslant d+k-1}$ with entries in $\mathbb{K}$ such that*

$$\begin{aligned} \textstyle\sum_{r \in \mathbb{Z}_k} \lambda_{\boldsymbol{\alpha} + r(e_u - e_v) - e_v} = 0, \quad \forall \boldsymbol{\alpha} \in \mathbb{Z}_k^V,\ |\boldsymbol{\alpha}| \leqslant d, uv \in E, \\ \lambda_0 = 1. \end{aligned} \tag{DCOL$_{k,d}$}$$

Then, (BCOL_k) does not have a Nullstellensatz Certificate of degree d.

Proof. Consider the linear subspace $N(E, d) \subseteq R_{V,k}$ of all polynomials that can be written in the form

$$\sum_{uv \in E} r_{uv} q_{uv}$$

for some $r_{uv} \in R_{V,k}$ of degree at most d. Clearly, $N(E,d)$ is spanned by all polynomials of the form

$$x^{\boldsymbol{\alpha}} q_{uv}(x) = \sum_{r=0}^{k-1} x^{\boldsymbol{\alpha}} x_u^{k-1-r} x_v^r, \quad \forall |\boldsymbol{\alpha}| \leqslant d,\ \forall \{u,v\} \in E.$$

Then, $1 \notin N(E,d)$ if and only if there exists a linear functional $\lambda : R_{V,k} \to \mathbb{K}$ such that $\lambda(1) = 1$ and $\lambda(f) = 0$ for every $f \in N(E,d)$. This last equation is equivalent to the equations

$$\lambda(x^{\boldsymbol{\alpha}} q_{uv}(x)) = \sum_{r=0}^{k-1} \lambda(x^{\boldsymbol{\alpha}} x_u^{k-1-r} x_v^r) = 0 \quad \forall \boldsymbol{\alpha} \in \mathbb{Z}_k^V, |\boldsymbol{\alpha}| \leqslant d,\ \forall \{u,v\} \in E.$$

Using the fact that $R_{V,k}$ is spanned by monomials $x^{\boldsymbol{\alpha}}$ with $\boldsymbol{\alpha} \in \mathbb{Z}_k^V$ and setting $\lambda_{\boldsymbol{\alpha}} := \lambda(x^{\boldsymbol{\alpha}})$, we can further rewrite the above equation as

$$\textstyle\sum_{r \in \mathbb{Z}_k} \lambda_{\boldsymbol{\alpha} + r(e_u - e_v) - e_v} = 0, \quad \forall \boldsymbol{\alpha} \in \mathbb{Z}_k^V,\ |\boldsymbol{\alpha}| \leqslant d, \{u,v\} \in E.$$

The statement follows. □

Definition 2.2.4. In matrix notation, let $\hat{A}_{E,d}\lambda = \hat{c}_{E,d}$ be the system ($\mathrm{DCOL}_{k,d}$). Any solution λ to this system is called a **Dual Nullstellensatz Certificate** of degree d.

Remark 2.2.5. Notice that the columns of $\hat{A}_{E,d}$ are indexed by monomials of degree at most $d + k - 1$. Hence, we can view each row of $\hat{A}_{E,d}$ as a polynomial in $R_{V,k}$.

2.2.2 Polynomial Calculus and Related Work

A study of lower bounds for Nullstellensatz certificates has already appeared in the context of *Propositional Proof Systems* in a paper by Beame *et al.* [BIK+94]. Lower bounds were found for systems of polynomial equations derived from the *Modular Counting Principle* and the *Pigeonhole Principle* [BCE+98]. Later, Clegg *et al.* [CEI96] worked with a stronger proof system that is now called *Polynomial Calculus* (PC). In this system, given polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, the goal is to find a proof of the statement $1 \in \langle f_1, \ldots, f_m \rangle$ using a sequence of polynomials $p_1, \ldots, p_t$, such that $p_t = 1$ and every p_i in the sequence is either

1. one of the $f_1, \ldots, f_m$, or

2. the linear combination $\alpha p + \beta q$ of some previous polynomials p, q in the sequence and $\alpha, \beta \in \mathbb{K}$, or
3. the product $x_j \cdot p$ of one previous polynomial in the sequence p and any variable x_j with $j \in [n]$.

It is not hard to see that the largest degree of the polynomials in the sequence is always smaller than or equal to the degree of a Nullstellensatz certificate (times the maximum of the degrees of the polynomials f_i). Thus, lower bounds for the degrees of PC refutations are lower bounds for the degrees of Nullstellensatz certificates. The converse it is not necessarily true. In fact, Clegg *et al.* [CEI96] showed an exponential separation between these two for some systems of polynomial equations derived from the *House-sitting Principle*, a generalization of the pigeonhole principle introduced by the authors.

Notice that lower bounds for the degrees of PC refutations can be found by constructing an operator $\phi : \mathbb{K}[x_1, \ldots, x_n]_d \to \mathbb{K}[x_1, \ldots, x_n]_d$ such that

a. $\phi(1) = 1$,
b. $\phi(f_i) = 0$ for all $i \in [m]$, and
c. for every $x^{\boldsymbol{\alpha}}$ of degree less than d and every $j \in [n]$

$$\phi(x_j x^{\boldsymbol{\alpha}}) = \phi(x_j \cdot \phi(x^{\boldsymbol{\alpha}})).$$

Such ϕ implies that no PC refutation of degree d exists (see [Raz98]). This is precisely how the bounds in [Raz98], [AR03], [MN15] and ultimately the bounds in the present thesis are built. The idea is to define the operator ϕ in a local fashion: each monomial $x^{\boldsymbol{\alpha}}$ is assigned a subset $F_{\boldsymbol{\alpha}}$ of the polynomials $f_1, \ldots, f_m$ and then $\phi(x^{\boldsymbol{\alpha}})$ is defined to be the reduction of $x^{\boldsymbol{\alpha}}$ modulo the ideal $\langle F_{\boldsymbol{\alpha}} \rangle$. Clearly, since we want ϕ to satisfy the properties a. to c. above, the sets $F_{\boldsymbol{\alpha}}$ should be chosen carefully.

For instance, for Boolean systems, Aleknovich and Razborov [AR03] construct the sets $F_{\boldsymbol{\alpha}}$ using expandability properties of the *polynomial-variable incidence graph*. Mikša and Nordström [MN15] use a similar construction using a suitable clustering of the polynomial-variable incidence graph. In our setup, the sets $F_{\boldsymbol{\alpha}}$ will correspond to suitable sub-forests that we construct using the non-k-colorability and large girth of our graphs (what we call *essential graphs* in the section below).

2.3 Large Girth and Nullstellensatz Certificates

Throughout this section $G = (V, E)$ will denote a graph with chromatic number $\chi(G) = k + 1$ for some $k \geqslant 3$ and girth $g \geqslant 3$. As before, let us identify the vertex set of G with the set $[n]$ and let us consider the ring $R_{V,k} = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_{V,k}$.

Our goal is to show that G does not have a Nullstellensatz certificate of degree $d \ll g$. As stated in Lemma 2.2.3 and Definition 2.2.4, this can be achieved by finding a Dual Nullstellensatz Certificate $\lambda = (\lambda_{\boldsymbol{\alpha}})_{|\boldsymbol{\alpha}| \leqslant d+k-1}$ satisfying the system

$$\hat{A}_{E,d} \cdot \lambda = \hat{c}_{E,d}. \tag{2.3.1}$$

The goal of this section is to exploit the sparsity of G to show that such λ can be defined locally. More concretely, for each $\boldsymbol{\alpha} \in \mathbb{Z}_k^V$ of degree at most $d + k - 1$ we will associate a subgraph $H_{\boldsymbol{\alpha}} = (U_{\boldsymbol{\alpha}}, F_{\boldsymbol{\alpha}})$ of G, that we called the *essential graph* of $\boldsymbol{\alpha}$ (see Definition 2.3.12). As we will see, the graphs $H_{\boldsymbol{\alpha}}$ encode the local reducibility of $x^{\boldsymbol{\alpha}}$, i.e., $x^{\boldsymbol{\alpha}}$ will be reducible modulo $\mathcal{I}_{F_{\boldsymbol{\alpha}}}$ if and only if it is reducible modulo $\mathcal{I}_F$ for every $F \supseteq F_{\boldsymbol{\alpha}}$ not "too large". Moreover, the sparsity of G will guarantee that each $H_{\boldsymbol{\alpha}}$ is k-colorable, so that the sub-system of linear equations

$$\hat{A}_{F_{\boldsymbol{\alpha}},d} \cdot \mu = \hat{c}_{F_{\boldsymbol{\alpha}},d} \tag{2.3.2}$$

has a "local" solution $\mu^{(\boldsymbol{\alpha})} = (\mu_{\boldsymbol{\beta}}^{(\boldsymbol{\alpha})})_{|\boldsymbol{\beta}| \leqslant d+k-1}$ for each $\boldsymbol{\alpha}$. Finally, by the reducibility property of $H_{\boldsymbol{\alpha}}$, we will see that the local solutions $\mu^{(\boldsymbol{\alpha})}$ for each $\boldsymbol{\alpha}$ can be patched together to obtain a global solution λ for (2.3.1), hence implying the non-existence of a Nullstellensatz certificate of degree d.

2.3.1 Orderings and Essential Graphs

Each bijection from $[n]$ to the vertices of G induces a monomial order $\preceq$ of $R_{V,k}$, namely the Graded Lexicographic Order (GLEX) where

$$x_n \preceq x_{n-1} \preceq \cdots \preceq x_1.$$

Given an edge $\{u, v\} \in E$ with $u < v$, we say that v is a *child* of u and that u is a *parent* of v. Also, paths $P = u_1 u_2 \ldots u_t$ in G satisfying $u_1 < u_2 < \cdots < u_n$ will be called *index-increasing paths*. If there exists an index-increasing path from u to v, we say that v is a descendant of u.

Definition 2.3.1. Let $x^{\boldsymbol{\alpha}}$ be a monomial with $\boldsymbol{\alpha} \in \mathbb{Z}_k^V$. The **descendant graph** of $x^{\boldsymbol{\alpha}}$ is the subgraph $H_{\boldsymbol{\alpha}}^{(0)} = (U_{\boldsymbol{\alpha}}^{(0)}, F_{\boldsymbol{\alpha}}^{(0)})$ of G induced by the vertices in the support of $\boldsymbol{\alpha}$ and their descendants.

The following lemmas show that due to the sparsity and $(k+1)$-colorability of G, the descendant graphs have a very special structure.

Lemma 2.3.2. *There exists a labelling of the vertex set V such that every index-increasing path of G has length at most k.*

Proof. Consider any $(k+1)$-coloring of the graph G, say with colors $1, 2, \ldots, k+1$. Label the vertices of G in a way such that the inequality $u < v$ holds for every vertex u in color class i and every v in color class j where $i < j$. Formally, this can be done as follows. First, let $n_i \geqslant 0$ be the number of vertices in the color class $i \in [k+1]$ and set $n_0 = 0$. Then, assign to each vertex in the color class $i \in [k+1]$ a unique label in the set

$$\left\{ \sum_{j=0}^{i-1} n_j + 1, \ldots, \sum_{j=0}^{i} n_j \right\}.$$

Since there are only $k+1$ colors, no index-increasing path will have length larger than k. □

Lemma 2.3.3. *Let $G = (V, E)$ be a graph with chromatic number $k+1$ and girth $g > 2k$. Order the vertices of G according to Lemma 2.3.2. Let $x^{\boldsymbol{\alpha}}$ be a monomial of degree at most $|\boldsymbol{\alpha}| < \frac{g}{2k} - 1$. Then, the descendant graph of $x^{\boldsymbol{\alpha}}$ is a forest.*

Proof. Suppose for the sake of a contradiction that $H_{\boldsymbol{\alpha}}^{(0)}$ has a cycle $C \subseteq F_{\boldsymbol{\alpha}}^{(0)}$. Let us partition the cycle C into index-increasing paths $P_1, \ldots, P_s$ and let $v_1, \ldots, v_s$ be the vertices with the smallest index on each of these paths. Notice that the set $U := \{v_1, \ldots, v_s\}$ has at least $\frac{s}{2}$ vertices. Since the length of each path P_i is at most k, we have that $g \leqslant |C| \leqslant ks$, thus $|U| \geqslant \frac{|C|}{2k}$.

Let $u \in V$ be a vertex in the support of $\boldsymbol{\alpha}$ and let $U(u)$ be the set of descendants of u that lie in U. Since G has girth $g > 2k$ and has no index-increasing path of length larger than k, any pair of vertices $v_i, v_j \in U(u)$ lie at distance at least $g - 2k$ in C. In particular, $|U(u)| \leqslant \frac{|C|}{g-2k}$.

Now, take any set of t vertices $u_1, \dots, u_t$ in the support of $\boldsymbol{\alpha}$ such that

$$U = \bigcup_{i=1}^{t} U(u_t).$$

Then,

$$\frac{|C|}{2k} \leqslant |U| \leqslant \sum_{i=1}^{t} |U(u_i)| \leqslant t\frac{|C|}{g-2k} \quad \Longrightarrow \quad \frac{g}{2k} - 1 \leqslant t \leqslant |\boldsymbol{\alpha}|.$$

□

From now on, we will assume that the vertices of G are ordered as in Lemma 2.3.2, so that the descendant graphs of monomials of low degree are always sub-forests of G. The following lemma is the core of our argument.

Lemma 2.3.4. *Let $x^{\boldsymbol{\alpha}}$ be a monomial and let $H = (U, F)$ be its descendant graph. Suppose that no pair of vertices in different connected components of H have common or adjacent parents in G. Then, for every sub-forest $H' = (U', F')$ of G containing H, the monomial $x^{\boldsymbol{\alpha}}$ is reducible modulo $\mathcal{I}_{F'}$ if and only if it is reducible modulo $\mathcal{I}_F$.*

Proof. Let $x^{\boldsymbol{\alpha}}$, H and H' be as in the statement. Clearly, if $x^{\boldsymbol{\alpha}}$ is reducible modulo $\mathcal{I}_F$ then it is reducible modulo $\mathcal{I}_{F'}$ as $F \subseteq F'$. Thus, let us assume that $x^{\boldsymbol{\alpha}}$ is reducible modulo $\mathcal{I}_{F'}$.

Let $H^* = (U^*, F^*)$ be a connected component of the graph $H' \setminus H$. Since H is a forest, there is at most one edge from H^* to each component of H. Suppose that H^* is connected to $\ell \geqslant 1$ components of H and let $u_1^*, \dots, u_\ell^* \in U^*$ and $u_1, \dots, u_\ell \in U$ be such that $u_i u_i^* \in F'$ for each $i \in [\ell]$. Then, by our hypothesis on H, for all $i \in [\ell]$ we have $u_i^* < u_i$ and no pair of the vertices u_i^*, u_j^* or u_i^*, u_j are adjacent for $i \neq j$.

Let $H'' = (U'', F'')$ be the graph obtained from H' after the deletion of the graph H^*. Our goal is to show that $x^{\boldsymbol{\alpha}}$ is reducible modulo the ideal $\mathcal{I}_{F''}$. Thus, by successively repeating this procedure with each of the remaining components of $H' \setminus H$, the reducibility of $x^{\boldsymbol{\alpha}}$ modulo $\mathcal{I}_F$ follows.

Since $x^{\boldsymbol{\alpha}}$ is reducible modulo $\mathcal{I}_{F'}$, it is the leading term of a polynomial f of the form

$$f(x) = \sum_{u'v' \in F''} r_{u'v'}(x) q_{u'v'}(x) + \underbrace{\sum_{i=1}^{\ell} r_{u_i^* u_i}(x) q_{u_i^* u_i}(x) + \sum_{u'v' \in F^*} r_{u'v'}(x) q_{u'v'}(x)}_{:= p(x)}, \tag{2.3.3}$$

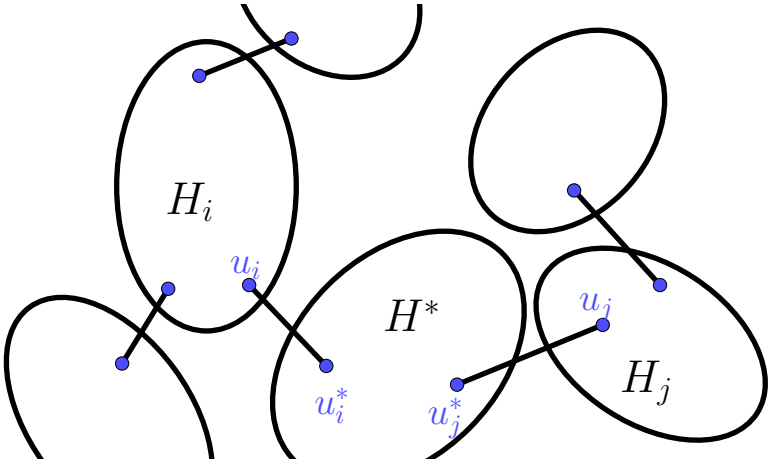


Figure 2.1: The graph of Lemma 2.3.4

for some polynomials $r_{u'v'}$ with $u'v' \in F'$ of degree at most d. We will show that it is possible to transform f into a polynomial $\tilde{f} \in \mathcal{I}_{F''}$ whose leading monomial is $x^{\boldsymbol{\alpha}}$. We do this by analyzing the degrees of the $x_{u_i^*}$ variables appearing in f for each $i \in [\ell]$. The reason behind such analysis is motivated by the following claim.

Claim 2.3.5. Let $f \in \mathcal{I}_{F'}$ be as above. Suppose that for each $i \in [\ell]$ the $x_{u_i^*}$-degree of f is at most $k-3$. Then, $x^{\boldsymbol{\alpha}}$ is reducible modulo $\mathcal{I}_{F''}$.

Proof. Since H^* is a tree, we can pick a partial coloring $b := (b_w)_{w \in U^* \setminus \{u_1^*, \ldots, u_\ell^*\}}$ of H^* that colors all the neighbors in H^* of each u_i^* with the same color. Indeed, fix a primitive k-th root of the unity ζ and a vertex $v_0 \in U^*$ of H^*. For every $w \in U^*$ let $d(w)$ be the distance in H^* from w to v_0. Then, define

$$b_w := \zeta^{d(w) \mod 2} \qquad \forall w \in U^* \setminus \{u_1^*, \ldots, u_\ell^*\}.$$

Now, if a vertex $u^* \in U^*$ lies at distance $d(u^*)$ to v_0, then all of its neighbors satisfy $d(w) \equiv d(u^*) + 1 \mod 2$ and b_w will be the same for all of them.

Consider the polynomial $f|_b$ obtained from f after the evaluation of the partial coloring b. Notice that the leading term of $f|_b$ is still $x^{\boldsymbol{\alpha}}$ as no vertex of H^* appears in the support of $\boldsymbol{\alpha}$. We claim that $f|_b \in \mathcal{I}_{F''}$. Indeed, consider any coloring $a := (a_{u''})_{u'' \in F''}$ of H'' where each $a_{u''}$ is a k-th root of the unity and let $f|_{a,b}$ be the polynomial obtained from $f|_b$ after the evaluation of a. Then, $f|_{a,b}$ is a polynomial containing only $x_{u_i^*}$ variables and it

vanishes on any coloring of H' that agrees with a and b. Now, the partial coloring induced by a and b colors the neighbors of each vertex u_i^* with at most two colors. Thus, at least $k-2$ colors are available for each vertex u_i^* to extend the partial coloring to a full coloring of H' and obtain a root of $f|_{a,b}$. Since the $x_{u_i^*}$-degree of $f|_{a,b}$ is at most $k-3$ for each $i \in [\ell]$, this implies that $f|_{a,b} = 0$ and the result follows. ♦

From the above claim, it is enough to reduce the $x_{u_i^*}$-degree of the polynomial f for each $i \in [\ell]$. We start with the following simplification.

Claim 2.3.6. We may assume that the polynomial p, defined in equation (2.3.3), and the polynomials $r_{u'v'}$ with $u'v' \in F''$ have $x_{u_i^*}$-degree at most $k-2$ for every $i \in [\ell]$. In particular, this property holds for f as well.

Proof. Let us fix any index $i \in [\ell]$. If a term of the form $c \cdot x_{u_i^*}^{k-1} x^{\boldsymbol{\beta}}$ appears in some $r_{u'v'}$ with $u', v \in F''$, then we replace such term by the polynomial $c \cdot [x_{u_i^*}^{k-1} - q_{u_i^* u_i}(x)] \cdot x^{\boldsymbol{\beta}}$ in $r_{u'v'}$ and add the polynomial $c \cdot q_{u'v'}(x) \cdot x^{\boldsymbol{\beta}}$ to $r_{u_i^* u_i}$. This way we obtain a representation of f such that all the $r_{u'v'}$ have $x_{u_i^*}$ degree at most $k-2$.

Next, we replace any appearance of $x_{u_i^*}^{k-1}$ in the terms of $p(x)$ with the polynomial $x_{u_i^*}^{k-1} - q_{u_i^* u_i}(x)$. The resulting polynomial is still in the ideal generated by the polynomials $q_{u_i^* u_i}(x)$ with $i \in [\ell]$ and $q_{u'v'}$ with $u'v' \in F^*$. Moreover, since the leading term of $q_{u_i^* u_i}(x)$ is $x_{u_i^*}^{k-1}$, then the new monomials appearing are smaller than $x^{\boldsymbol{\alpha}}$ in the GLEX order. Indeed, no monomial of p of the form $x_{u_i^*}^{k-1} \cdot x^{\boldsymbol{\beta}}$ can cancel out with a term of $\sum_{u'v' \in F''} r_{u'v'}(x) q_{u'v'}(x)$ as we have reduced the $x_{u_i^*}$-degree of each $r_{u'v'}$ with $\{u', v'\} \in F''$. Thus, such monomials would appear in f as well, implying that $x_{u_i^*}^{k-1} \cdot x^{\boldsymbol{\beta}} \preceq x^{\boldsymbol{\alpha}}$ and as a consequence, every term in $[x_{u_i^*}^{k-1} - q_{u_i^* u_i}(x)] \cdot x^{\boldsymbol{\beta}}$ is smaller than $x^{\boldsymbol{\alpha}}$ in the GLEX order as well. ♦

Our next goal is then to further reduce the degree of the $x_{u_i^*}$-variables. As in the proof of Claim 2.3.5, we can get rid of many of the terms involving some of the vertices of H^* by using a partial coloring $b = (b_w)_{w \in U^* \setminus \{u_1^*, \dots, u_\ell^*\}}$ that colors all the neighbors in H^* of each u_i^* with the same color. Let us denote the color used by the neighbors of u_i^* by $\zeta_i \in \mathbb{K}$ for each $i \in [\ell]$. Then, by evaluating the partial coloring b on the polynomial f, we obtain a

new polynomial $\tilde{f}$ whose leading monomial is still $x^{\boldsymbol{\alpha}}$. We can write $\tilde{f}$ as

$$\begin{aligned}\tilde{f}(x) &= \sum_{u'v'\in F''} \tilde{r}_{u'v'}(x)q_{u'v'}(x) + \sum_{i=1}^{\ell} \tilde{r}_{u_i^*u_i}(x)q_{u_i^*u_i}(x) + \sum_{i=1}^{\ell} \tilde{r}_i(x)q_{u_i^*u_i}(x_{u_i^*},\zeta_i),\\ &= \sum_{u'v'\in F''} \tilde{r}_{u'v'}(x)q_{u'v'}(x) + \underbrace{\sum_{i=1}^{\ell} \left[\tilde{r}_{u_i^*u_i}(x)q_{u_i^*u_i}(x) + \tilde{r}_i(x)q_{u_i^*u_i}(x_{u_i^*},\zeta_i)\right]}_{:=\tilde{p}(x)},\end{aligned}$$

for some polynomials $\tilde{r}_{u'v'}$ and $\tilde{r}_i$ of degree at most d. Notice that we have used the fact that all the neighbors in H^* of each u_i^* have been assigned the color ζ_i, so that if $w \in U^*$ is a neighbor of u_i^*, then

$$q_{u_i^*w}(x)|_b = \sum_{r=0}^{k-1} x_{u_i^*}^r \zeta_i^{k-1-r} = q_{u_i^*u_i}(x_{u_i^*},\zeta_i).$$

Now, for each $i \in [\ell]$ let us define the polynomial $t_i(x_{u_i^*}, x_{u_i})$ given by the equation

$$q_{u_i^*u_i}(x_{u_i^*},x_{u_i}) - q_{u_i^*u_i}(x_{u_i^*},\zeta_i) =: (x_{u_i}-\zeta_i)\cdot t_i(x_{u_i^*},x_{u_i}). \tag{2.3.4}$$

Notice that the leading monomial of each $t_i(x)$ is $x_{u_i^*}^{k-2}$. Moreover, for any k-th root of the unity $\zeta \neq \zeta_i$ we have

$$\langle q_{u_i^*u_i}(x_{u_i^*},\zeta_i), q_{u_i^*u_i}(x_{u_i^*},\zeta)\rangle = \langle t(x_{u_i^*},\zeta)\rangle. \tag{2.3.5}$$

We will successively reduce the $x_{u_i^*}$-degree of $\tilde{f}$ for each $i \in [\ell]$ as follows. First, set $f^{(0)} := \tilde{f}$, $p^{(0)} := \tilde{p}$ and $r_{u'v'}^{(0)} := r_{u'v'}$ for $\{u'v'\} \in F''$. Then, for each $i \in [\ell]$ and $\{u'v'\} \in F''$ write

$$\begin{aligned}p^{(i-1)}(x) &= x_{u_i^*}^{k-2} s^{(i-1)}(x) + \text{other terms with } x_{u_i^*}\text{-degree} < k-2,\\ r_{u'v'}^{(i-1)}(x) &= x_{u_i^*}^{k-2} r_{u'v'}^{(i-1,0)}(x) + \text{other terms with } x_{u_i^*}\text{-degree} < k-2,\end{aligned}$$

and define the polynomials

$$\begin{aligned}p^{(i)}(x) &:= p^{(i-1)}(x) - t_i(x)s^{(i-1)}(x),\\ r_{u',v'}^{(i)}(x) &:= r_{u'v'}^{(i-1)}(x) - t_i(x)r_{u'v'}^{(i-1,0)}(x),\\ f^{(i)}(x) &:= \sum_{u'v'\in F''} r_{u',v'}^{(i)}(x)q_{u'v'}(x) + p^{(i)}(x).\end{aligned}$$

Notice that the degree of each $r_{u'v'}^{(i)}$ is at most d. Moreover, we have the following:

Claim 2.3.7. For every $i \in [\ell]$, the leading monomial of $f^{(i)}$ is $x^{\boldsymbol{\alpha}}$.

Proof. We prove this by induction on i with the case $i = 0$ being trivial. Now, suppose that the leading term of $f^{(i-1)}$ is $x^{\boldsymbol{\alpha}}$. Since the polynomials $q_{u'v'}$ are free of $x_{u_i^*}$-variables for $\{u'v'\} \in F''$, we can write

$$\begin{aligned} f^{(i-1)}(x) &= \sum_{u'v' \in F''} r^{(i-1)}_{u'v'}(x) q_{u'v'}(x) + p^{(i-1)}(x), \\ &= \sum_{u'v' \in F''} \left(x^{k-2}_{u_i^*} r^{(i-1,0)}_{u'v'}(x) + \dots \right) q_{u'v'}(x) + \left(x^{k-2}_{u_i^*} s^{(i-1)}(x) + \dots \right), \\ &= x^{k-2}_{u_i^*} \left(\sum_{u'v' \in F''} r^{(i-1,0)}_{u'v'}(x) q_{u'v'}(x) + s^{(i-1)}(x) \right) + \dots, \end{aligned}$$

where the three dots consist of terms with $x_{u_i^*}$-degree less than $k-2$, all of them smaller than $x^{\boldsymbol{\alpha}}$ in GLEX order. However, by the definition of $f^{(i)}$ we have

$$\begin{aligned} f^{(i)}(x) &= f^{(i-1)}(x) - t_i(x) \left(\sum_{u'v' \in F''} r^{(i-1,0)}_{u'v'}(x) q_{u'v'}(x) + s^{(i-1)}(x) \right), \\ &= (x^{k-2}_{u_i^*} - t_i(x)) \left(\sum_{u'v' \in F''} r^{(i-1,0)}_{u'v'}(x) q_{u'v'}(x) + s^{(i-1)}(x) \right) + \dots. \end{aligned}$$

In other words, $f^{(i)}$ is obtained by replacing any appearance of the monomial $x^{k-2}_{u_i^*}$ in $f^{(i)}$ with the polynomial $(x^{k-2}_{u_i^*} - t_i(x))$. This operation does not affect $x^{\boldsymbol{\alpha}}$ as no vertex in H^* is in the support of $\boldsymbol{\alpha}$. Moreover, since the leading term of t_i is precisely $x^{k-2}_{u_i^*}$, the new monomials appearing in $f^{(i)}$ are smaller than $x^{\boldsymbol{\alpha}}$ in GLEX order. ⧫

Claim 2.3.8. $p^{(\ell)}(x) = 0$.

Proof. Let $a := (a_w)_{w \in U''}$ be any sequence with $a^k_w = 1$ for all $w \in U''$ and for every $i \in [\ell]$ let $p^{(i)}|_a$ be the polynomial obtained after the evaluation $x_w = a_w$ for all $w \in U''$. Let us first show that for every $i \in \{0, 1, \dots, \ell - 1\}$ we have

$$p^{(i)}|_a \in \langle q_{u_j^* u_j}(x_{u_j^*}, a_{u_j}), q_{u_j^* u_j}(x_{u_j^*}, \zeta_j) : \ j > i \rangle. \tag{2.3.6}$$

Indeed, for $i = 0$ the statement holds from the definition of the polynomial $p^{(0)}$. Thus, suppose that the statement holds for $p^{(i-1)}$. In particular, from the definition of $p^{(i)}$ we have that

$$p^{(i)}|_a \in \langle t_i(x_{u_i^*}, a_{u_i}), q_{u_j^* u_j}(x_{u_j^*}, a_{u_j}), q_{u_j^* u_j}(x_{u_j^*}, \zeta_j) : \ j \geqslant i \rangle$$

and the $x_{u_i^*}$-degree of $p^{(i)}|_a$ is at most $k-3$. Let $c = (c_{u_j^*})_{j>i}$ be any vanishing point of the ideal described in equation (2.3.6), in other words each $c_{u_j^*}$ is any root of the unity different to a_{u_i} and ζ_i. Let $p^{(i)}|_{a,c}$ be the polynomial obtained after the evaluation by c, so that

$$p^{(i)}|_{a,c} \in \langle t_i(x_{u_i^*}, a_{u_i}), q_{u_i^* u_j}(x_{u_i^*}, a_{u_i}), q_{u_i^* u_i}(x_{u_i^*}, \zeta_i)\rangle.$$

We see that $p^{(i)}|_{a,c}$ is a polynomial of degree at most $k-3$ with at least $k-2$ roots, namely any k-th root of the unity ζ different to ζ_i and a_{u_i} vanishes the polynomials $t_i(x_{u_i^*}, a_{u_i}), q_{u_i^* u_j}(x_{u_i^*}, a_{u_i})$ and $q_{u_i^* u_i}(x_{u_i^*}, \zeta_i)$. Since the point c was arbitrary, the equation (2.3.6) is proven for i.

From the above and by the definition of $p^{(\ell)}$ we conclude that

$$p^{(\ell)}|_a(x) \in \langle t_\ell(x_{u_\ell^*}, a_{u_\ell}), q_{u_\ell^* u_\ell}(x_{u_\ell^*}, a_{u_\ell}), q_{u_\ell^* u_\ell}(x_{u_\ell^*}, \zeta_\ell)\rangle.$$

Since the $x_{u_\ell^*}$-degree of $p^{(\ell)}$ is at most $k-3$, via a similar argument, we conclude that $p^{(\ell)}|_a$ vanishes for every possible a and the result follows. ♦

The claims above show that the polynomial

$$f^{(\ell)}(x) = \sum_{u'v' \in F''} r^{(\ell)}_{u',v'}(x) q_{u'v'}(x) \in \mathcal{I}_{F''}$$

has leading monomial $x^{\boldsymbol{\alpha}}$ and the result follows.

□

Remark 2.3.9. We have shown an even stronger result. Under the hypothesis of Lemma 2.3.4, if $x^{\boldsymbol{\alpha}}$ is the leading term of a polynomial of the form $\sum_{uv \in F'} r_{u'v'} q_{u'v'}$ where the polynomials $r_{u'v'}$ all have degree at most d, then $x^{\boldsymbol{\alpha}}$ is the leading term of polynomial of the form $\sum_{uv \in F^{(0)}_{\boldsymbol{\alpha}}} \tilde{r}_{u'v'} q_{u'v'}$ where each $\tilde{r}_{u'v'}$ has degree at most d as well.

As the following example shows, Lemma 2.3.4 might not be true when the connected components of the descendant graph of $x^{\boldsymbol{\alpha}}$ have common or adjacent parents. So, this assumption cannot be relaxed without changing the rest of the statement.

Example 2.3.10. Let $k = 3$ and consider the tree $G = (V, E)$ depicted in Figure 2.2. Consider the monomial $x^{\boldsymbol{\alpha}} := x_5^2 x_6 x_7 x_8^2 x_9$, we claim that $x^{\boldsymbol{\alpha}}$ is reducible modulo $\mathcal{I}_E$, but it is irreducible modulo $\mathcal{I}_F$ for any proper subset of edges $F \subseteq E$. Indeed, consider the polynomials

$$f_1(x) = (x_8 - x_9)(x_8 - x_{10})(x_9 - x_{10}),$$

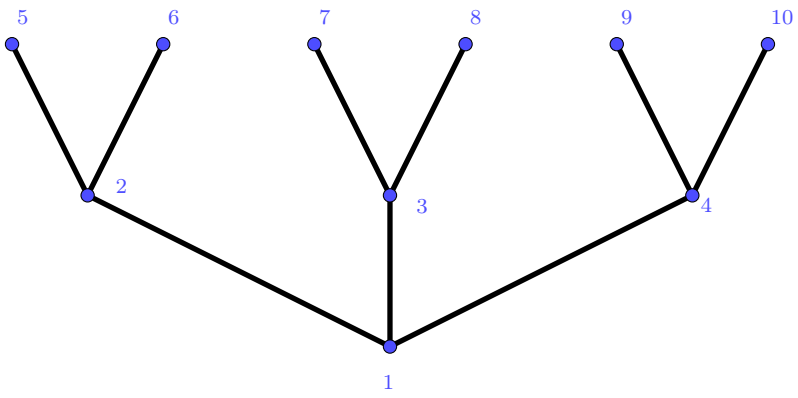


Figure 2.2: The graph of Example 2.3.10

$$f_2(x) = (x_5 - x_7)(x_6 - x_7)(x_7 - x_8),$$
$$f_3(x) = (x_5 - x_6)$$

Notice that the leading term of the product $f := f_1 f_2 f_3$ is $x^{\boldsymbol{\alpha}}$. We claim that f vanishes on all possible colorings of G. Indeed, let $a := (a_v)_{v \in V}$ be any coloring of the graph G where each a_v is a 3-rd root of the unity. If $f_1(a) \neq 0$, then a_8, a_9 and a_{10} are pairwise distinct. Since 4 is adjacent to both 9 and 10, this also implies that $a_4 = a_8$ and that $a_3 \neq a_4$. If in addition $f_2(a) \neq 0$ then $a_7 \neq a_8$ and both a_5 and a_6 are different to a_7. Since 3 is adjacent to both 7 and 8 and $a_4 = a_8$, this implies that $a_5, a_6 \in \{a_3, a_4\}$. Thus, we conclude that $a_5 = a_6$ and $f_3(a) = 0$. Otherwise, a_2, a_3 and a_4 would be pairwise distinct, which cannot happen as all of them have a neighbor in common. This shows the reducibility of $x^{\boldsymbol{\alpha}}$ modulo $\mathcal{I}_E$.

By the symmetry of the graph G and the way we have enumerated its vertices, it is not hard to see that the irreducibility of $x^{\boldsymbol{\alpha}}$ modulo $\mathcal{I}_F$ for any $F \subsetneq E$ follows from the following claim.

Claim 2.3.11. $x^{\boldsymbol{\alpha}}$ is irreducible modulo $\mathcal{I}_F$ for every set of the form $F = E \setminus \{u, v\}$ with $\{u, v\} \in \{\{1, 4\}, \{2, 6\}, \{3, 8\}, \{4, 10\}\}$.

The claim above can be verified with aid of a computer algebra system such as Macaulay2 [GS] by calculating a Gröbner basis of each of the four ideals $\mathcal{I}_F$ above. The details have been included in appendix A.

The above example motivates the following definition:

Definition 2.3.12. Let $x^{\boldsymbol{\alpha}}$ be a monomial in $R_{V,k}$. The **essential graph** of $x^{\boldsymbol{\alpha}}$ is the subgraph $H_{\boldsymbol{\alpha}} := (U_{\boldsymbol{\alpha}}, F_{\boldsymbol{\alpha}})$ of G constructed as follows:

1. Initially, set $H_{\boldsymbol{\alpha}} := H^{(0)}_{\boldsymbol{\alpha}}$ to be the descendant graph of $x^{\boldsymbol{\alpha}}$.
2. Let $U^* \subseteq U_{\boldsymbol{\alpha}}$ be set of parents of the vertices in $U_{\boldsymbol{\alpha}}$. If a pair of vertices $u, v \in U_{\boldsymbol{\alpha}}$ with parents $u^*, v^* \in U^*$ satisfies either $u^* = v^*$ or $u^*v^* \in E$, then we add the vertices u^*, v^* to $U_{\boldsymbol{\alpha}}$ along with all of their descendants. Then, we update $F_{\boldsymbol{\alpha}}$ to be the graph induced by this new set $U_{\boldsymbol{\alpha}}$.
3. We repeat step 2. until no pair of connected components of $H_{\boldsymbol{\alpha}}$ have common or adjacent parents.

Example 2.3.13. Consider the graph $G = (V, E)$ of Example 2.3.10 and the monomial $x^{\boldsymbol{\alpha}} := x_5^2 x_6 x_7 x_8^2 x_9$. Then, the descendant graph $H^0_{\boldsymbol{\alpha}}$ consist of all the leaves of the tree G, whereas the essential graph $H_{\boldsymbol{\alpha}}$ is the entire graph G. Recall that $x^{\boldsymbol{\alpha}}$ is irreducible modulo $\mathcal{I}_F$ for every subset of edges $F \subseteq E$, while being reducible modulo $\mathcal{I}_E$.

Corollary 2.3.14. *Let G be as above and let $\boldsymbol{\alpha}$ be a multi-index of degree at most d. Suppose that $2d < \frac{g}{2k} - 1$, then the essential graph of $x^{\boldsymbol{\alpha}}$ is a forest.*

Proof. Set initially $x^{\boldsymbol{\beta}} := x^{\boldsymbol{\alpha}}$. At each step of the construction of $H_{\boldsymbol{\alpha}}$, if parents u^* and v^* with $u^* \leqslant v^*$ are added to the graph, then let us update $x^{\boldsymbol{\beta}} := x^{\boldsymbol{\beta}} x_{u^*}$. Thus, at the end of the construction of $H_{\boldsymbol{\alpha}}$, the descendant graph of $x^{\boldsymbol{\beta}}$ equals $H_{\boldsymbol{\alpha}}$.

Now, at each step in the construction of $H_{\boldsymbol{\alpha}}$ we are reducing its number of connected components. Thus, the degree of $x^{\boldsymbol{\beta}}$ at the end of the construction is at most $2d$. By Lemma 2.3.3, $H_{\boldsymbol{\alpha}} = H^{(0)}_{\boldsymbol{\beta}}$ is a forest. □

Corollary 2.3.15. *Let $x^{\boldsymbol{\alpha}}$ be a monomial whose essential graph $H_{\boldsymbol{\alpha}}$ is a forest and let $H' = (U', F')$ be a larger forest containing $H_{\boldsymbol{\alpha}}$. Then, $x^{\boldsymbol{\alpha}}$ is reducible modulo $\mathcal{I}_{F_{\boldsymbol{\alpha}}}$ if and only if it is reducible modulo $\mathcal{I}_{F'}$.*

2.3.2 Main theorem

Before going into the proof of Theorem 2.1.1 let us recall some basic notation. For every subset of edges $F \subseteq E$ let us denote by

$$\hat{A}_{F,d}\lambda = \hat{c}_{F,d} \tag{2.3.7}$$

the system of linear equations ($\mathrm{DCOL}_{k,d}$) for the graph induced by F. Notice that the system (2.3.7) has a solution for every $d \geqslant 0$ whenever F is k-colorable. In particular, this holds whenever F is a forest.

By looking at the system ($\mathrm{DCOL}_{k,d}$), one sees that the columns of $\hat{A}_{F,d}$ can be indexed by monomials $x^{\boldsymbol{\alpha}}$ with $\boldsymbol{\alpha} \in \mathbb{Z}_k^V$ of degree at most $d+k-1$. We will assume that these columns are ordered using the GLEX order from left to right, where the largest monomials are the left most columns in $\tilde{A}_{F,d}$.

As it is custom in linear programming, let us call a set of monomials $\mathcal{B}$ a *basis* of $\hat{A}_{F,d}$ if the corresponding columns of $\hat{A}_{F,d}$ form a basis for its column space. If the system (2.3.7) has a solution, every basis $\mathcal{B}$ induces a corresponding *basic solution*, namely by setting $\lambda_{\boldsymbol{\alpha}} = 0$ for all $x^{\boldsymbol{\alpha}} \notin \mathcal{B}$ and solving the resultant system of equations with unique solution.

Lemma 2.3.16. *For every set of edges $F \subseteq E$ let $\mathcal{B}_{F,d}$ be the set of leading monomials of polynomials of the form $\sum_{uv \in F} r_{uv} q_{uv}$ where each r_{uv} has degree at most d. Then, $\mathcal{B}_{F,d} \cup \{1\}$ is a basis for the matrix $\hat{A}_{F,d}$.*

Proof. Using the indexing on the columns described above, we can identify each row of $\hat{A}_{F,d}$ with a polynomial in $R_{V,k}$. In fact these polynomials are either the constant polynomial 1 or polynomials of the form

$$x^{\boldsymbol{\alpha}} q_{uv}(x), \quad |\boldsymbol{\alpha}| \leqslant d, \ \{u,v\} \in F.$$

Thus, the row space of $\hat{A}_{F,d}$ corresponds precisely with the space of polynomials of the form $\sum_{uv \in F} r_{uv}(x) q_{uv}(x)$ where each r_{uv} has degree at most d. Let R be the row-reduced echelon form of $\tilde{A}_{F,d}$ and let $\mathcal{B}$ be the basis corresponding to the leading ones of R. We claim that $\mathcal{B} = \mathcal{B}_{F,d} \cup \mathcal{B}$. Indeed, since we have ordered the columns using the GLEX order, the leading terms of polynomials in the non-zero rows of R correspond to principal ones of R and $\mathcal{B} \subseteq \mathcal{B}_{F,d} \cup \{1\}$. Conversely, if $x^{\boldsymbol{\alpha}}$ is the leading monomial of the polynomial f in the row-span of $\hat{A}_{F,d}$, then we should be able to write f as linear combination of polynomials represented by rows of R. However, in such linear combination no cancellation of leading ones can occur and the leading term of f should be a monomial in $\mathcal{B}$. □

By Remark 2.3.9, we can rewrite corollary 2.3.15 as follows.

Corollary 2.3.17. *Let $x^{\boldsymbol{\alpha}}$ be a monomial whose essential graph $H_{\boldsymbol{\alpha}} = (U_{\boldsymbol{\alpha}}, F_{\boldsymbol{\alpha}})$ is a forest and let $H' = (U', F')$ be a larger forest containing $H_{\boldsymbol{\alpha}}$. Then, for any $d \geqslant 0$ and any $x^{\boldsymbol{\beta}}$ with $\operatorname{supp}(\boldsymbol{\beta}) \subseteq U_{\boldsymbol{\alpha}}$*

$$x^{\boldsymbol{\beta}} \in \mathcal{B}_{F',d} \Rightarrow x^{\boldsymbol{\beta}} \in \mathcal{B}_{F_{\boldsymbol{\alpha}},d}.$$

Proof. Since $\mathrm{supp}(\boldsymbol{\beta}) \subseteq U_{\boldsymbol{\alpha}}$, the essential graph $H_{\boldsymbol{\beta}}$ of $x^{\boldsymbol{\beta}}$ is a subforest of $H_{\boldsymbol{\alpha}}$. This follows from the fact that $H_{\boldsymbol{\alpha}}$ is closed under descendants and common or adjacent ancestors. In particular, $H_{\boldsymbol{\beta}}$ is subforest of H' as well. By Corollary 2.3.15 and Remark 2.3.9, if $x^{\boldsymbol{\beta}}$ is the leading term of a polynomial of the form $\sum_{uv \in F''} r_{uv} q_{uv}$ where each r_{uv} has degree at most d, then $x^{\boldsymbol{\beta}}$ is the leading term of a polynomial of the form $\sum_{uv \in F_{\boldsymbol{\beta}}} \tilde{r}_{uv} q_{uv}$ where each $\tilde{r}_{uv}$ has degree at most d as well. □

We are ready to prove our main result.

Proof of Theorem 2.1.1. Let $d \geqslant 0$ be such that $2(d+k-1) < \frac{g}{2k} - 1$. Then, for every monomial $x^{\boldsymbol{\alpha}}$ of degree at most $d+k-1$, its essential graph $H_{\boldsymbol{\alpha}} = (U_{\boldsymbol{\alpha}}, F_{\boldsymbol{\alpha}})$ is a forest. In particular, the system

$$\hat{A}_{F_{\boldsymbol{\alpha}},d} \cdot \mu = \hat{c}_{F_{\boldsymbol{\alpha}},d} \tag{2.3.8}$$

has a solution. Let $\mu^{(\boldsymbol{\alpha})}$ be the basic solution of (2.3.8) corresponding to the basis $\mathcal{B}_{F_{\boldsymbol{\alpha}},d}$ and set $\lambda_{\boldsymbol{\alpha}} := \mu^{(\boldsymbol{\alpha})}_{\boldsymbol{\alpha}}$. Notice that the essential graph of the constant polynomial 1 has no edges, thus the system (2.3.8) has only one equation, namely $\mu_0 = 1$ and as a consequence $\lambda_0 = 1$. We claim that $\lambda = (\lambda_{\boldsymbol{\alpha}})_{|\boldsymbol{\alpha}| \leqslant d+k-1}$ is a Dual Nullstellensatz Certificate of degree d, i.e.,λ is a solution to the system

$$\hat{A}_{E,d} \cdot \lambda = \hat{c}_{E,d}. \tag{2.3.9}$$

Indeed, let $x^{\boldsymbol{\alpha}}$ be a monomial of degree $|\boldsymbol{\alpha}| \leqslant d$ and let $\{u, v\} \in E$ be any edge of G. Our goal is to show that

$$\sum_{r \in \mathbb{Z}_k} \lambda_{\boldsymbol{\alpha} + r(e_u - e_v) - e_v} = 0. \tag{2.3.10}$$

Let $r \in \mathbb{Z}_k$ be such that the u-th and v-th coordinates of $\boldsymbol{\beta} := \boldsymbol{\alpha} + r(e_u - e_v) - e_v$ are non-zero. In other words, r is such that the support of $\boldsymbol{\beta}$ is maximal among all the multi-indices appearing in (2.3.10). In particular, for any other $r' \in \mathbb{Z}_k$ and $\boldsymbol{\eta} := \boldsymbol{\alpha} + r'(e_u - e_v) - e_v$ we have $\mathrm{supp}(\boldsymbol{\eta}) \subseteq \mathrm{supp}(\boldsymbol{\beta}) \subseteq U_{\boldsymbol{\beta}}$.

Let $R_{\boldsymbol{\eta}}$ and $R_{\boldsymbol{\beta}}$ be the row-reduced echelon forms of $\tilde{A}_{F_{\boldsymbol{\eta}},d}$ and $\tilde{A}_{F_{\boldsymbol{\beta}},d}$ respectively. We claim that the rows of $R_{\boldsymbol{\eta}}$ are rows of $R_{\boldsymbol{\beta}}$ as well. Indeed, the rows of $\tilde{A}_{F_{\boldsymbol{\eta}},d}$ are rows of $\tilde{A}_{F_{\boldsymbol{\beta}},d}$ and as a consequence every row in $R_{\boldsymbol{\eta}}$ is in the row span of the rows of $R_{\boldsymbol{\beta}}$. However, by Corollary 2.3.17, every column of $R_{\boldsymbol{\eta}}$ corresponding to a principal one of $R_{\boldsymbol{\beta}}$ is also a principal one of $R_{\boldsymbol{\eta}}$. Thus, each row of $R_{\boldsymbol{\eta}}$ cannot be obtained by non-zero combination of two or more different rows of $R_{\boldsymbol{\beta}}$.

Since every row of $R_{\boldsymbol{\eta}}$ appears in $R_{\boldsymbol{\beta}}$, for every column $\boldsymbol{\eta}'$ of $R_{\boldsymbol{\eta}}$ we have $\mu^{(\boldsymbol{\eta})}_{\boldsymbol{\eta}'} = \mu^{(\boldsymbol{\beta})}_{\boldsymbol{\eta}'}$. In particular, $\mu^{(\boldsymbol{\eta})}_{\boldsymbol{\eta}} = \mu^{(\boldsymbol{\beta})}_{\boldsymbol{\eta}}$ and

$$\begin{aligned}\sum_{r\in\mathbb{Z}_k} \lambda_{\boldsymbol{\alpha}+r(e_u-e_v)-e_v} &= \sum_{r\in\mathbb{Z}_k} \mu^{(\boldsymbol{\alpha}+r(e_u-e_v)-e_v)}_{\boldsymbol{\alpha}+r(e_u-e_v)-e_v}, \\ &= \sum_{r\in\mathbb{Z}_k} \mu^{(\boldsymbol{\beta})}_{\boldsymbol{\alpha}+r(e_u-e_v)-e_v} = 0\end{aligned}$$

as desired.

□

2.4 Concluding Remarks

In this chapter we have studied the behavior of the Nullstellensatz and Polynomial Calculus approach to graph k-colorability for graphs having large girth. We showed that as the girth of a non-k-colorable graph increases, the degrees of the Nullstellensatz certificates must grow as well. This was obtained by studying the structure of the principal ideals generated by polynomials in Bayer's formulation corresponding to sub-forests of the graph and applying a general technique introduced by Aleknovich and Razborov [AR03].

In the words of Aleknovich and Razborov, informally, "*everything we can infer in small degree we can also infer locally*". This is precisely what motivated our work: if a non-k-colorable graph G has a small Nullstellensatz certificate, then one should be able to detect its non-k-colorability by looking at the local structure of G. We observed that if the essential graph of monomials of low degree where forests, then it was possible to build dual Nullstellensatz Certificates in a local fashion. One of our future goals is to understand whether this sparsity property of the essential graphs can be further extended, say to essential graphs that are not trees, but other class of graphs such as bipartite.

One of the reasons why the Nullstellensatz method is appealing is that the linear systems used to find certificates of non-k-colorability using Bayer's formulation are quite sparse. In addition, computations over finite fields are possible. For instance, detecting non-3-colorability can be done by solving linear systems over $\mathbb{F}_2$. Thus, in principle, it may be possible to use methods that exploit the sparseness of the system such as Coppersmith's Block Wiedemann or Block Lanczos Methods which work on finite field algebra. Although, implementations of the Nullstellensatz method exist [Mar08a], to the best of our knowledge, an implementation using the aforementioned techniques is not available to the public.

The problem of characterizing when the Nullstellensatz method effectively certifies non-k-colorability is wide open. For the case $k = 3$, De Loera et al. [DLHMO10] obtained a characterization of all non-3-colorable graphs having degree one Nullstellensatz Certificate over $\mathbb{F}_2$. However, we do not know what classes of non-3-colorable graphs admit a degree four Nullstellensatz Certificate.

Open Problem 2.4.1. Characterize all non-3-colorable graphs whose Bayer's formulation requires a Nullstellensatz certificates of degree at most four over $\mathbb{F}_2$.

Even simpler questions like determining the size of the smallest degree of a Nullstellensatz certificate for proving the non-k-colorability of the complete graph K_{k+1} is open for general k. De Loera et al. [DMP+14] obtained computational results for K_{k+1} with $k \leqslant 10$ over fields $\mathbb{F}_q$ with $q \in \{2, 3, 5, 7\}$. We do not know the exact minimum degrees for $k \geqslant 8$.

Open Problem 2.4.2. Let p be a prime and let $k \geqslant 8$ be relatively prime to p. Find the smallest degree Nullstellensatz Certificate for proving the non-k-colorability of the complete graph K_{k+1} over $\mathbb{F}_p$.

Another interesting line of research is to study how the Nullstellensatz method behaves with respect to graph operations such as the Hajós construction and other similar operations. Recall that any $(k+1)$-critical graph G, i.e., a graph G such that $\chi(G) = k+1$, but $\chi(H) < k+1$ for every proper subgraph $H \subseteq G$, can be obtained from K_{k+1} using repeated iterations of the Hajós construction. Since the Nullstellensatz Certificates for detecting the non-k-colorability of $(k+1)$-critical graphs are not universally bounded, the following question arises.

Open Problem 2.4.3. [LLO15] Let G_1 and G_2 be $(k+1)$-critical graphs and let G constructed from G_1 and G_2 using the Hajós Construction. What is the relationship between the minimum degree Nullstellensatz certificates of G_1, G_2 and G?

Finally, it is our general belief that, if a non-k-colorable graph G has a small Nullstellensatz certificate, then one should be able to detect its non-k-colorability by looking at the local structure of the graph. Our results follow this line of reasoning by exploiting the fact that the *essential graphs* of monomials of low degree were forests for graphs of high girth to build dual certificates.

Open Problem 2.4.4. What families of graphs admit an ordering of its vertices in such a way that the *essential graphs* of monomials of low degree are forests?

In addition, it may be interesting to see if our methods can be extended to the case in which the essential graphs of monomials of low degree are not forests, but another family of graphs whose chromatic number is easy to calculate, such as bipartite graphs.

Chapter 3

Polyhedral Representations: Stable Set Polytope of Bipartite Graphs

3.1 Introduction

As discussed in the previous chapter, determining the chromatic number of a graph is one of the most important problems in graph theory, and combinatorics in general. There exist several algorithms to compute the chromatic number (in exponential time and space) using brute force, dynamic programming, or using hierarchies of systems of linear equations, among others. One of the most intuitive (and in most cases naive) way to compute lower bounds for the chromatic number of a graph is by first estimating the size of its largest clique. Certainly, if a graph has a clique of size k, then its chromatic should be at least k. However, the existence of graphs with large girth and large chromatic number makes this lower bound rather weak for general graphs. Yet, we may ask for what classes of graphs this estimate is the correct one? That is, for what classes of graphs G, its chromatic number equals the size of its maximum clique?

An answer to the above question is what we call *Perfect Graphs*. These graphs have the stronger property that for every node-induced subgraph, its chromatic and clique number are the same. They represent one of the cornerstones in combinatorics and optimization. Perfect graphs have very rich structural properties and have been in the scope of researchers for decades. For instance, it is easy to see that if G contains an induced odd cycle (called holes) or the complement of an odd cycle (called anti-holes), then G is not perfect. One of the most celebrated results in graph theory, states that this observation is tight: a graph is

perfect if and only it does not contain holes or anti-holes. Moreover, every perfect graph can be constructed from a special set of "elementary" perfect graphs, namely bipartite graphs, line graphs of bipartite graphs, their complements and the so called double-split graphs [CRST06].

Another key feature of perfect graphs, which may be a by-product of its rich structural properties, is that several hard combinatorial problems, such as graph coloring, maximum clique and maximum stable set are solvable (to arbitrary precision) in polynomial-time for perfect graphs. Moreover, for some of these problems, the only way we currently know how to solve them efficiently make use of *Semidefinite Programming*. For instance, the *Stable Set Problem*, which aims to find a maximum set (or weighted set) S of non-adjacent vertices in a graph G, i.e., a maximum size *stable set*, can be stated as an LP over the Stable Set Polytope of G denoted by STAB(G). It is often the case that this polytope has an exponential (in the size of G) number of facets, which may make such LP intractable. However, a result due to Lovász [Lov79], states that STAB(G) can be represented as a projection of a slice of the cone of positive semidefinite matrices of size $|V(G)|$, the so called *Theta Body* of G and denoted by $TH(G)$. Since optimizing over $TH(G)$ can be done (to arbitrary precision) in polynomial time, it follows that we can optimize over STAB(G) as well.

Despite these results, it is still wide open to determine whether it is possible to solve the Stable Set Problem for perfect graphs with the use of an LP based algorithm. A first step towards that goal would be to understand the following question.

Question 3.1.1. Does there exists a polynomial $p(x)$ such that for every perfect graph $G = (V, E)$, its stable set polytope is the projection of a slice of the cone $\mathbb{R}^r_+$ for some $r = O(p(|V| + |E|))$?

It is a result of Yannakakis [Yan91] that such a "lifted" representation of the stable set of perfect graphs exists when $r = |V|^{O(\log |V|)}$. That is, the question above is true if we replace the word "polynomial" with "super-polynomial". In addition, a result of Hu and Laurent [HL19], states that if the length of the decomposition into basic perfect graphs of G is not larger than d, then a lifted representation exists when $r = 4^d(|V| + |E|)$. To the best of our knowledge, these are the only general upper bounds known in the literature.

The lifted representation defined in Question 3.1.1 is called a *Polyhedral Extended Formulation* (or *Linear Extended Formulation*). The dimension r of the cone $\mathbb{R}^r_+$ defined by the extended formulation is called the size of the extension. The *extension complexity*

of a polytope P, denoted by $\text{xc}(P)$, is the smallest size of any extended formulation of P. The theory of linear extended formulations was first developed by Yannakakis in his seminal paper [Yan91]. Among other questions, this paper asked whether $\text{xc}(\text{STAB}(G))$ was polynomial in $|V| + |E|$ for any general graph G, not necessarily perfect. Interestingly, Yannankakis' question was just settled a few years ago by Fiorini et al. [FMP+15]. Not only they proved the existence of a family of graphs H_n on n vertices for which $\text{xc}(\text{STAB}(H_n)) \geqslant 1.5^{O(\sqrt{n})}$ (see also [KW15] for a short proof of this), but they showed that many well known polytopes such that the Traveling Salesman, Cut and Correlation polytopes do not admit small, i.e., tractable with respect to the size of the input graph, extended formulations.

There are still many open questions regarding tight analyses of the extension complexity of polytopes. For example, it is still wide open to determine the right regime of the extension complexity of "easier" polytopes such as the Spanning Tree Polytope (see for instance [KT18]). In a similar vein, it is still open to determine the right regime of the extension complexity of the stable set polytope of *basic* perfect graphs. For instance, it is not hard to see that the stable set polytope of a bipartite graph $G = (V, E)$ has $|V| + |E|$ facets. However, in [AFF+17], the authors showed that a linear extended formulation of size $O(|V|^2/\log|V|)$ exists. This extended formulation is constructed using the fact that every bipartite graph is the union of at most $|V|/\log|V|$ complete bipartite graphs. However, we do not know if this bound is tight. The best we know is a result in [AFF+17] which exhibits a family of bipartite graphs whose stable set polytope has extension complexity $\Omega(|V|\log|V|)$. This gap is the central topic of this chapter:

Question 3.1.2. Does there exist a family of bipartite graphs G_n with n vertices for which $\text{xc}(\text{STAB}(G_n))$ grows at a rate strictly faster than $O(n \log n)$?

The family of bipartite graphs satisfying the lower bound $\Omega(n \log n)$ are precisely the incidence graphs G_q of *Finite Projective Planes* $PG(2, q)$ of order $q = p^k$ for some prime p. These graphs are $(q + 1)$-regular, with $|V(G_q)| = 2(q^2 + q + 1)$ vertices and have the remarkable property of being (up to a constant factor) the densest graphs having no C_4 (equivalently, $K_{2,2}$) as a subgraph. In particular, G_q cannot be covered with fewer than $|E(G_q)| = (q + 1)(q^2 + q + 1) = \Omega(|V(G_q)|^{\frac{3}{2}})$ complete bipartite graphs.

It is still an open question to determine the right order of magnitude of the extension complexity of $\text{STAB}(G_q)$ for general $q \geqslant 2$ with some small exceptions. Aprile et al. [AFF+17] showed that $\text{xc}(\text{STAB}(G)) = |E(G)|$ for 3-regular bipartite graphs having no cycle of length four, hence settling the case $q = 2$. In this thesis we prove the following.

Theorem 3.1.3. *Let G be a 4-regular bipartite graph with no C_4. Then,*

$$\text{xc}(\text{STAB}(G)) \geqslant |E|. \tag{3.1.1}$$

We should point out that there exists infinite 4-regular bipartite graphs with girth at least 5. In fact, it is a result of Erdös and Sachs [ES63] the existence of families of d-regular graphs of arbitrary girth $g \geqslant 4$. Any such graph $G = (V, E)$ with these properties can be made bipartite by taking a pair of copies of V, say V_0 and V_1, and then adding edges between vertices $v_0 \in V_0, v_1 \in V_1$ if their respective vertices in G are adjacent. In addition, we show computational results showing that $\text{xc}(\text{STAB}(G_4)) \geqslant |E(G_4)|$.

Our results are far from being optimal. In fact, these bounds were first obtained by solving a large LP on a very small portion of the *slack matrix* of $\text{STAB}(G_q)$ for $q \in \{3, 4\}$. Thus, we believe there is still a lot of room for an improved bound. In fact, we conjecture the following.

Conjecture 3.1.4. *Let q be a prime power and let G_q be the incidence graph of the finite projective plane $PG(2, q)$. Then,*

$$\text{xc}(\text{STAB}(G_q)) \geqslant |E(G_q)|.$$

This chapter is organized as follows. First, we give some preliminaries and notation on linear extended formulations. Then, we review some of the current theory and connections regarding the non-negative rank of the so called clique vs. independent set matrix. Finally, we study the stable set polytopes of the incidence graphs of finite projective planes and show our main results.

3.2 Notation and Preliminaries

3.2.1 The Stable Set Problem

Throughout this chapter $G = (V, E)$ will denote a simple graph without loops or parallel edges. For a set of vertices $A \subseteq V$, we denote by $N(A)$ the set vertices not in A adjacent to some vertex in A. If $A = \{v\}$, we write $N(v) := N(\{v\})$. We say that a set of vertices A *covers* a set B if $B \subseteq N(A)$. For a pair of sets $A, B \subseteq V$, we denote by $E[A : B]$ the set of all edges that have one end point in A and the other in B.

We denote the chromatic number of G by $\chi(G)$ and its clique number of by $\omega(G)$. A set $S \subseteq V$ of vertices is called **stable** (or independent) if for every pair of vertices $u, v \in S$ we have $uv \notin E$. The maximum size of a stable set of G is called the *stability number* and it is denoted by $\alpha(G)$.

For general graphs, it is an **NP**-hard problem to compute $\chi(G)$, $\omega(G)$ or $\alpha(G)$. Regardless, one can attempt to compute $\alpha(G)$ by optimizing a linear function over the **stable set polytope** of G. This polytope is defined as

$$\mathrm{STAB}(G) := \mathrm{conv}(\{\mathbf{1}_S \in \{0,1\}^V : \ S \subseteq V \text{ is a stable set}\}).$$

Here, $\mathbf{1}_S \in \{0,1\}^V$ denotes the characteristic vector supported at the vertices of $S \subseteq V$ and $\mathrm{conv}(A)$ denotes the convex hull of a set $A \subseteq \mathbb{R}^V$, i.e., the smallest convex set containing A. The stable set polytope can be relaxed via what we call the *Fractional Stable Set* and *Clique Relaxation* polytopes defined as follows:

$$\begin{aligned} FRAC(G) &:= \{x \in \mathbb{R}^V_+ : \ x_u \leqslant 1, \ \forall u \in V; \ x_u + x_v \leqslant 1, \ \forall uv \in E\}, \\ \mathrm{QSTAB}(G) &:= \{x \in \mathbb{R}^V_+ : \ x(C) := \sum_{u \in C} x_u \leqslant 1, \ \text{for all cliques } C \subseteq V\}. \end{aligned} \tag{3.2.1}$$

Clearly, we have that

$$\mathrm{STAB}(G) \subseteq \mathrm{QSTAB}(G) \subseteq FRAC(G). \tag{3.2.2}$$

A graph $G = (V, E)$ is perfect if for every induced subgraph H of G we have that $\omega(H) = \chi(H)$. The strong perfect graph theorem states that G is perfect if and only if it does not contain holes or antiholes. Perfect graphs also satisfy the following properties.

Theorem 3.2.1. *Let $G = (V, E)$ be a graph. Then, G is perfect if and only if*

1. *(Lovász [Lov72]) every induced subgraph H of G satisfies*

$$\alpha(H) \cdot \omega(H) \geqslant |V(H)|. \tag{3.2.3}$$

2. *(Lovász [Lov72], Weak Perfect Graph Theorem) the complement graph $\bar{G}$ is perfect.*

3. *(Chvátal [Chv75])* $\mathrm{QSTAB}(G) = \mathrm{STAB}(G)$.

3.2.2 Linear Extended Formulations

Let $P = \{x \in \mathbb{R}^n : Ax \leqslant b\}$ be a polytope. A *linear extension* of P is a polyhedron $Q \subseteq \mathbb{R}^d$ and an affine map $\phi : \mathbb{R}^d \to \mathbb{R}^n$ such that $\phi(Q) = P$. The *size* of the extension is the number of facets of the polyhedron Q. The *extension complexity* of P, denoted by $\text{xc}(P)$, is the size of an extension of P of minimum size.

Lemma 3.2.2. *Let $P \subseteq \mathbb{R}^n$ be a polytope. The following are equivalent.*

1. $\text{xc}(P) \leqslant d$.
2. *There exists a full dimensional polytope $Q \subseteq \mathbb{R}^k$ with d-facets and an affine function $\phi : \mathbb{R}^k \to \mathbb{R}^n$ such that $\phi(Q) = P$.*
3. *There exists a plane $\mathcal{L} \subseteq \mathbb{R}^d$ and an affine map $\rho : \mathbb{R}^d \to \mathbb{R}^n$ such that $\rho(\mathbb{R}^d_+ \cap \mathcal{L}) = P$. In other words, P is the projection of a slice of the non-negative orthant $\mathbb{R}^d_+$.*
4. *There exist matrices $A \in \mathbb{R}^{d\times n}$, $U \in \mathbb{R}^{d\times \ell}$ and $b \in \mathbb{R}^d$ such that*
$$P = \{x \in \mathbb{R}^n : \ Ax + Uy \leqslant b \text{ for some } y \in \mathbb{R}^\ell\}.$$

As shown in the following well known results, extended formulations behave well under standard polyhedral operations.

Lemma 3.2.3. *Let $P \subseteq \mathbb{R}^n$ be a polytope.*

1. *Let $F \subseteq P$ be a face of P. Then, $\text{xc}(F) \leqslant \text{xc}(P)$.*
2. *(Polarity Extension Lemma) Suppose that $0 \in int(P)$ (so P is full-dimensional) and let $P^\circ := \{y \in \mathbb{R}^n : \ y^\top x \leqslant 1, \ \forall x \in P\}$ be the polar dual of P. Then $\text{xc}(P^\circ) = \text{xc}(P)$.*
3. *(Martin's Extension Lemma, [Mar91]) Let $\gamma \in \mathbb{R}$ be a constant and consider the polyhedron*
$$Q := \{y \in \mathbb{R}^n : y^\top x \leqslant \gamma, \ \forall x \in P\}.$$
Then, $\text{xc}(Q) \leqslant \text{xc}(P) + 1$.
4. *(Balas' Extension Lemma) Suppose that $P = \text{conv}\left(\bigcup_{i=1}^{\ell} P_i\right)$ is the convex hull of the union of polytopes $P_1, \ldots, P_\ell$. Then,*
$$\text{xc}(P) \leqslant \ell + \sum_{i=1}^{\ell} \text{xc}(P_i). \tag{3.2.4}$$

The following results will be useful later.

Lemma 3.2.4 (Fulkerson [Ful72])**.** *Let $A \in \mathbb{R}_+^{k\times n}$ be a non-negative matrix with non-zero columns and consider the pair of polyhedra*

$$P = \{x \in \mathbb{R}_+^n : Ax \leqslant \mathbf{1}\} \quad \text{and} \quad \operatorname{abk}(P) := \{y \in \mathbb{R}_+^n : y^\top x \leqslant 1,\ \forall x \in P\}.$$

The polyhedron $\operatorname{abk}(P)$ *is known as the anti-blocker of P. Let $B \in \mathbb{R}_+^{\ell\times n}$ be the matrix with the extreme points of P as its rows. Then, no column of B is the zero vector and*

$$\begin{aligned} \operatorname{abk}(P) &:= \{y \in \mathbb{R}_+^n :\ By \leqslant \mathbf{1}\}, \\ \operatorname{abk}(\operatorname{abk}(P)) &= P. \end{aligned}$$

From Martin's Extension lemma, we obtain the following.

Corollary 3.2.5. *Let P and* $\operatorname{abk}(P)$ *be as in the lemma above. Then,*

$$|\operatorname{xc}(P) - \operatorname{xc}(\operatorname{abk}(P))| \leqslant n + 1$$

3.2.3 Non-negative rank and lower bounds

Another key result of the seminal paper of Yannakakis [Yan91] is that the extension complexity of a polytope P (a purely geometric notion) is closely related to the existence of certain factorization of a particular matrix defined by P (a purely algebraic notion).

Definition 3.2.6. Let $M \in \mathbb{R}_+^{p\times q}$ be a non-negative matrix. We say that M admits a non-negative factorization of rank k if there exist matrices $U \in \mathbb{R}_+^{p\times k}$ and $W \in \mathbb{R}_+^{k\times q}$ such that $M = UW$. The non-negative rank of M, denoted by $\operatorname{rank}_+(M)$ is the smallest k for which M admits a non-negative factorization of rank k.

Let P be a polytope and consider any pair of descriptions of the form:

$$\begin{aligned} P &=: \{x \in \mathbb{R}^n : a_i^\top x \leqslant b_i,\ i \in [p]\} = \{x \in \mathbb{R}^n : Ax \leqslant b\}, \\ &=: \operatorname{conv}(v_1, \ldots, v_q). \end{aligned} \tag{3.2.5}$$

Further, let us assume that for each $i \in [p]$ there exists at least one $j \in [q]$ such that $a_i^\top v_j = b_i$. Then, the **slack matrix** associated to the above description is the $p \times q$ non-negative matrix M with coordinates

$$M_{ij} := b_i - a_i^\top v_j.$$

Theorem 3.2.7 ([Yan91]). *Let P be a polytope and let $M \in \mathbb{R}_+^{p\times q}$ be the slack matrix of P corresponding to the description (3.2.5). Then,*

$$\mathrm{xc}(P) = \mathrm{rank}_+(M).$$

The power behind this algebraic characterization of the extension complexity of a polytope is that it allows us to obtain lower bounds for the extension complexity of polytopes. For instance, we have that $\mathrm{rank}(M) \leqslant \mathrm{rank}_+(M)$ for any non-negative matrix M. Solely with this inequality, we can already say that for every graph G we have that $\mathrm{xc}(\mathrm{STAB}(G)) \geqslant |V(G)|$. However, as Example 3.2.8 below shows, this lower bound may be quite weak.

Example 3.2.8. Let $n \geqslant 2$ and let $x \in \mathbb{R}^n$ be any given vector with pairwise different entries. Consider the non-negative matrix $M \in \mathbb{R}_+^{n\times n}$ with entries $M_{ij} = (x_i - x_j)^2$. Let $x \otimes x \in \mathbb{R}^n$ be the entry-wise product of the vector x with itself i.e., $\otimes$ denotes the Hadamard Product of vectors. Notice that

$$M = (x \otimes x)\mathbf{1}^\top - 2xx^\top + \mathbf{1}(x \otimes x)^\top,$$

so the rank of M is at most three. We claim that $\mathrm{rank}_+(M) \geqslant \log(n)$. We prove this using induction on n. For $n = 2$, we have that $\mathrm{rank}_+(M) = \mathrm{rank}(M) = 2 \geqslant \log(2) = 1$. Thus, let us assume that $n > 2$ and let $M = \sum_{i=1}^r u_i v_i^\top$ be a non-negative factorization of M of rank r where $u_i \in \mathbb{R}_+^n$ and $v_i \in \mathbb{R}_+^n$. Since the diagonal of M equals zero, $\mathrm{supp}(u_i) \cap \mathrm{supp}(v_i) = \emptyset$ for every $i \in [r]$. In particular, at least one of $\mathrm{supp}(u_1)$ or $\mathrm{supp}(v_1)$ has at most $\frac{n}{2}$ elements, say $|\mathrm{supp}(u_1)| \leqslant \frac{n}{2}$. Now, consider the submatrix M' of M obtained after the removal of the rows and columns in $\mathrm{supp}(u_1)$. Notice that $\mathrm{rank}_+(M') \leqslant r - 1$ as we can remove the indices in $\mathrm{supp}(u_1)$ from the vectors $u_2, \ldots, u_r$ and $v_2, \ldots, v_r$ to obtain a factorization of M' of rank $r - 1$. Then, by our induction hypothesis

$$r - 1 \geqslant \mathrm{rank}_+(M') \geqslant \log(n/2) = \log(n) - 1.$$

Here are some simple properties of the non-negative rank of a matrix.

Lemma 3.2.9. *Let $M \in \mathbb{R}_+^{p\times q}$ be a non-negative matrix. Then,*

1. $\mathrm{rank}_+(M) = \mathrm{rank}_+(M^\top)$
2. *Suppose we can write M in block form as $M = (A, B)$, for some matrices A and B of appropriate size. Then* $\mathrm{rank}_+(M) \leqslant \mathrm{rank}_+(A) + \mathrm{rank}_+(B)$.

Lemma 3.2.10. *Let $M \in \mathbb{R}_+^{p\times q}$ be a non-negative matrix. Let* $\mathrm{cone}(M)$ *be the conic hull of the columns of M. Suppose that $a_1, \ldots, a_r \in \mathbb{R}_+^p$ are non-negative vectors such that* $\mathrm{cone}(M) \subseteq \mathrm{cone}(a_1, \ldots, a_r)$. *Then,* $\mathrm{rank}_+(M) \leqslant r$.

Proof. Let $a_1, \ldots, a_r$ be as in the statement and let $v_1, \ldots, v_q$ be the columns of M. By our assumptions, there exists non-negative values $\lambda_{ij} \geqslant 0$ such that $v_i = \sum_{j=1}^r \lambda_{ij} a_j$ for every $i \in [q]$. Hence,

$$M = \sum_{j=1}^{r} (\lambda_{1j}\ \lambda_{2j} \cdots\ \lambda_{qj})\, a_j. \tag{3.2.6}$$

The result follows. □

Corollary 3.2.11. *Let $M \in \mathbb{R}_+^{p\times q}$ be a non-negative matrix. Suppose we can write M in block form as $M = (A, B)$, for some matrices A and B such that* $\mathrm{cone}(B) \subseteq \mathrm{cone}(A)$. *Then,* $\mathrm{rank}_+(M) = \mathrm{rank}_+(A)$.

When dealing with matrices that have a rich combinatorial structure, lower bounds might be obtained by just looking at its sparsity structure.

Definition 3.2.12. A set $R \subseteq [p] \times [q]$ is called a **combinatorial rectangle** if $R = P \times Q$ for some pair of sets $P \subseteq [p]$ and $Q \subseteq [q]$. Given any set $A \subseteq [p] \times [q]$, a **rectangle cover** (of size t) is a collection of combinatorial rectangles $R_1, \ldots, R_t$ such that $A = \cup_{i\in[t]} R_i$.

For a non-negative matrix $M \in \mathbb{R}^{p\times q}$, the **rectangle covering number**, denoted by $\mathrm{rec}(M)$, is the minimum t for which the support $\mathrm{supp}(M) \subseteq [p] \times [q]$ admits a rectangle cover of size t.

Lemma 3.2.13. *Let $M \subseteq \mathbb{R}^{p\times q}$ be a non-negative matrix, then* $\mathrm{rank}_+(M) \geqslant \mathrm{rec}(M)$.

Proof. Let $M = \sum_{i=1}^r u_i v_i^\top$ be a non-negative factorization of M of rank r, where $u_i \in \mathbb{R}_+^p$ and $v_i \in \mathbb{R}_+^q$. Then,

$$\mathrm{supp}(M) = \bigcup_{i=1}^{r} \mathrm{supp}(u_i) \times \mathrm{supp}(v_i)$$

is a rectangle cover of $\mathrm{supp}(M)$. □

This technique is probably one of the most used across the literature to find lower bounds for the extension complexity of several polytopes in combinatorial optimization. For instance, one can show (see [KW15]), using this method, that the set disjointness matrix

$M \in \{0,1\}^{2^{[n]} \times 2^{[n]}}$ supported at entries $M_{A,B} := 1$ with $A \cap B = \emptyset$ has non-negative rank at least 1.5^n. Since the disjointness matrix appears as a submatrix of the slack matrix of the correlation polytope $P_{\text{corr}} := \{xx^\top : x \in \{0,1\}^n\}$, one has that $\text{xc}(P_{\text{corr}}) \geqslant 1.5^n$. Moreover, Fiorini et al. [FMP+15] showed that the correlation polytope is in fact a projection of a face of the Traveling Salesman, Cut and Stable Set polytopes of some graphs. Thus, solving an important question posed by Yannakakis in [Yan91], regarding the extension complexity of these polytopes.

We should point out that the rectangle cover does not always lead to good bounds on the non-negative rank. For instance, it is a result of [Rot14] the existence of a family of graphs on n vertices whose *Matching Polytope* has a extension complexity of at least $2^{\Omega(n)}$, yet the slack matrices of the standard formulation of the Matching Polytope admits a rectangle cover using $O(n^4)$ rectangles. In fact, in [Rot14] the following straightened version of the rectangle covering bound was used.

Lemma 3.2.14 (Hyperplane Separation Bound [BFPS15b], [Rot14])**.** *Let $M \in \mathbb{R}_+^{p \times q}$ be a non-negative matrix and let $W \in \mathbb{R}^{p \times q}$ be any matrix. Then,*

$$\text{rank}_+(M) \geqslant \frac{\langle W, M \rangle}{\|M\|_\infty \alpha} \tag{3.2.7}$$

with $\alpha := \max\{\langle W, xy^\top \rangle |\ x \in \{0,1\}^p, y \in \{0,1\}^q\}$.

Proof. Let $M = \sum_{i=1}^r u_i v_i^\top$ be a non-negative factorization of M of rank r, where $u_i \in \mathbb{R}_+^p$ and $v_i \in \mathbb{R}_+^q$. Then,

$$\langle W, M \rangle = \sum_{i=1}^r \langle W, u_i v_i^\top \rangle = \|M\|_\infty \sum_{i=1}^r \langle W, \frac{1}{\|M\|_\infty} u_i v_i^\top \rangle.$$

We claim that $\langle W, \frac{1}{\|M\|_\infty} u_i v_i^\top \rangle \leqslant \alpha$ for all $i \in [r]$. Indeed, notice that the entries of the matrix $R_i := \frac{1}{\|M\|_\infty} u_i v_i^\top$ lie in the interval $[0,1]$, and the support of R_i is precisely $\text{supp}(u_i) \times \text{supp}(v_i)$. After scaling, we may assume that $R_i = x_i y_i^\top$ for some vectors $x_i \in [0,1]^p$ and $y_i \in [0,1]^q$ in the unit cubes of $\mathbb{R}^p$ and $\mathbb{R}^q$ respectively. In particular, we can write each of these vectors as a convex combination of 0/1-vectors $x_i = \sum_{x \in \{0,1\}^p} \lambda_x x$ and $y_i = \sum_{y \in \{0,1\}^q} \mu_y y$, and write

$$R_i = \sum_{x \in \{0,1\}^p, y \in \{0,1\}^q} \lambda_x \mu_y x y^\top$$

where $\sum_{x\in\{0,1\}^p, y\in\{0,1\}^q} \lambda_x \mu_y = 1$. This implies that R_i lies in the convex hull of rank one 0/1-matrices and $\langle W, R_i\rangle \leqslant \alpha$. □

Finally, another interesting (although, often weaker) approach to find lower bounds for the rectangle covering number is using fooling sets.

Definition 3.2.15. Let M be a non-negative matrix. A set F of positive entries of the matrix M is called a **fooling set** if for every pair of entries $M_{ij}, M_{lk} \in F$ either $M_{ik} = 0$ or $M_{lj} = 0$. We denote by $\mathrm{fool}(M)$ the size of the largest fooling set of M.

Lemma 3.2.16. *We have* $\mathrm{fool}(M) \leqslant \mathrm{rec}(M)$.

Proof. Let F be a fooling set of M. Then, by the definition of fooling set, no pair of entries in F can appear in a single combinatorial rectangle of M. In particular, the size of any rectangle cover of M should be at least $|F|$. □

Computing $\mathrm{fool}(M)$ for general matrices M is an NP-hard problem [Shi13]. In addition, we have the following upper bound.

Lemma 3.2.17 ([FHLO15])**.** *For every non-negative matrix M we have*

$$\mathrm{fool}(M) \leqslant \mathrm{rank}(M)^2.$$

Proof. Let F be a fooling set of M and let M_F be the $|F| \times |F|$ submatrix of M whose diagonal are the entries $M_{s,t}$ for $(s,t) \in F$ and the rest of its entries are given by

$$M_F := (M_{ij} : (i,t), (s,j) \in F \text{ for some } s,t).$$

Then, the rank of the Hadamard product $M_F \otimes M_F^\top$ equals $|F|$. In particular,

$$|F| = \mathrm{rank}(M_F \circ M_F^\top) \leqslant \mathrm{rank}(M_F)^2 \leqslant \mathrm{rank}(M)^2.$$

□

3.2.4 Communication Protocols and Upper-bounds

Another interesting characterization of the extension complexity of a polytope comes from communication complexity. Informally, a communication protocol is an algorithm to generate a conversation between two parties, that we call Alice and Bob. In this set up, Alice is given a constraint $a_i^\top x \leqslant b_i$ of a polytope P, i.e., a row of the slack matrix M of P and Bob is given one of the points $v_j \in P$ as in the description (3.2.5) of P, i.e., a column of the slack matrix. Their objective is to determine the value $M_{ij} = b_i - a_i^\top v_j$ by sharing some information between each other. The amount of this information, called the **communication complexity** of the protocol, is often measured in bits and the goal is to minimize the number of bits shared between the parties before successfully output the value M_{ij}. The following example illustrates this concept for the stable set polytope.

Example 3.2.18. [Yannakakis [Yan91]] Let $G = (V, E)$ be graph with $|V| = n$. Suppose that Alice is given a clique $C \subseteq V$ and Bob is given a stable set $S \subseteq V$. Their objective is found out if C and S have a vertex in common.

One trivial way of doing this is for one of them to communicate to the other their set completely. For this, Alice or Bob may have to send a total of n bits (the number of cliques or the number of stable sets of G may be of the order of 2^n, so enumeration of these sets beforehand would not work either).

Instead, we can do the following. First, if C has a vertex $v \in C$ having at most $\frac{n}{2}$ neighbors, then Alice sends v to Bob. Sharing this information uses $O(\log n)$ bits. Notice that this also tells Bob that $C \subseteq N(v)$ where $|N(v)| \leqslant \frac{n}{2}$. If $v \notin S$, then Bob and Alice can eliminate all the vertices not in $N(v)$ from the graph, thus obtaining a graph with at most $\frac{n}{2}$ vertices. Similarly, if S has a vertex v with at least $\frac{n}{2}$ neighbors, then Bob can send v to Alice. This would also tell Alice that that $I \subseteq V \setminus N(v)$ and if $v \notin C$, they can eliminate at least $\frac{n}{2}$ vertices of the graph again.

Now, if all the vertices of C have degree greater than $\frac{n}{2}$ and all vertices in I have degree less than $\frac{n}{2}$, then $C \cap I = \emptyset$. So at each step of the communication they have either found a vertex in the intersection, found out that $C \cap S = \emptyset$ or have reduced the size of the graph by a factor of 2. Thus, at most $\log n$ vertices are communicated between Alice and Bob in order to know the size of $C \cap S$. Thus, in total $O(\log^2(n))$ number of bits are communicated between Alice and Bob.

♦

The relation between the complexity of a communication protocol for the slack matrix of a polytope and its linear extension complexity is stated in the theorem below.

Theorem 3.2.19 ([Yan91]). *Let P be a polytope and let M be the slack matrix defined by a formulation as in (3.2.5) of P. Suppose that there exists a (deterministic) communication protocol of complexity c that computes M. Then,* $\text{xc}(P) \leqslant 2^c$.

The following corollary is, what is to the best of our knowledge, the best upper bound to the extension complexity of stable set polytopes for perfect graphs.

Definition 3.2.20. For a graph $G = (V, E)$ the **clique vs. independence set** matrix M_G of G is the matrix whose rows are indexed by cliques $C \subseteq V$, columns are indexed by stable sets $S \subseteq V$ of G and entries are defined as

$$M_G(C, S) = |C \cap S|.$$

Corollary 3.2.21 ([Yan91]). *Let $G = (V, E)$ be a graph with n vertices and let M_G be its clique vs. independence set matrix. Then,*

$$\text{rank}_+(M_G) \leqslant n^{O(\log n)}. \tag{3.2.8}$$

In particular, if G is perfect then $\text{xc}(\text{STAB}(G)) \leqslant n^{O(\log n)}$.

Proof. We showed in Example 3.2.18 that there exists a (deterministic) communication protocol using at most $O(\log^2 n)$ bits for the clique vs. independent set matrix M_G. Thus, $\text{rank}_+(M_G) \leqslant n^{O(\log n)}$. Finally, if G is perfect, its stable set polytope can be written as

$$\text{STAB}(G) = \{x \in \mathbb{R}^V_+ : x(C) \leqslant 1,\ \forall C \subseteq V \text{ clique}\}.$$

Let SM be the portion of the slack matrix corresponding to the clique inequalities. Then, for every clique C and every stable set S, we have that

$$SM_{C,S} = 1 - \mathbf{1}_S(C) = 1 - |C \cap S| = 1 - M_G(C, S).$$

Hence, any (deterministic) communication protocol for M_G can be used for SM. In particular, $rank_+(SM) \leqslant n^{O(\log n)}$ and the result follows. □

For general graphs, a result of Mika Göös (see [GÏ15]) states that Yannakakis' bound cannot be replaced by a polynomial bound. More concretely, he proved the existence of a family of graphs $\{G_n\}_{n\geqslant 1}$ on n vertices satisfying

$$\operatorname{rank}_+(M_{G_n}) \geqslant n^{\Omega(\log^{0.128} n)}.$$

Informally, the bound is obtained by constructing a function, via repeated composition of a gadget, that exposes a large enough gap between a pair of complexity classes called the *co-non-deterministic* and *unambiguous query complexity* (see [GÏ15] for details).

The problem of determining whether Yannakakis' bound is tight for perfect graphs is still wide open. There exist upper bounds for some special classes of perfect graphs. For instance, $\operatorname{STAB}(G)$ admits a representation whose slack matrix has $|V|+|\mathcal{C}|$ rows, where $\mathcal{C}$ is the set of maximal cliques of G. Hence, if G is perfect and $|\mathcal{C}|$ is polynomial in $|V|$, then $\operatorname{xc}(\operatorname{STAB}(G))$ is polynomial. This is the case for bipartite graphs (having at most $|V|^2$ cliques), chordal graphs (having at most $|V|$ maximal cliques), complete graphs K_n and their complements $\overline{K_n}$. The stable set polytope of line graphs of bipartite graphs, double-split graphs and their complements all admit a linear extension of size $|V|+|E|$. Every perfect graph admits a decomposition into these "basic" perfect graphs by some graph operations, namely 2-joins and skew partitions (see [CRST06]). Hu and Laurent [HL19] showed that these graph operations increase the extension complexity of the resulting graph up to a factor of four, thus an upper bound of $4^d(|V|+|E|)$ is obtained for all perfect graphs that admit a decomposition of length d into basic perfect graphs.

It is possible to use communication protocol techniques to find upper bounds for other classes of perfect graphs. For instance, if $\omega(G)$ is small, then Alice can communicate to Bob the whole clique C given to her using at most $\omega(G)\log n$ bits. Thus, $\operatorname{xc}(\operatorname{STAB}(G)) \leqslant n^{\omega(G)}$. Another interesting example comes from claw-free perfect graphs (see [FFGT15]), that is, perfect graphs without having an induced $K_{1,3}$. Indeed, if Alice is given a clique C, she picks a vertex $v \in C$ and sends it to Bob, this uses at most $\log n$ bits. Then, Bob gathers all the vertices in the given stable set S that are adjacent to v and send those to Alice. There are at most two of these vertices as G is claw-free, hence it takes at most $2\log n$ to communicate these to Alice. At this stage Alice knows $|C\cap S|$ and outputs this value. This shows that $\operatorname{xc}(\operatorname{STAB}(G)) \leqslant O(n^3)$ for claw-free perfect graphs. Clearly, the same technique shows that perfect graphs G without an induced $K_{1,r}$ satisfy $\operatorname{xc}(\operatorname{STAB}(G)) \leqslant O(n^r)$.

Despite the fact that several upper and lower bounds for the extension complexity of stable sets of perfect graphs have been established, there is still little knowledge on the exact order of magnitude of the size of their optimal polyhedral extension. Even for

simple sub-classes of perfect graphs, such as bipartite graphs or any other basic perfect graph, we do not know the right order of magnitude of their extensions. It is the hope that understanding simple sub-classes of perfect graphs will allow us to better understand key open questions in the area, such as Yannakakis' Question 3.1.1. This is precisely the objective of the next section.

3.3 Stable Sets of Bipartite Graphs

Throughout this section $G = (V, E)$ will denote a connected bipartite graph with bipartition $V = U \cup W$. In addition, we write $n := |V|$ and $m := |E|$ to denote the sizes of the vertex and edge sets of G. By Theorem 3.2.1, we know that $\text{STAB}(G) = FRAC(G)$ and

$$n \leqslant \text{xc}(\text{STAB}(G)) \leqslant n + m. \tag{3.3.1}$$

These bounds can be improved considerably. Aprile et al. [AFF+17] showed that the upper bound can be improved to $O\left(\frac{n^2}{\log(n)}\right)$. In addition, they provided an infinite family of bipartite graphs, namely the incidence graphs of finite projective planes, satisfying

$$\text{xc}(\text{STAB}(G)) = \Omega(n \log n). \tag{3.3.2}$$

It is open to determine the right regime of the extension complexity of stable set polytopes for bipartite graphs. The goal of this section is to study this problem with some more detail. Since the techniques and terminology used in our results are inspired by the results in [AFF+17], in Sections 3.3.1 and 3.3.2 below we reproduce Aprile et al. bounds. Then, in Section 3.3.3 we prove our bounds for the 4-regular case and in Section 3.3.4 we show some computational results for the incidence graphs of the projective plane of order four.

3.3.1 Upper bound: Biclique Coverings and the Edge Polytope

The upper bound is proven in two steps. First, consider the edge polytope of G which is defined as

$$\begin{aligned} P_{edge}(G) &= \text{conv}(\mathbf{1}_u + \mathbf{1}_v : uv \in E), \\ &= \left\{ x \in \mathbb{R}^n_+ : \begin{array}{rl} x(V) = 2, & \\ x(S) - x(N(S)) \leqslant 0, & S \subseteq V \text{ stable} \end{array} \right\}. \end{aligned} \tag{3.3.3}$$

Since G has no isolated vertices, then

$$\begin{aligned} \mathrm{STAB}(G) &= \mathbb{R}^n_+ \cap \{x \in \mathbb{R}^n : y^\top x \leqslant 1,\ \forall y \in P_{edge}(G)\}, \\ &= \mathrm{abk}(P_{edge}(G)). \end{aligned} \tag{3.3.4}$$

In particular, by Martin's Extension Lemma (see Lemma 3.2.3), we have that

$$\mathrm{xc}(\mathrm{STAB}(G)) \leqslant n + 1 + \mathrm{xc}(P_{edge}(G)). \tag{3.3.5}$$

Thus, it is enough to find upper bounds for the extension complexity of $P_{edge}(G)$. Now, notice that if G is the union of graphs $H_1, \ldots, H_\ell$, then $P_{edge}(G) = \mathrm{conv}(\cup_i P_{edge}(H_i))$ and by Balas' Extension Lemma (see Lemma 3.2.3) $\mathrm{xc}(P_{edge}(G)) \leqslant \ell + \sum_i \mathrm{xc}(P_{edge}(H_i))$. Therefore, it is possible to beat the quadratic bound on $\mathrm{STAB}(G)$ if we manage to find a sub-quadratic covering of G using graphs with small extension complexity. The following result, due to Tuza [Tuz84], shows one of such coverings.

Theorem 3.3.1 ([Tuz84])**.** *Let $G = (V, E)$ be a bipartite graph. Then, there exist a family $\{H_i\}_{i \leqslant t}$ of complete bipartite subgraphs of G such that $E = \cup_{i \leqslant t} E(H_i)$ and*

$$t = O\left(\frac{n}{\log n}\right)$$

Corollary 3.3.2 ([AFF+17])**.** *Let G be a bipartite graph. Then,* $\mathrm{xc}(\mathrm{STAB}(G)) = O\left(\frac{n^2}{\log(n)}\right)$.

Proof. By Tuza's theorem, G can be covered with t complete bipartite graphs for some $t = O(n/\log n)$. Now, it is not hard to see that for a complete bipartite graph $K_{a,b}$ we have $\mathrm{xc}(P_{edge}(K_{a,b})) \leqslant a + b$. Indeed, we have that

$$P_{edge}(K_{a,b}) = \left\{ x \in \mathbb{R}^{a+b}_+ : \begin{array}{l} x([a]) + x([b]) = 2, \\ x([a]) - x([b]) = 0 \end{array} \right\}. \tag{3.3.6}$$

In particular, by Balas' Extension Lemma, we have

$$\mathrm{xc}(\mathrm{STAB}(G)) \leqslant n + 1 + t + tn = O\left(\frac{n^2}{\log n}\right). \tag{3.3.7}$$

□

Using a counting argument, Tuza (see [Tuz84]) showed the existence of bipartite graphs $G = (V, E)$ with bipartition $V = U \cup W$ satisfying:

1. $|U| = |W|$,
2. $|E| \geqslant \frac{|U|^2}{4}$,
3. G has no $K_{r,r}$ for $r = \lceil \log(|U|) \rceil$.

In particular, a biclique covering of such graphs has size $\Omega(n/\log(n))$. Thus, a natural idea would be to study the extension complexity of the stable set polytope of these graphs. In fact, Aprile et al. [AFF+17] lower bound is obtained from bipartite graphs with no $K_{2,2}$, i.e., cycles C_4 of length 4, which we study in the following sections.

3.3.2 Lower bounds: Finite Projective Planes

Throughout this section we denote by M_G the portion of the slack matrix of STAB(G) corresponding to the cliques of G. Then, the rows of M_G are indexed by edges $uv \in E$ and the columns by stable sets $S \subseteq V$, where $M_G(uv, S) = 1$ if and only if neither u nor v appear in S. First, let us show a simple characterization of maximal combinatorial rectangles of the matrix M_G.

Definition 3.3.3. Let $A \subseteq U$ and $B \subseteq W$ be any pair of subsets of vertices of G. Then, $R_{A,B}$ is the *combinatorial rectangle* of M_G whose rows are the set of edges $E[A : B]$ and columns are the stable sets $S \subseteq V \setminus (A \cup B)$.

Lemma 3.3.4. *Let R be a maximal combinatorial rectangle of M_G. Then, there exist $A \subseteq U$ and $B \subseteq N(A) \subseteq W$ such that $R = R_{A,B}$.*

Proof. Suppose that $R = \{1\}^{F \times \mathcal{S}}$ for some set of edges $F \subseteq E$ and some collection of stable sets $\mathcal{S}$ of G. Let $A := F \cap U$ and $B := F \cap W \subseteq N(A)$ be the end-points of the edges in F. We claim that $R = R_{A,B}$. Indeed, by definition of the sets A and B, any row of R is contained in $E[A : B]$. Similarly, any stable set $S \in \mathcal{S}$ satisfies $S \subseteq V \setminus (A \cup B)$. Hence, R is a sub-rectangle of $R_{A,B}$. Since R is maximal, the result follows. □

One common technique to obtain rectangle covering bounds is to find a set of weights $w_{(uv,S)}$ for entries (uv, S) in the support of the matrix M_G in such a way that the sum

$w(R) := \sum_{(uv,S)\in R} w_{(uv,S)}$ is at most one for every combinatorial rectangle R of M_G. Then, it follows that

$$w(M_G) := \sum_{(uv,S)\in M_G} w_{(uv,S)} \leqslant \mathrm{rec}(M_G). \tag{3.3.8}$$

In other words, we can always lower bound the rectangle covering number of M_G with the following linear programming problem:

$$\begin{aligned} \max \quad & \sum_{(uv,S)\in M_G} w_{(uv,S)}, \\ s.t. \quad & \sum_{uv\in E[A:B]} \sum_{\substack{S \text{ stable}, \\ S\cap A = S\cap B = \emptyset}} w_{(uv,S)} \leqslant 1, \quad \forall A \subseteq U, B \subseteq N(A), \end{aligned} \tag{3.3.9}$$

Clearly, this linear program may be hard to solve as the number of maximal rectangles in M_G might be exponential in $|V|$, in the worst case. However, we may be able to reduce the size of this program by using symmetries of the graph G (see sections below). Also, notice that this technique can be obtained from the Hyperplane Separation Bound (Lemma 3.2.14) if we set very large negative weights $w_{(uv,S)}$ for every entry (uv, S) outside the support of M_G.

Example 3.3.5. In order to illustrate this technique, let us show that $\mathrm{rank}_+(M_{K_{p,q}}) = p+q$. The upper bound can be obtained by analyzing the block structure of $K_{p,q}$. Indeed, let us first identify the edges of $K_{p,q}$ as all pairs $(i, j) \in [p] \times [q]$. The stable sets of $K_{p,q}$ must be contained in exactly one of its partitions, so we write these as $(S, \emptyset)$ or $(\emptyset, T)$ for some $S \subseteq [p]$ and $T \subseteq [q]$. Then, for each $i \in [p]$ the submatrix with rows (i, j) has the following form:

	$(S,\emptyset) : i \notin S$			$(S,\emptyset) :\ i \in S$			$(\emptyset,T) :\ T \subseteq [q]$
$(i,1)$	1	$\cdots$	1	0	$\cdots$	0	
$(i,2)$	1	$\cdots$	1	0	$\cdots$	0	
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	A
$(i,q-1)$	1	$\cdots$	1	0	$\cdots$	0	
(i,q)	1	$\cdots$	1	0	$\cdots$	0	

for some matrix A not depending on i. In fact, we can decompose A as

$$A = \begin{array}{c|c|cccccc} (\emptyset, T): & |T| \leqslant q-2 & [q]\setminus\{1\} & [q]\setminus\{2\} & \cdots & [q]\setminus\{q\} & [q] \\ \hline (i,1) & & 1 & 0 & \cdots & 0 & 0 \\ (i,2) & A' & 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots & \vdots \\ (i,q) & & 0 & 0 & \cdots & 1 & 0 \end{array}$$

Thus, the non-negative rank of A is q. This shows that $M_{K_{p,q}}$ admits the block decomposition

$$M_{K_{p,q}} = \begin{pmatrix} A_1 & A \\ \vdots & \vdots \\ A_p & A \end{pmatrix} \tag{3.3.10}$$

for some matrices A_i with non-negative rank equal to one and some matrix A with non-negative rank equal to q. In particular,

$$\begin{aligned} \operatorname{rank}_+(M_{K_{p,q}}) &\leqslant \operatorname{rank}_+\left((A_1 \ \cdots A_p)\right) + \operatorname{rank}_+\left((A \ \cdots A)\right), \\ &\leqslant \sum_{i=1}^{n} \operatorname{rank}_+(A_i) + \operatorname{rank}_+(A) = p+q. \end{aligned} \tag{3.3.11}$$

Now, for the lower bound consider weights $w_{(ij,[p]\setminus\{i\})} := \frac{1}{q}$ and $w_{(ij,[q]\setminus\{j\})} := \frac{1}{p}$ for every $ij \in E$, and $w_{(ij,S)} := 0$ otherwise. Let $A \subseteq [p]$, $B \subseteq [q]$ and let $R_{A,B}$ be a maximal rectangle of $M_{K_{p,q}}$. If $\min\{|A|, |B|\} \geqslant 2$, then $w(R_{A,B}) = 0$ as such rectangle won't contain columns corresponding to stable sets of size $p-1$ or $q-1$. Thus, without loss of generality, we may assume that $A = \{i\}$ for some $i \in [p]$ (the case $B = \{j\}$ is similar). Then,

$$w(R_{\{i\},B}) = \begin{cases} \frac{1}{q} + \frac{1}{p}, & \text{if } |B| = 1, \\ \frac{|B|}{q}, & \text{otherwise.} \end{cases}$$

This shows that $w(R_{A,B}) \leqslant 1$ for every maximal rectangle $R_{A,B}$. Moreover,

$$w(M_G) = \sum_{ij \in E} w(R_{\{i\},\{j\}}) = |E| \left(\frac{1}{p} + \frac{1}{q}\right) = p+q.$$

♦

Finally, let us reproduce the proof of the lower bound given by Aprile et al. [AFF+17]. We should point out that this result was stated for a particular class of graphs, but the result applies for all regular bipartite graphs without a C_4. The following technical lemma will be needed.

Lemma 3.3.6. *Let x, y and z be non-negative integers.*

1. *Suppose that $x \leqslant y$. Then,*
$$\sum_{\ell=x}^{y} \binom{\ell}{x} = \binom{y+1}{x+1}. \tag{3.3.12}$$

2. *Suppose that x, y and z are positive. Then,*
$$\sum_{\ell=0}^{z} \binom{x+\ell}{\ell}\binom{z+y-\ell}{z-\ell} = \binom{x+y+z+1}{z}. \tag{3.3.13}$$

3. *Suppose that $y \leqslant z$, then*
$$\frac{y}{z}\sum_{k=1}^{z-y} \frac{\binom{z-y}{k}}{\binom{z-1}{k}} = \frac{z-y}{z}. \tag{3.3.14}$$

4. *Suppose that $x + y \leqslant z$, then*
$$\frac{y}{z}\sum_{k=1}^{z-y-x} \frac{\binom{z-y-x}{k}}{(k+x)\binom{z-1}{k+x}} = \frac{1}{z}\binom{x+y-1}{y}^{-1}. \tag{3.3.15}$$

We defer the proof of this lemma to Appendix B.1.

Theorem 3.3.7 (Aprile et al. [AFF+17] (re-stated))**.** *Let $G = (U \cup W, E)$ be a d-regular bipartite graph without a C_4. Then,*

$$\mathrm{xc}(\mathrm{STAB}(G)) = \Omega(n \ln d).$$

Proof. We say that an entry (uv, S) in the support of M_G is *special* if there exists some $X \subseteq N(v)$ such that $S = S(X) := X \cup (W \setminus N(X))$. Now, define the weight of a special entry $(uv, S(X))$ as

$$w(uv, S(X)) := \frac{1}{d|X|\binom{d-1}{|X|}}. \tag{3.3.16}$$

Set the weights $w_{(uv,S)}$ of any other entry (uv, S) in the support of M_G to be equal to zero. We claim that $w(R_{A,B})$ is at most one for every maximal rectangle $R_{A,B}$. Indeed, first suppose that $B = \{v\}$ for some $v \in W$. Then, a special entry $(uv, S(X))$ is covered by the rectangle $R_{A,B}$ if and only if $X \subseteq N(v) \setminus A$. Suppose that $|A \cap N(v)| = t$ so that the total cost of the special entries in $R_{A,B}$ equals:

$$\begin{aligned} w(R_{A,B}) &= t \sum_{k=1}^{d-t} \binom{d-t}{k} \frac{1}{(dk)\binom{d-1}{k}} \leqslant t \sum_{k=1}^{d-t} \binom{d-t}{k} \frac{1}{d\binom{d-1}{k}}, \\ &= \frac{d-t}{d} < 1. \end{aligned}$$

The last inequality follows from Lemma 3.3.6 part 3. Now, suppose that the rectangle $R_{A,B}$ satisfies $|B| \geqslant 2$. Let $v \in B$ be fixed and let us calculate the number of special entries in $R_{A,B}$ of the form $(uv, S(X))$. Since G has no C_4, then the number of common neighbors of any pair of vertices in B is at most one. In particular, if a set $X \subseteq N(u)$ satisfies $B \subseteq N(X)$, then X must contain the set X_v of all unique common neighbors of v and each $v' \in B \setminus \{v\}$. Let $k_v := |X_v|$ so that

$$\begin{aligned} \sum_{u \in N(v) \cap A} \sum_{X \subseteq N(v) \setminus (A \cup X_v)} w(uv, S(X)) &= t \sum_{k=0}^{d-t-k_v} \binom{d-t-k_v}{k} \frac{1}{d(k+k_v)\binom{d-1}{k+k_v}}, \\ &= \frac{1}{d} \binom{t+k_v-1}{t}^{-1} \leqslant \frac{1}{dk_v}. \end{aligned}$$

The last equation follows from Lemma 3.3.6 part 4. Notice that, by the regularity of G, the inclusion $B \subseteq N(X_v)$ implies that $|B| \leqslant dk_v$ for every $v \in B$. Thus, if we sum the above over all vertices $v \in B$, we obtain

$$w(R_{A,B}) \leqslant \sum_{v \in B} \frac{1}{dk_v} = \sum_{v \in B} \frac{1}{|B|} \frac{|B|}{dk_v} \leqslant 1. \tag{3.3.17}$$

It only remains to count the total weight of all the special entries in M_G. This is equal to

$$\begin{aligned} w(M_G) &= \sum_{uw \in E} \sum_{k=1}^{d-1} \binom{d-1}{k} \frac{1}{(dk)\binom{d-1}{k}}, \\ &= \frac{|E|}{d} \sum_{k=1}^{d-1} \frac{1}{k} \geqslant \frac{|V|}{2} \int_1^d \frac{1}{x}\, dx = \frac{|V|}{2} \ln d. \end{aligned}$$

The result follows. □

From the above theorem, the largest possible lower bound is obtained for regular bipartite graphs having the largest number of edges, but not having a C_4. A result by Reiman [Rei58] states that any bipartite graph with no C_4 satisfies

$$|E| \leqslant \frac{n}{4}(1+\sqrt{4n-3}). \tag{3.3.18}$$

It turns out that this upper bound is asymptotically correct and it is attained by the incidence graph of **finite projective planes**.

Definition 3.3.8 (See [Bae52])**.** Let q be a prime power. The *finite projective plane* $\mathrm{PG}(2,q)$ is the pair $(\mathcal{P},\mathcal{L})$ consisting of a set of points $\mathcal{P}$ and lines $\mathcal{L}$ such that:

1. every pair of points $p,p' \in \mathcal{P}$ pass through a unique line $\ell \in \mathcal{L}$,
2. every pair of lines $\ell,\ell' \in \mathcal{L}$ intersect in exactly one point,
3. there exist four points such that no line passes through more than two of them, and
4. every line $\ell \in \mathcal{L}$ contains exactly $q+1$ points.

The *incidence graph* of the plane $\mathrm{PG}(2,q)$, which we denote by G_q, is the bipartite graph with vertex set $\mathcal{P}\cup\mathcal{L}$ and edges (p,ℓ) for every $p\in\mathcal{P}$, $\ell\in\mathcal{L}$ satisfying $p\in\ell$. Every plane $\mathrm{PG}(2,q)$ satisfies that $|\mathcal{L}| = |\mathcal{P}| = q^2+q+1$, hence by the $(q+1)$-regularity of G_q, we have that

$$\begin{aligned} |V(G_q)| &= 2(q^2+q+1), \\ |E(G_q)| &= (q+1)(q^2+q+1). \end{aligned}$$

Corollary 3.3.9. *Let G_q be the incidence graph of the finite projective plane $\mathrm{PG}(2,q)$ and let $n = |V(G_q)|$, then*

$$\mathrm{xc}(\mathrm{STAB}(G_q)) = \Omega(n\ln n). \tag{3.3.19}$$

3.3.3 4-regular bipartite graphs

As stated in the previous sections it is still an open question to determine whether Aprile et al. bounds are tight. In order to further understand this problem, it is a good idea to study the case when G is a d-regular bipartite graph with no C_4 for small d. The case

$d = 3$ was already settled by Aprile et al. [AFF+17] by exposing a fooling set of size $|E|$ in M_G, whence proving that $\text{rank}_+(M_G) = |E|$. In this section, we settle the case $d = 4$ and in the following section we show computational results for the projective plane of order 4 (a special case of $d = 5$).

It is important to point out that there exist infinite families of d-regular graphs having no C_4 for any fixed $d \geqslant 2$. In fact, we have the following classical result due to Erdös and Sachs.

Theorem 3.3.10 (Erdös-Sachs [ES63])**.** *Let $d \geqslant 2$, $g \geqslant 4$, $n \geqslant 2\sum_{t=1}^{g-2}(d-1)^t$. Then, there exists a d-regular graph with $2n$ vertices and girth at least g.*

Note that a C_4-free d-regular graph $G = (V, E)$ can be easily transformed into a C_4-free d-regular bipartite graph. Indeed, we simply make a pair of copies V_1 and V_2 of V, then we add an edge between vertices $v_1 \in V_1$ and $v_2 \in V_2$ if their respective copies in V are adjacent.

Throughout the rest of this section, $G = (U \cup W, E)$ will denote a d-regular C_4-free bipartite graph with $d \geqslant 3$. In addition, for a set $X \subseteq U$ we let $S(X) := X \cup W \setminus N(X)$ be the maximal stable set generated by X. Recall that an entry $(uv, S(X))$ is in a rectangle $R_{A,B}$ if and only if $X \cap A = \emptyset$ and $B \subseteq N(X)$. The main goal of this section is to prove the following theorem.

Theorem 3.3.11. *Let $G = (V, E)$ be a d-regular bipartite graph with no C_4. If $d \geqslant 4$, then*

$$\text{rank}_+(M_G) \geqslant \begin{cases} \left(\frac{(d-1)(2d^2-3d)}{2w_2(d)} + \frac{1}{d}\right)|E|, & \text{if } d \geqslant 5, \\ |E|, & \text{if } d = 4. \end{cases} \tag{3.3.20}$$

where

$$w_2(d) := \begin{cases} \frac{1}{16}(4d^4 - 7d^3 + 2d^2) + 1 = 39 & \text{if } d = 4, \\ \frac{1}{16}(4d^4 - 7d^3 - d^2 + 7d - 3) & \text{if } d \geqslant 5 \text{ is odd}, \\ \frac{1}{16}(4d^4 - 7d^3 + 2d^2) & \text{if } d \geqslant 6 \text{ is even}. \end{cases} \tag{3.3.21}$$

Remark 3.3.12. Notice that, for large d, the bounds produced by Theorem 3.3.11 are of order $O\left(\frac{1}{d}|E|\right) = O(n)$, which are significantly weaker than the bounds $\Omega\left(\frac{\log d}{d}|E|\right) = \Omega(n \log d)$ produced by Aprile et al. in Theorem 3.3.7.

The idea behind the proof of this theorem is quite simple. This time, the set of special entries that we will consider are entries of the form $(uv, S(X))$ with $|X| = 2$ and X not too

far from u, i.e., $X \subseteq N(N(u))$. We will show that the rectangles $R_{A,B}$ having the largest number of special entries are those satisfying $B = \{v\}$ and $A \subseteq N(v)$ with $|A| = \lceil |N(v)|/2 \rceil$ for some $v \in W$. This, with the exception of the case $d = 4$, for which a small correction is needed.

In order to prove Theorem 3.3.11, we will show that the number of special entries in a rectangle $R_{A,B}$ of the form $B = \{v\}$ and $A \subseteq N(v)$ with $|A| = t$ is equal to

$$f(t) := \frac{1}{2}t(d-t)(2d^2 - 3d + 1 - t). \tag{3.3.22}$$

Some technical inequalities regarding f will be needed. The proof of Lemma 3.3.13 below can be found in Appendix B.2.

Lemma 3.3.13. *Let $d \geqslant 4$, consider the function $f(x) := \frac{1}{2}x(d-x)(2d^2-3d+1-x)$ and let $t^* := \operatorname{argmax}\{f(t) : t \in [0,d] \text{ integer}\}$. Then,*

1. *$t^* = \lfloor \frac{d}{2} \rfloor$ and*

$$f(t^*) = \begin{cases} \frac{1}{16}(4d^4 - 7d^3 - d^2 + 7d - 3) & \text{if } d \text{ is odd,} \\ \frac{1}{16}(4d^4 - 7d^3 + 2d^2) & \text{if } d \text{ is even.} \end{cases} \tag{3.3.23}$$

2. *If $d \geqslant 5$, then*

$$(d^2 - d + 1)(d-1) \leqslant f(t^*). \tag{3.3.24}$$

If $d = 4$, then

$$(d^2 - d + 1)(d-1) = f(t^*) + 1. \tag{3.3.25}$$

In particular, for $d \geqslant 4$

$$(d^2 - 2d + 1)(d-1) \leqslant f(t^*). \tag{3.3.26}$$

3. *For $d \geqslant 4$ we have*

$$\max\left\{ \left(\frac{3}{2}d\right)^2, \left(\frac{2}{3}d\right)^3, \frac{(d+1)^2(d-1)^2}{8}, \left(\frac{d^2-d-1}{2}\right)^2 \right\} \leqslant f(t^*). \tag{3.3.27}$$

Lemma 3.3.14. *Let $R_{A,B}$ be a maximal rectangle and let $w(R_{A,B})$ be the number of entries $(uv, S(X))$ in $R_{A,B}$ such that $X \subseteq N(N(u)) \setminus \{u\}$, $v \in N(X)$ and X has size $|X| = 2$. Then,*

$$w(R_{A,B}) \leqslant w_2(d) := \begin{cases} \frac{1}{16}(4d^4 - 7d^3 + 2d^2) + 1 = 39 & \text{if } d = 4, \\ \frac{1}{16}(4d^4 - 7d^3 - d^2 + 7d - 3) & \text{if } d \geqslant 5 \text{ is odd,} \\ \frac{1}{16}(4d^4 - 7d^3 + 2d^2) & \text{if } d \geqslant 6 \text{ is even.} \end{cases} \tag{3.3.28}$$

Proof. Let us call an entry $(uv, S(X))$ in the support of M_G special if $X \subseteq N(N(u)) \setminus \{u\}$, $v \in N(X)$ and X has size $|X| = 2$. Our goal is to compute the number of special entries in a maximal rectangle $R_{A,B}$. If $R_{A,B}$ has at least one special entry, then there exists a pair of vertices $u', u'' \in U \setminus A$ such that $B \subseteq N(u') \cup N(u'')$, i.e.,$u'$ and u' *cover* B. Thus, let us choose u' and u'' such that $B \subseteq N(u') \cup N(u'')$ and $\alpha := \max\{|N(u') \cap B|, |N(u'') \cap B|\}$ is as large as possible. We consider the following cases:

1. Suppose that $\alpha \geqslant 3$ and let $u^* \in U$ such that $B_1 := N(u^*) \cap B$ has at least three vertices. Since G has no C_4, any special entry $(uv, S(X))$ in $R_{A,B}$ satisfies $u^* \in X$. Indeed, if a pair of vertices u', u'' covers B, then either $|N(u') \cap B_1| \geqslant 2$ or $|N(u'') \cap B_1| \geqslant 2$. Since no pair of vertices in G have two or more common neighbors, we must have $u^* \in \{u', u''\}$.

   Let $B_2 := B \setminus B_1$. We consider three scenarios.

   (a) If $|B_2| \geqslant 2$, then there exists at most one $u^{**} \in U$ such that $B_2 \subseteq N(u^{**})$. In this case, any special entry $(uv, S(X))$ in $R_{A,B}$ must satisfy $X = \{u^*, u^{**}\}$. It follows that the number of special entries is at most

   $$\begin{aligned} |E[A : B]| \leqslant (d-1) \cdot |B| &= (d-1)(|B_1| + |B_2|), \\ &\leqslant (2d)(d-1), \\ &\leqslant (d^2 - 2d + 1)(d-1). \end{aligned} \tag{3.3.29}$$

   Let $f(x) := \frac{1}{2}x(d-x)(2d^2 - 3d + 1 - x)$ and let $t^* := \text{argmax}\{f(t) : t \in [0, d] \text{ integer}\}$. By Lemma 3.3.13 part 2, $(d^2 - 2d + 1)(d-1) \leqslant f(t^*)$.

   (b) If $B_2 = \{v^*\}$, then there is at most $d - |N(v^*) \cap A|$ choices for a vertex $u^{**} \notin A$ satisfying $B_2 \subseteq N(u^{**})$. Let $t := |N(v^*) \cap A|$ so that the number of special entries in $R_{A,B}$ is at most

   $$\begin{aligned} |E[A : B]| \cdot (d-t) &\leqslant ((d-1)|B_1| + t) \cdot (d-t), \\ &\leqslant ((d-1)d + t) \cdot (d-t), \\ &\leqslant (d(d-1) + 1) \cdot (d-1), \\ &= (d^2 - d + 1) \cdot (d-1). \end{aligned} \tag{3.3.30}$$

   This last inequality follows from the fact that the function $g(t) := ((d-1)d + t) \cdot (d-t)$ decreases for non-negative t and in our set-up $t := |N(v^*) \cap A| \geqslant 1$.

By Lemma 3.3.13 part 2

$$\begin{aligned} (d^2-d+1)\cdot(d-1) &\leqslant f(t^*) && \text{if } d \geqslant 5, \\ (d^2-d+1)\cdot(d-1) &= f(t^*)+1 && \text{if } d = 4. \end{aligned} \tag{3.3.31}$$

If v^* has a common neighbor with all the vertices in B_1, we can improve the above bound a little. Indeed, let B_{10} be the vertices in $v \in B_1$ such that $|N(v) \cap N(v^*) \cap A| = 0$ and let $B_{11} = B_1 \setminus B_{10}$. Then,

$$\begin{aligned} |E[A:B]| &\leqslant (d-2)|B_{10}| + (d-1)|B_{11}|, \\ &\leqslant (d-2)(d-t) + (d-1)t, \\ &= d^2 - 2d + t. \end{aligned}$$

Thus, the number of special entries in $R_{A,B}$ is at most

$$\begin{aligned} |E[A:B]| \cdot (d-t) &\leqslant ((d^2-2d+t)\cdot(d-t), \\ &= (d^2-2d+1)\cdot(d-1) \leqslant f(t^*). \end{aligned} \tag{3.3.32}$$

(c) If $B_2 = \emptyset$, then for every $uv \in E[A:B]$ and any $X := \{u^*, u^{**}\} \subseteq N(N(u)) \setminus A$ the special entry $(uv, S(X))$ is in $R_{A,B}$. Now, for every pair of vertices $v', v'' \in N(u)$ we have $N(v') \cap N(v'') = \{u\}$, hence $|N(N(u)) \setminus \{u\}| = d(d-1)$. Thus, we have at most $d^2 - d - 1 - |A|$ choices for $u^{**} \in X$. The total number of special entries in $R_{A,B}$ is at most

$$\begin{aligned} E[A:B](d^2-d-1-|A|) &= |A|(d^2-d-1-|A|), \\ &\leqslant \left(\frac{d^2-d-1}{2}\right)^2. \end{aligned} \tag{3.3.33}$$

By Lemma 3.3.13 part 3, $\left(\frac{d^2-d-1}{2}\right)^2 \leqslant f(t^*)$.

2. Suppose that $\alpha = 2$, so that $|B| \leqslant 4$ and there exists at least a pair of vertices in B, say v^* and v^{**} that are adjacent to a vertex $u^* \in U$. Thus, let $B_1 := B \cap N(u^*)$, $B_2 := B \setminus B_1$. We consider the following cases:

   (a) Suppose that $|B_2| = 2$ and let $u^{**} \in U$ such that $B_2 \subseteq N(u^{**})$. We claim that there exist at most three sets $X \subseteq U$ of size two such that $B \subseteq N(X)$. Indeed, suppose that $X = \{u', u''\} \neq \{u^*, u^{**}\}$ covers B. Since G has no C_4, then $N(u')$

and $N(u'')$ contain exactly one element of B_1 and one element of B_2. Thus, we have at most two choices for such set $X \neq \{u^*, u^{**}\}$. Thus, the total number of special entries in $R_{A,B}$ is at most

$$\begin{aligned} |E[A:B]| \cdot 3 &\leqslant (d-1)|B| \cdot 3 \leqslant 12(d-1), \\ &\leqslant \left(\frac{3}{2}d\right)^2. \end{aligned} \tag{3.3.34}$$

This last inequality holds for $d \geqslant 4$. Indeed, notice that

$$\left(\frac{3}{2}d\right)^2 - 12(d-1) = \frac{1}{4}(9d^2 - 48d + 48). \tag{3.3.35}$$

The parabola $g(d) := 9d^2 - 48d + 48$ is increasing for $d \geqslant 3$ and $g(4) = 0$. Since $\left(\frac{3}{2}d\right)^2 \leqslant f(t^*)$ holds by Lemma 3.3.13, this case follows.

(b) Suppose that $|B_2| = 1$, so that $B = \{b_1, b_2, b_3\}$ and we may assume that $|N(b_1) \cap N(b_2) \cap N(b_3)| = \emptyset$. In addition, let $t_i := |N(b_i) \cap A|$. Any set X of size two covering B should contain the unique (if it exists) vertex that covers exactly two of the vertices in B and any extra vertex covering the remaining vertex. For instance, any special entry $(ub_i, S(X))$ can be obtained by choosing a vertex $b_j \in B$ such that $B \setminus \{b_j\}$ is covered by a vertex $u_0 \in U \setminus A$. Then, we add u_0 to X and add any of the $d - t_j$ vertices in $N(b_j) \setminus A$ to X (u does not appear in $N(b_j)$ as we assumed the vertices in B do not have a common neighbor). Thus, the total number of special entries in $R_{A,B}$ is upper bounded by

$$\sum_{i=1}^{3} t_i \sum_{j=1}^{3} (d - t_j) = (t_1 + t_2 + t_2)(3d - t_1 - t_2 - t_3) \leqslant \left(\frac{3d}{2}\right)^2. \tag{3.3.36}$$

Since $\left(\frac{3}{2}d\right)^2 \leqslant f(t^*)$ holds by Lemma 3.3.13 this case follows.

(c) Suppose that $|B_2| = 0$ and $B = \{b_1, b_2\}$. Suppose that $ub_i \in E[A:B]$ and $X := \{u^*, u^{**}\} \subseteq N(N(u)) \setminus A$ covers B. We have two options for X, either $B \subseteq N(u^*)$ and u^{**} can be any vertex in $N(N(u)) \setminus (A \cup \{u^*\})$ (giving us $d(d-1) - |A|$ choices for sets X) or $|B \cap N(u^*)| = |B \cap N(u^{**})| = 1$ (giving us $2(d-1) - |A|$ choices for sets X). In total, the number of special entries in $R_{A,B}$ is at most

$$|A|((d+2)(d-1) - 2|A|) \leqslant 2\left(\frac{(d+2)(d-1)}{4}\right)^2 = \frac{(d+1)^2(d-1)^2}{8}. \tag{3.3.37}$$

Since $\frac{(d+1)^2(d-1)^2}{8} \leqslant f(t^*)$ holds by Lemma 3.3.13 this case follows.

3. Suppose that $\alpha = 1$, so that $|B| \leqslant 2$. We consider two cases.

   (a) Suppose that $B = \{v_1, v_2\}$. In this case, there does not exist a vertex $u' \in U$ such that $B \subseteq N(u')$, hence we can assume that every set $X := \{u_1, u_2\}$ covering B satisfies $u_1 \in N(v_1)$ and $u_2 \in N(v_2)$. Let t_1 and t_2 be the number of vertices in A that are adjacent to v_1 and v_2 respectively. Then, the number of special entries in $R_{A,B}$ is at most

   $$|E[A:B]| \cdot (d-t_1)(d-t_2) = (t_1+t_2)(d-t_1)(d-t_2) \leqslant \left(\frac{2d}{3}\right)^3. \tag{3.3.38}$$

   By Lemma 3.3.13, this case follows as well.

   (b) Suppose that $B = \{v\}$ and let t be the number of vertices in A. Let $uv \in E[A:B]$ and let $X := \{u^*, u^{**}\} \subseteq N(N(u)) \setminus A$ be a set covering v. We have two options for X, either $X \subseteq N(v) \setminus A$ (with $\binom{d-t}{2}$ choices) or $|X \cap N(v)| = 1$ (with $(d-t)(d-1)^2$ choices). In total, the number of special entries in $R_{A,B}$ is at most

   $$\begin{aligned} t\left(\binom{d-t}{2} + (d-t)(d-1)^2\right) &= \frac{1}{2}t(d-t)(d-t-1+2d^2-4d+2), \\ &= \frac{1}{2}t(d-t)(2d^2-3d+1-t) = f(t). \end{aligned} \tag{3.3.39}$$

   This case follows as well.

□

From the results of the lemma above, it is natural to define weights $w_{(uv,S)} = \frac{1}{w_2(d)}$ for every special entry of (uv, S) of M_G. Hence, we would have $w(R_{A,B}) \leqslant 1$ for every rectangle $R_{A,B}$. However, this will give us a total weight of

$$w(M_G) = \sum_{uv \in E} w(R_{\{u\}\{v\}}) = \frac{f(1)}{w_2(d)}|E| = \frac{(d-1)(2d^2-3d)}{2w_2(d)}|E|, \tag{3.3.40}$$

which is not larger than $0.77|E|$ for every $d \geqslant 4$. Fortunately, it is possible to improve this lower bound with the use of entries of the form $(uv, U \setminus \{u\})$ as we show next. We will need the following technical lemma, whose proof can be found in Appendix B.3.

Lemma 3.3.15. *Let $d \geqslant 4$ and let $w_2(d)$ be as defined in Lemma 3.3.14. Then,*

1. *For every $d \geqslant 4$ we have*
$$\frac{2d \cdot (d-1)^2}{d-2} \leqslant w_2(d). \tag{3.3.41}$$
2. *For every $d \geqslant 5$*
$$\frac{1}{2}d(2d^2 - 3d) \leqslant w_2(d). \tag{3.3.42}$$
3. *For every $d \geqslant 6$ we have*
$$2d^3 - 7d^2 + 7d - 2 \leqslant w_2(d). \tag{3.3.43}$$

We are ready to prove Theorem 3.3.11.

Proof of Theorem 3.3.11. Once again, let us call an entry (uv, S) in the support of M_G special if $S = S(X)$ for some $X \subseteq N(N(u)) \setminus \{u\}$, such that $v \in N(X)$ and X has size $|X| = 2$. Let $w_2 := w_2(d)$ be as defined in the statement of Lemma 3.3.14 and let $f(x) := \frac{1}{2}x(d-x)(2d^2 - 3d + 1 - x)$ as in Lemma 3.3.13. For a given entry (uv, S) in the support of M_G define the weights:

$$w_{(uv,S)} := \begin{cases} \frac{1}{w_2} & \text{if } (uv, S) \text{ is special,} \\ \alpha & \text{if } S = U \setminus \{u\}, \\ 0 & \text{otherwise,} \end{cases} \tag{3.3.44}$$

for some $\alpha > 0$ to be determined later. Our goal is to find an appropriate α so that the weights of any rectangle $w(R_{A,B}) := \sum_{(uv,S) \in R_{A,B}} w_{(uv,S)}$ is at most one. First, if $|A| \geqslant 2$ then no entry of the form $(uv, U \setminus \{u\})$ is in $R_{A,B}$ and by Lemma 3.3.14

$$w(R_{A,B}) = \sum_{(uv,S) \in R_{A,B},\ \text{special}} w_{(uv,S)} \leqslant \frac{w_2}{w_2} = 1. \tag{3.3.45}$$

Thus, from now on suppose that $A = \{u\}$ for some $u \in U$. We consider three cases.

1. Suppose that $B = \{v\}$ for some $v \in N(u)$. Then, the number of special entries in $R_{A,B}$ is equal to $f(1)$. In addition, there is only one entry in $R_{A,B}$ of the form $(uv, U \setminus \{u\})$. Thus, the total weight of this rectangle is
$$w(R_{A,B}) = \frac{f(1)}{w_2} + \alpha. \tag{3.3.46}$$

This value is less than or equal to one if and only if

$$\alpha \leqslant 1 - \frac{f(1)}{w_2} = 1 - \frac{(d-1)(2d^2-3d)}{2w_2}. \tag{3.3.47}$$

2. Suppose that $B = \{b_1, b_2\}$. Then, the number of special entries in $R_{A,B}$ is equal to $2(d-1)^2$. Indeed, since u is adjacent to both vertices in B, the set X covering B consists of one neighbor of b_1 and one neighbor of b_2 both different to v, hence a total of $(d-1)^2$ of such pairs exists. For each of those $(ub_1, S(X))$ and $(ub_2, S(X))$ are in $R_{A,B}$. In addition, the entries $(ub_1, U \setminus \{u\})$ and $(ub_2, U \setminus \{u\})$ are in $R_{A,B}$. Thus, the total weight of this rectangle is

$$w(R_{A,B}) = \frac{2(d-1)^2}{w_2} + 2\alpha. \tag{3.3.48}$$

This value is less than or equal to one if and only if

$$\alpha \leqslant \frac{1}{2} - \frac{(d-1)^2}{w_2}. \tag{3.3.49}$$

3. If $|B| \geqslant 3$, then no pair of vertices $X \subseteq U \setminus \{u\}$ would cover the set B as this would imply that a pair of vertices in G has at least two neighbors in common. Hence, $R_{A,B}$ does not have a special entry. However, $R_{A,B}$ has $|B|$ entries of the form $(uv, U \setminus \{v\})$, one of each $v \in B$. Thus, the total weight of this rectangle is

$$w(R_{A,B}) = |B|\alpha. \tag{3.3.50}$$

This value is less than or equal to one for every $|B| \geqslant 3$ if and only if

$$\alpha \leqslant \frac{1}{d}. \tag{3.3.51}$$

From the above, if we want the weights of all maximal rectangles to be at most one, then we should set

$$\alpha := \min\left\{\frac{1}{d}, \frac{1}{2} - \frac{(d-1)^2}{w_2}, 1 - \frac{(d-1)(2d^2-3d)}{2w_2}\right\}. \tag{3.3.52}$$

Now, we have that $\frac{1}{d} \leqslant \frac{1}{2} - \frac{(d-1)^2}{w_2}$ if and only if

$$\frac{2d \cdot (d-1)^2}{d-2} \leqslant w_2. \tag{3.3.53}$$

By Lemma 3.3.15, this holds when $d \geqslant 4$. Similarly, we have that $\frac{1}{d} \leqslant 1 - \frac{f(1)}{w_2}$ if and only if

$$\frac{d \cdot f(1)}{d-1} = \frac{1}{2} d(2d^2 - 3d) \leqslant w_2. \tag{3.3.54}$$

By Lemma 3.3.15, this holds for $d \geqslant 5$. Notice also that for $d = 4$ we have

$$\frac{1}{2} d(2d^2 - 3d) = 40 > w_2(4) = 39. \tag{3.3.55}$$

Finally, we have that $\frac{w_2 - 2(d-1)^2}{2w_2} \leqslant \frac{w_2 - f(1)}{w_2}$ if and only if

$$2f(1) - 2(d-1)^2 = 2d^3 - 7d^2 + 7d - 2 \leqslant w_2.$$

By Lemma 3.3.15, this holds for $d \geqslant 6$. Moreover, for $d = 4$ we have

$$2d^3 - 7d^2 + 7d - 2 = 42 > w_2(4) = 39. \tag{3.3.56}$$

In conclusion, we have that

$$\alpha := \begin{cases} \frac{1}{d} & \text{if } d \geqslant 5, \\ \frac{w_2 - f(1)}{w_2} & \text{if } d = 4. \end{cases} \tag{3.3.57}$$

Moreover, the total weight of the matrix M_G equals

$$\begin{aligned} w(M_G) &= \sum_{uv \in E} w(R_{\{u\},\{v\}}), \\ &= \left(\frac{f(1)}{w_2} + \alpha \right) |E|, \\ &= \begin{cases} \left(\frac{(d-1)(2d^2-3d)}{2w_2} + \frac{1}{d} \right) |E|, & \text{if } d \geqslant 5, \\ |E|, & \text{if } d = 4. \end{cases} \end{aligned} \tag{3.3.58}$$

□

3.3.4 The projective plane of order 4: A linear programming approach

Let $G_q = (\mathcal{L} \cup \mathcal{P}, E)$ be the incidence graph of the projective plane of order q. The vertex set of G_q consists of a set of lines $\mathcal{L}$, a set of points $\mathcal{P}$ and the set of edges have the form

$\ell p \in E$ for every line $\ell \in \mathcal{L}$ and every point $p \in \ell$ passing through the line. The objective of this section is to obtain lower bounds for $\text{xc}(\text{STAB}(G_4))$ by explicitly solving the *fractional relaxation* of the rectangle covering bound, i.e., by solving the linear programming problem stated in equation (3.3.9). For convenience, we rewrite this problem and its dual here.

$$\begin{array}{lll} \min & \sum_{R\in\mathcal{R}} y_R & \\ s.t. & \sum_{(i,j)\in R} y_R \geqslant 1,\ \forall (i,j) \in \text{supp}(M), & \\ & y_R \geqslant 0,\ \forall R \in \mathcal{R}, & \end{array} \qquad \begin{array}{lll} \max & \sum_{(i,j)} w_{(i,j)} & \\ s.t. & \sum_{(i,j)\in R} w_{(i,j)} \leqslant 1,\ \forall R \in \mathcal{R}, & \\ & 0 \leqslant w_{(i,j)},\ \forall (i,j) \in \text{supp}(M). & \end{array} \tag{3.3.59}$$

Here, $\mathcal{R}$ denotes the set of all combinatorial rectangles of M. As we mentioned before, the main difficulty with this formulation is that the number constraints and the number of variables of this LP can be too large. This is the case, even for the slack matrices of reasonable sized graphs such as G_4, having just 42 vertices and 105 edges. Indeed, the number of maximal stable sets $S(X) := X \cup \mathcal{P} \setminus N(X)$ of G_q is equal to 2^{q^2+q+1}, the number of entries $(\ell p, S(X))$ in the support of M_{G_q} is equal to

$$|E| \cdot |\{X \subseteq \mathcal{L} \setminus \{\ell\} : X \cap N(p) > 0\}| = |E| \cdot 2^{q^2}(2^{q+1} - 1). \tag{3.3.60}$$

In addition, the number of maximal rectangles $R_{A,B}$ is at least the number of rectangles of the form $R_{A,N(A)}$ which is equal to $2^{q^2+q+1} - 1$. Thus, even for $q = 4$, the number of variables and constrains of the LPs is already larger than $105 \cdot 2^{42} > 4.6 \cdot 10^{14}$.

Of course, this does not mean that such large LPs are unsolvable. We could potentially use column generation techniques along with separation algorithms for the feasible region of the LP. In addition, one way to reduce the size of this LP is exploit the symmetries of G_q. This is what we do next.

Definition 3.3.16. For any line $\ell \in \mathcal{L}$, any point $p \in \mathcal{P}$ and any subset of lines $X \subseteq \mathcal{L}$, we call the triple (ℓ, p, X) **valid** if $p \in \ell$, $\ell \notin X$ and $p \in \ell'$ for some $\ell' \in X$. In other words, (ℓ, p, X) is valid if $(\ell p, S(X))$ is in the support of M_{G_q}.

We will consider only the columns of the matrix M_{G_q} corresponding to maximal stable sets $S(X)$. Since we are interested in lower bounds for the non-negative rank of M_{G_q}, the fractional rectangle cover number of this sub-matrix will suffice. Hence, we are interested

in solving the following linear program.

$$\begin{aligned} \max \quad & \sum_{(\ell,p,X) \text{ valid}} w_{\ell,p,X} \\ s.t. \quad & \sum_{\ell p \in E[A:B]} \sum_{\substack{X:(\ell,p,X) \text{ valid,} \\ X \text{ covers } B}} w_{\ell,p,X} \leqslant 1, \quad \forall A \subseteq \mathcal{L}, B \subseteq N(A), \\ & w_{\ell,p,X} \geqslant 0, \quad \forall\ (\ell,p,X) \text{ valid.} \end{aligned} \tag{P}$$

Let Γ_q be the group of automorphisms of the plane $PG(2,q)$. That is, Γ_p is the set of all point bijections $\sigma : \mathcal{P} \to \mathcal{P}$ that map lines into lines, i.e., for every line $\ell = \{p_1, \ldots, p_{q+1}\} \in \mathcal{L}$ we have that $\sigma(\ell) := \{\sigma(p_1), \ldots, \sigma(p_{q+1})\} \in \mathcal{L}$. In particular, such automorphisms σ also define bijections $\sigma : \mathcal{L} \to \mathcal{L}$ of lines (notice the slight abuse of notation).

Finite projective planes $PG(2,q)$ can be identified with the non-trivial subspaces of the vector space $\mathbb{F}_q^3$. The set of lines $\mathcal{L}$ corresponds to 2-dimensional subspaces and the set of points $\mathcal{P}$ corresponds to the 1-dimensional subspaces of $\mathbb{F}_q^3$. In particular, any invertible linear mapping $\sigma : \mathbb{F}_q^3 \to \mathbb{F}_q^3$ induces an automorphism of $PG(2,q)$ (notice that multiples of σ generates the same automorphism). In addition, it can be shown that if $q = p^r$ for some $r \geqslant 1$, the mapping $(x,y,z) \mapsto (x,y,z)^p := (x^p, y^p, z^p)$ also generates an automorphism of $PG(2,q)$. Moreover, we have the following.

Theorem 3.3.17 (The Fundamental Theorem of Projective Geometry, see [Bae52])**.** *Let $q := p^r$ for some prime p and integer $r \geqslant 1$. The elements of Γ_q are the automorphism of the form $(x,y,z) \mapsto \sigma((x,y,z))^{sp}$ where $s \in \{0, \ldots, r-1\}$ and $\sigma : \mathbb{F}_q^3 \to \mathbb{F}_q^3$ is invertible. Moreover,*

$$|\Gamma_q| = r(q^3-1)(q^3-q)(q^3-q^2). \tag{3.3.61}$$

Now, for every feasible solution $w := (w_{\ell,p,X})_{\ell,p,X}$ to (P) and every automorphism $\sigma \in \Gamma_p$ define the vector

$$w^\sigma := (w^\sigma_{\ell,p,X})_{\ell,p,X} = (w_{\sigma^{-1}(\ell),\sigma^{-1}(p),\sigma^{-1}(X)})_{\ell,p,X}.$$

We claim that any such w^σ is also a feasible solution to (P). Indeed, since σ maps lines into lines, the triple $(\sigma^{-1}(\ell), \sigma^{-1}(p), \sigma^{-1}(X))$ is valid if and only if the triple (ℓ,p,X) is valid. Also, for every $A \subseteq \mathcal{L}$ and every $B \subseteq N(A)$ we have that $\sigma(\ell)\sigma(p) \in E[A:B]$ if and only if $\ell p \in E[\sigma^{-1}(A) : \sigma^{-1}(B)]$. Thus, w^σ satisfies the inequalities:

$$\sum_{\ell p \in E[A:B]} \sum_{\substack{X:(\ell,p,X) \text{ valid,} \\ X \text{ covers } B}} w^\sigma_{\ell,p,X} = \sum_{\ell p \in E[A:B]} \sum_{\substack{X:(\ell,p,X) \text{ valid,} \\ X \text{ covers } B}} w_{\sigma^{-1}(\ell),\sigma^{-1}(p),\sigma^{-1}(X)},$$

$$= \sum_{\sigma(\ell')\sigma(p')\in E[A:B]} \sum_{\substack{\sigma(X'):(\sigma(\ell'),\sigma(p'),\sigma(X')) \text{ valid},\\ \sigma(X') \text{ covers } B}} w_{\ell',p',X'},$$

$$= \sum_{\ell'p'\in E[\sigma^{-1}(A):\sigma^{-1}(B)]} \sum_{\substack{X':(\ell',p',X') \text{ valid},\\ X' \text{ covers } \sigma^{-1}(B)}} w_{\ell',p',X'} \leqslant 1.$$

By the convexity of the feasible region of (P), for every feasible solution w, we have that $\hat{w} := \frac{1}{|\Gamma_q|}\sum_{\sigma\in\Gamma_q} w^\sigma$ is feasible as well. In particular, we may assume the existence of an optimal solution w^* to (P) satisfying $(w^*)^\sigma = w^*$ for every $\sigma \in \Gamma_q$.

Now, let us call any feasible solution w to (P) an *invariant feasible solution* if $w = w^\sigma$ holds for every $\sigma \in \Gamma_q$. For every $A \subseteq \mathcal{L}$ and every $B \subseteq N(A)$, an invariant feasible solution w also satisfies the equation

$$\sum_{\ell p\in E[A:B]} \sum_{\substack{X:(\ell,p,X) \text{ valid},\\ X \text{ covers } B}} w_{\ell,p,X} = \sum_{\ell p\in E[A:B]} \sum_{\substack{X:(\ell,p,X) \text{ valid},\\ X \text{ covers } B}} w^\sigma_{\ell,p,X},$$

$$= \sum_{\ell p\in E[\sigma^{-1}(A):\sigma^{-1}(B)]} \sum_{\substack{X:(\ell,p,X) \text{ valid},\\ X \text{ covers } \sigma^{-1}(B)}} w_{\ell,p,X}.$$

If we consider Γ_q as acting on the set of pairs $\{(A,B) : A \subseteq \mathcal{L}, B \subseteq N(A)\}$, the above equation tells us that it is enough to consider just one inequality per orbit $\mathcal{O}_{(A,B)} = \{(\sigma(A),\sigma(B)) : \ \forall\sigma \in \Gamma_q\}$. In addition, since $w = w^\sigma$ if we consider Γ_q as acting on valid triples $\{(\ell,p,X) : p \in \ell,\ \ell \in \mathcal{L}\setminus X,\ X \subseteq \mathcal{L}\}$, then it is enough to consider only a single variable $w_{\ell,p,X}$ per orbit $\mathcal{O}_{(\ell,p,X)} := \{(\sigma(\ell),\sigma(p),\sigma(X)) : \ \sigma \in \Gamma_q\}$. Consider orbit partitions given by

$$\{(\ell,p,X) : \ (\ell,p,X) \text{ valid}\} = \bigcup_{i=1}^{n_1} \mathcal{O}_{(\ell_i,p_i,X_i)},$$

$$\{(A,B) : A \subseteq \mathcal{L}, B \subseteq N(A)\} = \bigcup_{j=1}^{n_2} \mathcal{O}_{(A_j,B_j)},$$

for some valid triples $(\ell_1,p_1,X_1),\dots,(\ell_{n_1},p_{n_1},X_{n_1})$ and pairs $(A_1,B_1),\dots,(A_{n_2},B_{n_2})$. Now, for every pair (A_i,B_i) and every triple (ℓ_j,p_j,X_j) let $W_{i,j}$ be the number of valid entries $(\ell,p,X) \in \mathcal{O}_{(\ell_j,p_j,X_j)}$ that are in R_{A_i,B_i}, i.e.,

$$W_{i,j} := \left|\{\sigma \in \Gamma_q : \ \sigma(\ell_j) \in A_i, \sigma(p_j) \in B_i, \sigma(X_j) \cap A_i = \emptyset, \sigma(X_j) \text{ covers } B_i\}\right|. \quad (3.3.62)$$

Then, we can write the linear program (P) as:

$$\begin{aligned} \max \quad & \sum_{j=1}^{n_1} |\mathcal{O}_{(\ell_j,p_j,X_j)}|\ w_j, \\ s.t. \quad & \sum_{j=1}^{n_1} W_{i,j}\ w_j \leqslant 1, \quad \forall i \in \{1,\dots,n_2\}, \\ & w_j \geqslant 0, \quad \forall j \in \{1,\dots,n_1\}. \end{aligned} \tag{3.3.63}$$

We can find an equivalent linear program to (3.3.63) by changing the objective value as follows. Suppose that $A_1 = \{\ell_0\}$ and $B_1 = \{p_0\}$ for some line $\ell_0 \in \mathcal{L}$ and point $p_0 \in \ell_0$. Then, for every $\ell p \in E$, we know that $(\{\ell\},\{p\}) \in \mathcal{O}_{(A_1,B_1)}$ and as a result, the equation

$$\sum_{X:(\ell,p,X)\text{ valid}} w_{\ell,p,X} = \sum_{X:(\ell_0,p_0,X)\text{ valid}} w_{\ell_0,p_0,X} \tag{3.3.64}$$

holds for every invariant solution w. In particular, we have

$$\begin{aligned} \sum_{(\ell,p,X)\text{ valid}} w_{\ell,p,X} &= \sum_{\ell p \in E} \sum_{X:(\ell,p,X)\text{ valid}} w_{\ell,p,X}, \\ &= |E| \cdot \sum_{X:(\ell_0,p_0,X)\text{ valid}} w_{\ell_0,p_0,X}, \\ &= |E| \cdot \sum_{j=1}^{n_1} W_{1,j}\ w_{\ell_j,p_j,X_j}. \end{aligned}$$

Thus, we obtain the equivalent problem:

$$\begin{aligned} \max \quad & \sum_{j=1}^{n_1} W_{1,j}\ \ w_j, \\ s.t. \quad & \sum_{j=1}^{n_1} W_{i,j}\ w_j \leqslant 1, \quad \forall i \in \{1,\dots,n_2\}, \\ & w_j \geqslant 0, \quad \forall j \in \{1,\dots,n_1\}. \end{aligned} \tag{P_{sym}}$$

The optimal value of (P_{sym}) can be scaled by a factor of $|E|$ to obtain the optimal value ot (P). One can compute the formulation (P_{sym}) as follows:

1. First, compute the orbits $\mathcal{O}_{(\ell_j,p_j,X_j)}$ and $\mathcal{O}_{(A_i,B_i)}$. For that, we first compute the orbits of subsets of lines $X \subseteq \mathcal{L}$. This can be done in a recursive fashion: we know that there is only one orbit when $|X| \in \{1,2\}$, once orbits representatives $\mathcal{O}_k$ for sets of size $|X| = k$ have been computed, we generate the orbits representatives $\mathcal{O}_{k+1}$ of sets of length $|X| = k+1$ by adding a single line to the representatives in $\mathcal{O}_k$, compute their orbits and prune orbits already calculated.

   The orbits $\mathcal{O}_{(\ell_j,p_j,X_j)}$ can be computed from the sets in $\mathcal{O}_k$ by picking a a representative in $X^* \in \mathcal{O}_k$, then pick a line $\ell \in X^*$ and a point $p \in \ell$ covered by $X := X^* \setminus \{\ell\}$ and add or prune the orbit $\mathcal{O}_{(\ell,p,X)}$. This process can be done in parallel over the set $\mathcal{O}_k$.

   The orbits $\mathcal{O}_{(A_i,B_i)}$ are more expensive to compute. First, we pick a representative $A \in \mathcal{O}_k$, and then we compute and prune the orbits $\mathcal{O}_{(A,B)}$ for every $B \subseteq N(A)$ satisfying $A \subseteq N(B)$. Again, this can be done in parallel over the set $\mathcal{O}_k$.

2. Next, we need to compute the values $W_{i,j}$. This is computed by taking a representative of $\mathcal{O}_{(A_i,B_i)}$ and counting the number of valid (ℓ,p,X) triples in the orbit $\mathcal{O}_{(\ell_j,p_j,X_j)}$ satisfying $\ell \in A$, $p \in B$, $A_i \cap X = \emptyset$ and $B \subseteq N(X)$. This can be done in parallel over all pairs (i,j). Although, these can be generated by column or by row, if one has a guess on where the optimal basis should be.

We have coded the procedures above using `python3` and `sage`. The package `sage.designs.block_design` was particularly useful to obtain the incidence graphs of projective planes and its group of automorphisms. The code is be available at

https://github.com/silverquimera/projectivePlanes_xc.

We tested our implementation with the cases $q \in \{2,3,4,5\}$. As a general overview, the cases $q = 2$ and $q = 3$ were relatively easy to compute, the case $q = 4$ was solved by limiting the amount of columns to be computed, but the case $q = 5$ seemed to be hard to tackle with our techniques. Here, we give some more details on the results we obtained.

For $q = 2$, there is a total of $n_1 = 13$ orbits of valid triples (ℓ,p,X) and $n_2 = 161$ orbits of pairs (A,B) with $A \subseteq \mathcal{L}$ and $B \subseteq N(A)$. An optimal solution with objective value equal to $|E|$ was found. This solution is supported at a single valid triple class $w_{(\ell^*,p^*,X^*)} = \frac{1}{8}$. Here, the set $X^* = \{\ell_1,\ell_2\}$ consist of a pair of lines and ℓ^* is any third line intersecting ℓ_1 at p^* and intersecting ℓ_2 at another point.

For $q = 3$, there is a total of $n_1 = 96$ orbits of valid triples (ℓ, p, X) and $n_2 = 12687$ orbits of pairs (A, B) with $A \subseteq \mathcal{L}$ and $B \subseteq N(A)$. An optimal solution with objective value equal to $|E|$ was found. One of the solutions is supported at a pair valid triple orbits:

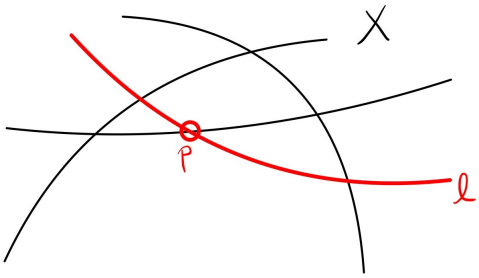
1. The triple (ℓ_1, p_1, X_1) where $|X_1| = 2$ and exactly one line in X_1 passes through p. The weight of this triple is $w_{(\ell_1,p_1,X_1)} = \frac{1}{36}$.
2. The triple (ℓ_2, p_2, X_2) where $X_1 = \mathcal{L} \setminus \{\ell_2\}$. The weight of this triple is $w_{(\ell_1,p_1,X_1)} = \frac{1}{4}$.

For the case $q = 4$ it was possible to compute the orbits $\mathcal{O}_{(\ell,p,X)}$ of triples (ℓ, p, X) and orbits $\mathcal{O}_{(A,B)}$ of pairs (A, B) for the plane. In total, the number of orbits of valid triples equals $n_1 = 1517$ and the number of orbits of pairs equals $n_2 = 20534180$. However, computing the weights $W_{i,j}$ is a little costly. This, as some orbits $\mathcal{O}_{(\ell_j,p_j,X_j)}$ have a considerable size and checking the validity of the statement "$(\ell^*, p^*, X^*) \in R_{A_i,B_i}$ for each $(\ell^*, p^*, X^*) \in \mathcal{O}_{(\ell_j,p_j,X_j)}$" ends up being computationally intensive, given the size of the matrix.

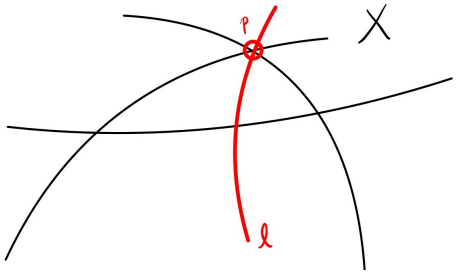
Nevertheless, for cases $q = 2$ and $q = 3$, we observed that the optimal solutions were sparse and these were supported at triples (ℓ, p, X) with X satisfying either $|X| \leqslant q$ or $|X| = q^2 + q$. For the case $q = 4$, these triples corresponded to the first 20 and last columns of the matrix W. Computing a single of these columns required about 6 hours in a Dell PowerEdge R840 with four Intel Xeon Gold 6230 20-core 2.1 GHz (Cascade Lake) and 768 GB of RAM (parallel computation of the weights $W_{i,j}$ was used with the 80 physical cores of the machine). As a first trial, the first 10 columns were computed and the problem was constructed using `python`'s `mip` package, exported using the `.lp` format and then loaded into `CPLEX`.

An optimal solution of value $|E|$ was found for the problem. The solution obtained is supported at four valid triples (ℓ, p, X):

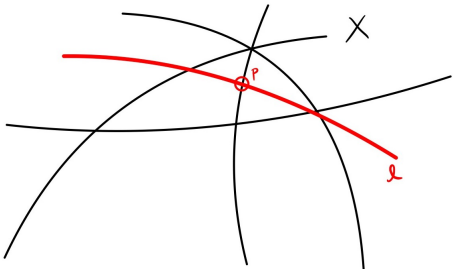
(VT 1.) X consist of three lines (not passing through the same point), ℓ is a fourth line traversing the lines in X (i.e.,not passing through any of the points of intersection of the three lines), and the point p is the intersection of ℓ and one of the lines in X (see picture below). The value for this variable is $w_{(\ell,p,X)} = 1/1800$, the coefficient in the objective function is $288|E|$.



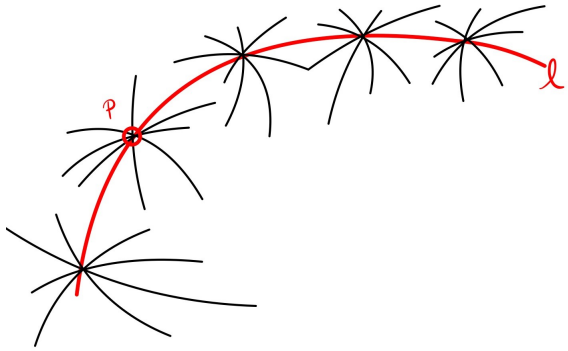
(VT 2.) X consist of three lines (not passing through the same point), but this time, ℓ passes through the point p which is the intersection of two of the three lines in X. The value is $w_{(\ell,p,X)} = 1/240$ and the coefficient in the objective function is $96|E|$.



(VT 3.) X consist of four lines, three of these passing through a single point p^* and the fourth one intersecting each line at other three points. Then, the line ℓ is a line that passes through one three points of intersection of X different to p^*. Finally, p is the point of intersection of ℓ with one of the first three lines. The value is $w_{(\ell,p,X)} = 1/2400$ and the coefficient in objective function is $576|E|$.



(VT 4.) X is the set of all lines, except for line ℓ. The point p is any point in ℓ. The value is $w_{(\ell,p,X)} = 1/5$ and the coefficient in the objective function is $|E|$.



Moreover, the tight constraints of this solution were obtained at the following six maximal rectangles:

(AB 1.) Rectangles $R_{A,B}$ where $A = \{\ell\}$, $B = \{p\}$ and $\ell p \in E$, with dual variable $y_{(A,B)} = 0$.

(AB 2.) Rectangles $R_{A,B}$ where $A = \{\ell\}$,$B = \{p_1, p_2\}$ and $\ell p_1, \ell p_2 \in E$, with dual variable $y_{(A,B)} = \frac{1}{2}|E|$.

(AB 3.) Rectangles $R_{A,B}$ where $A = \{\ell_1, \ell_2\}$,$B = \{p\}$ and $\ell_1 p, \ell_2 p \in E$, with dual variable $y_{(A,B)} = \frac{3}{14}|E|$.

(AB 4.) Rectangles $R_{A,B}$ where $A = N(p^*)$ and $B = N(\ell^*)$ for some $p^* \in \mathcal{P}$ and $\ell^* \in \mathcal{L}\backslash N(p^*)$, with dual variable $y_{(A,B)} = \frac{2}{7}|E|$.

(AB 5.) Rectangles $R_{A,B}$ as in (AB 4.), but with the exception that one line of A is has an extra line ℓ^{**} passing through one of the points in B. Formally, $B = N(\ell^*)$ for some line $\ell^* \in \mathcal{L}$, $A = (N(p^*) \cup \{\ell^{**}\}$ for some point $p^* \in \mathcal{P} \setminus B$ and some line $\ell^{**} \in \mathcal{L} \setminus N(p^*)$. The dual value equals $y_{(A,B)} = 0$.

(AB 6.) Rectangles $R_{A,B}$ where $A = \{\ell\}$ and $B = N(\ell)$ for some $\ell \in \mathcal{L}$, with dual variable $y_{(A,B)} = 0$.

The remaining constraints have a slack greater than or equal to 0.015. Due to the large number of rectangles R_{A_i,B_i} that contain at least one valid entry of the form (VT 1.)-(VT 4.), we were not able to verify by hand the feasibility of this solution. Nevertheless, we were able to verify the set of constraints described in the following lemma. See Appendix B.4 for the corresponding proof.

Lemma 3.3.18. *Consider the weights $w_{(\ell,p,X)}$ defined by the valid triples (VT 1.)-(VT 4.) above and set $w_{(\ell,p,X)} = 0$ for any other valid triple. Let $R_{A,B}$ be a maximal rectangle of M_{G_4}, then*

1. *the weight $w(R_{A,B}) := \sum_{(\ell,p,X)\in R_{A,B}} w_{(\ell,p,X)}$ is at most one when*
   - *(a) $|A| = 1$, $|B| \geqslant 1$,*
   - *(b) $|A| \geqslant 1$, $|B| = 1$,*
2. *the weight $w(R_{A,B})$ equals to one for the pairs (A, B) described in (AB 1.)-(AB 6.).*

A good amount of work was invested with the case $q = 5$, however our implementation did not allow us to even compute the orbits $\mathcal{O}_{(A_i,B_i)}$ for $|A_i| \geqslant 6$, thus another approach should be used to solve that case. One alternative is to use a separation oracle for the feasible set of (P_{sym}). For instance, one could start with a relaxed version of (P_{sym}) by adding just a subset of constraints, such as those described by (AB 1.)-(AB 6.), to obtain a partial solution $w^* = (w^*_{(\ell_j,p_j,X_j)})_{j\in[n_1]}$. Then, we could verify the feasibility of w^* using the following integer programming problem:

Lemma 3.3.19. *A non-negative vector $w = (w_{(\ell_j,p_j,X_j)})_{j\in[n_1]}$ is feasible to (P_{sym}) if and only if the optimal value of the following integer program is at most one:*

$$
\begin{aligned}
\max \quad & \sum_{j\in n_1} w_{(\ell_j,p_j,X_j)} \cdot \sum \left(z_{(\ell,p,X)} : (\ell,p,X) \in \mathcal{O}_{(\ell_j,p_j,X_j)} \right), \\
s.t. \quad & z_{(\ell,p,X)} \leqslant a_\ell \qquad \forall (\ell,p,X) \in \mathcal{O}_{(\ell_j,p_j,X_j)}, \forall j \in [n_1], \\
& z_{(\ell,p,X)} \leqslant b_p, \qquad \forall (\ell,p,X) \in \mathcal{O}_{(\ell_j,p_j,X_j)}, \forall j \in [n_1], \\
& z_{(\ell,p,X)} + a_{\ell^*} \leqslant 1 \qquad \forall \ell^* \in X, \forall (\ell,p,X) \in \mathcal{O}_{(\ell_j,p_j,X_j)}, \forall j \in [n_1], \\
& z_{(\ell,p,X)} + b_{p^*} \leqslant 1 \qquad \forall p^* \notin N(X), \forall (\ell,p,X) \in \mathcal{O}_{(\ell_j,p_j,X_j)}, \forall j \in [n_1], \\
& b_p \leqslant \sum (a_\ell : \ell \in N(p)), \qquad \forall p \in \mathcal{P}, \\
& a_\ell \leqslant \sum (b_p : p \in N(\ell)), \qquad \forall \ell \in \mathcal{L}, \\
& a_\ell, b_p, z_{(\ell,p,X)} \in \{0,1\}, \forall (\ell,p,X) \in \mathcal{O}_{(\ell_j,p_j,X_j)}, \forall j \in [n_1], \forall p \in \mathcal{P}, \forall \ell \in \mathcal{L}.
\end{aligned}
\tag{IP_{sep}}
$$

Proof. Let $w = (w_{(\ell_j,p_j,X_j)})_{j\in[n_1]}$ be given. For a given triple (ℓ_j, p_j, X_j) in the support of w, consider binary variables $z_{(\ell,p,X)}$ over triples (ℓ, p, X) in the orbit $\mathcal{O}_{(\ell_j,p_j,X_j)}$. Next, consider binary variables a_ℓ for each line $\ell \in \mathcal{L}$ and b_p for each point $p \in \mathcal{P}$.

The idea is to represent a pair (A, B) of lines and points using the binary variables $(a_\ell)_{\ell \in \mathcal{L}}$ and $(b_p)_{p \in \mathcal{P}}$ and "activate" the variable $z_{(\ell,p,X)}$ only when the triple (ℓ, p, X) is in the rectangle $R_{A,B}$. This occurs when the following conditions are met:

1. $\ell \in A$, which can be encoded as

$$z_{(\ell,p,X)} \leqslant a_\ell.$$

2. $p \in B$, which can be encoded as

$$z_{(\ell,p,X)} \leqslant b_p.$$

3. $X \cap A = \emptyset$, which can be encoded as

$$z_{(\ell,p,X)} + a_{\ell^*} \leqslant 1 \quad \forall \ell^* \in X.$$

4. $N(X) \supseteq B$, which can be encoded as

$$z_{(\ell,p,X)} + b_{p^*} \leqslant 1 \quad \forall p^* \notin N(X).$$

Finally, we add constraints pertaining the relationship between A and B. These are:

5. Each point in B is in at least one line of A, which can be encoded as:

$$b_p \leqslant \sum (a_\ell : \ell \in N(p)).$$

6. Each line in A must contain at least one point of B, so that $R_{A,B}$ is a maximal rectangle. This can be encoded as

$$a_\ell \leqslant \sum (b_p : p \in N(\ell)).$$

Now, given a feasible solution z, a, b to (IP_{sep}), if we set $A := \{\ell : a_\ell > 0\}$ and $B := \{p \in \mathcal{P} : b_p > 0\}$ then

$$\sum_{(\ell,p,X) \in \mathcal{O}_{(\ell_j, p_j, X_j)}} z_{(\ell,p,X)} \leqslant W_{ij} \tag{3.3.65}$$

where $i \in [n_2]$ is such that $(A, B) \in \mathcal{O}_{(A_i,B_i)}$. In particular, the objective value of this particular solution is at most the i-th constraint of (P_{sym}) and the result follows.

□

Remark 3.3.20. Notice that setting $a_\ell = b_p = \frac{1}{2}$ for every $\ell \in \mathcal{L}$, $p \in \mathcal{P}$ and $z_{(\ell,p,X)} = \frac{1}{2}$ for every valid triple (ℓ, p, X) gives a feasible solution to the linear relaxation of (IP_{sep}) with value

$$\frac{1}{2} \sum_{j \in [n_1]} |\mathcal{O}_{(\ell_j,p_j,X_j)}| w_{(\ell_j,p_j,X_j)}. \tag{3.3.66}$$

This value is equal to half the value of w in the objective of (P_{sym}), which can be as large as $|E|$. Thus, the integrality gap of this IP can be significantly large.

Finally, if the optimal value (z^*, a^*, b^*) of (IP_{sep}) corresponding to w^* is larger than one, then we add the constraint corresponding to the pair $A^* := \{\ell : a^*_\ell > 0\}$ and $B^* := \{p \in \mathcal{P} : b^*_p > 0\}$ and repeat the procedure until a feasible solution is found.

Our experiments indicated that (IP_{sep}) may be computationally intensive when the orbits $\mathcal{O}_{(\ell_j,p_j,X_j)}$ have a considerable size. For instance, it took almost three days to verify, using (IP_{sep}), whether the solution given by (VT 1.)-(VT4.) for the case $q = 4$ was feasible. However, it takes no longer than a few seconds to verify feasibility by simple inspection over the $n_2 = 20534180$ constraints. The catch is that computing the whole set of orbits $\mathcal{O}_{(A_i,B_i)}$ was a non-trivial task that required also a few days of computation. It would be interesting to see whether this method can help in finding the optimal solution to (IP_{sep}) for the case $q = 5$. We leave these analyses for future work.

3.4 Concluding Remarks

In this chapter we gave a brief overview of the methods and current results of the theory polyhedral extended formulations of stable set polytopes of perfect graphs. The importance of this problem lies in the heart of understanding the efficacy of SDPs versus LPs for solving combinatorial optimization problems.

We focused our attention to the case of stable set polytopes of bipartite graphs. We revisited the bounds due to Aprile et al. [AFF+17] and showed that these were applicable to any d-regular bipartite graph having no C_4. Although, not explicitly written in the thesis, we also attempted to improve Aprile et al. bounds by considering different types of "special" entries of the matrix M_G with no success. However, we believe that these bounds can be improve considerably. We showed a lower bound of $|E|$ for the extension

complexity of 4-regular bipartite graphs and showed computational lower bounds for the projective plane of order 4 (a 5-regular graph).

There are many questions that are left unsolved at the moment. Most prominently, the right order of magnitude of the extension complexity of stable sets of bipartite graphs is still unknown. As we showed in the last portion of Section 3.3.1, dense bipartite graphs having no bicliques of large size need also large biclique coverings. Given the strong connection between *biclique partitions* and the non-negative rank of the Clique vs Stable matrix (see [HS12] and the Alon-Saks-Seymour conjecture), these are great candidates to obtain better lower bounds on the extension complexity of stable set polytopes of bipartite graphs. We conjecture the following.

Conjecture 3.4.1. *Let $G = (V, E)$ be a bipartite graph with $\Omega(n^2)$ edges and having no $K_{r,r}$ for $r = \Omega(\log(n))$. Then,* $\text{xc}(\text{STAB}(G)) = \Omega(n^2/\log(n))$.

Determining the extension complexity of the stable set polytope of the incidence graph of the projective plane of order five posed a great computational challenge for us. Yet, we believe that this case should be doable by a cutting plane algorithm as the one presented in last portion of Section 3.3.4.

Open Problem 3.4.2. Find an optimal solution to the fractional rectangle covering LP for the stable set polytope of the projective plane of order 5.

A natural generalization of the approach followed by Theorem 3.3.11 is to consider entries $(uv, S(X))$ with $X \subseteq N(N(v))$ and $|X| = k$, for some $k > 2$. For any given $k \leqslant d(d-1)$ and any maximal rectangle $R_{A,B}$ we should study the values

$$w_{d,k}(R_{A,B}) := |\{(uv, S(X)) \in R_{A,B} : X \subseteq N(N(u)),\ |X| = k\}|. \tag{3.4.1}$$

Open Problem 3.4.3. Let G_q be the incidence graph of the finite projective plane of order q. Let $w^*_{q+1,k} := \max\{w_{q+1,k}(R_{A,B}) :\ R_{A,B} \text{ is maximal}\}$ and let $\ell p \in E(G_q)$ be a given edge of G_q. Determine the value

$$w^*_{q+1} := \max_k \ \frac{w_{q+1,k}(R_{\{\ell\}\{p\}})}{w^*_{q+1,k}}. \tag{3.4.2}$$

Notice that $\text{xc}(\text{STAB}(G_q)) \geqslant w^*_{q+1}|E|$. Is $w^*_{q+1} = \Omega(1)$?

For rectangles satisfying $|B| = 1$, we have a closed formula for $w_{d,k}(R_{A,B})$.

Lemma 3.4.4. *Let G be a d-regular C_4-free bipartite graph. Let $uv \in E$ be an edge of G and let $k \leqslant d(d-1)$. Then, for every rectangle $R_{A,B}$ where $B = \{v\}$ and $A \subset N(v)$ we have*

$$w_{d,k}(R_{A,B}) = \begin{cases} |A| \left(\binom{d(d-1)+1-|A|}{k} - \binom{(d-1)^2}{k} \right), & \text{if } k \leqslant d(d-1) - |A|, \\ 0, & \text{else.} \end{cases} \tag{3.4.3}$$

Proof. For a fixed $u_0 \in A$, let us count the number of entries $(u_0 v, S(X))$ in $R_{A,B}$. For all of those entries, we should have that $X \subseteq N(N(u_0)) \setminus A$, $|X| = k$ and $X \cap N(v) \neq \emptyset$. The number of ways we can choose such set equals

$$\binom{d(d-1)+1-|A|}{k} - \binom{(d-1)^2}{k}. \tag{3.4.4}$$

Indeed, the total number of vertices in $N(N(u_0)) \setminus A$ is $d(d-1)+1-|A|$. This holds as $A \subseteq N(v) \subseteq N(N(u_0))$. Of these, exactly $(d-1)^2$ are not adjacent to v, as G is C_4-free, so X cannot be chosen solely from this set. The result follows by adding the number of entries $(u_0 v, S(X))$ over all $u_0 \in A$. □

Using computer software, it seems that for $d \geqslant 4$ the value (3.4.3) reaches its maximum at $|A| = 1$ whenever $k \geqslant \binom{d}{2}$. However, we do not know whether the values $w_{d,k}(R_{A,B})$ reach a maximum at rectangles satisfying $B = \{v\}$ for some $v \in W$ as was in the case $k = 2$.

We believe that Aprile et al. [AFF+17] bounds for regular bipartite graphs can be improved considerably. At least, for the cases $q = 3$ and $q = 4$, the set of special entries used to obtain their bounds for the finite projective plane yield unsatisfactory solutions to the fractional rectangle covering LP. However, it may be the case that for large q the difference between their solution and the optimal solution reduces considerably. Still, we conjecture the following.

Conjecture 3.4.5. *Let $G = (V, E)$ be a regular bipartite graph having no C_4. Then,* $\mathrm{xc}(\mathrm{STAB}(G)) \geqslant |E|$. *In particular, there exists a family of bipartite graphs $\{G_n\}_{n \geqslant 2}$ on n vertices such that* $\mathrm{xc}(\mathrm{STAB}(G_n)) = \Omega(n^{3/2})$.

Finally, it would be interesting to see whether techniques that exploit symmetry of the underlying polytope or graph, such as the ones explored when computing $\mathrm{xc}(STAB(G_4))$, can yield theoretic lower bounds for the extension complexity of highly symmetric polytopes. In particular, we may explore such analysis for the stable set polytopes of incidence graphs of other combinatorial designs and Cayley Graphs for large classes of groups.

Chapter 4

Conclusions and Future Work

In this thesis we studied the efficacy of a few convex algebraic geometric approaches to solve combinatorial optimization problems such as Graph Coloring and Stable Set Problems. First, we considered the Nullstellensatz method for detecting the non-k-colorability of graphs. We showed that the size of the linear systems required to detect non-k-colorabilty grow exponentially in the girth of the graph. This is the first, to the best of our knowledge, example of an intrinsic graph property that implies the need of large enough Nullstellensatz certificates to detect the non-k-colorability of a graph.

Then, we studied the theory of polyhedral extended formulations for stable set polytopes of perfect graphs. In particular, we studied the efficacy of extended formulations for the stable set polytope of regular bipartite graphs. Although, we were not able to find general improvements to Aprile et al. results, we think that their bounds can be improved considerably. We showed that the extension complexity of the stable set polytope of any 4-regular bipartite graph is at least the number of edges in the graph. We also obtained computational results for the extension complexity of the stable set polytope of the projective plane of order four.

There remain several open questions regarding the efficacy and limitations of these methods. Some of these which we already discussed in previous chapters. In the following section, we go over some extra questions that pertain the main discussion of the thesis as a whole.

4.1 The Nullstellensatz Method

In the early 90s, Grötschel, Lovász and Schrijver [GLS93b] showed, using the Lovász Theta Body, a polynomial time algorithm to color a perfect graph. It is still an open question to determine whether a polynomial-time *combinatorial* algorithm exists for the same problem.

Open Problem 4.1.1. Does there exist a polynomial-time *combinatorial* algorithm to color a perfect graph?

Several approximations to this problem are known. For instance, Chudnovsky, Lagoutte, Seymour and Spirkl [CLSS17] showed a combinatorial algorithm that outputs in time $O(n^{(\omega(G)+1)^2})$ a coloring of a perfect graph G with n-vertices. Polynomial-time algorithms are also known for some sub-families of perfect graphs, such as *bull-free* perfect graphs [Pen12] and perfect graphs with *no balanced skew-partitions* [CTTV15]. Can the Nullstellensatz method help to create such algorithms?

In principle, if a graph G with n vertices does not have a Nullstellensatz Certificate for its non-k-colorability of degree at most $(k-1)\cdot n$, then G is k-colorable. However, the size of the corresponding system is $(kn)^{\Omega(kn)}$, which makes this method impractical for determining the chromatic number of a given graph. Nevertheless, it may be the case that for some families $\mathcal{G}$ of graphs, every $G \in \mathcal{G}$ with $\chi(G) > k$ has a Nullstellensatz Certificate for its non-k-colorability of degree at most d, independent of k and the size of G. In such cases, we may use the Nullstellensatz method to determine (in polynomial time) the chromatic number of any graph in the family. For instance, we may ask the following.

Open Problem 4.1.2. Does there exist a universal constant d such that every *perfect graph*, with chromatic number larger than k, has a Nullstellensatz Certificate of degree at most d for its non-k-colorability?

In order to attack this question, it may be a good idea to start with basic perfect graphs, i.e., bipartite graphs, line graphs of bipartite graphs, double-split graphs and their complements. We know that every non-bipartite graph has a Nullstellensatz Certificate of degree one for its non-2-colorability (see [DLLMM08]), but results for the remaining basic graphs are unknown. The next step may be to understand how the sizes of minimum degree Nullstellensatz certificates are altered when performing perfect graph operations such as taking complements or considering 2-joins and skew-partitions.

Another interesting problem, which goes in line with the core ideas of the thesis, is to understand the benefits and disadvantages of using different polynomial systems to encode

the same underlying combinatorial variety. For instance, it was observed in [DLLMM08] that one can reduce the degree of the Nullstellensatz Certificates by carefully appending redundant polynomial equations to the original system. Another alternative is to consider *extended* systems of polynomial equations:

Definition 4.1.3. Let $p_1, \ldots, p_m \in \mathbb{K}[\mathbf{x}]$ and $q_1, \ldots, q_t \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$ be polynomials on n and $n + d$ variables over some field $\mathbb{K}$. Consider the systems of polynomial equations

$$p_1(\mathbf{x}) = \cdots = p_m(\mathbf{x}) = 0, \tag{S1}$$

$$q_1(\mathbf{x}, \mathbf{y}) = \cdots = q_t(\mathbf{x}, \mathbf{y}) = 0. \tag{S2}$$

We say that the system (S2) is an *algebraic extended formulation* of the system (S1) if the following conditions hold:

1. If (S1) has no solution (over $\bar{\mathbb{K}}$) then (S2) has no solution (over $\bar{\mathbb{K}}$).
2. If (S2) has a solution, then there exists some $(\mathbf{x}_0, \mathbf{y}_0) \in \mathbb{K}^{n+d}$ such that $(\mathbf{x}_0, \mathbf{y}_0)$ is a solution to (S2) and $\mathbf{x}_0$ is a solution to (S1).

Notice that polynomials $q_1, \ldots, q_t \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$ define algebraic extended formulations of any set of polynomials $p_1, \ldots, p_m$ in the *elimination ideal* (see [CLO07])

$$\langle q_1, \ldots, q_t \rangle \cap \mathbb{K}[\mathbf{x}].$$

Open Problem 4.1.4. Suppose that the system (S1) has a minimum Nullstellensatz Certificate of degree d for its unfeasibilty. Does there exist an algebraic extended formulation (S2) whose minimum Nullstellensatz Certificate has degree $d_0 < d$?

4.2 Extension Complexity of the Stable Set Polytope of Perfect Graphs

The problem of determining the extension complexity of the stable polytope of perfect graphs remains wide open. Probably, a good next step to consider is to understand whether there exist perfect graphs having no short decomposition into basic perfect graphs. In particular, Hu and Laurent [HL19] upper-bounds would not be useful for those examples.

Open Problem 4.2.1 ([HL19])**.** Does there exist a class of perfect graphs which does not admit a decomposition tree into basic perfect graphs of logarithmic depth? If so, what is their extension complexity?

Mika Göös [GÏ5] bounds on the non-negative rank of M_G for general graphs, may serve as an indication that Yannakakis' bound of $n^{O(\log n)}$ may be tight even for perfect graphs. However, we do not have enough evidence to support this conjecture.

Open Problem 4.2.2. Is it possible to lift Göös' [GÏ5] techniques from *co-non-deterministic* vs. *unambiguous communicating complexity* to provide hard examples of stable set polytopes of perfect graphs having large extension complexity?

There are interesting connections between extension complexity and results regarding hardness of approximation of combinatorial optimization problems. Several approximation algorithms for combinatorial problems are built using LP relaxations of a corresponding IP formulation of the problem. Here, the idea is to use a *rounding algorithm*, that takes a fractional solution x_{LP} to the LP relaxation and transforms it into an integral solution x_{IP} to the IP, whose objective value is not too far from the optimum. The integrality gap of the linear relaxation is thus an indicative on how well the approximation algorithm will behave.

In theory, if the integrality gap of the relaxation is large, then one might increase the performance of the LP relaxation by adding cutting planes. How many inequalities are needed to reduce the integrality gap of our original LP relaxation by a considerable factor? For instance, Bazzi, Fiorini, Pokutta and Svensson [BFPS15a] showed the following theorem.

Theorem 4.2.3 ([BFPS15a])**.** *For every $\varepsilon > 0$ and for infinitely many values of n, there exists an n-vertex graph G such that every LP relaxation of size $n^{\Omega(\frac{\log n}{\log\log n})}$ of the Stable Set Polytope of G has integrality gap $\frac{1}{\varepsilon}$.*

This motivates the following question.

Open Problem 4.2.4. Let $\varepsilon > 0$. Does there exist a universal constant $d(\varepsilon)$ such that for every perfect graph G with n vertices, STAB(G) admits an LP relaxation of size $O(n^{d(\varepsilon)})$ with integrality gap at most $1 + \varepsilon$?

Finally, another interesting line of research, which may apply to both the Nullstellensatz Method and the theory of Polyhedral Extended Formulations is to carry out a *smoothed analysis* of the effectiveness of these methods. As we mentioned before, computational results in [DLLMM08], showed that the Nullstellensatz Method performed well over several non-3-colorable instances. Thus, we may ask the following.

Open Problem 4.2.5. Let $G \sim \mathcal{G}(n,p)$ be an Erdös-Rényi random graph with $\chi(G) > 3$ *almost surely* (say, $\ln(\frac{1}{1-p})\frac{n}{2\ln(n)}) \gg 3$, or $p = 0.9$ and n large enough). What is the *expected* size of a minimum Nullstellensatz Certificate for the non-3-colorability of G?

Smoothed analyses pertaining the extension complexity of the Stable Set Polytope exist. Braun, Fiorini and Pokutta [BFP16] showed that the extension complexity of STAB(G) remains high even for random graphs. For instance, the showed that $\text{xc}(\text{STAB}(G)) = 2^{\Omega(n/\log n)}$ with probability at least $1 - 2^{-2^n}$ for random graphs $G \sim \mathcal{G}(n,p)$ with $p \geqslant 2^{-\binom{n/2}{2}+n}$.

McDiarmid and Yolov [MY19] gave a model to draw *Generalized Split Graphs* uniformly at random. A graph G is a generalized split graph if both G and its complement allow a partition $V = C_0 \cup C_1 \cdots \cup C_k$ into cliques where C_i and C_j do not have an edge in common whenever $1 \leqslant i < j \leqslant k$. A result of Prömel and Steger [PS92] states that almost all perfect graphs are in fact generalized split graphs. Thus, McDiarmid and Yolov model is not too far from a model that draws random perfect graphs (see [MY19] for a precise statement).

Open Question 4.2.6. Let G be a generalized split graph. What is $\text{xc}(\text{STAB}(G))$?

One first step towards this question is the following.

Open Question 4.2.7. Do generalized split graphs admit a decomposition tree into basic perfect graphs of logarithmic depth?

4.3 Semidefinite Extension Complexity and Beyond

In this thesis, we studied the *polyhedral* extended formulations of stable set polytopes of various graphs. A natural generalization is to consider *spectrahedral* extended formulations. In fact these were the starting point of our thesis project: When are SDPs preferred over

LPs? As we mentioned in the introduction, the Stable Set Polytope of perfect graphs are, in our view, one the best examples to analyze the differences in efficiency of these methods.

However, another line of research is to further understand the power and limitations of SDPs themselves. As we mentioned before, Lovász's Theta Body provides a small semidefinite extended formulation for the Stable Set Polytope of perfect graphs. Thus, a natural problem is the following.

Open Problem 4.3.1. What combinatorial properties of a graph G guarantee that $\text{xc}_{SDP}(\text{STAB}(G))$ is polynomial in $|V(G)|$?

A first approach would be to consider hierarchies derived from lift and project methods. For instance, consider the *Lovász-Schrijver (SDP) Operator* LS_+ [LS91]. When applied to a polytope $P \subseteq \mathbb{R}^n$, the operator $LS_+(P)$ is a projection of a spectrahedron in $\mathbb{S}^n_+$, satisfying $P \subseteq LS_+(P)$. This operator already satisfies that $LS_+(FRAC(G)) = \text{STAB}(G)$ for every perfect graph G. Thus, it is natural to ask:

Open Problem 4.3.2. What combinatorial properties of a graph G guarantee that $LS_+(FRAC(G)) = \text{STAB}(G)$?

Graphs satisfying the above equality are called *LS_+-perfect graphs*. Partial results have been obtained towards a characterization of LS_+-perfect graphs. In fact, it is conjectured (see [BENT11],[BENT14], [BENT17]) that LS_+-perfect graphs are precisely all those graphs G for which $\text{STAB}(G)$ admits a description using only facets of $\text{STAB}(G')$ for subgraphs $G' \subsetneq G$ that are *near-bipartite*, i.e., for some vertex $v \in V(G')$ the graph induced by $V(G') \setminus (N(v) \cup \{v\})$ is bipartite. More formally,

Conjecture 4.3.3 ([BENT11])**.** *A graph G is LS_+-perfect if and only if*

$$\text{STAB}(G) = \bigcap_{\substack{G' \subsetneq G \\ G' \text{ near-biparite}}} \text{STAB}(G') =: NB(G). \tag{4.3.1}$$

It is known that if $NB(G) = \text{STAB}(G)$, then G is LS_+-perfect. Moreover, a partial converse is true (see [BENT17]): if G is LS_+-perfect and $\text{STAB}(G)$ is generated by the non-negative inequlities, the clique inequalities and a single constraint $\sum_{v \in V} a_v x_v \leqslant b\}$ for some non-zero a_v for every $v \in V$, i.e., G is a *full-support perfect graph*, then $NB(G) = \text{STAB}(G)$. It would be interesting to further relax the "near-perfection" condition to obtain similar extensions of this result.

Finally, another class of a well known generalization of Lovász's Theta Body are the *Theta Bodies of Polynomial Ideals* proposed by Gouveia, Parrilo and Thomas [GPT10]. When applied to the Stable Set Polytopes of graphs, these take the form

$$TH_k(G) := \{x \in \mathbb{R}^n : f(x) := a^\top x + \beta \geqslant 0 \text{ and } f \text{ is } k\text{-sos over STAB}(G)\}. \tag{4.3.2}$$

Here, the statement "f is k-sos over STAB(G)" means that it is possible to write f as a sum of squares

$$f(x) = \sum_{i=1}^{\ell} h_i^2(x) + r(x), \tag{4.3.3}$$

for some polynomials h_i of degree at most k and some polynomial r vanishing on the characteristic vectors of stable sets of G. We should point out that the set $TH_k(G)$ is a spectrahedron (see [GPT10]). It is a result of Lovász [Lov94] that $TH_1(G)$ is precisely the theta body of G. Thus, $TH_1(G) = \text{STAB}(G)$ if and only if G is perfect.

Open Problem 4.3.4. Characterize all graphs G satisfying $TH_2(G) = \text{STAB}(G)$.

References

[AFF+17] Manuel Aprile, Yuri Faenza, Samuel Fiorini, Tony Huynh, and Marco Macchia. Extension complexity of stable set polytopes of bipartite graphs. In *Graph-theoretic concepts in computer science*, volume 10520 of *Lecture Notes in Comput. Sci.*, pages 75–87. Springer, Cham, 2017.

[AKR+16] Noga Alon, Alexandr Kostochka, Benjamin Reiniger, Douglas B. West, and Xuding Zhu. Coloring, sparseness and girth. *Israel J. Math.*, 214(1):315–331, 2016.

[Alo99] Noga Alon. Combinatorial Nullstellensatz. *Combin. Probab. Comput.*, 8(1-2):7–29, 1999. Recent trends in combinatorics (Mátraháza, 1995).

[AR03] Michael V. Alekhnovich and Alexander A. Razborov. Lower bounds for polynomial calculus: the nonbinomial ideal case. *Tr. Mat. Inst. Steklova*, 242(Mat. Logika i Algebra):23–43, 2003.

[Bae52] Reinhold Baer. *Linear algebra and projective geometry.* Academic Press Inc., New York, N. Y., 1952.

[Bay82] David Allen Bayer. *The Division Algorithm and the Hilbert Scheme.* ProQuest LLC, Ann Arbor, MI, 1982. Thesis (Ph.D.)–Harvard University.

[BCE+98] Paul Beame, Stephen Cook, Jeff Edmonds, Russell Impagliazzo, and Toniann Pitassi. The relative complexity of np search problems. *Journal of Computer and System Sciences*, 57(1):3–19, 1998.

[BENT11] Silvia M. Bianchi, Mariana S. Escalante, Graciela L. Nasini, and Levent Tunçel. Near-perfect graphs with polyhedral $N_+(G)$. In *LAGOS'11—VI Latin-American Algorithms, Graphs and Optimization Symposium*, vol-

ume 37 of *Electron. Notes Discrete Math.*, pages 393–398. Elsevier Sci. B. V., Amsterdam, 2011.

[BENT14] Silvia M. Bianchi, Mariana S. Escalante, Graciela L. Nasini, and Levent Tunçel. Some advances on Lovász-Schrijver semidefinite programming relaxations of the fractional stable set polytope. *Discrete Appl. Math.*, 164(part 2):460–469, 2014.

[BENT17] Silvia M. Bianchi, Mariana S. Escalante, Graciela L. Nasini, and Levent Tunçel. Lovász-Schrijver SDP-operator, near-perfect graphs and near-bipartite graphs. *Math. Program.*, 162(1-2, Ser. A):201–223, 2017.

[BFP16] Gábor Braun, Samuel Fiorini, and Sebastian Pokutta. Average case polyhedral complexity of the maximum stable set problem. *Math. Program.*, 160(1-2, Ser. A):407–431, 2016.

[BFPS15a] Abbas Bazzi, Samuel Fiorini, Sebastian Pokutta, and Ola Svensson. No small linear program approximates vertex cover within a factor $2-\varepsilon$. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science—FOCS 2015*, pages 1123–1142. IEEE Computer Soc., Los Alamitos, CA, 2015.

[BFPS15b] Gábor Braun, Samuel Fiorini, Sebastian Pokutta, and David Steurer. Approximation limits of linear programs (beyond hierarchies). *Math. Oper. Res.*, 40(3):756–772, 2015.

[BIK+94] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 794–806. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

[CEI96] Matthew Clegg, Jeffery Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 174–183. ACM, New York, 1996.

[Chv73] Václav Chvátal. Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Math.*, 4:305–337, 1973.

[Chv75] Václav Chvátal. On certain polytopes associated with graphs. *J. Combinatorial Theory Ser. B*, 18:138–154, 1975.

[CLO05] David A. Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[CLO07] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[CLSS17] Maria Chudnovsky, Aurélie Lagoutte, Paul Seymour, and Sophie Spirkl. Colouring perfect graphs with bounded clique number. *J. Combin. Theory Ser. B*, 122:757–775, 2017.

[CRST06] Maria Chudnovsky, Neil Robertson, Paul Seymour, and Robin Thomas. The strong perfect graph theorem. *Ann. of Math. (2)*, 164(1):51–229, 2006.

[CT12] Eden Chlamtac and Madhur Tulsiani. *Convex Relaxations and Integrality Gaps*, pages 139–169. Springer US, Boston, MA, 2012.

[CTTV15] Maria Chudnovsky, Nicolas Trotignon, Théophile Trunck, and Kristina Vušković. Coloring perfect graphs with no balanced skew-partitions. *J. Combin. Theory Ser. B*, 115:26–65, 2015.

[DLHMO10] Jesús A. De Loera, Christopher J. Hillar, Peter N. Malkin, and Mohamed Omar. Recognizing graph theoretic properties with polynomial ideals. *Electron. J. Combin.*, 17(1):Research Paper 114, 26, 2010.

[DLLMM08] Jesús A. De Loera, Jon Lee, Peter N. Malkin, and Susan Margulies. Hilbert's Nullstellensatz and an algorithm for proving combinatorial infeasibility. In *ISSAC 2008*, pages 197–206. ACM, New York, 2008.

[DLLMM15] Jesús A. De Loera, Jon Lee, Susan Margulies, and Jacob Miller. Weak orientability of matroids and polynomial equations. *European J. Combin.*, 50:56–71, 2015.

[DMP+14] Jesús A. De Loera, Susan Margulies, Michael Pernpeintner, Eric Riedl, David Rolnick, Gwen Spencer, Despina Stasi, and Jon Swenson. Grobner Bases and Nullstellensatze for Graph-Coloring Ideals. *ArXiv e-prints*, October 2014.

[EG18] Geoffrey Exoo and Jan Goedgebeur. Bounds for the smallest k-chromatic graphs of given girth. 2018.

[Erd59] Paul Erdős. Graph theory and probability. *Canad. J. Math.*, 11:34–38, 1959.

[ES63] Paul Erdős and Horst Sachs. Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahl. *Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe*, 12:251–257, 1963.

[FFGT15] Yuri Faenza, Samuel Fiorini, Roland Grappe, and Hans Raj Tiwary. Extended formulations, nonnegative factorizations, and randomized communication protocols. *Math. Program.*, 153(1, Ser. B):75–94, 2015.

[FHLO15] Mirjam Friesen, Aya Hamed, Troy Lee, and Dirk Oliver Theis. Fooling-sets and rank. *European Journal of Combinatorics*, 48:143–153, 2015. Selected Papers of EuroComb'13.

[FMP+15] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf. Exponential lower bounds for polytopes in combinatorial optimization. *J. ACM*, 62(2):Art. 17, 23, 2015.

[FRR06] Bálint Felszeghy, Balázs Ráth, and Lajos Rónyai. The lex game and some applications. *J. Symbolic Comput.*, 41(6):663–681, 2006.

[Ful72] Delbert R. Fulkerson. Anti-blocking polyhedra. *J. Combinatorial Theory Ser. B*, 12:50–71, 1972.

[GÏ5] Mika Göös. Lower bounds for clique vs. independent set. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science—FOCS 2015*, pages 1066–1076. IEEE Computer Soc., Los Alamitos, CA, 2015.

[GKP10] Bruno Grenet, Pascal Koiran, and Natacha Portier. The multivariate resultant is NP-hard in any characteristic. In *Mathematical foundations of computer science 2010*, volume 6281 of *Lecture Notes in Comput. Sci.*, pages 477–488. Springer, Berlin, 2010.

[GLS93a] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, second edition, 1993.

[GLS93b] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric algorithms and combinatorial optimization*, volume 2 of *Algorithms and Combinatorics*. Springer-Verlag, Berlin, second edition, 1993.

[GPT10] João Gouveia, Pablo A. Parrilo, and Rekha R. Thomas. Theta bodies for polynomial ideals. *SIAM J. Optim.*, 20(4):2097–2118, 2010.

[GS] Daniel R. Grayson and Michael E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/.

[Hil93] David Hilbert. Ueber die vollen Invariantensysteme. *Math. Ann.*, 42(3):313–373, 1893.

[HL19] Hao Hu and Monique Laurent. On the linear extension complexity of stable set polytopes for perfect graphs. *European J. Combin.*, 80:247–260, 2019.

[HS12] Hao Huang and Benny Sudakov. A counterexample to the Alon-Saks-Seymour conjecture and related problems. *Combinatorica*, 32(2):205–219, 2012.

[Kol88] János Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988.

[KT18] Kaveh Khoshkhah and Dirk Oliver Theis. Fooling sets and the spanning tree polytope. *Information Processing Letters*, 132:11–13, 2018.

[KW15] Volker Kaibel and Stefan Weltge. A short proof that the extension complexity of the correlation polytope grows exponentially. *Discrete Comput. Geom.*, 53(2):397–401, 2015.

[Laz77] Daniel Lazard. Algèbre linéaire sur $K[X_1, \cdots, X_n]$, et élimination. *Bull. Soc. Math. France*, 105(2):165–190, 1977.

[LLO15] Bo Li, Benjamin Lowenstein, and Mohamed Omar. Low degree Nullstellensatz certificates for 3-colorability. *ArXiv e-prints*, March 2015.

[LN17] Massimo Lauria and Jakob Nordström. Graph colouring is hard for algorithms based on Hilbert's Nullstellensatz and Gröbner bases. In *32nd Computational Complexity Conference*, volume 79 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 2, 20. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2017.

[Lov68] László Lovász. On chromatic number of finite set-systems. *Acta Math. Acad. Sci. Hungar.*, 19:59–67, 1968.

[Lov72] László Lovász. A characterization of perfect graphs. *J. Combinatorial Theory Ser. B*, 13:95–98, 1972.

[Lov79] László Lovász. On the Shannon capacity of a graph. *IEEE Trans. Inform. Theory*, 25(1):1–7, 1979.

[Lov94] László Lovász. Stable sets and polynomials. *Discrete Math.*, 124(1-3):137–153, 1994. Graphs and combinatorics (Qawra, 1990).

[LPS88] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[LS91] László Lovász and Alexander Schrijver. Cones of matrices and set-functions and 0-1 optimization. *SIAM J. Optim.*, 1(2):166–190, 1991.

[Mar91] Richard Kipp Martin. Using separation algorithms to generate mixed integer model reformulations. *Oper. Res. Lett.*, 10(3):119–128, 1991.

[Mar08a] Susan Margulies. *Computer Algebra, Combinatorics, and Complexity: Hilbert's Nullstellensatz and Np-Complete Problems*. PhD thesis, USA, 2008.

[Mar08b] Simon Marshall. Another simple proof of the high girth, high chromatic number theorem. *Amer. Math. Monthly*, 115(1):68–70, 2008.

[MN08] Kazunori Mizuno and Seiichi Nishihara. Constructive generation of very hard 3-colorability instances. *Discrete Appl. Math.*, 156(2):218–229, 2008.

[MN15] Mladen Mikša and Jakob Nordström. A generalized method for proving polynomial calculus degree lower bounds. In *30th Conference on Computational Complexity*, volume 33 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages 467–487. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2015.

[MY19] Colin McDiarmid and Nikola Yolov. Random perfect graphs. *Random Structures Algorithms*, 54(1):148–186, 2019.

[Pen12] Irena Penev. Coloring bull-free perfect graphs. *SIAM J. Discrete Math.*, 26(3):1281–1309, 2012.

[PS92] Hans Jürgen Prömel and Angelika Steger. Almost all Berge graphs are perfect. *Combin. Probab. Comput.*, 1(1):53–79, 1992.

[Raz98] Alexander A. Razborov. Lower bounds for the polynomial calculus. *Comput. Complexity*, 7(4):291–324, 1998.

[Rei58] István Reiman. Über ein Problem von K. Zarankiewicz. *Acta Math. Acad. Sci. Hungar.*, 9:269–273, 1958.

[Rom16] Romero Barbosa, Julian. Applied hilbert's nullstellensatz for combinatorial problems. Available at http://hdl.handle.net/10012/10897, 2016.

[Rot14] Thomas Rothvoss. The matching polytope has exponential extension complexity. In *STOC'14—Proceedings of the 2014 ACM Symposium on Theory of Computing*, pages 263–272. ACM, New York, 2014.

[Shi13] Yaroslav Shitov. On the complexity of boolean matrix ranks. *Linear Algebra and its Applications*, 439(8):2500–2502, 2013.

[Tao07] Terence Tao. Hilbert's nullstellensatz. https://terrytao.wordpress.com/2007/11/26/hilberts-nullstellensatz/, 2007.

[Tuz84] Zsolt Tuza. Covering of graphs by complete bipartite subgraphs: complexity of 0-1 matrices. *Combinatorica*, 4(1):111–116, 1984.

[Yan91] Mihalis Yannakakis. Expressing combinatorial optimization problems by linear programs. *J. Comput. System Sci.*, 43(3):441–466, 1991.

APPENDICES

Appendix A

Proof of Claim 2.3.11

A.1 A proof using Macaulay2

Let us first give a computer-dependent proof of Claim 2.3.11. For this, we simply have to calculate the leading terms of a Gröbner basis of the ideals $\mathcal{I}_{F_1}, \mathcal{I}_{F_2}, \mathcal{I}_{F_3}$ and $\mathcal{I}_{F_4}$ where $F_1 = E \setminus \{1, 4\}$, $F_2 = E \setminus \{2, 6\}$, $F_3 = E \setminus \{3, 8\}$ and $F_4 = E \setminus \{4, 10\}$. Then, we check that $x^{\boldsymbol{\alpha}} = x_5^2 x_6 x_7 x_8^2 x_9$ is not divisible by any of these. The leading terms output by Macaulay2 are the following:

```
Leading Monomials for I_{F_1}
      {-2} | x_4x_9      |
      {-2} | x_4^2       |
      {-2} | x_3x_7      |
      {-2} | x_3^2       |
      {-2} | x_2x_5      |
      {-2} | x_2^2       |
      {-2} | x_1x_2      |
      {-2} | x_1^2       |
      {-3} | x_9^3       |
      {-3} | x_7^3       |
      {-3} | x_6^3       |
      {-3} | x_5^3       |
      {-3} | x_1x_3x_6   |
```

```
      {-3} | x_1x_3x_5   |
      {-4} | x_1x_6^2x_7 |
      {-4} | x_1x_5^2x_7 |
      {-4} | x_1x_5^2x_6 |

Leading Monomials for I_{F_2}
      {-2} | x_4x_9            |
      {-2} | x_4^2             |
      {-2} | x_3x_7            |
      {-2} | x_3^2             |
      {-2} | x_2^2             |
      {-2} | x_1x_3            |
      {-2} | x_1x_2            |
      {-2} | x_1^2             |
      {-3} | x_9^3             |
      {-3} | x_8^3             |
      {-3} | x_7^3             |
      {-3} | x_5^3             |
      {-3} | x_2x_3x_5         |
      {-3} | x_1x_4x_8         |
      {-3} | x_1x_4x_7         |
      {-3} | x_1x_4x_5         |
      {-4} | x_2x_4x_5x_7      |
      {-4} | x_2x_3x_4x_8      |
      {-4} | x_1x_8^2x_9       |
      {-4} | x_1x_7^2x_9       |
      {-4} | x_1x_7^2x_8       |
      {-4} | x_1x_5^2x_9       |
      {-4} | x_1x_5^2x_8       |
      {-4} | x_1x_5^2x_7       |
      {-5} | x_2x_5x_7^2x_9    |
      {-5} | x_2x_4x_7^2x_8    |
      {-5} | x_2x_4x_5^2x_8    |
      {-5} | x_2x_3x_8^2x_9    |
      {-6} | x_2x_5x_7x_8^2x_9 |
      {-6} | x_2x_5^2x_8^2x_9  |
```

```
      {-6} | x_2x_5^2x_7^2x_8  |

Leading Monomials for I_{F_3}
    {-2} | x_4x_9              |
      {-2} | x_4^2               |
      {-2} | x_3^2               |
      {-2} | x_2x_5              |
      {-2} | x_2^2               |
      {-2} | x_1x_3              |
      {-2} | x_1x_2              |
      {-2} | x_1^2               |
      {-3} | x_9^3               |
      {-3} | x_7^3               |
      {-3} | x_6^3               |
      {-3} | x_5^3               |
      {-3} | x_2x_3x_6           |
      {-3} | x_1x_4x_7           |
      {-3} | x_1x_4x_6           |
      {-3} | x_1x_4x_5           |
      {-4} | x_3x_4x_5x_7        |
      {-4} | x_2x_3x_4x_7        |
      {-4} | x_1x_7^2x_9         |
      {-4} | x_1x_6^2x_9         |
      {-4} | x_1x_6^2x_7         |
      {-4} | x_1x_5^2x_9         |
      {-4} | x_1x_5^2x_7         |
      {-4} | x_1x_5^2x_6         |
      {-5} | x_3x_5^2x_6x_9      |
      {-5} | x_3x_4x_5^2x_6      |
      {-5} | x_2x_4x_6^2x_7      |
      {-5} | x_2x_3x_7^2x_9      |
      {-6} | x_3x_5^2x_7^2x_9    |
      {-6} | x_3x_5^2x_6x_7^2    |
      {-6} | x_2x_6^2x_7^2x_9    |
      {-7} | x_3x_5x_6^2x_7^2x_9 |

Leading Monomials for I_{F_3}
```

```
{-2} | x_4^2                |
   {-2} | x_3x_7             |
   {-2} | x_3^2              |
   {-2} | x_2x_5             |
   {-2} | x_2^2              |
   {-2} | x_1x_3             |
   {-2} | x_1x_2             |
   {-2} | x_1^2              |
   {-3} | x_8^3              |
   {-3} | x_7^3              |
   {-3} | x_6^3              |
   {-3} | x_5^3              |
   {-3} | x_2x_3x_6          |
   {-3} | x_1x_4x_8          |
   {-3} | x_1x_4x_7          |
   {-3} | x_1x_4x_6          |
   {-3} | x_1x_4x_5          |
   {-4} | x_3x_4x_5x_8       |
   {-4} | x_2x_4x_6x_7       |
   {-4} | x_2x_3x_4x_8       |
   {-4} | x_1x_7^2x_8        |
   {-4} | x_1x_6^2x_8        |
   {-4} | x_1x_6^2x_7        |
   {-4} | x_1x_5^2x_8        |
   {-4} | x_1x_5^2x_7        |
   {-4} | x_1x_5^2x_6        |
   {-5} | x_4x_5^2x_6x_7     |
   {-5} | x_3x_4x_5^2x_6     |
   {-5} | x_2x_4x_7^2x_8     |
   {-5} | x_2x_4x_6^2x_8     |
   {-6} | x_4x_5^2x_7^2x_8   |
   {-6} | x_3x_5^2x_6x_8^2   |
   {-6} | x_2x_6^2x_7^2x_8   |
   {-7} | x_4x_5x_6^2x_7^2x_8 |
```

The code used to generate these terms is the following:

```
clearAll
--Number of Colors
k=3;

-- Number of Vertices
n=10;

-- Edge set of the graph
E=matrix{{1,2},{1,3},{2,5},{2,6},{3,7},{3,8},{4,9},{4,10}}; --F1
--E=matrix{{1,2},{1,3},{1,4},{2,5},{3,7},{3,8},{4,9},{4,10}}; --F2
--E=matrix{{1,2},{1,3},{1,4},{2,5},{2,6},{3,7},{4,9},{4,10}}; --F3
--E=matrix{{1,2},{1,3},{1,4},{2,5},{2,6},{3,7},{3,8},{4,9}}; --F4

--Number of edges
m=numgens target E;


-- Define the ring and Monomial Order
R=QQ[x_1..x_n, MonomialOrder=>GLex]

--Polynomials p_u
M_I=matrix{{x_1^k-1}};
for i from 1 to n do (
    M_I=M_I|matrix{{x_i^k-1}};
    );

--Polynomials q_uv
M_J=matrix{{(x_(E_(0,0))^k-x_(E_(0,1))^k)//(x_(E_(0,0))-x_(E_(0,1)))}};
for  j from 1 to m-1 do (
 M_J=M_J|matrix{{(x_(E_(j,0))^k-x_(E_(j,1))^k)//(x_(E_(j,0))-x_(E_(j,1)))}};
    );

--Define the ideal
ColId=ideal(M_I|M_J);

--Find a Grobner basis
```

```
G=gb(ColId);
GensG=gens G;

--Output the leading terms of the basis
transpose(leadTerm(GensG))
```

A.2 A second proof using the LEX order

Before diving into the proof of Claim 2.3.11, it will be useful to introduce some of the terminology found in [FRR06] to our set up. Let $G = (V, E)$ be a graph with $V = [n]$ and let $k \geqslant 3$. For any monomial $x^{\boldsymbol{\beta}}$ with $\boldsymbol{\beta} \in \mathbb{Z}_k^V$ let $\mathcal{V}^0_{\boldsymbol{\beta}}(G) \subseteq \mathbb{K}^V$ be the set of all k-colorings of G and for each $i \in [n-1]$ define the set

$$\mathcal{V}^i_{\boldsymbol{\beta}}(G) := \left\{ (a_{i+1}, \ldots, a_n) : \begin{array}{c} (x, a_{i+1}, \ldots, a_n) \in \mathcal{V}^{i-1}_{\boldsymbol{\beta}}(G), \\ \text{for at least } \boldsymbol{\beta}_i + 1 \text{ colors } x \in \mathbb{K} \end{array} \right\}.$$

In other words, $\mathcal{V}^i_{\boldsymbol{\beta}}(G)$ is the set of all partial colorings of the vertices $i+1, \ldots, n$ that can be extended in at least $\boldsymbol{\beta}_i + 1$ ways to a partial coloring in $\mathcal{V}^{i-1}_{\boldsymbol{\beta}}(G)$.

Lemma A.2.1 ([FRR06])**.** *Let $LM_{LEX}(f) := x^{\boldsymbol{\beta}}$ be the leading monomial of a polynomial $f \in \mathcal{I}_E$ with respect the LEX order. Then, $|\mathcal{V}^{n-1}_{\boldsymbol{\beta}}(G)| \leqslant \boldsymbol{\beta}_n$.*

Proof of Lemma A.2.1. Let $f_0 =: f$ and for every $i \in [n-1]$ let f_i and g_i be the polynomials given by the equation

$$f_{i-1}(x) =: x_i^{\boldsymbol{\beta}_i} f_i(x_{i+1}, \ldots, x_n) + g_i(x_i, \ldots, x_n).$$

Notice that the x_i-degree of g_i is less than $\boldsymbol{\beta}_i$ as $x^{\boldsymbol{\beta}}$ is the leading term of f with respect the LEX order. We claim that each f_i and g_i vanishes at $\mathcal{V}^i_{\boldsymbol{\beta}}$. Indeed, this certainly holds for $i = 0$ as $f_0 \in \mathcal{I}_F$. Now, if the statement holds for $f_{i-1} = x_i^{\boldsymbol{\beta}_i} f_i + g_i$, for every $a \in \mathcal{V}^i_{\boldsymbol{\beta}}(G)$ the polynomial

$$x_i^{\boldsymbol{\beta}_i} f_i(a) + g_i(x_i, a)$$

has at least $\boldsymbol{\beta}_i + 1$ roots, implying that $f_i(a) = g_i(a) = 0$.

The statement follows since the x_n-degree of f_{n-1} is at most $\boldsymbol{\beta}_n$ and $|\mathcal{V}^{n-1}_{\boldsymbol{\beta}}(G)| > \boldsymbol{\beta}_n$ implies that f_{n-1} hast at least $\boldsymbol{\beta}_n + 1$ roots. If f_{n-1} is the zero polynomial, then the monomial $x^{\boldsymbol{\beta}}$ does not appear in f which is a contradiction. □

	Monomial $x^{\boldsymbol{\beta}}$	Condition	Polynomial $f \in \mathcal{I}_{F_i}$ with $LM(f) = x^{\boldsymbol{\beta}}$
1	x_u^2	$uv \in F_i,\ u < v$	$q_{uv}(x)$
2	$x_u x_v$	$uv, uw \in F_i,\ u < v < w$	$(x_u + x_v + x_w)(x_v - x_w)$
3	$x_1 x_u x_v$	$1u, 1\bar{v}, \bar{v}v, u\bar{u} \in F_i$ $1 < \bar{v} < u < v < \bar{u}$	$(x_1 + x_u + x_{\bar{v}})(x_u + x_v + x_{\bar{u}})(x_v - x_{\bar{u}})$
4	$x_1 x_u^2 x_v$	$1\bar{u}, 1\bar{v}, \bar{u}u, \bar{v}v, \bar{v}w \in F_i$ $1 < \bar{u} < \bar{v} < u < v < w$	$(x_1 + x_{\bar{u}} + x_{\bar{v}})(x_u - x_v)(x_u - x_w)(x_v - x_w)$
5	$x_1 x_u^2 x_v$	$1\bar{u}, 1\bar{w}, \bar{u}u, \bar{u}v, \bar{w}w \in F_i$ $1 < \bar{u} < \bar{w} < u < v < w$	$(x_1 + x_{\bar{u}} + x_{\bar{w}})(x_u - x_v)(x_u - x_w)(x_v - x_w)$

Table A.1: Reducible monomials modulo $\mathcal{I}_{F_i}$

Let $G = (V, E)$ be the graph of Example 2.3.10 and let $F_1, \ldots, F_4$ be as defined in the previous subsection. Let $H_i = (V, F_i)$ the corresponding subgraphs of G with edge set equal to F_i. Suppose that $f \in \mathcal{I}_{F_i}$ is a polynomial whose leading monomial is $x^{\boldsymbol{\alpha}} = x_5^2 x_6 x_7 x_8^2 x_9$. We may assume that no monomial $x^{\boldsymbol{\beta}} \neq x^{\boldsymbol{\alpha}}$ appearing in f is reducible, otherwise we may simply replace f by $f - g$ where $g \in \mathcal{I}_{F_i}$ and $LM(g) = x^{\boldsymbol{\beta}}$. In particular, no multiples of the reducible monomials in Table A.1 appear in f (notice that $x^{\boldsymbol{\alpha}}$ is not a multiple of any of the monomials in the table).

We will show that the leading monomial of f with respect the LEX order does not contain any $x_1, \ldots, x_4$ variables. Once we prove this the result follows as any choice of colors for the vertices $5, 6, \ldots, 10$ can always be extended to a coloring of H_i. Indeed, the only way such a coloring cannot be extended is if it forces the colors of the vertices $2, 3$ and 4 to be all different *and* 1 is adjacent to all $2, 3$ and 4. But this two conditions are never satisfied in H_i. In particular, $|\mathcal{V}^9_{\boldsymbol{\beta}}(H_i)| \geqslant 3$ for every monomial $x^{\boldsymbol{\beta}}$ with $\operatorname{supp}(\boldsymbol{\beta}) \subseteq \{5, \ldots, 10\}$ and f must be the zero polynomial, a contradiction. This proves the irreducibility of $x^{\boldsymbol{\alpha}}$ modulo $\mathcal{I}_{F_i}$. We consider each F_i separately.

1. Consider the the graph H_1 (see Figure A.1) obtained from G after the deletion of the edge $\{1, 4\}$. This graph contains has two connected components which we call $H' = (U', F')$ and $H'' = (U'', F'')$. Let $x^{\boldsymbol{\beta}}$ be the leading term of f with respect to the LEX order. Since H' and H'' are not connected, if we write $x^{\boldsymbol{\beta}} =: x^{\boldsymbol{\beta}'} x^{\boldsymbol{\beta}''}$ where

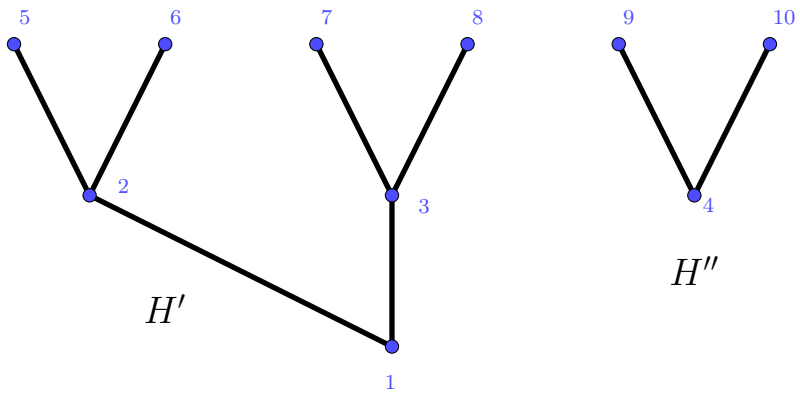


Figure A.1: The graph of Example 2.3.10 minus the edge $\{1, 4\}$

$\operatorname{supp}(\boldsymbol{\beta}') \subseteq U'$ and $\operatorname{supp}(\boldsymbol{\beta}'') \subseteq U''$, then

$$|\mathcal{V}^7_{\boldsymbol{\beta}'}(H')| \geqslant \boldsymbol{\beta}_8 \text{ and } |\mathcal{V}^9_{\boldsymbol{\beta}''}(H'')| \geqslant \boldsymbol{\beta}_{10} \Longrightarrow |\mathcal{V}^9_{\boldsymbol{\beta}}(H)| \geqslant \boldsymbol{\beta}_{10}$$

We claim that $|\mathcal{V}^9_{\boldsymbol{\beta}''}(H'')| \geqslant \boldsymbol{\beta}_{10}$. Indeed, by the first and second rows of Table A.1, no multiples of x_4^2 and x_4x_9 appear in f, thus

$$x^{\boldsymbol{\beta}''} \in \{x_4 x_{10}^{\boldsymbol{\beta}_{10}}, x_9^{\boldsymbol{\beta}_9} x_{10}^{\boldsymbol{\beta}_{10}}\}.$$

Now, pick any color $\zeta \in \mathbb{K}$ for vertex 10, if $\boldsymbol{\beta}_4 = 1$ we can color vertex 9 with color ζ as well so that vertex 4 has two colors available. If $\boldsymbol{\beta}_4 = 0$, then we can pick any color for vertex 9 and vertex 4 will always have at least one color available.

Let us prove that $1, 2, 3 \in \operatorname{supp}(\boldsymbol{\beta}')$ implies that $|\mathcal{V}^7_{\boldsymbol{\beta}'}(H')| \geqslant \boldsymbol{\beta}_8$.

1.1. Suppose that $x_1 | x^{\boldsymbol{\beta}'}$ so that $\mathcal{V}^1_{\boldsymbol{\beta}'}(H')$ is the set of all partial colorings $(a_i)_{i\geqslant 2}$ that satisfy $a_2 = a_3$. By the second row of Table A.1, $2 \notin \operatorname{supp}(\boldsymbol{\beta}')$. Thus, $\mathcal{V}^2_{\boldsymbol{\beta}'}(H')$ is the set of all partial colorings $(a_i)_{i\geqslant 3}$ that satisfy $a_3 \notin \{a_5, a_6\}$ (this way we can always pick a color for vertex 2 satisfying $a_2 = a_3$).

1.1.1. Suppose further that $x_1x_3 | x^{\boldsymbol{\beta}'}$. Then, $\mathcal{V}^3_{\boldsymbol{\beta}'}(H')$ is the set of all partial colorings $(a_i)_{i\geqslant 5}$ that satisfy $a_5 = a_6 = a_7 = a_8$. By the second and third rows of Table A.1, neither 5 or 6 or 7 appear in the support of $\boldsymbol{\beta}'$. Then, we can write

$$x^{\boldsymbol{\beta}'} = (x_1x_3x_8^{\boldsymbol{\beta}_8})$$

From here we see that $|\mathcal{V}^7_{\boldsymbol{\beta}'}(H')| \geqslant \boldsymbol{\beta}_8$. Indeed, pick any color $\zeta \in \mathbb{K}$ for vertex 8. Then color all the vertices $5, 6$ and 7 with color ζ. We have two choices of colors for vertex 3, say we color vertex 3 with ζ'. Then we color vertex 2 with ζ'. The resulting partial coloring can be extended in two ways to a coloring of H'.

1.1.2. Suppose that $3 \notin \operatorname{supp}(\boldsymbol{\beta}')$. Then, a partial coloring $(a_i)_{i\geqslant 5}$ is in $\mathcal{V}^3_{\boldsymbol{\beta}'}(H')$ only if we can pick a color a_3 satisfying $a_3 \notin \{a_5, a_6\}$ and $a_3 \notin \{a_7, a_8\}$. Equivalently, the set $\{a_5, a_6, a_7, a_8\}$ must have at most two different colors. By the fourth and fifth rows of Table A.1, the monomials $x_5^2x_6, x_5^2x_7, x_6^2x_7$ do not divide $x^{\boldsymbol{\beta}'}$.

1.1.1.2.1 If $\boldsymbol{\beta}_5 = 2$ then $\boldsymbol{\beta}_6 = \boldsymbol{\beta}_7 = 0$. In that case for any given color of vertex 8, we can color the vertices $6, 7$ with this same color. Now, for any choice of color for vertex 5, the vertices 5 to 8 use at most two colors.

1.1.1.2.2. If $\boldsymbol{\beta}_6 = 2$ then $\boldsymbol{\beta}_7 = 0$. Here, we pick the same color for 7 and 8 and choose any color of 6. We always have at least two choices for 5 so that the vertices 5 to 8 use at most two colors. We can then proceed as above.

1.1.1.2.3. If $\boldsymbol{\beta}_5$ and $\boldsymbol{\beta}_6$ are at most one, then we pick any pair of colors for vertices 7 and 8. We would have always at least two colors available for vertices 5 and 6 such that the number of colors appearing on the vertices 5 to 8 is at most two.

1.2. Suppose that $1 \notin \operatorname{supp}(\boldsymbol{\beta})$. Then any partial coloring $(a_i)_{i\geqslant 2}$ is in $\mathcal{V}^1_{\boldsymbol{\beta}'}(H')$. Suppose that $x_2|x^{\boldsymbol{\beta}'}$, hence $\mathcal{V}^2_{\boldsymbol{\beta}'}(H')$ is the set of partial colorings $(a_i)_{i\geqslant 3}$ such that $a_5 = a_6$. By the second row of Table A.1 $5 \notin \operatorname{supp}(\boldsymbol{\beta}')$. Again, we have two cases:

1.2.1. If $3 \in \operatorname{supp}(\boldsymbol{\beta}')$, then $7 \notin \operatorname{supp}(\boldsymbol{\beta}')$. Pick any color for vertex 8, color 7 with this color as well. Then, pick any color for vertex 6 and color 5 with this same color. Then, both 2 and 3 have two colors available. Any choice is possible to be extended to a coloring of H' as vertex 1 is adjacent to only two vertices.

1.2.2. If $3 \notin \operatorname{supp}(\boldsymbol{\beta}')$, then we pick any colors for vertices 6, 7 and 8. Then, we color vertex 5 with the color of 6. Since 3 is adjacent to only 7 and 8 we always have at least one color available for it. We have two colors available for vertex 2 as well. This can be further extended to a coloring of H'.

This shows that $2 \notin \operatorname{supp}(\boldsymbol{\beta}')$.

1.3. Finally, suppose that $x_3|x^{\boldsymbol{\beta}'}$. Then, by the second row of Table A.1, $7 \notin \operatorname{supp}(\boldsymbol{\beta})$. We pick any color of vertex 8 and use it on vertex 7. Pick any colors for vertices 5 and 6. This guarantees that have at least two choices for 3, which can be extended to colorings of H'.

The above proves that $1, 2, 3 \notin \operatorname{supp}(\boldsymbol{\beta})$. The case $4 \notin \operatorname{supp}(\boldsymbol{\beta})$ follows from the fact that any coloring of the vertices 5 to 8 can always be extended to a coloring of H'. Thus, in fact we have shown that $|\mathcal{V}^7_{\boldsymbol{\beta}'}(H')| \geqslant \boldsymbol{\beta}_8$ as long as $\boldsymbol{\beta}$ does is not a multiple of the monomials in Table A.1 as desired.

2. Now consider the graph $H = H_i$ with edge set $F = F_i$ for some $i \in \{2, 3, 4\}$. Then, we have the following:

   2.1. Suppose that $x_1|x^{\boldsymbol{\beta}}$. Then, $\mathcal{V}^1_{\boldsymbol{\beta}}(H)$ is the set of all partial colorings $(a_i)_{i\geqslant 2}$ such that $a_2 = a_3 = a_4$. By the second row in Table A.1, we have that $2, 3 \notin \operatorname{supp}(\boldsymbol{\beta})$. Then, $\mathcal{V}^3_{\boldsymbol{\beta}}(H)$ is the set of all partial colorings $(a_i)_{i\geqslant 4}$ such that the children of 2 and 3 use at most two colors and one of the remaining colors is used by vertex 4. This way we can always color the vertices $2, 3$ and 4 with the same color.

      2.1.1. Suppose that $x_1x_4|x^{\boldsymbol{\beta}}$. Then, $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ is the set of partial colorings $(a_i)_{i\geqslant 5}$ such that the children of $2, 3$ and 4 use at most one color. By the third row in Table A.1 none of the children of 2 and 3 are in $\operatorname{supp}(\boldsymbol{\beta})$. Additionally, by the second row of Table A.1, we have $9 \notin \operatorname{supp}(\boldsymbol{\beta}')$ if 4 has both children in H. In any case, given any color for the largest children of vertex 4, we can always use the same color on all the children of $2, 3$ and 4 as required.

      2.1.2. Suppose that $4 \notin \operatorname{supp}(\boldsymbol{\beta})$. Then, $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ is the set of partial colorings $(a_i)_{i\geqslant 5}$ such that the children of $2, 3$ and 4 use at most two colors. By row fourth and fifth of Table A.1 no monomial $x_u^2x_v$ divides $x^{\boldsymbol{\beta}}$ for every child u of 2 or 3 and any v with $u < v$.

         2.1.2.1. If $x_1x_u^2|x^{\boldsymbol{\beta}}$ for some children u of 2 or 3, then $\boldsymbol{\beta}_v = 0$ for all $v > u$. Color the vertices $v > u$ using the same color and color u with any plausible color. Then, for every children of w of 2 or 3 with $w < u$, we have at least two choices for which we can obtain a partial coloring of H coloring the children of $2, 3$ and 4 with at most two colors.

         2.1.2.2. If $\boldsymbol{\beta}_u \leqslant 1$ for every children of 2 or 3, then we pick any color for the children of 4 in H. Then, for every children of u of 2 or 3, we have at least two choices for which we can obtain a partial coloring of H coloring the children of $2, 3$ and 4 with at most two colors.

2.2. Suppose that $1 \notin \operatorname{supp}(\boldsymbol{\beta})$, so $\mathcal{V}^1_{\boldsymbol{\beta}}(H)$ is the set of partial colorings $(a_i)_{i\geqslant 2}$ such that the set $\{a_2, a_3, a_4\}$ has at most two colors. Suppose that $x_2|x^{\boldsymbol{\beta}}$ and let u be the largest children of 2 in H. Then, $\mathcal{V}^2_{\boldsymbol{\beta}}(H)$ is the set of colorings $(a_i)_{i\geqslant 3}$ such that the children of 2 in H use exactly one color and either $a_3 = a_4$ or the colors a_u, a_3 and a_4 are all different.

2.2.1. Suppose that $x_2x_3|x^{\boldsymbol{\beta}}$ and let v and w be the largest children of 3 and 4 in H respectively. In this case, $\mathcal{V}^3_{\boldsymbol{\beta}}(H)$ is the set of partial colorings $(a_i)_{i\geqslant 4}$ such that the children of 3 are colored with the same color, $a_v = a_u$ and $a_4 \neq a_u$. Indeed, if $a_4 = a_u$ then the only way we would be able to extend the coloring to a coloring in $\mathcal{V}^2_{\boldsymbol{\beta}}(H)$ is by setting $a_3 = a_4$. Also, if $a_4 \neq a_u$ and $a_v \neq a_u$ then either $a_4 = a_v$, in which case the only available extension in $\mathcal{V}^2_{\boldsymbol{\beta}}(H)$ is to set $a_3 \notin \{a_u, a_4\}$, or $a_4 \neq a_v$ and the only available extension in $\mathcal{V}^2_{\boldsymbol{\beta}}(H)$ is to set $a_3 = a_4$. We claim that the monomial $x_2x_3x_u$ is reducible modulo $\mathcal{I}_F$. First, notice that

$$h(x) := (x_2 - x_3)(x_2 - x_4)(x_3 - x_4) \in \mathcal{I}_F.$$

Indeed, since 1 is adjacent to $2, 3$ and 4, it must be the case that at least two of x_2, x_3 and x_4 are the same. In particular, we have that

$$h(x) - (x_3 - x_4)q_{2u}(x) + (x_2 - x_4)q_{3v}(x) \in \mathcal{I}_F$$

and the leading term of the polynomial above is in fact $x_2x_3x_u$. Thus, we may assume that no children of 2 is in the support of $\boldsymbol{\beta}$.

2.2.1.1. Suppose that $x_2x_3x_4|x^{\boldsymbol{\beta}}$, so $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ is the set of partial colorings $(a_i)_{i\geqslant 5}$ such that the children of $2, 3$ and 4 use at most one color. In addition, w is the only possible child of 4 in the support of $\boldsymbol{\beta}$. We claim that $x_2x_3x_4x_v$ is reducible, indeed consider the polynomials:

$$\begin{aligned} f_1(x) &= (x_4 + x_v + x_w)(x_v - x_w), \\ f_2(x) &= (x_3 + x_u + x_v), \\ f_3(x) &= (x_2 - x_3 - x_4 + x_u). \end{aligned}$$

Let $a = (a_i)_{i\geqslant 1}$ be a coloring of H. If f_1 does not vanish on a then $a_v \neq a_w$ and since 4 is adjacent to w, it also holds that $a_4 = a_v$. If in addition f_2 does not vanish on a, then either $a_u = a_3$ or $a_u = a_v = a_4$.

In any case, since 1 is adjacent to $2, 3$ and 4 we must have that $a_2 \in \{a_3, a_4\} \setminus \{a_u\}$ and $f_3(a) = 0$. This shows that $f_1 f_2 f_3 \in \mathcal{I}_F$.
From the above, we may assume that no children of 2 or 3 is in the support of $\boldsymbol{\beta}$ and we can write $x^{\boldsymbol{\beta}} = x_2 x_3 x_4 x_w^{\boldsymbol{\beta}_w}$. But then, for every given color to w we can color the rest of the children of $2, 3$ and 4 with this color as well. Each of the vertices $2, 3$ and 4 would have exactly the same two choices of colors available, thus we can always extend any of those choices to a coloring of H.

2.2.1.2. Suppose that $4 \notin \operatorname{supp}(\boldsymbol{\beta})$, then $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ is the set of partial colorings $(a_i)_{i \geqslant 5}$ such that the children of 2 and 3 use the same color $a_u = a_v$ and the children of $2, 3$ and 4 use at most two colors. In particular, a necessary condition for a partial coloring $(a_i)_{i \geqslant 5}$ for not being in $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$ is that both children of 4 are in H. In that case we claim that $x_2 x_3 x_v^2 x_9$ is reducible modulo $\mathcal{I}_F$. Indeed, consider the polynomials

$$\begin{aligned} f_1(x) &= (x_v - x_9)(x_v - x_{10})(x_9 - x_{10}), \\ f_2(x) &= (x_3 + x_u + x_v), \\ f_3(x) &= (x_2 - x_3 - x_4 + x_u). \end{aligned}$$

Notice that if f_1 does not vanish at a coloring a of H, then all a_v, a_9 and a_{10} are pairwise different. Since 4 is adjacent to both 9 and 10, we conclude that $a_4 = a_v$. From here, one can prove that $f_1 f_2 f_3 \in \mathcal{I}_F$ following the same analysis made for the monomial $x_2 x_3 x_4 x_v$ above.
From the above, if $x_2 x_3 x_v^2 | x^{\boldsymbol{\beta}}$ and 4 has both children in H then $9 \notin \operatorname{supp}(\boldsymbol{\beta})$. But then, given any color for the vertex 10 we can color 9 with the same color. Furthermore, given any color for v, we can color all the children of vertices 2 and 3 with the same color. Thus, using at most two colors among the children of $2, 3$ and 4 and coloring the children of 2 and 3 with the same color as desired.
If $\boldsymbol{\beta}_v \leqslant 1$, then given any pair of colors for the vertices 9 and 10, say ζ and ζ', then we color v with any of these two colors. Next, we color all the children of 2 and 3 with the color used for vertex v. Thus, using at most two colors among the children of $2, 3$ and 4 and coloring the children of 2 and 3 with the same color as desired.

2.2.2. Suppose that $3 \notin \operatorname{supp}(\boldsymbol{\beta})$. Again, let w be the largest children of 4. In this case a partial coloring $(a_i)_{i \geqslant 4}$ is in $\mathcal{V}^3_{\boldsymbol{\beta}}(H)$ if the children of 2 use the

same color and either no children of 3 is colored with color a_4 (this way we can color 3 and 4 with the same color), or $a_u \neq a_4$ and the children of 3 are colored with colors in $\{a_4, a_u\}$ (this way we can color $3, 4$ and u with pairwise different colors).

2.2.2.1 Suppose that $x_2x_4|x^{\boldsymbol{\beta}}$, so $\mathcal{V}^4_{\boldsymbol{\beta}}$ is the set of partial colorings $(a_i)_{i\geqslant 5}$ such that the children of 2 use color a_u, the children of 4 use color a_w and either $a_u \neq a_w$ in which case the children of 3 are colored with color $a_v \notin \{a_u, a_w\}$, or $a_u = a_w$ in which case if the children of 3 use two colors, one of those should be equal to a_u. The only plausible children of 4 in the support of $\boldsymbol{\beta}$ is w. We claim that the monomial $x_2x_4x_u^2x_v$ is reducible for every child v of 3. Indeed, consider the polynomials:

$$\begin{aligned} f_1(x) &:= (x_u + x_v + x_w)(x_u - x_w)(x_v - x_w) \\ f_2(x) &:= (x_4 + x_v + x_w) \\ f_3(x) &:= (x_2 - x_3). \end{aligned}$$

Any coloring a of H should vanish on $f_1f_2f_3$: if $f_1(a)$ is not zero then $a_v \neq a_w$ and $a_u = a_v$. If additionally $f_2(a)$ is non-zero, then $a_4 = a_u = a_v$ because 4 and w are adjacent. Since 3 and v are adjacent we have $a_3 \neq a_4$ and since 2 and u are adjacent, we conclude that $a_2 = a_3$ and $f_3(a) = 0$.

2.2.2.1.1 Since $x_2x_4x_u^2x_v$ is reducible, if x_u^2 divides $x^{\boldsymbol{\beta}}$ then no children of 3 appear in the support of $\boldsymbol{\beta}$. Now, given any color for w, say ζ, we color the all the children of 3 and 4 with color ζ as well. Given any color for u, say ζ', we color any other children of 2 with color ζ' as well. This partial coloring is in $\mathcal{V}^4_{\boldsymbol{\beta}}$ regardless of the choice of colors for w and u.

2.2.2.1.2 Suppose that $\boldsymbol{\beta}_u \leqslant 1$. We further have two cases:

2.2.2.1.2.1. Both children of 3 are in H. Then, we claim that the monomial $x_2x_4x_ux_7$ is reducible. Indeed, consider the polynomials:

$$\begin{aligned} f_1(x) &:= (x_2 + x_u + x_w)(x_4 + x_7 + x_8)(x_u - x_w)(x_7 - x_8) \\ f_2(x) &:= (x_2 - x_4)(x_7 - x_w)(x_8 - x_w)(x_7 - x_8) \\ f_3(x) &:= f_1(x) - f_2(x). \end{aligned}$$

For any coloring a of H if $f_1(a) \neq 0$, then $a_7 \neq a_8$, $a_u \neq a_w$, $a_4 \in \{a_7, a_8\}$ and since 2 is adjacent to u, we have $a_2 = a_w$. Since the colors a_2, a_3 and a_4 are not pairwise distinct and 4 is adjacent to w, then $a_2 = a_3 \notin \{a_7, a_8\}$. This implies that $a_u \in \{a_7, a_8\}$ and the colors a_7, a_8 and a_w are pairwise distinct, so $a_7 + a_8 + a_w = 0$. We claim that $f_1(a) = f_2(a)$. Indeed, if $a_4 \neq a_u$ then $\{a_4, a_u\} = \{a_7, a_8\}$ and $a_4 + a_u + a_w = 0$, thus

$$\begin{aligned}(a_2 + a_u + a_w)(a_4 + a_7 + a_8)(a_u - a_w) = \\ (a_2 - a_4)(a_4 - a_w)(a_u - a_w) = \\ (a_2 - a_4)(a_7 - a_w)(a_8 - a_w).\end{aligned}$$

Suppose now that $a_4 = a_u$ and suppose that $a_4 = a_7$ (the case $a_4 = a_8$ is similar). Then,

$$\begin{aligned}(a_2 + a_u) + a_w = -a_8 + a_w = -(a_8 - a_w), \\ a_4 + (a_7 + a_8) = a_4 - a_2 = -(a_2 - a_4), \\ a_u - a_w = a_7 - a_w,\end{aligned}$$

and $f_1(a) = f_2(a)$ as desired.
Thus, if $\boldsymbol{\beta}_u = 1$ then $6 \notin \operatorname{supp}(\boldsymbol{\beta})$. Now, given any color for w, say ζ, we can color any other children of 4 with ζ as well. Given any color for 8, say ζ', we can color 7 with color ζ' as well. Next, for u we pick any color ζ'' not equal to ζ' and color any other children of 2 with color ζ'' as well. We have two choices for vertex 4, let ω be one of those choices. If $\omega \neq \zeta'$, then we can color vertex 3 with color ω as well and any choice available for 2 can be extended to a coloring of H. If $\omega = \zeta'$, then $\zeta'' \neq \omega$ and we can color 3 with some color $\omega' \notin \{\omega, \zeta'\}$. Here any color available for 2 can be extended to a coloring of H as well.

2.2.2.1.2.2. Suppose that only one children of 3 lie in H, then we can proceed as in the case above as the children of 3 use at most one color. Indeed, we color the children of 4 with color ζ, the child of 3 with any color ζ' and the children of 2 with any color $\zeta'' \neq \zeta'$. We have two choices to color vertex 4, say we use color ω. If $\omega \neq \zeta'$ we can color 3 with ω as well and proceed as above. If $\omega = \zeta'$ then $\zeta'' \neq \omega$ and we proceed as above.

2.2.2.2. Suppose that $4 \notin \operatorname{supp}(\boldsymbol{\beta})$. Then, a partial coloring $(a_i)_{i\geqslant 5}$ is in $\mathcal{V}^4_{\boldsymbol{\beta}}$ if the children of 2 use one color, namely a_u, and either the children of 3 and 4 are colored with at most two colors, or the children of 3 and 4 use three colors, but if the children of either 3 or 4 use two colors one of those should be equal to a_u.

2.2.2.2.1. Suppose that $x_2x_u|x^{\boldsymbol{\beta}}$.

2.2.2.2.1.1. If $\boldsymbol{\beta}_u = 1$, then $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$ is the set of partial colorings such that either the children of 3 and 4 are colored with at most two colors (hence we can always guarantee an extension coloring 3 and 4 with the same color) or the children of 3 and 4 are colored using three colors, but the children of at least one of 3 or 4 use exactly one color (this way we can guarantee at least two choices for u such that we can color 3, 4 and u with different colors). Thus, if there is a partial coloring not in $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$ a necessary condition is that the vertices $7, \ldots, 10$ all appear in H. If that is the case the monomials $x_2x_ux_7^2x_9$ and $x_2x_ux_7x_8^2x_9$ are reducible:

$$
\begin{aligned}
f_1(x) &= (x_7 - x_8)(x_7 - x_9)(x_9 - x_{10}),\\
f_2(x) &= (x_7 - x_8)(x_8 - x_9)(x_8 - x_9)(x_9 - x_{10}),\\
f_3(x) &= (x_u - x_7 - x_8 - x_9 - x_{10}),\\
f_4(x) &= (x_2 - (x_3 + x_4 - x_u)).
\end{aligned}
$$

Let a be a coloring of H. If $f_1(a)$ or $f_2(a)$ are non-zero then the partial coloring $(a_7, \ldots, a_{10})$ is not in $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$. In particular, a_3 and a_4 must be different and $a_3 = -a_7 - a_8$, $a_4 = -a_9 - a_{10}$. If additionally $f_3(a)$ is non-zero then a_u should be equal a_3 or a_4. In that case, since 2 is adjacent to u, a_u must be equal to $a_3 + a_4 - a_u$. The polynomials $f_4f_3f_1$ and $f_4f_3f_2$ must be in $\mathcal{I}_F$ and our claim follows.

From the above, we conclude that $\boldsymbol{\beta}_u = 1$ and $\boldsymbol{\beta}_7 = 2$ implies $\boldsymbol{\beta}_9 = 0$. In that case we can always color the vertices 9 and 10 using the same color, thus any choice of color for 10 can be extended to a coloring in $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$. This holds also in the case that $\boldsymbol{\beta}_7 = 1$ and $\boldsymbol{\beta}_8 = 2$. If $\boldsymbol{\beta}_7, \boldsymbol{\beta}_8$ are at most one, then for any choices of colors for 9 and 10, we have at least two choices for 7 and 8 so that the number of colors used by $7, 8, 9$ and 10 is at most two. Thus, the resulting

partial coloring will be in $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$, so this case cannot happen for $\boldsymbol{\beta}$ either.

2.2.2.2.1.2. Suppose that $x_2x_u^2|x^{\boldsymbol{\beta}}$. Then a partial coloring in $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$ should necessarily color the children of 3 and 4 using two colors. Otherwise, there will be an option for u so that the colors of 3 and 4 are different, but the color of u is the same to one these two. If 4 has two children in H, then the monomial $x_2x_u^2x_v^2x_9$ is reducible for any child v of 3. Similarly, if 3 has two children in H then the monomial $x_2x_u^2x_7^2x_8$ is reducible. Indeed, consider the polynomials

$$\begin{aligned} f_1(x) &= (x_v - x_9)(x_v - x_{10})(x_9 - x_{10}),\\ f_2(x) &= (x_u - x_9)(x_u - x_{10}),\\ f_3(x) &= (x_2 - x_3). \end{aligned}$$

$$\begin{aligned} g_1(x) &= (x_7 - x_8)(x_7 - x_w)(x_8 - x_w),\\ g_2(x) &= (x_u - x_7)(x_u - x_8),\\ g_3(x) &= (x_2 - x_4) \end{aligned}$$

Again, let a be any coloring of H. If $f_1(a) \neq 0$, then the colors a_v, a_9, a_{10} are all different and $a_4 = a_v$. If in addition $f_2(a) \neq 0$, then $a_u = a_v = a_4$. Since 2 is adjacent to u we conclude that $a_2 = a_3$ and the polynomial $f_1f_2f_3$ vanishes on a. A similar analysis works for $g_1g_2g_3$.

Suppose that $\boldsymbol{\beta}_v = 2$ for some child of 3 and 4 has two children in H. Then, $\boldsymbol{\beta}_9 = 0$ so for any choice of color for 10, we can also color 9 with the same color. If 3 has only one children in H, then any coloring of v gives rise to a coloring that uses at most two colors on the children of 3 and 4, thus in $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$ as desired. If 3 has both of its children in H and $v = 8$, then $\boldsymbol{\beta}_7 \leqslant 1$. For any choice of coloring for 8, the vertex 7 has at least two colors available to obtain a partial coloring in $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$. If $v = 7$, then $\boldsymbol{\beta}_8 = 0$ otherwise $x^{\boldsymbol{\beta}}$ is reducible. But then, we can color the vertices of $8, 9$ and 10 using the same color, thus any choice of color for 7 gives a partial coloring in $\mathcal{V}^u_{\boldsymbol{\beta}}(H)$. A similar reasoning works if $\boldsymbol{\beta}_v = 2$ for some child v of 3 and 4 has only one children in H.

Now, suppose that $\boldsymbol{\beta}_v \leqslant 1$ for every children v of 3. Then, given any coloring of the children of 4 we have always at least two plausible colors for the children of 3 so that the total number of colors used by the children of 3 and 4 is at most two as desired.

2.2.3 Suppose that $3, 4$ and no child of 2 is in the support of $\boldsymbol{\beta}$. Then, $\mathcal{V}^u_{\boldsymbol{\beta}}$ is the set of any plausible partial colorings $(a_i)_{i\geqslant 7}$ of the vertices $7, \ldots, 10$. Indeed, if the number of colors used by the children of 3 and 4 is at most two, then we color the children of 2 using the same color. The resulting coloring will be in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ (see 2.2.2.2. above). If the children of 3 and 4 use three colors, then either the children of 3 or 4 use one color or there is some color $\{a_7, a_8\} \cap \{a_9, a_{10}\}$. In the first case, say the children of 3 use different colors and the children of 4 use at most one color, we color the children of 2 with one of the colors used by one of the children of 3. In the second case, we color 2 with the color in the intersection $\{a_7, a_8\} \cap \{a_9, a_{10}\}$. The resulting coloring is in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ (see 2.2.2.2. above).

2.3. Suppose that $1, 2 \notin \operatorname{supp}(\boldsymbol{\beta})$ and $3 \in \operatorname{supp}(\boldsymbol{\beta})$. Let v be the largest child of 3. Then, $\mathcal{V}^3_{\boldsymbol{\beta}}(H)$ is the set of colorings $(a_i)_{i\geqslant 4}$ such that the children of 3 use the same color and either the children of 2 use one color, or the children of 2 use two colors $a_5 \neq a_6$ and either $a_4 \notin \{a_5, a_6\}$ (hence, regardless of the color given for 3, the colors for 2 and 4 will be the same) or $a_v \in \{a_5, a_6\} \setminus \{a_4\}$ (hence, any plausible color for 3 is either equal to a_4 or equal to the only color available for 2). From the above, we may assume that both vertices of 2 lie in H, otherwise any partial coloring $(a_i)_{i\geqslant 4}$ would be in $\mathcal{V}^3_{\boldsymbol{\beta}}(H)$.

2.3.1. Suppose that $x_3x_4|x^{\boldsymbol{\beta}}$ and let w be the largest child of 4 in H. Then, $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ is the set of colorings $(a_i)_{i\geqslant 5}$ such that the children of 3 use at most one color, the children of 4 is at most one color and either $a_5 = a_6$, or $a_5 \neq a_6$ and the children of 3 and 4 satisfy $a_v = a_w \in \{a_5, a_6\}$.

2.3.1.1. Suppose that $x_3x_4x_5|x^{\boldsymbol{\beta}}$. If $\boldsymbol{\beta}_5 = 1$, then $\mathcal{V}^5_{\boldsymbol{\beta}}(H)$ is the set of colorings $(a_i)_{i\geqslant 6}$ such that the children of 3 and 4 use at most one coloring. We claim that $x_3x_4x_5x_v$ is reducible. Indeed consider the polynomials:

$$
\begin{aligned}
f_1(x) &= (x_3 + x_4 + x_w)(x_4 + x_5 + x_6)(x_5 - x_6)(x_v - x_w),\\
f_2(x) &= (x_3 - x_4)(x_5 - x_6)(x_5 - x_w)(x_6 - x_w),\\
f_3(x) &= f_1(x) - f_2(x).
\end{aligned}
$$

Notice that the leading term of f_3 is $x_3x_4x_5x_v$, the proof that f_3 vanishes on every coloring of H is similar to that of the polynomial f_3 in 2.2.2.1.2.1.

From the above, we may assume that $v \notin \operatorname{supp}(\boldsymbol{\beta})$. But then, given any color for the vertex w, say a_w, we may color the children of 3 and 4 using color a_w. The resulting partial coloring is in $\mathcal{V}^5_{\boldsymbol{\beta}}(H)$.

2.3.1.2. Now, suppose that $\boldsymbol{\beta}_5 = 2$. Then $\mathcal{V}^5_{\boldsymbol{\beta}}(H)$ is the set of colorings $(a_i)_{i\geqslant 6}$ such that 6 and the children of 3 and 4 use at most one coloring. We claim that $x_3x_4x_5^2x_6$ is reducible. Indeed, consider the polynomials

$$\begin{aligned} f_1(x) &:= (x_5 - x_6)(x_5 - x_w)(x_6 - x_w), \\ f_2(x) &:= (x_3 - x_4)(x_4 + x_v + x_w) + (x_4^2 + x_4x_u + x_u^2), \\ f_3(x) &:= f_1(x)f_2(x). \end{aligned}$$

Let $(a_i)_i$ be a coloring of H and suppose that $f_1(a) \neq 0$. Then, a_5, a_6 and a_w are pairwise distinct, in particular $a_2 = a_w$. If a_4, a_v and a_w are pairwise distinct, then $f_2(a) = 0$ so let us assume this is not the case. If $a_4 \neq a_v$, then $a_v = a_w$ and hence $a_3 \neq a_w = a_2$. So a_3 should be equal to a_4 and $f_2(a) = 0$. If $a_4 = a_v$, then $a_3 \neq a_4$ and as a consequence $a_3 = a_2 = a_w$. In this case we have

$$f_2(a) = (a_3 - a_4)(2a_4 + a_3) + 3a_4^2 = a_3^2 + a_3a_4 + a_4^2 = 0.$$

The above equality follows as $a_3 \neq a_4$. This shows that $x_3x_4x_5^2x_6$ is reducible.

From the above, we may assume that $6, v \notin \operatorname{supp}(\boldsymbol{\beta})$. Thus, given any coloring of vertex w, we may use the same color on the vertex 6 and the children of 3 and 4. The resulting partial coloring will be in $\mathcal{V}^5_{\boldsymbol{\beta}}(H)$.

2.3.2. Suppose that $4 \notin \operatorname{supp}(\boldsymbol{\beta})$. Here we consider two cases:

2.3.2.1 Suppose that both children of 3 are in H and let w be the unique child of 4. Then $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ is the set of partial colorings $(a_i)_{i\geqslant 5}$ such that the children of 3 use one color and either $a_5 = a_6$, or $a_5 \neq a_6$ and $a_w \in \{a_5, a_6\}$ (this way we can always extend to a coloring satisfying $a_2 = a_4$), or a_5, a_6 and a_w are pairwise distinct and $a_v \in \{a_5, a_6\}$ (this way we can choose a color $a_4 \in \{a_5, a_6\} \setminus \{a_v\}$).

2.3.2.1.1. Suppose that $x_3x_5|x^{\boldsymbol{\beta}}$. We claim that the monomial $x_3x_5^2x_6x_8^2$ is reducible. Indeed, consider the polynomials

$$f_1(x) := x_8^2 + x_8x_w + x_w^2,$$
$$f_2(x) := (x_5 - x_6)(x_5 - x_8)(x_6 - x_8),$$
$$f_3(x) := (x_3 - x_4)f_1(x)f_2(x).$$

Let $a = (a_i)_{i\geqslant 1}$ be a coloring of H. If $f_1(a) \neq 0$ then $a_8 = a_{10}$. If in addition $f_2(a) \neq 0$ then a_5, a_6 and a_8 are pairwise disjoint and $a_2 = a_8 = a_{10}$. But then a_3 and a_4 should be equal, 3 and 4 are both adjacent to vertices having color equal to a_2. This shows that $f_3(a) = 0$.

From the above, if $\boldsymbol{\beta}_5 = 2$ and $6 \in \operatorname{supp}(\boldsymbol{\beta})$ then $\boldsymbol{\beta}_8 \leqslant 1$. In this case, for any given color of w, say a_w, we have at least two options for $a_8 \neq a_w$. For any given colors a_5 and a_6, we always have that either $a_5 = a_6$ or one of a_8 or a_w is in $\{a_5, a_6\}$. Thus, the resulting partial coloring will be in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$.

Now, if $\boldsymbol{\beta}_5 = 2$ and $6 \notin \operatorname{supp}(\boldsymbol{\beta})$, given any coloring of the children of 3 and 4, that colors the children of 3 with the same color, we can always choose $a_6 = a_w$. Then, for any choice of a_5 either $a_5 = a_6$ or $a_w \in \{a_5, a_6\}$ and the partial coloring is in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$.

2.3.2.1.2. If $\boldsymbol{\beta}_5 \leqslant 1$, given any partial coloring of the children of 3 and 4 which colors the children of 3 with the same color, we can pick $a_5 \in \{a_7, a_8\}$ thus obtaining a partial coloring in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ regardless of the choice for a_6. This shows that $3 \notin \operatorname{supp}(\boldsymbol{\beta})$ if both children of 3 are in H.

2.3.3.2. Suppose that both children of 4 are in H and let v be the unique child of 3. Then $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ is the set of partial colorings $(a_i)_{i\geqslant 5}$ such that either $a_5 = a_6$, or $a_5 \neq a_6$ and $\{a_9, a_{10}\} \subseteq \{a_5, a_6\}$ (this way we can always extend to a coloring satisfying $a_2 = a_4$), or a_5, a_6, a_9 are pairwise distinct, $a_9 = a_{10}$ and $a_v \in \{a_5, a_6\}$ (this way we can choose a color $a_4 \in \{a_5, a_6\} \setminus \{a_v\}$), or a_5, a_6 and a_w are pairwise distinct, $a_9 \neq a_{10}$ and $a_v = a_{w'}$ where $\{w, w'\} = \{9, 10\}$ (this way the unique colors available for 2 and 4 are always available for vertex 3).

By the same reasoning as in 2.3.2.1.1, the monomial $x_3x_5^2x_6x_v^2$ is reducible. We claim that the following monomials are reducible as well.

$$x^{\boldsymbol{\beta}^{(1)}} = x_3x_5x_6^2x_v^2x_9,$$

$$x^{\boldsymbol{\beta}^{(2)}} = x_3 x_5^2 x_v^2 x_9,$$
$$x^{\boldsymbol{\beta}^{(3)}} = x_3 x_5^2 x_6 x_9.$$

Indeed, let $a = (a_i)_{i \geqslant 1}$ be a 3-coloring of H. Consider the polynomials:

$$f_1(x) = (x_v - x_9)(x_v - x_{10})(x_9 - x_{10}),$$
$$g_1(x) = (x_5 - x_6)(x_6 - x_9)(x_6 - x_{10}),$$
$$h_1(x) = (x_3 + x_5 + x_6) f_1(x) g_1(x).$$

Notice that $LM(h_1) = x^{\boldsymbol{\beta}^{(1)}}$. If $f_1(a) \neq 0$, then a_v, a_9 and a_{10} are pairwise distinct, in particular $a_4 = a_v$. If in addition $g_1(a) \neq 0$, then $a_6 = a_v$ and $a_5 \in \{a_9, a_{10}\}$. In particular, $a_2 \neq a_6 = a_4$ and since $a_3 \neq a_v = a_4$, we must have that $a_3 = a_2$, thus $a_3 + a_5 + a_6 = 0$ and $h_1(a) = 0$. Next, consider the polynomials:

$$f_2(x) = (x_v - x_9)(x_v - x_{10})(x_9 - x_{10}),$$
$$g_2(x) = (x_5 + x_6 + x_v)(x_5 - x_6),$$
$$h_2(x) = (x_3 + x_5 + x_6) f_2(x) g_2(x).$$

Notice that $LM(h_2) = x^{\boldsymbol{\beta}^{(2)}}$. If $f_2(a) \neq 0$, then a_v, a_9 and a_{10} are pairwise distinct, in particular $a_4 = a_v$. If in addition $g_2(a) \neq 0$, then $a_5 \neq a_6$ and $a_v \in \{a_5, a_6\}$, in particular $a_2 \neq a_v = a_4$. Since $a_4 = a_v$, this implies that $a_3 = a_2 = -a_5 - a_6$ and $h_2(a) = 0$. Finally, consider the polynomials

$$f_3(x) = (x_5 - x_6)(x_9 - x_{10}),$$
$$g_{31}(x) = (x_v - x_9)(x_v - x_{10}),$$
$$g_{32}(x) = (x_5 - x_v)(x_6 - x_v),$$
$$h_3(x) = ((x_3 + x_9 + x_{10}) g_{31}(x) - (x_3 + x_5 + x_6) g_{32}(x)) f_3(x).$$

Notice that $LM(h_3) = x^{\boldsymbol{\beta}^{(3)}}$. If $f_3(a) \neq 0$, then $a_5 \neq a_6$ and $a_9 \neq a_{10}$. We consider several cases:

– If $a_v \in \{a_9, a_{10}\}$, then $g_{32}(a) = 0$. If in addition $g_{31}(a) \neq 0$, then a_5, a_6 and a_v are pairwise distinct. But then, $a_2 = a_v$ and the only way a is valid coloring is if $a_3 = a_4$. This implies that $a_3 + a_9 + a_{10} = 0$ and $h_3(a) = 0$.

– If $a_v \notin \{a_9, a_{10}\}$ and $g_{31}(a) \neq 0$, then $\{a_5, a_6\} = \{a_9, a_{10}\}$ and as a consequence

$$a_3 + a_5 + a_6 = a_3 + a_9 + a_{10},$$
$$(a_v - a_9)(a_v - a_{10}) = (a_5 - a_v)(a_6 - a_v).$$

This implies that $h_3(a) = 0$.

– If $a_v \notin \{a_9, a_{10}\}$ and $g_{31}(a) = 0$, then $a_v \in \{a_5, a_6\}$. Since $a_4 = a_v$, this implies that $a_2 \neq a_4$ and the only way a is valid coloring is if $a_3 = a_2$. This implies that $a_3 + a_5 + a_6 = 0$ and $h_3(a) = 0$.

By the above case analysis we conclude that $x^{\boldsymbol{\beta}^{(3)}}$ is reducible.

2.3.3.2.1. Suppose that $x_3x_5^2|x^{\boldsymbol{\beta}}$. If in addition $\boldsymbol{\beta}_6 \geqslant 1$, then $\boldsymbol{\beta}_v \leqslant 1$ and $\boldsymbol{\beta}_9 = 0$. Given any color for vertex 10, say a_{10}, we can use the color $a_9 = a_{10}$ for vertex 9. Then, for vertex v we have two choices $a_v \neq a_{10}$. Then, for any pair of colors a_5, a_6 for vertices 5 and 6, the resulting partial coloring $(a_i)_{i\geqslant 5}$ is in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ (see 2.3.3.2.).

If $\boldsymbol{\beta}_6 = 0$, but $x_3x_5^2x_v^2|x^{\boldsymbol{\beta}}$, then $\boldsymbol{\beta}_9 = 0$. Given any color a_{10} for vertex 10 we can use $a_9 = a_{10}$ for vertex 9. Given any color a_v for vertex v, we use $a_6 = a_v$ for vertex 6. Then, for any given color a_5 for vertex 5, the partial color $(a_i)_{i\geqslant 5}$ is in $\mathcal{V}^4_{\boldsymbol{\beta}}$ (see 2.3.3.2.).

Finally, suppose that $\boldsymbol{\beta}_6 = 0$ and $\boldsymbol{\beta}_v \leqslant 1$. Then, given any colors a_9, a_{10} for vertices 9 and 10, we can pick $a_v \in \{9, 10\}$ for vertex v and $a_6 = a_v$ for vetex 6 we set. Then, for any color a_5 given to vertex 5, the resulting partial coloring $(a_i)_{i\geqslant 5}$ is in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$. Indeed, this follows as at least one child of 2 and 4 uses color a_v (see 2.3.3.2.).

2.3.3.2.2. Suppose that $x_3x_5|x^{\boldsymbol{\beta}}$. If $\boldsymbol{\beta}_6 = 2$ and $\boldsymbol{\beta}_v = 2$ then $\boldsymbol{\beta}_9 = 0$. In this case we can color vertices 9 and 10 with the same color, say $a_9 = a_{10}$. Given any colors a_6 and a_v for 6 and v, we choose any color $a_5 \in \{a_6, a_v, a_9\}$. If $a_6 = a_v = a_9$, we can choose any other color as well. In any case, we would have at least two choices for a_5 so that $(a_i)_{i\geqslant 5}$ is in $\mathcal{V}^4_{\boldsymbol{\beta}}$ (see 2.3.3.2.).

If $\boldsymbol{\beta}_6 = 2$ and $\boldsymbol{\beta}_v \leqslant 1$, then given any pair of colors a_9, a_{10}, we choose $a_v \in \{a_9, a_{10}\}$ (if $a_9 = a_{10}$ we can pick any color $a_v \neq a_9$). Given any color a_6, we choose any color $a_5 \in \{a_6, a_v\}$ (if $a_6 = a_6$ we can pick any other color a_5). The resulting partial coloring will be in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ (see 2.3.3.2.).

If $\boldsymbol{\beta}_6 \leqslant 1$, then given any colors a_v, a_9 and a_{10} we find an extension in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ as follows. If $a_9 \neq a_{10}$, then we take $\{a_5, a_6\} \subseteq \{a_9, a_{10}\}$. If $a_9 = a_{10}$, then we can either take $a_6 = a_9$ and take any color for a_5, or choose $a_6 \neq a_9$ and $a_5 \in \{a_6, a_9\}$. In either case we have always at least one color available which we can use on both vertices 2 and 4.

2.3.3.2.3. Suppose that $\boldsymbol{\beta}_5 = 0$. In this case given any colors for a_6, a_v, a_9 and a_{10} we can color $a_5 = a_6$, thus obtaining a partial coloring in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ (see 2.3.3.2.).

2.4. Suppose that $x_4 | x^{\boldsymbol{\beta}}$ and $1, 2, 3 \notin \operatorname{supp}(\boldsymbol{\beta})$.

2.4.1. Suppose that both children of 4 are in H. Since $\boldsymbol{\beta}_4 = 1$, we must have that $\boldsymbol{\beta}_9 = 0$. Now, given any color for vertex 10, we can this same color on vertex 9. Given any coloring for the children of 2 and 3 we proceed as follows. If the children of 2 and 3 use at most two colors, then regardless of a choice of color for 4, we can always color vertices 2 and 3 with the same color. Thus, let us assume that the children of 2 and 3 use three different colors.

Suppose that both children of 3 are in H (the other case is similar) and let u be the unique children of 2. Let a_u, a_7 and a_8 be the colors given to the children of 2 and 3 and let $a_9 = a_{10}$ be the color given to the children of 4. Choose any color a_4 for vertex 4. The only color available for vertex 3 is $a_3 = a_u$, whereas vertex 2 has the colors $a_2 \in \{a_7, a_8\}$ available. If $a_4 = a_u$, then $a_4 = a_3$ and we will obtain a valid coloring regardless of the choice for a_2. If $a_4 \in \{a_7, a_8\}$, then we can always pick $a_2 = a_4$ and again we would obtain a valid partial coloring for H. This shows that any coloring $(a_i)_{i \geqslant 5}$ satisfying $a_9 = a_{10}$ is in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$.

2.4.2. Suppose that 4 has only a single children w in H. Then $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$ is the set of colorings $(a_i)_{i \geqslant 5}$ such that either the children of 2 and 3 uses at most two colors, or they use three colors but either $a_5 = a_6$ or $a_7 = a_8$, or they use three colors with $a_5 \neq a_6$, $a_7 \neq a_8$ and $a_4 \in \{a_5, a_6\} \cap \{a_7, a_8\}$. We claim that the monomial $x_4 x_5 x_6^2 x_7^2 x_8$ is reducible. Indeed, consider the polynomials

$$\begin{aligned} f(x) &= (x_7 - x_8)(x_7 - x_w)(x_8 - x_w), \\ g(x) &= (x_5 - x_6)(x_6^2 + x_6 x_w + x_w^2), \\ h(x) &= (x_4 + x_5 + x_6). \end{aligned}$$

Let $a = (a_i)_{i \geqslant 1}$ be a coloring of H. If $f(a) \neq 0$, then a_7, a_8 and a_{10} are

pairwise distinct, in particular $a_3 = a_w$. If in addition $g(a) \neq 0$, then $a_6 = a_w$ and $a_5 \neq a_6$, in particular $a_2 + a_5 + a_6 = 0$. Since $a_4 \in \{a_2, a_3\}$ and $a_4 \neq a_w$, we conclude that $a_4 = a_2$ and $a_4 + a_5 + a_6 = 0$. This shows that $h(a) = 0$ and $x_4x_5x_6^2x_7^2x_8$ is reducible.

2.4.2.1. Suppose that $x_4x_5x_6^2x_7^2|x^{\boldsymbol{\beta}}$. Then $\boldsymbol{\beta}_8 = 0$ and given any color a_w we can color vertex 8 with $a_8 = a_w$. Given any colors a_6 and a_7, we can always color $a_5 \in \{a_6, a_w\}$ (if $a_6 = a_w$ we can use any color for vertex 5 instead). The resulting coloring is in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$.

2.4.2.2. Suppose that $x_4x_5x_6^2|x^{\boldsymbol{\beta}}$ and $\boldsymbol{\beta}_7 \leqslant 1$. Then, given any colors a_w and a_8, we choose a color $a_7 \in \{a_8, a_w\}$ (if $a_8 = a_w$ we can choose any a_7). Then as the case above, given any color for a_6 we can always choose a color $a_5 \in \{a_6, a_w\}$. The resulting coloring is in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$.

2.4.2.2. Suppose that $x_4x_5|x^{\boldsymbol{\beta}}$ and $\boldsymbol{\beta}_6 \leqslant 1$. Then, given any colors a_7, a_8 and a_w, we can choose $a_5, a_6 \in \{a_7, a_8\}$ (if $a_7 = a_8$ we can pick any a_6 and choose $a_5 \in \{a_6, a_7\}$). This way, the children of 2 and 3 use at most two colors, thus the partial coloring is in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$.

2.4.2.3. Suppose that $\boldsymbol{\beta}_5 = 0$. Then, for any choice of colors a_6, a_7, a_8 and a_w, we can always color $a_5 = a_6$, hence obtaining a partial coloring in $\mathcal{V}^4_{\boldsymbol{\beta}}(H)$.

This shows that x_4 does not appear on the support of $x^{\boldsymbol{\beta}}$ and the result follows.

Appendix B

Technical Lemmas of Chapter 3

B.1 Proof of Lemma 3.3.6

In this section we prove the following lemma.

Lemma B.1.1. *Let x, y and z be non-negative integers.*

1. *Suppose that $x \leqslant y$. Then,*
$$\sum_{\ell=x}^{y} \binom{\ell}{x} = \binom{y+1}{x+1}. \tag{B.1.1}$$

2. *Suppose that x, y and z are positive. Then,*
$$\sum_{\ell=0}^{z} \binom{x+\ell}{\ell} \binom{z+y-\ell}{z-\ell} = \binom{x+y+z+1}{z}. \tag{B.1.2}$$

3. *Suppose that $y \leqslant z$, then*
$$\frac{y}{z} \sum_{k=1}^{z-y} \frac{\binom{z-y}{k}}{\binom{z-1}{k}} = \frac{z-y}{z}. \tag{B.1.3}$$

4. *Suppose that $x + y \leqslant z$, then*
$$\frac{y}{z} \sum_{k=1}^{z-y-x} \frac{\binom{z-y-x}{k}}{(k+x)\binom{z-1}{k+x}} = \frac{1}{z} \binom{x+y-1}{y}^{-1}. \tag{B.1.4}$$

Proof. 1. This can be proven with a simple induction argument, along with Pascal's identity $\binom{y+1}{x+1} = \binom{y}{x} + \binom{y}{x+1}$. Indeed, let $x \geqslant 1$ be given. For $y = x$ we have $\binom{y}{x} = \binom{y+1}{x+1}$. If the equation holds for $y \geqslant x$, then

$$\begin{aligned} \sum_{\ell=x}^{y+1} \binom{\ell}{x} &= \sum_{\ell=x}^{y} \binom{\ell}{x} + \binom{y+1}{x}, \\ &= \binom{y+1}{x+1} + \binom{y+1}{x} = \binom{y+2}{x+2}. \end{aligned} \tag{B.1.5}$$

Thus the equation holds for $y+1$ and the result follows.

2. Consider the generating function

$$f_a(\mathbf{x}) := \frac{1}{(1-\mathbf{x})^{a+1}} = \sum_{n=0}^{\infty} \binom{n+a}{a} \mathbf{x}^n. \tag{B.1.6}$$

It follows that

$$f_{a+b+1}(\mathbf{x}) = f_a(\mathbf{x}) f_b(\mathbf{x}). \tag{B.1.7}$$

If we look at the n-th terms of the above equation we obtain

$$\binom{a+b+n+1}{n} = \sum_{k+\ell=n} \binom{a+\ell}{\ell} \binom{b+k}{k}. \tag{B.1.8}$$

Set $x := a, y := b, z := n$ and $k := z - \ell$ to obtain the desired equation.

3. We have that

$$\frac{y}{z} \sum_{k=1}^{z-y} \frac{\binom{z-y}{k}}{\binom{z-1}{k}} = \frac{y}{z} \sum_{k=1}^{z-y} \frac{(z-y)!}{k!(z-y-k)!} \frac{k!(z-k-1)!}{(z-1)!}, \tag{B.1.9}$$

$$= \frac{y}{z} \frac{(z-y)!}{(z-1)!} \sum_{k=1}^{z-y} \frac{(z-k-1)!}{(z-y-k)!} \frac{(y-1)!}{(y-1)!}, \tag{B.1.10}$$

$$= \frac{y}{z} \frac{(z-y)!(y-1)!}{(z-1)!} \sum_{k=1}^{z-y} \binom{z-k-1}{y-1}, \tag{B.1.11}$$

$$= \frac{y}{z} \binom{z-1}{y-1}^{-1} \sum_{\ell=y-1}^{z-2} \binom{\ell}{y-1}, \tag{B.1.12}$$

$$= \frac{y}{z}\binom{z-1}{y-1}^{-1}\binom{z-1}{y}, \quad \text{[By Part 1]} \tag{B.1.13}$$

$$= \frac{y}{z}\frac{\frac{(z-1)!}{y!(z-y-1)!}}{\frac{(z-1)!}{(y-1)!(z-y)!}} = \frac{1}{z}\frac{(z-y)!}{(z-y-1)!}, \tag{B.1.14}$$

$$= \frac{z-y}{z}. \tag{B.1.15}$$

4. We have that

$$\frac{y}{z}\sum_{k=0}^{z-y-x}\frac{\binom{z-y-x}{k}}{(k+x)\binom{z-1}{k+x}}, \tag{B.1.16}$$

$$= \frac{y}{z}\sum_{k=0}^{z-y-x}\frac{(z-y-x)!}{k!(z-y-x-k)!}\frac{(x+k)!(z-x-1-k)!}{(k+x)(z-1)!}, \tag{B.1.17}$$

$$= \frac{y}{z}\sum_{k=0}^{z-y-x}\frac{(x+k-1)!}{k!}\frac{(z-x-1-k)!}{(z-y-x-k)!}, \tag{B.1.18}$$

$$= \frac{y}{z}\frac{(z-y-x)!}{(z-1)!}\sum_{k=0}^{z-y-x}\frac{(x+k-1)!}{k!}\frac{(x-1)!}{(x-1)!}\frac{(z-x-1-k)!}{(z-y-x-k)!}\frac{(y-1)!}{(y-1)!}, \tag{B.1.19}$$

$$= \frac{y}{z}\frac{(z-y-x)!}{(z-1)!}(x-1)!(y-1)!\sum_{k=0}^{z-y-x}\binom{x-1+k}{k}\binom{z-x-1-k}{z-y-x-k}, \tag{B.1.20}$$

$$\text{[Set } \hat{z} := z-y-x, \hat{x} := x-1 \text{ and } \hat{y} := y-1\text{]}, \tag{B.1.21}$$

$$= \frac{y}{z}\frac{(z-y-x)!}{(z-1)!}(x-1)!(y-1)!\sum_{k=0}^{\hat{z}}\binom{\hat{x}+k}{k}\binom{\hat{z}+\hat{y}-k}{\hat{z}-k}, \tag{B.1.22}$$

$$\text{[Apply Part 2.]}, \tag{B.1.23}$$

$$= \frac{y}{z}\frac{(z-y-x)!}{(z-1)!}(x-1)!(y-1)!\binom{\hat{z}+\hat{x}+\hat{y}+1}{\hat{z}}, \tag{B.1.24}$$

$$= \frac{y}{z}\frac{(z-y-x)!}{(z-1)!}(x-1)!(y-1)!\binom{z-1}{z-y-x}, \tag{B.1.25}$$

$$= \frac{y}{z}\frac{(z-y-x)!}{(z-1)!}(x-1)!(y-1)!\frac{(z-1)!}{(z-y-x)!(y+x-1)!}, \tag{B.1.26}$$

$$= \frac{1}{z}\frac{(x-1)!y!}{(y+x-1)!} = \frac{1}{z}\binom{y+x-1}{y}^{-1} \leqslant \frac{1}{zx}, \tag{B.1.27}$$

(B.1.28)

□

B.2 Proof of Lemma 3.3.13

In this section, we prove Lemma 3.3.13, which we re-state for convenience.

Lemma B.2.1. *Let $d \geqslant 4$, consider the function $f(x) := \frac{1}{2}x(d-x)(2d^2-3d+1-x)$ and let $t^* := \operatorname{argmax}\{f(t) : t \in [0,d] \text{ integer}\}$. Then,*

1. *$t^* = \lfloor \frac{d}{2} \rfloor$ and*

$$f(t^*) = \begin{cases} \frac{1}{16}(4d^4 - 7d^3 - d^2 + 7d - 3) & \text{if } d \text{ is odd,} \\ \frac{1}{16}(4d^4 - 7d^3 + 2d^2) & \text{if } d \text{ is even.} \end{cases} \tag{B.2.1}$$

2. *If $d \geqslant 5$, then*

$$(d^2 - d + 1)(d-1) \leqslant f(t^*). \tag{B.2.2}$$

If $d = 4$, then

$$(d^2 - d + 1)(d-1) = f(t^*) + 1. \tag{B.2.3}$$

In particular, for $d \geqslant 4$

$$(d^2 - 2d + 1)(d-1) \leqslant f(t^*). \tag{B.2.4}$$

3. *For $d \geqslant 4$ we have*

$$\max\left\{\left(\frac{3}{2}d\right)^2, \left(\frac{2}{3}d\right)^3, \frac{(d+1)^2(d-1)^2}{8}, \left(\frac{d^2-d-1}{2}\right)^2\right\} \leqslant f(t^*). \tag{B.2.5}$$

We divide the proof of Lemma 3.3.13 into several parts.

Lemma B.2.2. *Let $d \geqslant 4$ and consider the function $f(x) := \frac{1}{2}x(d-x)(2d^2-3d+1-x)$ and let $t^* := \operatorname{argmax}\{f(t) : t \in [0,d]\}$. Then, $t^* = \lfloor \frac{d}{2} \rfloor$ and*

$$f(t^*) = \begin{cases} \frac{1}{16}(4d^4 - 7d^3 - d^2 + 7d - 3) & \text{if } d \text{ is odd,} \\ \frac{1}{16}(4d^4 - 7d^3 + 2d^2) & \text{if } d \text{ is even.} \end{cases} \tag{B.2.6}$$

Proof. We claim that $t^* = \lfloor \frac{d}{2} \rfloor$. Indeed, we have that

$$\begin{aligned} f(x) &= \frac{1}{2}x(x^2 - x(2d^2 - 2d + 1) + 2d^3 - 3d^2 + d), \\ f'(x) &= \frac{1}{2}(x^2 - x(2d^2 - 2d + 1) + 2d^3 - 3d^2 + d) + \frac{1}{2}(2x^2 - (2d^2 - 2d + 1)x), \\ &= \frac{1}{2}(3x^2 - 2x(2d^2 - 2d + 1) + 2d^3 - 3d^2 + d), \\ f''(x) &= \frac{1}{2}(6x - 2(2d^2 - 2d + 1)), \\ &= 3x - (2d^2 - 2d + 1) = 3x - d^2 - (d-1)^2. \end{aligned} \tag{B.2.7}$$

Then, $f''(x)$ is increasing and $f''(d) = d - d^2 - (d-1)^2 < 0$ for every $d \geqslant 2$. This implies that the parabola $f'(x)$ is decreasing on the interval $[0, d]$. Also, notice that for every $d \geqslant 2$

$$\begin{aligned} f'(0) &= \frac{1}{2}d(2d^2 - 3d + 1) > 0, \\ f'(d) &= -\frac{1}{2}d(2d^2 - 4d + 1) < 0. \end{aligned}$$

Hence, f attains an unique (fractional) maximum in the interval $[0, d]$, which is attained at the smallest root x^* of the polynomial $f'(x)$. However, since we are interested in the maximum value of f over the integers, it is enough to find an unit interval containing x^*. For that end, consider the values

$$f'\left(\frac{d-1}{2}\right) = \frac{7}{8}(d-1)^2, \qquad f'\left(\frac{d}{2}\right) = \frac{-1}{8}d^2. \tag{B.2.8}$$

Then, $x^* \in [\frac{d-1}{2}, \frac{d}{2}]$ and the maximum value of f over the integers should be attained in one of $t^* \in \{\frac{d-1}{2}, \frac{d+1}{2}\}$ if d is odd and $t^* \in \{\frac{d-2}{2}, \frac{d}{2}\}$ if d is even. If we evaluate f at these points, we obtain:

$$\begin{aligned} f\left(\frac{d-2}{2}\right) &= \frac{1}{16}(4d^4 - 7d^3 - 3d^2 + 7d - 1), \\ f\left(\frac{d-1}{2}\right) &= \frac{1}{16}(4d^4 - 7d^3 - d^2 + 7d - 3), \\ f\left(\frac{d}{2}\right) &= \frac{1}{16}(4d^4 - 7d^3 + 2d^2), \\ f\left(\frac{d+1}{2}\right) &= \frac{1}{16}(4d^4 - 7d^3 - 3d^2 + 7d - 1), \end{aligned}$$

This shows that

$$f\left(\frac{d+1}{2}\right) < f\left(\frac{d-1}{2}\right), \quad \text{and} \quad f\left(\frac{d-2}{2}\right) < f\left(\frac{d}{2}\right).$$

The result follws. □

Lemma B.2.3. *Let f and t^* be as above. If $d \geqslant 5$, then*

$$(d^2 - d + 1)(d - 1) \leqslant f(t^*). \tag{B.2.9}$$

If $d = 4$, then

$$(d^2 - d + 1)(d - 1) = f(t^*) + 1. \tag{B.2.10}$$

In particular, for $d \geqslant 4$

$$(d^2 - 2d + 1)(d - 1) \leqslant f(t^*). \tag{B.2.11}$$

Proof. Since $d \geqslant 4$, then $t^* \geqslant 2$. Now,

$$\begin{aligned} f(2) - (d^2 - 2d + 1)(d - 1) &= (d - 2)(2d^2 - 3d - 1) - (d^2 - 2d + 1)(d - 1), \\ &= d^3 - 5d^2 + 3d + 3 := g(d). \end{aligned}$$

We claim that $g(d)$ is an increasing function for $d \geqslant 4$. Indeed, we have

$$\begin{aligned} g'(d) &= 3d^2 - 10d + 3, \\ g''(d) &= 6d - 10. \end{aligned}$$

Hence, g' is increasing for $d \geqslant 4$ and $g'(4) = 11 > 0$. Moreover, we have that $g(4) = -1$ and $g(5) = 18$. The result follows. □

Lemma B.2.4. *For every $d \geqslant 4$ we have*

$$\frac{(d+1)^2(d-1)^2}{8} \leqslant f(t^*). \tag{B.2.12}$$

Proof. We have that

$$f\left(\frac{d-1}{2}\right) - \frac{(d+1)^2(d-1)^2}{8} = \frac{1}{16}(2d^4 - 7d^3 + 3d^2 + 7d - 5). \tag{B.2.13}$$

Now, set $g(d) := 2d^4 - 7d^3 + 3d^2 + 7d - 5$ so that

$$\begin{aligned} g'(d) &= 8d^3 - 21d^2 + 6d + 7, \\ g''(d) &= 24d^2 - 42d + 6, \\ g^{(3)} &= 48d - 42. \end{aligned}$$

Thus, $g''(d)$ is increasing for $d \geqslant 4$ and $g''(4) = 222$. Hence, $g'(d)$ is increasing for $d \geqslant 4$ and $g'(4) \geqslant 8(4^3) - 21(4^2) = (4^2)(32 - 21) > 0$. This shows that g is increasing for $d \geqslant 4$. The result follows as

$$g(4) \geqslant 2(4)^4 - 7(4)^3 - 5 = (4^3)(8 - 7) - 5 > 0.$$

□

Lemma B.2.5. *For every $d \geqslant 4$ we have*

$$\left(\frac{d^2 - d - 1}{2}\right)^2 \leqslant f(t^*). \tag{B.2.14}$$

Proof. We have

$$\left(\frac{d^2 - d - 1}{2}\right)^2 = \frac{1}{16}(4d^4 - 8d^3 - 4d^2 + 8d + 4).$$

Hence,

$$f\left(\frac{d-1}{2}\right) - \left(\frac{d^2 - d - 1}{2}\right)^2 = \frac{1}{16}(d^3 + 3d^2 - d - 7).$$

Let $g(d) := d^3 + 3d^2 - d - 7$, then

$$\begin{aligned} g'(d) &= 3d^2 + 6d - 1, \\ g''(d) &= 6d + 6. \end{aligned}$$

Hence, g' is increasing and $g'(4) \geqslant 3(4^2) - 1 > 0$. In particular, g is increasing and $g(4) \geqslant 4^3 - 11 > 0$ implies that $g(d) > 0$ for every $d \geqslant 4$. □

Lemma B.2.6. *For every $d \geqslant 4$, we have*

$$\left(\frac{2}{3}d\right)^3 \leqslant f(t^*) \tag{B.2.15}$$

Proof. Notice that $(\frac{2}{3}d)^3 \leqslant \frac{1}{16}(5d^3)$. Then,

$$f\left(\frac{d-1}{2}\right) - \frac{1}{16}(8d^3) = \frac{1}{16}(4d^4 - 12d^3 - d^2 + 7d).$$

Let $g(d) := 4d^4 - 12d^3 - d^2 + 7d$ so that

$$\begin{aligned} g'(d) &= 16d^3 - 36d^2 - 2d + 7, \\ g''(d) &= 48d^2 - 72d - 2, \\ g^{(3)}(d) &= 96d - 72. \end{aligned}$$

In particular, g'' is increasing when $d \geqslant 4$, $g''(4) > 0$. Thus, g' is increasing for $d \geqslant 4$ and $g'(4) \geqslant (4^2)(16(4)-36)-8 > 0$. Hence, g is increasing and $g(4) = (4^3)(16-12)-4^2+28 > 0$. The result follows. □

Lemma B.2.7. *For every $d \geqslant 4$, we have*

$$\left(\frac{3}{2}d\right)^2 \leqslant f(t^*). \tag{B.2.16}$$

Proof. We claim that $\left(\frac{3}{2}d\right)^2 \leqslant \left(\frac{d^2-d-1}{2}\right)^2 \leqslant f(t^*)$ for $d \geqslant 5$. Indeed, this inequality holds if and only if

$$\frac{3}{2}d \leqslant \frac{d^2-d-1}{2}. \tag{B.2.17}$$

Consider the function $g(d) := d^2 - 4d - 1$. Then, $g'(d) = 2d - 4$ which implies that g is increasing for $d \geqslant 2$. Since $g(5) = 4 > 0$ our claim follows. Finally, for $d = 4$ we have

$$\left(\frac{3}{2}d\right)^2 = 36 < f\left(\frac{d}{2}\right) = (4^3 - 7(4) + 2) = 38. \tag{B.2.18}$$

The result follows. □

B.3 Proof of Lemma 3.3.15

In this section, we prove Lemma 3.3.13, which we re-state for convenience.

Lemma B.3.1. *Let $d \geqslant 4$ and let*

$$w_2(d) := \begin{cases} \frac{1}{16}(4d^4 - 7d^3 + 2d^2) + 1 = 39 & \text{if } d = 4, \\ \frac{1}{16}(4d^4 - 7d^3 - d^2 + 7d - 3) & \text{if } d \geqslant 5 \text{ is odd}, \\ \frac{1}{16}(4d^4 - 7d^3 + 2d^2) & \text{if } d \geqslant 6 \text{ is even}. \end{cases} \tag{B.3.1}$$

Then,

1. *For every $d \geqslant 4$ we have*
$$\frac{d \cdot 2(d-1)^2}{d-2} \leqslant w_2(d). \tag{B.3.2}$$
2. *For every $d \geqslant 5$*
$$\frac{1}{2}d(2d^2 - 3d) \leqslant w_2(d). \tag{B.3.3}$$
3. *For every $d \geqslant 6$ we have*
$$2d^3 - 7d^2 + 7d - 2 \leqslant w_2(d). \tag{B.3.4}$$

Proof. 1. First of all, notice that for $d = 4$ we have

$$\frac{d \cdot 2(d-1)^2}{d-2} = 36 < w_2(d) = 39. \tag{B.3.5}$$

Now, we claim that

$$\frac{d \cdot 2(d-1)^2}{d-2} \leqslant \left(\frac{d^2 - d - 1}{2}\right)^2 \tag{B.3.6}$$

for every $d \geqslant 5$ and the result follows from Lemma 3.3.13. Indeed, we have that $\frac{2d}{d-2} \leqslant 4$ for every $d \geqslant 4$, hence it is enough to prove that $4(d-1)^2 \leqslant \left(\frac{d^2-d-1}{2}\right)^2$. This last inequality is equivalent to

$$0 \leqslant (d^2 - d - 1) - 4(d-1) = d^2 - 5d + 3, \tag{B.3.7}$$

which holds for every $d \geqslant 5$.

2. Similarly, let us prove that

$$\begin{aligned} & \frac{d(2d^2 - 3d)}{2} \leqslant \left(\frac{d^2 - d - 1}{2}\right)^2, \\ \iff \quad & 2d^2(2d - 3) \leqslant (d^2 - d - 1)^2, \end{aligned} \tag{B.3.8}$$

holds for every $d \geqslant 5$. Let $g(d) := (d^2 - d - 1)^2 - 2d^2(2d - 3)$ and notice that $g(5) = 11$. Then,

$$\begin{aligned} g(d) &= d^4 - 6d^3 + 5d^2 + 2d + 1, \quad g(5) = 11, \\ g'(d) &= 4d^3 - 18d^2 + 10d + 2, \quad g'(5) = 102, \\ g''(d) &= 12d^2 - 36d + 10, \quad g''(5) = 130 \\ g^{(3)}(d) &= 24d - 36, \quad g^{(3)}(5) = 84. \end{aligned} \tag{B.3.9}$$

We conclude that g, g', g'' and $g^{(3)}$ are non-decreasing functions for $d \geqslant 5$ and the result follows.

3. Finally, let us prove that

$$\begin{aligned} & 2d^3 - 7d^2 + 7d - 2 \leqslant \left(\frac{d^2 - d - 1}{2}\right)^2, \\ \iff \quad & 8d^3 - 28d^2 + 28d - 8 \leqslant d^4 - 2d^3 - d^2 + 2d + 1, \\ \iff \quad & 0 \leqslant g(d) := d^4 - 10d^3 + 27d^2 - 26d + 9, \end{aligned} \tag{B.3.10}$$

holds for every $d \geqslant 7$. Indeed, we have

$$\begin{aligned} g(d) &= d^4 - 10d^3 + 27d^2 - 26d + 9, \quad g(7) = 121, \\ g'(d) &= 4d^3 - 30d^2 + 54d - 26, \quad g'(7) = 254, \\ g''(d) &= 12d^2 - 60d + 54, \quad g''(7) = 222 \\ g^{(3)}(d) &= 24d - 60, \quad g^{(3)}(7) = 108. \end{aligned} \tag{B.3.11}$$

We conclude that g, g', g'' and $g^{(3)}$ are non-decreasing functions for $d \geqslant 7$. Finally, when $d = 6$ we have

$$2d^3 - 7d^2 + 7d - 2 = 220 < w_2(6) = \frac{1}{16}(4d^4 - 7d^3 + 2d^2) = 234. \tag{B.3.12}$$

The result follows. □

B.4 Proof of Lemma 3.3.18

In this section we proof Lemma 3.3.18, which we re-state here for convenience.

Lemma B.4.1. *Consider the weights $w_{(\ell,p,X)}$ defined by the valid triples (VT 1.)-(VT 4.) below and set $w_{(\ell,p,X)} = 0$ for any other valid triple. Let $R_{A,B}$ be a maximal rectangle of M_{G_4}, then*

1. *the weight $w(R_{A,B}) := \sum_{(\ell,p,X)\in R_{A,B}} w_{(\ell,p,X)}$ is at most one when*
   - *(a) $|A| = 1$, $|B| \geqslant 1$,*
   - *(b) $|A| \geqslant 1$, $|B| = 1$,*
2. *the weight $w(R_{A,B})$ equals to one for the pairs (A, B) such that:*

(AB 1.) Rectangles $R_{A,B}$ where $A = \{\ell\}$, $B = \{p\}$ and $\ell p \in E$.

(AB 2.) Rectangles $R_{A,B}$ where $A = \{\ell\}$,$B = \{p_1, p_2\}$ and $\ell p_1, \ell p_2 \in E$.

(AB 3.) Rectangles $R_{A,B}$ where $A = \{\ell_1, \ell_2\}$,$B = \{p\}$ and $\ell_1 p, \ell_2 p \in E$.

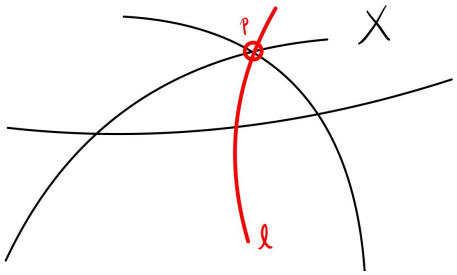
(AB 4.) Rectangles $R_{A,B}$ where $A = N(p^*)$ and $B = N(\ell^*)$ for some $p^* \in \mathcal{P}$.

(AB 5.) Rectangles $R_{A,B}$ as in (AB 4.), but with the exception that one line of A is has an extra line ℓ^{**} passing through one of the points in B. Formally, $B = N(\ell^*)$ for some line $\ell^* \in \mathcal{L}$, $A = (N(p^*) \cup \{\ell^{**}\}$ for some point $p^* \in \mathcal{P} \setminus B$ and some line $\ell^{**} \in \mathcal{L} \setminus N(p^*)$.

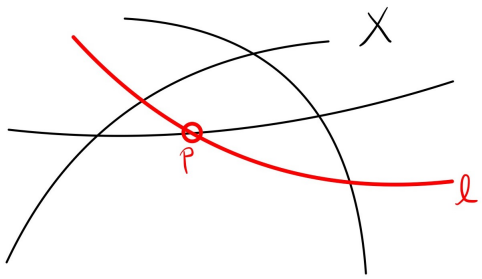
(AB 6.) Rectangles $R_{A,B}$ where $A = \{\ell\}$ and $B = N(\ell)$ for some $\ell \in \mathcal{L}$.

In order to prove this lemma, let us use the following conventions:

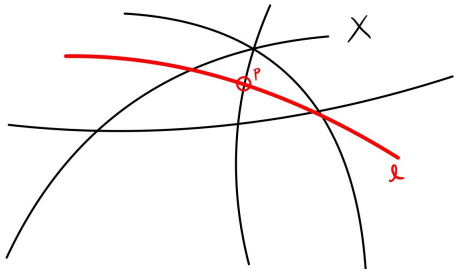
VT 1. We say that (ℓ, p, X) is of **Type 1** if $X = \{\ell_1, \ell_2, \ell_3\}$, where $\ell_1 \cap \ell_2 \cap \ell_3 = \emptyset$, $\ell_1 \cap \ell_2 = \{p\}$ and $\ell \notin X$ is a line such that $p \in \ell$. In addition, we set $w_1^* := \frac{1}{240}$.



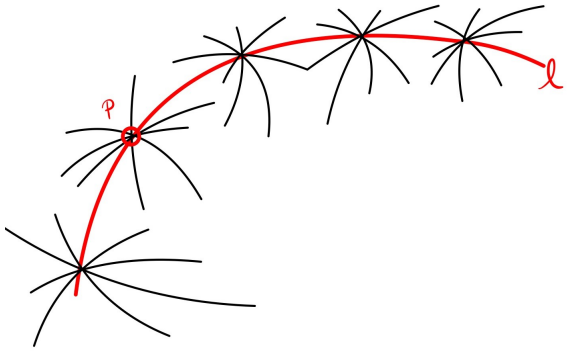
VT 2. We say that (ℓ, p, X) is of **Type 2** if $X = \{\ell_1, \ell_2, \ell_3\}$, where $\ell_1 \cap \ell_2 \cap \ell_3 = \emptyset$, $p \in \ell_1 \setminus (\ell_2 \cup \ell_3)$ and $\ell \notin X$ is a line such that $p \in \ell$ and ℓ does not passes through a point of intersection of the lines in X, i.e. $\ell \cap \ell_i \cap \ell_j = \emptyset$ for all different $i, j \in \{1, 2, 3\}$. In addition, we set $w_2^* := \frac{1}{1800}$.



VT 3. We say that (ℓ, p, X) is of **Type 3** if $X = \{\ell_1, \ell_2, \ell_3, \ell_4\}$, where $(\ell, p, X \setminus \{\ell_3\})$ is of Type 2 and ℓ_3 is the line that passes through the point of intersection of the lines ℓ_1 and ℓ_2 and the point of intersection of the lines ℓ and ℓ_4. In addition, we set $w_3^* := \frac{1}{2400}$.



VT 4. We say that (ℓ, p, X) is of **Type 4** if $X = \mathcal{L} \setminus \{\ell\}$ and p is any point in ℓ. In addition, we set $w_4^* := \frac{1}{5}$.



We proceed to prove each part of the lemma in the following subsections.

B.4.1 Rectangles of the form $R_{A,\{p\}}$, (AB 1.), (AB 2.) and (AB 6.)

Consider a rectangle of the form $R_{A,\{p\}}$ for some set of lines $A \subseteq \mathcal{L}$ of size t.

1. The number of entries (ℓ, p, X) of Type 1 in $R_{A,\{p\}}$ equals (choose two lines ℓ_1, ℓ_2 passing through p and choose any third line ℓ_3 not passing through p)

$$t \cdot \binom{q+1-t}{2} \cdot \binom{q^2}{1}\Big|_{q=4} \in \{96, 96, 48, 0\}. \tag{B.4.1}$$

2. The number of entries (ℓ, p, X) of Type 2 in $R_{A,\{p\}}$ equals (choose a line ℓ_1 passing through p, then choose a point p' not in ℓ or ℓ_1, choose two lines passing through p', but not passing through p)

$$t \cdot \binom{q+1-t}{1} \cdot \binom{q^2-q}{1} \cdot \binom{q}{2}\Big|_{q=4} \in \{288, 432, 432, 288\} \tag{B.4.2}$$

3. The number of entries (ℓ, p, X) of Type 3 in $R_{A,\{p\}}$ equals (choose a line ℓ_1 passing through p and choose a point p^* in ℓ_1. Then, choose a line ℓ_4 not passing through either p or p^*. Set ℓ_3 to be the line that passes through p^* and the intersection of ℓ and ℓ_4 and choose a line ℓ_2 passing through p^* different to ℓ_3 and ℓ_1)

$$t \cdot \binom{q+1-t}{1} \cdot \binom{q}{1} \cdot \binom{q-1}{1} \cdot \binom{q^2-q}{1}\Big|_{q=4} \in \{576, 864, 864, 576\} \tag{B.4.3}$$

4. The number of entries (ℓ, p, X) of Type 4 in $R_{A,\{p\}}$ equals 1 if $t = 1$ and 0 otherwise.

From the above, any feasible solution (w_1, w_2, w_3, w_4) supported on entries of types 1 to 4 must satisfy the following inequalities:

$$\begin{aligned} 96w_1 + 288w_2 + 576w_3 + w_4 &\leqslant 1, \\ 96w_1 + 432w_2 + 864w_3 &\leqslant 1, \\ 48w_1 + 432w_2 + 864w_3 &\leqslant 1, \\ 288w_2 + 576w_3 &\leqslant 1. \end{aligned} \tag{B.4.4}$$

Notice that the second inequality dominates the third and fourth inequalities above. In addition, the values $(w_1^*, w_2^*, w_3^*, w_4^*)$ satisfy:

$$\begin{aligned} 96\frac{1}{240} + 288\frac{1}{1800} + 576\frac{1}{2400} + \frac{1}{5} &= 1, \\ 96\frac{1}{240} + 432\frac{1}{1800} + 864\frac{1}{2400} &= 1, \end{aligned} \tag{B.4.5}$$

as desired.

B.4.2 Rectangles of the form $R_{\{\ell\},B}$, (AB 3.)

Now, consider a rectangle of the form $R_{\{\ell\},B}$ for some line $\ell \in \mathcal{L}$ and a set of points $B \subseteq \ell$ with $\ell \geqslant 2$. We consider the following cases:

1. Suppose that $|B| \geqslant 4$. Then, no entries of type 1, 2 or 3 are in $R_{\{\ell\},B}$ as each for each of those entries (ℓ, p, X), the set X intersects the line ℓ in at most three points. The number of entries of type 4 equals

   $$|B| \leqslant (q+1)|_{q=4} = 5.$$

   Thus, every feasible solution (w_1, w_2, w_3, w_5) satisfies the inequality

   $$5w_5 \leqslant 1 \tag{B.4.6}$$

   which is tight for the values $(w_1^*, w_2^*, w_3^*, w_4^*)$.

2. Suppose that $|B| = 3$. Similarly, no entries (ℓ, p, X) of type 1 are in $R_{\{\ell\},B}$ as for those entries the set X intersects the line ℓ at most two points. Let us fix a point $p \in B$ and count the number of entries (ℓ, p, X) of types 2 to 4.

(a) The number of entries of type 2 can be counted as follows. First, we choose a line ℓ_1 passing through p (q possibilities), then we choose a line ℓ_2 passing through a second point in B (q possibilities) and finally we choose a line ℓ_3 passing through the third point of B, but not through the intersection of ℓ_1 and ℓ_2 ($q-1$ possibilities). Thus, the total number of entries in this case equals:

$$|B| \cdot q^2(q-1)|_{q=4} = 144. \tag{B.4.7}$$

(b) Suppose that (ℓ, p, X) is an entry of type 4 in $R_{\{\ell\},B}$ with $X = \{\ell_1, \ell_2, \ell_3, \ell_4\}$. The set of lines X has the following characteristics:

- The lines ℓ_1, ℓ_2 and ℓ_3 all pass through a point p^* and cover the three points in B, including p.
- The line ℓ_4 passes through the point p' of intersection of lines ℓ and ℓ_3.

The number of sets X satisfying these properties can be counted as follows: choose a point p^* outside of ℓ (q^2 choices), set ℓ_1 to be the line passing through p^* and p. Choose one point p' in B other than p (two choices), set ℓ_3 to be the line that passes through p^* and p' and choose a line ℓ_4 passing through p' other than ℓ and ℓ_3 ($q-1$ choices). Finally, set ℓ_2 to be the line passing through p^* and the remaining point of B. In total, the number of entries of type 3 in $R_{\{\ell\},B}$ is

$$|B| \cdot q^2 \cdot (|B|-1) \cdot (q-1)|_{q=4} = 288 \tag{B.4.8}$$

(c) The number of entries of type 4 in $R_{\{\ell\},B}$ is $|B| = 3$.

From the above, every feasible solution $(w_1, \ldots, w_4)$ satisfies

$$144w_2 + 288w_3 + 3w_5 \leqslant 1. \tag{B.4.9}$$

Note that the values $(w_1^*, w_2^*, w_3^*, w_4^*)$ satisfy

$$144\frac{1}{1800} + 288\frac{1}{2400} + 3\frac{1}{5} = 0.8.$$

3. Next, suppose that $|B| = 2$. Let $B = \{p, p'\}$ and consider a triple (ℓ, p, X) in $R_{\{\ell\},B}$. We study each case separately.

(a) Suppose that (ℓ, p, X) is of type 1. We can count the number of such entries as follows: first we pick two lines ℓ_1, ℓ_2 passing through p ($\binom{\{q}{2\}}$ choices), then we select a line ℓ_3 passing through p' (q choices). In total, we have

$$|B| \cdot \binom{q}{2} \cdot \binom{q}{1}|_{q=4} = 48. \tag{B.4.10}$$

(b) Suppose that (ℓ, p, X) is of type 2. We can count the number of such entries as follows: first we pick a lines ℓ_1 passing through p (q choices), then we select a line ℓ_2 passing through p' (q choices). Finally we choose a third point p'' in ℓ ($q-1$ choices) and a line ℓ_3 passing through p'', but not passing through the intersection of ℓ_1 and ℓ_2 ($q-1$ choices). This gives us a total of

$$|B| \cdot q^2 \cdot (q-1)^2|_{q=4} = 288. \tag{B.4.11}$$

(c) Suppose that (ℓ, p, X) is of type 3. There are two cases here:

- The set X is such that the lines ℓ_3 and ℓ_4 pass through p'. We can count these entries as follows: first, we pick a line ℓ_1 passing through p (q choices). Then, choose a point p^* in the line ℓ (q choices) and set ℓ_3 to be the line passing through p' and $p^a st$.Next, we select another line ℓ_4 passing through p' ($q-1$ choices). Finally, we select a third point p'' in ℓ ($q-1$ choices) and set ℓ_2 to be the line passing through p'' and p^*. This gives us a total of

  $$|B| \cdot q^2 \cdot (q-1)^2|_q = 288$$

  of entries of this type.
- The set X is such that the lines ℓ_3 and ℓ_4 pass through a point p'' different to p'. We can count these entries as follows: first, we pick a line ℓ_1 passing through p (q choices).Then, we select a line ℓ_2 passing through p' (q choices). Finally, we select a third point p'' in ℓ ($q-1$ choices) and set ℓ_3 to be the line passing through p'' and the intersection of the lines ℓ_1 and ℓ_2 and select a fourth line ℓ_4 passing through p'' ($q-1$ choices). This gives us a total of

  $$|B| \cdot q^2 \cdot (q-1)^2|_{q=4} = 288$$

In total, the number of entries of type 3 in $R_{\{\ell\},B}$ is

$$4 \cdot q^2 \cdot (q-1)^2 = 576.$$

4. Finally, the number of entries of type 4 in $R_{\{\ell\},B}$ is $|B| = 2$.

In conclusion, every feasible solution $(w_1, \ldots, w_4)$ satisfies

$$48w_1 + 288w_2 + 576w_3 + 2w_5 \leqslant 1. \tag{B.4.12}$$

Note that the values $(w_1^*, w_2^*, w_3^*, w_4^*)$ satisfy

$$48\frac{1}{240} + 288\frac{1}{1800} + 576\frac{1}{2400} + 2\frac{1}{5} = 1.$$

It is worth mentioning that the rectangles we have covered so far are the only rectangles where entries of type 4 can appear. Thus, from now on we will consider rectangles $R_{A,B}$ where $|A| \geqslant 2$, $|B| \geqslant 2$ and entries of types 1 ,2 and 3 will only be considered.

B.4.3 Rectangles of the form $R_{A,B}$ with $|B| = 5$ collinear: Cases (AB 4.) and (AB 5.).

Suppose that B consist of $q+1$ colinear points and let ℓ^* the unique line passing through these points. Now, any set of lines X with at most q lines covering these points must contain the line ℓ^*. In particular, each type 1, 2 and 3 entry (ℓ, p, X) in $R_{A,B}$ satisfies that $\ell^* \in X$. Let $p_0, \ldots, p_q \in B$ be the points in B and let $t_i \in [q]$ be the number of lines in A passing through p_i for each $i \in [0, q]$. Again, we use the expectation notation $\mathbb{E}(\mathbf{t}^s) = \frac{1}{q+1}\sum_{i=0}^{q} t_i^s$, $\mathrm{Var}(\mathbf{t}) = \mathbb{E}(\mathbf{t}^2) - \mathbb{E}(\mathbf{t})^2$. The following inequality will be useful:

$$\begin{aligned} 0 &\leqslant \mathbb{E}(\mathbf{t}(\mathbf{t} - \mathbb{E}(\mathbf{t}))^2), \\ &= \mathbb{E}(\mathbf{t}^3) - 2\,\mathbb{E}(\mathbf{t}^2)\,\mathbb{E}(\mathbf{t}) + \mathbb{E}(\mathbf{t})^3, \\ &= \mathbb{E}(\mathbf{t}^3) - \mathbb{E}(\mathbf{t})^3 - 2\,\mathbb{E}(\mathbf{t})\,\mathrm{Var}(\mathbf{t}) \end{aligned} \tag{B.4.13}$$

Lemma B.4.2. *the total number of entries of type 1 in $R_{A,B}$ is at most*

$$a_1\sum_{i=0}^{q} t_i + a_2\sum_{i=0}^{q} t_i^2 + a_3\sum_{i=0}^{q} t_i^3 + a_4\left(\sum_{i=0}^{q} t_i\right)^2 + a_5\left(\sum_{i=0}^{q} t_i\right)\left(\sum_{i=0}^{q} t_i^2\right) + a_6\left(\sum_{i=0}^{q} t_i\right)^3, \tag{B.4.14}$$

where

$$a_1 := q^3, \quad a_2 := -(q^2 - q), \quad a_3 := -1,$$
$$a_4 := -q, \quad a_5 := 1, \quad a_6 := 0.$$

Proof. First, we count the number of entries (ℓ, p_0, X) of type 1 in $R_{A,B}$. We can select the lines in X in the following way. As mentioned before, ℓ^* should be in X. Next, we choose a line passing through p_0, which is not in A nor equal to ℓ^*, this gives us $q - t_0$ possibilities.

Then, we choose any line not passing through p_0, such line should pass through some p_i for some $i \in [1, q]$, hence we have a total of $\sum_{i=1}^{q}(q - t_i)$ of options for such line. Hence, the number of entries (ℓ, p_0, X) of type 1 in $R_{A,B}$ is equal to

$$t_0 \cdot (q - t_0) \cdot \left(q^2 - \sum_{i=1}^{q} t_i \right). \tag{B.4.15}$$

Thus, the number of entries of type 1 in $R_{A,B}$ is equal to

$$\begin{aligned} &\sum_{i=0}^{q} (q \cdot t_i - t_i^2) \cdot \left(q^2 + t_i - \sum_{j=0}^{q} t_j \right), \\ &= q^3 \sum_{i=0}^{q} t_i + q \sum_{i=0}^{q} t_i^2 - q \left(\sum_{i=0}^{q} t_i \right)^2 - q^2 \sum_{i=0}^{q} t_i^2 - \sum_{i=0}^{q} t_i^3 + \left(\sum_{i=0}^{q} t_i^2 \right) \left(\sum_{i=0}^{q} t_i \right), \end{aligned} \tag{B.4.16}$$

□

Lemma B.4.3. *The total number of entries of type 2 in $R_{A,B}$ is at most*

$$a_1 \sum_{i=0}^{q} t_i + a_2 \sum_{i=0}^{q} t_i^2 + a_3 \sum_{i=0}^{q} t_i^3 + a_4 \left(\sum_{i=0}^{q} t_i \right)^2 + a_5 \left(\sum_{i=0}^{q} t_i \right) \left(\sum_{i=0}^{q} t_i^2 \right) + a_6 \left(\sum_{i=0}^{q} t_i \right)^3, \tag{B.4.17}$$

where

$$\begin{aligned} a_1 := \frac{q^4 - 2q^3 + q^2}{2}, a_2 := \frac{2q^2 - 1}{2}, \quad a_3 := \frac{q - 2}{2q}, \\ a_4 := -\frac{2q^2 - 1}{2}, \quad a_5 := -\frac{q - 2}{q}, \quad a_6 := \frac{q - 2}{2q}. \end{aligned}$$

Proof. First, we compute the number of entries (ℓ, p_0, X) of type 2 in $R_{A,B}$. We can select the lines in X in the following way. As mentioned before, ℓ^* should be in X. Next, we need to choose a pair of lines, not passing through p_0, that in addition do not intersect at a point in ℓ^* or ℓ. Now, a pair of lines that intersect ℓ^* at different points can be chosen by first selecting a pair p_i and p_j of points in ℓ^* and then choosing one of the $(q - t_i)$ and

$(q - t_j)$ lines passing through each and different to ℓ^*. Thus the total number of these is

$$\begin{aligned}
\sum_{\substack{i,j\in[1,q]\\ i\neq j}} (q-t_i)(q-t_j) &= \frac{1}{2}\left(\sum_{i=1}^{q}(q-t_i)\right)^2 - \frac{1}{2}\sum_{i=1}^{q}(q-t_i)^2, \\
&= \frac{q^2}{2}\,\mathbb{E}(q-\mathbf{t})^2 - \frac{q}{2}\,\mathbb{E}\left((q-\mathbf{t})^2\right), \\
&= \frac{q^2-q}{2}\,\mathbb{E}(q-\mathbf{t})^2 - \frac{q}{2}\,\mathrm{Var}(q-\mathbf{t}), \\
&\leqslant \frac{q^2-q}{2}\,(q-\mathbb{E}(\mathbf{t}))^2\,, \\
&= \frac{q^4-q^3}{2} - \frac{2q^3-2q^2}{2}\,\mathbb{E}(\mathbf{t}) + \frac{q^2-q}{2}\,\mathbb{E}(\mathbf{t})^2.
\end{aligned} \tag{B.4.18}$$

Now, we need to subtract the number of pairs of lines that intersect in a point of ℓ. In order to calculate those, let $p_0, p'_1, \ldots, p'_q$ be the points of ℓ and let $t'_1 := t'_1(\ell, p_0), \ldots, t'_q := t'_q(\ell, p_0)$ be the number of lines in $A \setminus \{\ell\}$ passing through each of these points. Notice that

$$\sum_{i=1}^{q} t_i = \sum_{i=1}^{q} t'_i.$$

Then, the number of pair of lines intersecting at these points is equal to

$$\begin{aligned}
\sum_{i=1}^{q}\binom{q-t'_i}{2} &= \frac{1}{2}\sum_{i=1}^{q}(q^2 - q - (2q-1)t'_i + t'^2_i), \\
&= \frac{q^3-q^2}{2} - \frac{q(2q-1)}{2}\,\mathbb{E}(\mathbf{t}') + \frac{q}{2}\,\mathbb{E}(\mathbf{t}'^2), \\
&= \frac{q^3-q^2}{2} - \frac{q(2q-1)}{2}\,\mathbb{E}(\mathbf{t}') + \frac{q}{2}\,\mathbb{E}(\mathbf{t}')^2 + \frac{q}{2}\,\mathrm{Var}(\mathbf{t}'), \\
&\geqslant \frac{q^3-q^2}{2} - \frac{(2q^2-q)}{2}\,\mathbb{E}(\mathbf{t}) + \frac{q}{2}\,\mathbb{E}(\mathbf{t})^2.
\end{aligned} \tag{B.4.19}$$

Thus, the total number of entries (ℓ, p_0, X) of type 2 in $R_{A,B}$ is at most

$$\begin{aligned}
&t_0 \cdot \left(\frac{q^4 - 2q^3 + q^2}{2} - \frac{2q^3 - 4q^2 + q}{2} \mathbb{E}(\mathbf{t}) + \frac{q^2 - 2q}{2} \mathbb{E}(\mathbf{t})^2 \right), \\
&= t_0 \cdot \left(\frac{q^4 - 2q^3 + q^2}{2} - \frac{2q^2 - 4q + 1}{2} \sum_{i=1}^{q} t_i + \frac{q-2}{2q} \left(\sum_{i=1}^{q} t_i \right)^2 \right), \\
&= t_0 \cdot \left(\frac{q^4 - 2q^3 + q^2}{2} + \frac{2q^2 - 4q + 1}{2} t_0 - \frac{2q^2 - 4q + 1}{2} \sum_{i=0}^{q} t_i + \cdots \right. \\
&\left. \cdots + \frac{q-2}{2q} \left(\sum_{i=0}^{q} t_i \right)^2 - \frac{q-2}{q} t_0 \sum_{i=0}^{q} t_i + \frac{q-2}{2q} t_0^2 \right).
\end{aligned} \tag{B.4.20}$$

Moreover, the total number of entries of type 2 in $R_{A,B}$ is at most

$$a_1 \sum_{i=0}^{q} t_i + a_2 \sum_{i=0}^{q} t_i^2 + a_3 \sum_{i=0}^{q} t_i^3 + a_4 \left(\sum_{i=0}^{q} t_i \right)^2 + a_5 \left(\sum_{i=0}^{q} t_i \right) \left(\sum_{i=0}^{q} t_i^2 \right) + a_6 \left(\sum_{i=0}^{q} t_i \right)^3, \tag{B.4.21}$$

where

$$\begin{gathered}
a_1 := \frac{q^4 - 2q^3 + q^2}{2}, a_2 := \frac{2q^2 - 4q + 1}{2}, \quad a_3 := \frac{q-2}{2q}, \\
a_4 := -\frac{2q^2 - 4q + 1}{2}, \quad a_5 := -\frac{q-2}{q}, \quad a_6 := \frac{q-2}{2q}.
\end{gathered}$$

□

Lemma B.4.4. *The number of entries of type 3 in $R_{A,B}$ is at most*

$$a_1 \sum_{i=0}^{q} t_i + a_2 \sum_{i=0}^{q} t_i^2 + a_3 \sum_{i=0}^{q} t_i^3 + a_4 \left(\sum_{i=0}^{q} t_i \right)^2 + a_5 \left(\sum_{i=0}^{q} t_i \right) \left(\sum_{i=0}^{q} t_i^2 \right) + a_6 \left(\sum_{i=0}^{q} t_i \right)^3, \tag{B.4.22}$$

where

$$\begin{gathered}
a_1 := q^2(q-1)^2, \quad a_2 := (q-1)(2q-1), \quad a_3 := -(q-1), \\
a_4 := -(q-1)(2q-1), \quad a_5 := q-1, \quad a_6 := 0.
\end{gathered}$$

Proof. First, we calculate the number of entries (ℓ, p_0, X) of type 3 in $R_{A,B}$. We can select the lines in X in the following way. As mentioned before, ℓ^* should be in X. Now, we need

to select three lines: two lines passing through a single point in the line ℓ^* and one line passing through the intersection of one of these two lines and ℓ. Thus, we first choose one of the points p_i in ℓ^*, then select a line passing through p_i, say ℓ_i (we have $q - t_i$ choices for such line). Then, we select a line passing through the point of intersection of ℓ_i and ℓ and one of the $q-1$ remaining points of ℓ^* (thus we have at most $q-1$ choices, as it may be the case that such line is in A for some of these points). Finally, we select a second line passing through p_i (thus we have $q - t_i - 1$ choices here). In total, the number of entries (ℓ, p_0, X) of type 3 is at most

$$\begin{aligned} &t_0 \sum_{i=1}^{q} (q-1)(q-t_i)(q-t_i-1) = t_0 \sum_{i=1}^{q} (q-1)(q^2 - q - (2q-1)t_i + t_i^2), \\ &= t_0 \sum_{i=1}^{q} q(q-1)^2 - (q-1)(2q-1)t_i + (q-1)t_i^2, \\ &= q^2(q-1)^2 t_0 - (q-1)(2q-1)t_0 \sum_{i=0}^{q} t_i + (q-1)t_0 \sum_{i=0}^{q} t_i^2 + (q-1)(2q-1)t_0^2 - (q-1)t_0^3. \end{aligned} \tag{B.4.23}$$

Thus, the number of entries of type 3 in $R_{A,B}$ is at most

$$\begin{aligned} &q^2(q-1)^2 \sum_{i=0}^{q} t_i - (q-1)(2q-1)\left(\sum_{i=0}^{q} t_i\right)^2 + (q-1)\left(\sum_{i=0}^{q} t_i\right)\left(\sum_{i=0}^{q} t_i^2\right) + \dots \\ &\cdots + (q-1)(2q-1)\sum_{i=0}^{q} t_i^2 - (q-1)\sum_{i=0}^{q} t_i^3. \end{aligned} \tag{B.4.24}$$

□

We can resume the results obtained in the lemmas above for the case $q = 4$ with the following table:

Type	y^*	a_1	a_2	a_3	a_4	a_4	a_5
1	$\frac{1}{240}$	64	-12	-1	-4	1	0
2	$\frac{1}{1800}$	72	$\frac{17}{2}$	$\frac{1}{4}$	$-\frac{17}{2}$	$-\frac{1}{2}$	$\frac{1}{4}$
3	$\frac{1}{2400}$	144	21	-3	-21	3	0
Total:		$\frac{11}{30}$	$-\frac{263}{7200}$	$\frac{-19}{3600}$	$\frac{-217}{7200}$	$\frac{37}{7200}$	$\frac{1}{7200}$

Thus, the weight of the rectangle $R_{A,B}$ is at most:

$$\frac{11}{30}\sum_{i=0}^{4} t_i - \frac{263}{7200}\sum_{i=0}^{4} t_i^2 - \frac{19}{3600}\sum_{i=0}^{4} t_i^3 - \frac{217}{7200}\left(\sum_{i=0}^{4} t_i\right)^2 + \frac{37}{7200}\left(\sum_{i=0}^{4} t_i\right)\left(\sum_{i=0}^{4} t_i^2\right) + \frac{1}{7200}\left(\sum_{i=0}^{4} t_i\right)^3. \tag{B.4.25}$$

If we use the expected notation, this formula is equal to

$$\begin{aligned}
&\frac{11}{6}\,\mathbb{E}(\mathbf{t}) - \frac{1315}{7200}\,\mathbb{E}(\mathbf{t}^2) - \frac{190}{7200}\,\mathbb{E}(\mathbf{t}^3) - \frac{5425}{7200}\,\mathbb{E}(\mathbf{t})^2 + \frac{925}{7200}\,\mathbb{E}(\mathbf{t})\,\mathbb{E}(\mathbf{t}^2) + \frac{125}{7200}\,\mathbb{E}(\mathbf{t})^3,\\
&= \frac{11}{6}\,\mathbb{E}(\mathbf{t}) - \frac{6740}{7200}\,\mathbb{E}(\mathbf{t})^2 + \frac{315}{7200}\,\mathbb{E}(\mathbf{t})^3 - \frac{1315}{7200}\,\mathrm{Var}(\mathbf{t}) - \frac{190}{7200}\,\mathbb{E}(\mathbf{t}(\mathbf{t}-\mathbb{E}(\mathbf{t}))^2) + \frac{735}{7200}\,\mathbb{E}(\mathbf{t})\,\mathbb{E}(\mathbf{t}^2),\\
&= \frac{11}{6}\,\mathbb{E}(\mathbf{t}) - \frac{6740}{7200}\,\mathbb{E}(\mathbf{t})^2 + \frac{1050}{7200}\,\mathbb{E}(\mathbf{t})^3 - \left(\frac{1315}{7200} - \frac{735}{7200}\,\mathbb{E}(\mathbf{t})\right)\mathrm{Var}(\mathbf{t}) - \frac{190}{7200}\,\mathbb{E}(\mathbf{t}(\mathbf{t}-\mathbb{E}(\mathbf{t}))^2).
\end{aligned} \tag{B.4.26}$$

Unfortunately, the above value can get larger than one for some values of $\mathbf{t}$. In fact, even if for the case $t_i = 1$ for all $i \in [0,4]$ we obtain approximately 1.016 and the maximum value is approximately 1.036, this is attained when $t_i = 2$ for exactly one i and $t_i = 1$ for the rest. Thus, we need to improve our bounds more by taking into account how the lines in A intersect outside the points $p_0, \ldots, p_q$. For instance:

Lemma B.4.5. *Suppose that A consist of five lines ℓ_i with $i \in [0,q]$ each passing through p_i and all intersecting at a point $p^* \notin \ell^*$, i.e., (A,B) is of the form (AB 4.). Then the weight of $R_{A,B}$ is equal to one.*

Proof. We can simply use the same calculations of the above lemmas, but this time we take into account that the lines intersect a single point. This is useful to compute Type 2 entries exactly:

1. For type 1, our formula is exact. Thus, the total number of entries in this case equals (see the table above)

$$64(5) - 12(5) - 1(5) - 4(25) + 1(25) + 0(125) = 180. \tag{B.4.27}$$

2. For type 2, our formula is almost exact, the only thing is that we need to subtract, as shown in the proof of lemma B.4.3, the value

$$\frac{q}{2}\sum_{i=0}^{q} \mathrm{Var}(\mathbf{t}'(\ell_i, p_i)) \tag{B.4.28}$$

where $\mathbf{t}'(\ell_i, p_i)$ is the distribution of the intersections of ℓ_i with the lines $A \setminus \{\ell_i\}$ across the points in $\ell_i \setminus \{p_i\}$. For each i, the variance $\mathrm{Var}(\mathbf{t}'(\ell_i, p_i))$ equals $(q-1)$ as all q lines are concentrated in a single point of ℓ_i. Hence,

$$\frac{q}{2}\sum_{i=0}^{q}\mathrm{Var}(\mathbf{t}'(\ell_i, p_i)) = \frac{(q-1)q(q+1)}{2}. \tag{B.4.29}$$

Our original upper bound equals:

$$72(5) + \frac{17}{2}(5) + \frac{1}{4}(5) - \frac{17}{2}(25) - \frac{1}{2}(25) + \frac{1}{4}(125) = 210. \tag{B.4.30}$$

Then, we subtract $\frac{(q-1)q(q+1)}{2} = 30$ and the total number of entries of type 2 in $R_{A,B}$ is 180.

3. Finally, for type 3 the computation above is exact as all the lines in A share a single point. Thus, the number of entries of type 3 equals

$$144(5) + 21(5) - 3(5) - 21(25) + 3(25) + 0(125) = 360. \tag{B.4.31}$$

From the above, the total weight of the rectangle $R_{A,B}$ is

$$\frac{180}{240} + \frac{180}{1800} + \frac{360}{2400} = 1.$$

□

Lemma B.4.6. *Suppose that A consist of six lines: ℓ_i with $i \in [0, q]$ and a line ℓ^{**}. For $i \in [0, q]$ the line ℓ_i passes through p_i and the line ℓ^{**} passes through p_0, i.e., the pair (A, B) is of the form (AB 5.). Then the weight of $R_{A,B}$ is equal to one.*

Proof. Again, we can use some of the calculations of the above lemmas.

1. For type 1, our formula is exact. Thus, the total number of entries in this case equals

$$\begin{aligned} &64(4+2) - 12(4+2^2) - 1(4+2^3) - 4(6^2) + 1(6)(8) + 0(6)^3, \\ =&64(6) - 12(8) - 1(12) - 4(36) + 1(48) + 0(216) = 180 \end{aligned} \tag{B.4.32}$$

2. Let us compute the number of entries (ℓ, p, X) of Type 2. Once a point $p \in B$ and a line A are selected, the set X can be chosen as follows. First, the line ℓ^* should be in X. We select a pair of points $p', p'' \in B \setminus \{p\}$, one line ℓ', passing through p', and one line ℓ'', passing through p''. If ℓ, ℓ' and ℓ'' do intersect that the same point, we add ℓ' and ℓ'' to X.

   (a) Suppose $p = p_0$ and $\ell = \ell^{**}$. We have $\binom{q}{2}$ choices for the points p' and p''. We have $(q-1)^2$ choices for the lines ℓ' and ℓ'', however $q-2$ of these pairs intersect at a point in ℓ. Thus, the number of choices for X is

$$\binom{q}{2}((q-1)^2 - (q-2))|_{q=4} = 42. \tag{B.4.33}$$

   (b) Suppose that $p = p_0$ and $\ell = \ell_0$. We have $\binom{q}{2}$ choices for the points p' and p''. We have $(q-1)^2$ choices for the lines ℓ' and ℓ'', however $q-1$ of these pairs intersect at a point in ℓ. Thus, the number of choices for X is

$$\binom{q}{2}((q-1)^2 - (q-1))|_{q=4} = 36. \tag{B.4.34}$$

   (c) Suppose that $p = p_i$ and $\ell = \ell_i$ for some $i \in [q]$. We select a pair of points p' and p'' in $B \setminus \{p\}$. We have two possibilities:

      i. $p_0 \in \{p', p''\}$. There are $q-1$ pairs of this type. We have $(q-1)(q-2)$ choices for the lines ℓ' and ℓ'', however $q-2$ of these intersect at a point in ℓ. Thus, the number of choices for X is

$$(q-1)[(q-1)(q-2) - (q-2)]|_{q=4} = 12. \tag{B.4.35}$$

      ii. $p_0 \notin \{p', p''\}$. There are $\binom{q-1}{2}$ pairs of this type. We have $(q-1)^2$ choices for the lines ℓ' and ℓ'', however $q-1$ of these intersect at a point in ℓ. Thus, the number of choices for X is

$$\binom{q-1}{2}((q-1)^2 - (q-1))|_{q=4} = 18. \tag{B.4.36}$$

   In conclusion, the number of entries of Type 2 in $R_{A,B}$ is equal to

$$32 + 46 + 4(12 + 18) = 198 \tag{B.4.37}$$

3. Finally, for Type 3 we need to redo our calculations as this time the way the lines in A intersect matters. We compute the number of entries (ℓ, p, X) of Type 3 for each $p \in B$ and $\ell \in A$. Once the point p and line ℓ are chosen, we can select the set X as follows: first we choose a point different to p in B, say p' and select a line ℓ' passing through p'. Next, we select a line ℓ'' passing through the point of intersection of ℓ' and ℓ. The line ℓ'' would intersect ℓ^* at some point, say $p'' \in B$. Finally, we select another line ℓ''' passing through p'.

   (a) Suppose that $p = p_0$ and $\ell = \ell^{**}$. The point p' can be chosen in q ways and the line ℓ' can be chosen in $q-1$ ways. In this case, ℓ' intersects ℓ^{**} at the point of intersection of ℓ^{**} and some line $\ell_k \in A$ for some k. Thus, we have at most $q-2$ choices for the line ℓ''. We have $q-2$ choices for the line ℓ'''. From here, the number of ways to choose the set X equals

$$q(q-1)(q-2)^2|_{q=4} = 48. \tag{B.4.38}$$

   (b) Suppose that $p = p_0$ and $\ell = \ell_0$. The point p' can be chosen in q ways and the line ℓ' can be chosen in $q-1$ ways. Here, ℓ' intersects ℓ_0 at some point different to p^*. Hence, there are $q-1$ choices for the line ℓ''. Finally, we have $q-2$ choices for the line ℓ'''. The number of ways to choose the set X equals

$$q(q-1)^2(q-2)|_{q=4} = 72. \tag{B.4.39}$$

   (c) Suppose that $p = p_i$ and $\ell = \ell_i$ for some $i \in [q]$. We have two possibilities for p':

      i. Suppose that $p' = p_0$. In this case, the number of choices for the line ℓ' is equal to $q-2$. This, as ℓ_0, ℓ^* and ℓ^{**} pass through p_0. Next, the line ℓ'' can be chosen in $q-1$ ways and the line ℓ''' can be chosen in $q-3$ ways. In total, the number of choices for X is

$$(q-1)(q-2)(q-3)|_{q=4} = 6. \tag{B.4.40}$$

      ii. Suppose that $p' \neq p_0$, so we have $q-1$ choices for p'. Then, we have $q-1$ choices for the line ℓ'. Of these, one of those passes through the point of intersection of ℓ^{**} and ℓ, which gives us $q-2$ ways of choosing ℓ''. The remaining $q-2$ of these choices, allow us to choose the line ℓ'' in $q-1$ ways. The line ℓ''' can be chosen in $q-2$ ways. In total, the number of choices for X is

$$(q-1)[(q-2)+(q-2)(q-1)](q-2) = q(q-1)(q-2)^2|_{q=4} = 48. \tag{B.4.41}$$

In conclusion, the number of triples of Type 3 in $R_{A,B}$ equals

$$48 + 72 + 4(48 + 6) = 336. \tag{B.4.42}$$

From the above, the total weight of the rectangle $R_{A,B}$ is

$$\frac{180}{240} + \frac{198}{1800} + \frac{336}{2400} = 1.$$

□