Technische Universität München

On the Structure of Gröbner Bases for Graph Coloring Ideals

Master's Thesis

Author:
Michael Pernpeintner

Supervisors:
Jesús A. De Loera, UC Davis
Raymond Hemmecke, TU München

University of California, Davis

September 28, 2014

I hereby declare that this thesis is my own work and that no other sources have been used except those clearly indicated and referenced.

Davis, CA, 28 September 2014.

CONTENTS

LIST OF ALGORITHMS

LIST OF TABLES

LIST OF FIGURES

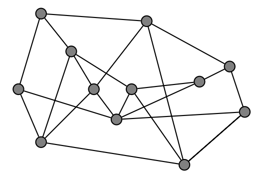
LIST OF SYMBOLS

$a \vert b$	a divides b
$\mathcal{B}_I$	Standard monomials of an ideal I
$\mathfrak{c}(\mathcal{G})$	Complexity pattern of a Gröbner basis $\mathcal{G}$
$\mathfrak{ch}(\mathcal{G})$	Characteristic of a Gröbner basis $\mathcal{G}$
$\binom{V}{2}$	Set of 2-element subsets of V
$\chi(G)$	Chromatic number of a graph G
$\overline{G}$	Complement of a graph G
C_n	Cycle graph
$\mathfrak{d}(\mathcal{G})$	Degree of a Gröbner basis $\mathcal{G}$
$\deg(p)$	Degree of a polynomial p
$\deg(v)$	Degree of a vertex v
$\delta(G)$	Minimum degree of a graph G
$\Delta(G)$	Maximum degree of a graph G
$\mathrm{disc}(f)$	Discriminant of a polynomial f
f'	First derivative of a univariate function f
F_k	k-th Fibonacci number, starting with $F_1 = F_2 = 1$
$\mathbb{F}_p$	Finite field with p elements, p prime
$\langle F \rangle$	Ideal generated by a polynomial set F
$\gcd(p, q)$	Greatest common divisor of p and q
$G\vert_W$	Subgraph of G, induced by $W \subset V$
$\mathcal{I}_G$	Coloring ideal of a graph G
$\overline{\mathbb{K}}$	Algebraic closure of $\mathbb{K}$
$K_{k,m,n}$	Complete tripartite graph
K_n	Clique graph
$\mathfrak{l}(\mathcal{G})$	Length of a Gröbner basis $\mathcal{G}$
$\mathcal{L}_I$	Leading ideal of I
$\mathrm{lcm}(p, q)$	Least common multiple of p and q
$\mathrm{len}(p)$	Length of a polynomial p

LIST OF SYMBOLS (CONT'D)

$\mathbb{N}$	Set of natural numbers $\{1, 2, 3, \ldots\}$
$\mathcal{N}(v)$	Neighborhood of a vertex v
$\mathrm{mdeg}(p)$	Multi-degree of a polynomial p
$\omega(G)$	Clique number of a graph G
$\mathbb{P}$	Set of prime numbers
P_n	Path graph
$\mathrm{Res}(f, g)$	Resultant of two polynomials f and g
$\mathfrak{s}(\mathcal{G})$	Support of a Gröbner basis $\mathcal{G}$
$\mathbb{S}_n$	Symmetric group (group of permutations) of size n
S_n	Star graph
$\succ$	Term order on $\mathbb{K}[x_1, \ldots, x_n]$
$\mathrm{supp}(p)$	Support of a polynomial p
$\mathcal{V}_I$	Algebraic variety of an ideal I
W_n	Wheel graph
ξ_k	First k-th root of unity, $\xi_k = e^{\frac{2\pi i}{k}}$, also without index

Graph $G = (V, E)$



Ideal $\mathcal{I}_G$

$$\left\langle \begin{matrix} x_i^k - 1 \ \forall i \in V \\ \sum_{i=0}^{k-1} x_u^{k-1-i} x_v^i \ \forall (u,v) \in E \end{matrix} \right\rangle$$

Gröbner basis $\mathcal{G}_G$

$$\begin{matrix} \{x_1 + x_2 + x_3, \\ x_2^2 + x_2x_3 + x_3x_4 + x_4^2, \\ x_3^2 + x_3x_4 + x_4^2, x_4^3 + 1\} \end{matrix}$$

Is G k-colorable?

$$\begin{cases} \text{Yes} & \text{if } \mathcal{G}_G \neq \{1\} \\ \text{No} & \text{otherwise} \end{cases}$$

Fig. 0.1: Overall approach for graph coloring

ABSTRACT

In this thesis, we look at a well-known connection between the graph coloring problem and the solvability of certain systems of polynomial equations. In particular, we examine the connection between the structure of a graph and the structure of the Gröbner bases of the graph's coloring ideal.

From a theoretical viewpoint, we show some properties of such Gröbner bases, and we develop a polynomial-time algorithm to compute a Gröbner basis for chordal graphs.

From the experimental side, we state results about specific Gröbner bases and about the Gröbner fan for a variety of graph families. Moreover, some heuristics and techniques are explored that reduce the computational complexity.

The relevance of heuristic methods is justified by a section about expected intrinsic hardness of Gröbner basis computations.

ZUSAMMENFASSUNG

In dieser Arbeit betrachten wir die Verbindung zwischen dem Graphenfärbungsproblem und der Lösbarkeit bestimmter polynomieller Gleichungssysteme. Im Speziellen untersuchen wir den Zusammenhang zwischen der Struktur eines Graphen und der Struktur der Gröbnerbasen des zugehörigen Färbungsideals.
Wir zeigen einige Eigenschaften solcher Gröbnerbasen auf und konstruieren einen Algorithmus, der in polynomieller Zeit eine Gröbnerbasis für chordale Graphen erzeugt.
Daneben zeigen wir spezifische Gröbnerbasen für einige Familien von Graphen, und treffen Aussagen über ihre Komplexität sowie Eigenschaften der zugehörigen Gröbnerfächer.
Außerdem untersuchen wir einige Heuristiken, die dazu geeignet sind, den Rechenaufwand der verwendeten Algorithmen zu senken.
In einem Kapitel über die intrinsische Komplexität der Berechnung von Gröbnerbasen rechtfertigen wir die Relevanz heuristischer Methoden und der Betrachtung von Spezialfällen.

ACKNOWLEDGEMENTS

I would like to thank the American Mathematical Society for financial support and the unique opportunity to work together with a fantastic group of people during the MRC conference *Algebraic and Geometric Methods in Applied Discrete Mathematics* in Snowbird, the workshop *Solving Polynomial Equations* in San Francisco and the *Joint Mathematics Meetings* in San Antonio.
These people, with whom I was able to collaborate and who gave many inspiring comments about my thesis, are Hanna Alpert, Susan Margulies, Eric Riedl, David Rolnick, Gwen Spencer, Despina Stasi and Jon Swenson. In particular, Chapter 7 is a result of the meeting in Snowbird, and Chapter 5 is based on a paper draft by Gwen Spencer. Both chapters will be published in a paper next year.

Finally, I sincerely thank my advisors Jesús A. De Loera and Raymond Hemmecke, who introduced me to the fascinating topic of Gröbner bases, who made it possible for me to write this thesis, and who always gave me excellent support in every respect.

1. INTRODUCTION

The study of the graph coloring problem, one of the most famous and most-examined problems in graph theory, with algebraic methods has been pursued for several decades now. It is based on the fact that the solutions, that is, the proper colorings of a graph, can be seen as the common roots of a set of polynomials, which was first considered in [3]. This encoding moves the problem from graph theory to algebraic geometry, where different solving methods can be applied.
In 1965, Bruno Buchberger proposed the method of Gröbner bases as a tool to systematically treat polynomial ideals. Gröbner bases are special generators of ideals, they allow for a unique representation of an ideal, and they are convenient for algorithmical handling. Using Gröbner bases, the theory of polynomial systems, and also other fields of algebraic geometry, could be approached computationally. Given a Gröbner basis for an ideal I, it can be decided efficiently whether a polynomial p lies in I or not, and two ideals can be tested for equality by the same method. Therefore, Gröbner bases are the foundation of the algorithmic treatment of polynomial ideals.
In the case of graph coloring, the high-level structure of the algorithm is shown in Figure 0.1. For different combinatorial problems which can be encoded algebraically, the steps are the same, just the system of polynomials representing the problem changes. [16] gives some examples which can be solved using this approach.
Unfortunately, there is no known efficient algorithm to compute Gröbner bases of ideals. Therefore, we try to find direct connections between graphs and their respective Gröbner bases, such that statements about the corresponding Gröbner bases can be made without computing them. We focus on certain classes of graphs, since there is little hope that Gröbner bases can be completely read off the structure of a graph in general.

In short, we try to find specific properties of graph coloring ideals and a way to use the additional information that we get from the input graph for the computation of a Gröbner basis.

2. PRELIMINARIES FROM GRAPH THEORY

2.1 Notation

When we talk about a graph without further specification, we always mean an undirected simple graph $G = (V, E)$ with vertex set V and edge set $E \subseteq \binom{V}{2}$. In most cases, the vertex set will be $V = \{1, \dots, n\}$ for notational convenience.
The set $\mathcal{N}(v) := \{w \in V : \{v, w\} \in E\}$ of vertices which are connected with a vertex v is the *neighborhood* of v in G. Two vertices that are in each others neighborhood are *adjacent*. We call $\deg(v) := |\mathcal{N}(v)|$ the *degree* of v, and the minimal and maximal degree of a vertex in G are denoted by $\delta(G)$ and $\Delta(G)$, respectively. For a subset $W \subseteq V$, the subgraph $G|_W := \left(W, \binom{W}{2} \cap E\right)$ is called *induced* by W. The *complement* of G is $\overline{G} := \left(V, \binom{V}{2} \setminus E\right)$. A graph that contains an edge between every pair of vertices is called a *clique* or a *complete graph*, and its complement is an *empty graph* or an *independent set*. We call the size $\omega(G)$ of the largest induced clique of G the *clique number* of G.
A sequence of pairwise distinct vertices $v_1, \dots, v_k$ such that $\{v_i, v_{i+1}\} \in E \ \forall \ i \in \{1, \dots, k-1\}$ is called a *path* in G. If $v_1 = v_k$, then the path is a *cycle*. For a cycle $(v_1, \dots, v_k)$, every edge $\{v_i, v_j\}$ that connects two cycle vertices and does not lie on its border, is called a *chord* of the cycle. Note that a cycle is induced if and only if it does not contain any chord.
Figure 2.1 illustrates some of the definitions above.

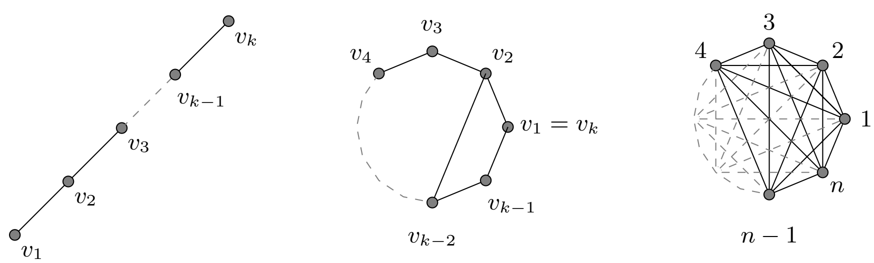


Fig. 2.1: A path, a cycle with a chord, and a complete graph

Remark 1. In general, different labelings of the vertices (that is, permutations of V by elements in $\mathbb{S}_n$) have different properties, when it comes to Gröbner bases. As we will see below, every such permutation can also be modeled by a suitable *monomial order* on the used polynomial ring, but sometimes it is easier to keep the monomial order and change the vertex order instead.

2.2 The Colorability Problem

2.2.1 Problem Definition

Definition 1. Let $G = (V, E)$ be a graph. The *k-colorability problem* is the problem of finding a function $c : V \to \{1, \ldots, k\}$ satisfying

$$c(u) \neq c(v) \quad \forall \ \{u, v\} \in E \quad .$$

If such a function exists, we call G *k-colorable* and c a (proper) k-coloring of G.

Definition 2. The *chromatic number* $\chi(G)$ of a graph G is defined as the smallest number k such that G is k-colorable, i.e.,

$$\chi(G) := \min\{k \in \mathbb{N} : G \text{ is } k\text{-colorable}\} \quad .$$

2.2.2 $\mathcal{NP}$-Completeness

From a complexity-theoretic viewpoint, it is reasonable to classify algorithms by their worst-case running time, compared to the size of the input. Important classes of computational complexity are $\mathcal{P}$ and $\mathcal{NP}$, among many others. A thorough introduction to complexity theory can be found in [1]. In this book, concepts such as Turing machines are used to provide rigorous definitions of complexity classes. For example, it is necessary to define what a "computational step" is, in order to count the steps needed to execute an algorithm. We will not go down to this level of detail, but rather assume that the underlying computational model does not matter (see [1], Chapter 1.6.1). Also, we will not only consider decision problems (that is, outputs of the form 0 or 1), but also outputs such as a valid coloring or the chromatic number of a graph. To understand the concepts used in this thesis, we only need the definitions of the two above-mentioned classes, and the 3SAT problem, which is commonly used as the "original" $\mathcal{NP}$-complete problem, which serves as a basis for showing that other problems are $\mathcal{NP}$-complete as well.

Definition 3. An algorithm F is said to be in the complexity class $\mathcal{P}$ if there is a polynomial $p \in \mathbb{R}[x]$ such that the number of computational steps that F performs is $\leq p(n)$ for all inputs of encoding length n and for all $n \in \mathbb{N}$. Such an algorithm is also called a *polynomial-time* algorithm.

An algorithm F is said to be in the complexity class $\mathcal{NP}$ if, given an input x and a certificate u, both of polynomial length in n, there exists a polynomial-time algorithm which decides whether u is a solution for $F(x)$.

Definition 4. A problem P is called *$\mathcal{NP}$-hard* if, given an algorithm $F \in \mathcal{NP}$ which solves P, *any* other problem $P' \in \mathcal{NP}$ can be solved in polynomial time. If there exists such an F, then P is called *$\mathcal{NP}$-complete*.

The process of finding a polynomial-time algorithm for P', using the one for P, is called a *polynomial-time reduction* of P' to P. Therefore, $\mathcal{NP}$-completeness of a problem P can be shown by two steps: First, show that it lies in $\mathcal{NP}$ by providing an algorithm, together with a suitable certificate, and second, reduce a known $\mathcal{NP}$-complete problem to P. It is customary to use 3SAT as the starting problem, since it can be directly shown to be $\mathcal{NP}$-complete, and it has a structure which allows for an "easy" reduction to many problems.

Definition 5. The 3SAT problem consists of deciding whether or not a given boolean formula has a satisfying assignment. The formulae used for this problem are conjunctions of clauses, which again are 3-literal disjunctions using n boolean variables $x_1, \ldots, x_n$. Therefore, a 3SAT instance has the form

$$\begin{aligned} S &= \bigwedge_{i=1}^{k} C_i \\ &= \bigwedge_{i=1}^{k} \left(v_1^{(i)} \vee v_2^{(i)} \vee v_3^{(i)} \right), \end{aligned}$$

where each v is either a variable or its negation.

Theorem 1 (Cook-Levin theorem)**.** 3SAT is $\mathcal{NP}$-complete.

Proof. See for example [1], Theorem 2.10. □

Theorem 2. 3COL, the problem of finding out if a given graph is 3-colorable, is $\mathcal{NP}$-complete.

Proof [35].
3COL lies in $\mathcal{NP}$: For a given graph G and a coloring number k, an obvious certificate is given by a coloring function c. It is easy to see that one can verify in polynomial time that at most k colors are used, and that no pair of nodes joined by an edge receive the same color.

3COL is $\mathcal{NP}$-hard: We will reduce 3SAT to 3COL. Let an arbitrary 3SAT instance S on variables $x_1, \ldots, x_n$ be given by clauses $C_1, \ldots, C_k$, in other words,

$$S = C_1 \wedge \ldots \wedge C_k \quad .$$

We start building $G = (V, E)$ by setting

$$V := \{v_1, \overline{v_1}, v_2, \overline{v_2}, \ldots, v_n, \overline{v_n}, T, F, B\} \quad ,$$

where the v_i and $\overline{v_i}$ represent variables and their negations, and the vertices T, F, and B stand for **true** , **false** , and *base*, respectively. The first edges that we add, are triangles $\{\{v_i, \overline{v_i}\}, \{\overline{v_i}, B\}, \{B, v_i\}\}$ for all i, and an additional triangle $\{\{T, F\}, \{F, B\}, \{B, T\}\}$.

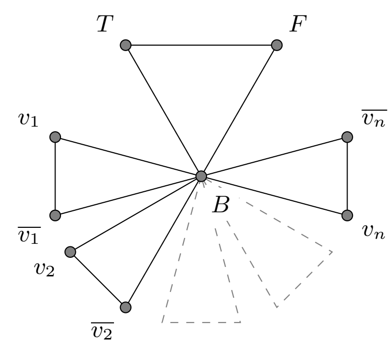


Fig. 2.2: Skeleton of G for general truth assignments

At this stage, we already see that for each i, exactly one of the vertices v_1 and $\overline{v_1}$ will be assigned the same color as the T-vertex, and the other one will get the same color as F. Thus, every coloring of the skeleton graph (Figure 2.2) corresponds to a truth assignment on the variables, and vice versa. Now, the goal is to add more edges to G such that the proper 3-colorings are in one-to-one correspondence with the *satisfying* assignments of S.
To do so, create a graph $G_i = (V_i, E_i)$ with

$$V_i = \left(w_i^{(1)}, \dots, w_i^{(6)}\right)$$

and

$$E_i = \left\{\{w_i^{(1)}, w_i^{(4)}\}, \{w_i^{(2)}, w_i^{(5)}\}, \{w_i^{(3)}, w_i^{(6)}\}, \{w_i^{(4)}, w_i^{(5)}\}, \{w_i^{(5)}, w_i^{(6)}\}\right\}$$

for every $i \in \{1, \dots, k\}$, that is, for every clause $C_i = x_i^{(1)} \vee x_i^{(2)} \vee x_i^{(3)}$ in S, and attach it to G by adding the edge set

$$\left\{\{w_i^{(1)}, T\}, \{w_i^{(2)}, T\}, \{w_i^{(3)}, T\}, \{v_i^{(1)}, w_i^{(1)}\}, \{v_i^{(2)}, w_i^{(2)}\}, \{v_i^{(3)}, w_i^{(3)}\}, \{w_i^{(4)}, T\}, \{w_i^{(6)}, F\}\right\}$$

to E. If C_i contains a literal which is the negation of a variable x_j, then replace the node v_j by $\overline{v_j}$. Now we can directly check that this substructure is 3-colorable if and only if C_i is satisfied by the existing assignment, i.e., at least one of the vertices that represent the literals of C_i, is colored **true**.

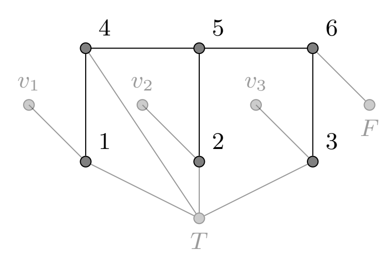


Fig. 2.3: Clause graph G_i corresponding to $C_i = x_i^{(1)} \vee x_i^{(2)} \vee x_i^{(3)}$

$\Rightarrow$ Let all three literals be colored **false**. Then $v_i^{(1)}$ and $v_i^{(2)}$ have to be **base**, $v_i^{(4)}$, $v_i^{(3)}$ and $v_i^{(6)}$ receive **false**, **base**, and **true**, respectively, and therefore $v_i^{(5)}$ cannot be colored without destroying the proper 3-coloring.

⇐ There are seven cases in which at least one of the literals is colored **true**, which can easily be checked by hand. Let for example $v_i^{(1)}$ be **true** and both $v_i^{(2)}$ and $v_i^{(3)}$ be **false**. Then $w_i^{(1)} \leftarrow$ **false**, $w_i^{(1)} \leftarrow$ **false**, $w_i^{(1)} \leftarrow$ **false**, $w_i^{(1)} \leftarrow$ **false**, $w_i^{(1)} \leftarrow$ **false**, $w_i^{(1)} \leftarrow$ **false** results in a proper 3-coloring. All other cases are completely analogous.

Finally, we show that G can be 3-colored if and only if there is a satisfying assignment for S.

⇒ If we are given a proper 3-coloring, then assign to each variable x_i the value **true** if the corresponding vertex has the same color as T, and **false** if the corresponding vertex has the same color as F. We have shown above that only these two colors can occur, and by construction of G, this assignment guarantees that each clause contains a **true** literal. Therefore, we found a satisfying assignment for S.

⇐ Suppose we have a satisfying assignment for S. Then we color the vertices T, F, and B arbitrarily, assign to all vertices corresponding to **true** literals the same color as T, and complete the coloring by assigning **false** to all remaining vertices. Note that the subgraphs G_i are separated by the vertices $v_i, \overline{v_i}, T, F, B$, such that the shown partial colorings can be assembled to a proper 3-coloring for G. Thus, we have shown above that such a coloring is proper for G.

The proof gives a polynomial-time construction for reducing 3Sat to 3Col, which shows the claim. □

Remark 2. Although the class $\mathcal{NP}$ seems to be much more extensive than $\mathcal{P}$, it is still unknown if the inclusion $\mathcal{P} \subset \mathcal{NP}$ is strict. In other words, no one knows whether solving a problem is strictly harder than verifying a given solution. However, it is widely conjectured that $\mathcal{P} \neq \mathcal{NP}$, which is why many theorems, for example the ones in Section 5, assume this conjecture as a condition.

2.2.3 Conventional Solving Methods

The graph coloring problem can be attacked in multiple ways, all of which have their respective advantages and disadvantages. Since the algebraic approach is new in the sense that it does not operate on the input graph itself, but on an algebraic construction which is obtained from the graph in a pre-processing step, we will give in this section a short (and not extensive) overview over known methods to solve the colorability problem. They are taken from [36], which also gives a computational comparison and detailed information about all approaches and the respective algorithms.

Heuristics

A heuristic builds a feasible, but not necessarily optimal solution and generally runs very fast. For example, the Greedy algorithm is a heuristic which starts by choosing a vertex order (either randomly or based on graph properties) and then assigns colors to the vertices along the order, picking the first available color for each vertex. A color is available if it is not already used for any of the current vertex' neighbors. Obviously, the number of colors needed is not always optimal, but it can be shown that there always exists a vertex order for which the greedy algorithm produces a $\chi(G)$-coloring. The DSATUR algorithm is a refinement of the GREEDY algorithm, where the vertex order is established dynamically.

Constructive methods

In this class of methods, a coloring is built and changed successively, until an optimal solution is obtained. BACKTRACKING, for instance, builds a search tree for possible solutions (proper and improper), which is then explored. In the worst case, the solution space has to be searched completely, such that the method is exact and terminates in exponential time. However, its main feature is that by using a clever search order, its running time can be decreased drastically in many cases, while still giving an optimal solution.

Optimization-based methods

What optimization-based methods have in common, is an objective function, which is defined on the space of candidate solutions, and which serves as an indicator for the quality of the current solution. Therefore, such an algorithm navigates through the space of solutions, trying to find an optimal value of the objective function. The solution space and the moving directions vary between different algorithms.

Belonging to the class of algorithms that operate on complete, improper colorings, SIMULATEDANNEALING and TABUCOL start with an initial assignment (whose choice can be made randomly or using a heuristic) and successively change the colors of some vertices until a proper coloring is found. The sub-optimality of the current coloring is evaluated using a cost function, which indicates by how much the solution can be improved. The choice of vertices, whose colors are changed, depends on the exact algorithm and is different for SIMULATEDANNEALING and TABUCOL. In both cases, the goal is to decrease the cost function to 0, which corresponds to a proper coloring.

An example for an algorithm that searches the space of partial, proper solutions, is PARTIALCOL. Here, the number k of available colors is fixed, and if a vertex cannot be colored properly at one step, it is added to a set S of uncolored vertices. Hence, the objective is to decrease the cardinality of S to 0. The moves in the search space are picked via tabu search, similar to TABUCOL.

Some algorithms exclusively examine proper solutions. They use constructive algorithms as the underlying search operators which allow for navigating through the space of candidate solutions. An example is the ITERATEDGREEDY algorithm.

Finally, it is possible to define a *coloring polytope* by various types of inequalities, which encode restrictions on the colorings as half-planes in $\mathbb{R}^n$. For example, the Branch-and-Cut algorithm in [40] iteratively partitions the coloring polytope and strengthens the defining inequalities, until an integral solution is found, which corresponds to a proper coloring.

Hybrids

Of course, different classes can be combined to obtain more efficient algorithms. A common approach is to find an initial solution with a heuristic, which is chosen with regards to the cost function used in the remainder of the algorithm. This decreases the number of optimization steps from the initial to the final solution. Also, the search of different solution spaces can be combined in order to overcome stagnation of the objective value. When the search becomes inefficient in one space, the current solution is translated to another space, where the search can be continued more successfully. Besides complete and partial solutions, also a space of longest paths on a directed version of the graph can be used, as done in the VSS algorithm (see [30]).

2.3 Interesting Classes of Graphs

2.3.1 Planar Graphs

Definition 6. A graph $G = (V, E)$ is called *planar*, if it can be drawn in $\mathbb{R}^2$ without crossing edges. Such a drawing is a *planar embedding* of G.

It is well-known that every planar graph G is 4-colorable (see [2]), and 2-colorability of G can be verified in polynomial time, since this is equivalent to G not containing an odd cycle ([14], Proposition 1.6.1). Therefore, the only interesting question about the chromatic number of a planar graph is whether $\chi(G) = 3$ or $\chi(G) = 4$. It turns out that even this problem is $\mathcal{NP}$-hard (see [23]).

Definition 7. A graph $G = (V, E)$ is called *maximal planar*, if $G' =: (V, E')$ is non-planar for every strict superset $E' \supset E$.

While in general, the number of edges in a graph can be quadratic in the number of vertices, there is a linear bound for planar graphs. More precisely:

Lemma 1. Let $G = (V, E)$ be planar. Then $|E| \leq 3|V| - 6$, and equality holds if and only if G is maximal planar. Moreover, this is equivalent to the property that every face of G is a triangle, in which case G is also called *triangulated*.

Proof. See [14], Proposition 4.2.8 and Corollary 4.2.10. □

If all faces of G except one are triangles, then G is a *near-triangulated* graph.

Theorem 3 (Grötzsch)**.** Let G be a planar graph. If G does not contain a triangle, then $\chi(G) \leq 3$.

Proof. See for example [14], Theorem 5.1.3. □

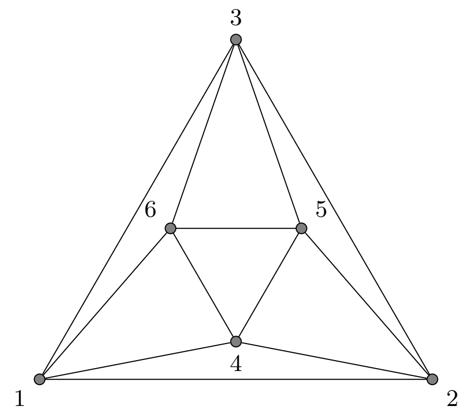


Fig. 2.4: The octahedral graph O_6

The *octahedral graph* is defined as the "two-layer triangle" shown in Figure 2.4, isomorphic to the complete tripartite graph $K_{2,2,2}$ (see Section 6.5). It is easily seen to have chromatic number 3, and since $|E| = 12 = 3|V| - 6$, it is maximal planar. Coming from the octahedral graph, we build an infinite family of *iterated octahedral graphs* by successively adding 3-vertex-layers in the graph's center (see Figure 2.5). In each step, 3 vertices and 9 edges are added, therefore keeping the two crucial properties, maximal planarity and 3-colorability, unchanged. The graph with $3n$ vertices in n layers will be denoted by O_{3n}.

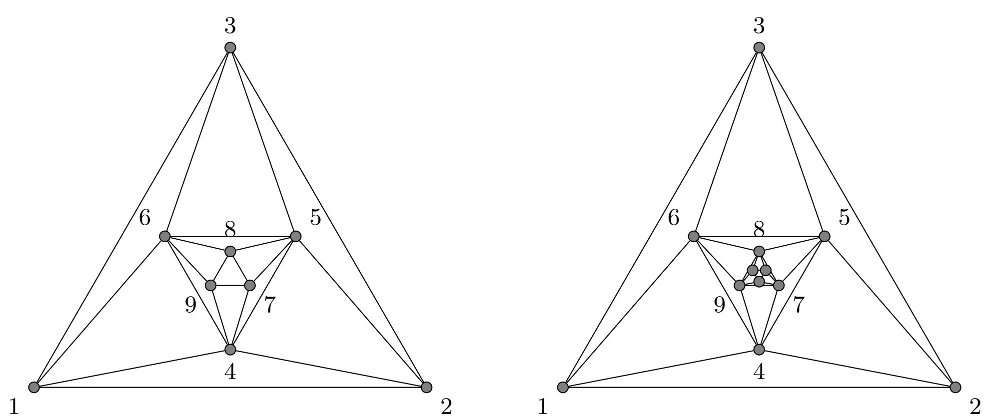


Fig. 2.5: The iterated octahedral graphs O_9 and O_{12}

2.3.2 Perfect graphs

The notion of *perfect graphs* was first introduced by Berge in [4], and several graph-theoretic problems which are $\mathcal{NP}$-complete in general, have been shown to be solvable in polynomial time for perfect graphs. Examples are graph coloring, maximum clique and maximum independent set (see [25]). Loosely speaking, perfect graphs are the graphs which have a large chromatic number if and only if they also contain large cliques. Thus, the only thing that prevents a small coloring is a large complete subgraph.

Definition 8. A graph $G = (V, E)$ is called *perfect* if $\omega(H) = \chi(H)$ for every induced subgraph H of G.

Perfect graphs contain a lot of interesting classes of graphs, for example bipartite, chordal, comparability, or perfectly orderable graphs [28].

Definition 9. A graph $G = (V, E)$ is *chordal* if every induced cycle of length more than 3 has a chord. Equivalently,

$$G \text{ is chordal} \iff (\forall\ W \subseteq V:\ G|_W \simeq C_k\ \Rightarrow k = 3)\ .$$

Example 1. In Figure 2.6, the first graph is non-chordal, since the induced cycle $(1, 2, 4, 5)$ has length 4. In contrast, the second graph, obtained by adding the chord $\{1, 4\}$, is chordal.

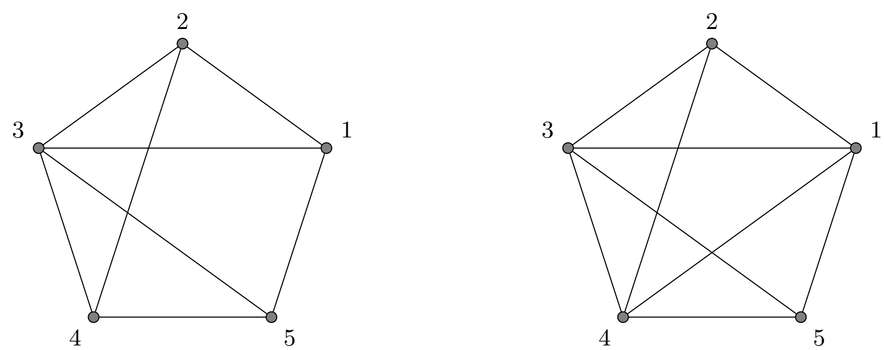
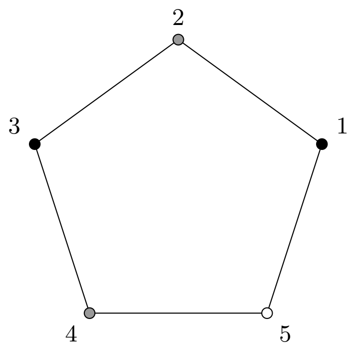


Fig. 2.6: Non-chordal and chordal graph

Lemma 2. Every chordal graph is perfect.

Proof. See [14], Proposition 5.5.2. □

Example 2. A very simple family of non-perfect graphs is given by the odd cycles C_{2n+1}, $n \geq 2$. Their clique number is 2, but they are easily seen to have chromatic number 3: Trying to color them with two colors, we inevitably get to a point where a vertex, whose neighbors already have two different colors, needs to be assigned its color. At this point, we need a third color for a proper coloring. Figure 2.7 illustrates this coloring stage for two odd cycles. Here, the assigned colors are black and gray, and the white node has no color yet.
A more sophisticated imperfect graph with $\omega(G) = 2$ and $\chi(G) = 4$ is the so-called *Grötzsch graph*, which is shown in Figure 2.8. From Theorem 3, we can conclude that it is non-planar.



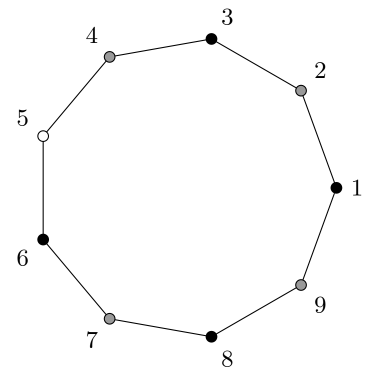


Fig. 2.7: Partial 2-colorings of C_5 and C_9

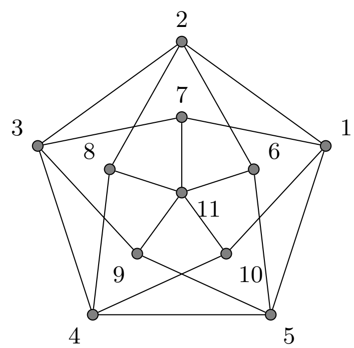


Fig. 2.8: The Grötzsch graph

2.3.3 Uniquely k-colorable Graphs

A proper k-coloring of a graph $G = (V, E)$ induces a partition

$$V = V_1 \cup \ldots \cup V_k$$

of the vertex set, such that the V_i are independent sets, by grouping vertices according to their color. If this partition is unique, then G is called *uniquely k-colorable*. An equivalent definition is

Definition 10. A graph $G = (V, E)$ is *uniquely k-colorable* if for any pair of proper k-colorings c_1 and c_2

$$c_1(v_1) = c_1(v_2) \iff c_2(v_1) = c_2(v_2) \quad \forall\, v_1, v_2 \in V \quad .$$

Remark 3. Note that for a uniquely k-colorable graph, there are still $k!$ proper colorings, which are generated by permuting the colors assigned to the subsets V_i.

Lemma 3. Let $G = (V, E)$ be uniquely k-colorable. Then $\delta(G) \geq k - 1$.

Proof. Suppose there is some $v \in V$ with $\deg(v) < k - 1$. Clearly, $|c(\mathcal{N}(v))| \leq k - 2$, such that $\exists\, c_1, c_2 \in \{1, \dots, k\} \setminus c(\mathcal{N}(v))$ with $c_1 \neq c_2$. Let now be $c : V \to \{1, \dots, k\}$ be the unique k-coloring of G. Setting $c(v) := c_1$ and $c(v) := c_2$ results in two distinct proper k-colorings, which is a contradiction. □

Theorem 4. For all $n \geq 12$, there exists a triangle-free uniquely 3-colorable graph $G = (V, E)$ with $|V| = n$.

Proof. See [9], Theorem 1. The authors construct the base case, a graph with 12 vertices, explicitly, and give an inductive construction for larger graphs, which maintains the demanded properties. □

Lemma 4. Let $G = (V, E)$ be a uniquely k-colorable graph on n vertices. Then $\chi(G) = k$, that is, G is not $(k-1)$-colorable.

Proof. Suppose the opposite, and let $c : V \to \{1, \dots, k-1\}$ be an arbitrary $(k-1)$-coloring of G. Then we immediately obtain n distinct k-colorings $c_1, \dots, c_n : V \to \{1, \dots, k\}$ by setting

$$c_i(j) := \begin{cases} c(j) & \text{if } i \neq j \\ k & \text{if } i = j \end{cases} .$$

□

Lemma 5. Let $G = (V, E)$ be a maximal planar graph. If G is 3-colorable, then this coloring is unique.

Proof [12]. Assume that $|V| \geq 4$, since the statement is trivially true for K_3, the only maximal planar graph on 3 vertices. We will start by coloring an arbitrary triangle of G and show that this partial coloring determines the colors of every vertex in G.
Consider a planar embedding of G. By Lemma 1, each $e \in E$ is the boundary of two triangles. Take a triangle t_{v_1,v_2,v_3} and assign it three different colors. Now let $v \in V \setminus \{v_1, v_2, v_3\}$ be a vertex that is not colored yet. Then there is a sequence of triangles

$$t_{v_1,v_2,v_3}, t_{v_2,v_3,v_4}, \dots, t_{v_{p-2},v_{p-1},v_p}$$

which each share an edge, such that all vertices involved are distinct and $v_p = v$. It is evident that the unique proper coloring is realized by setting $c(v_4) := c(v_1)$, $c(v_5) := c(v_2)$ and so on until $c(v) := c(v_{p-3})$. This means, v can only receive one color, and therefore G is uniquely 3-colorable. □

Remark 4. Lemma 5 is not true for $k > 3$. Since every planar graph G, and in particular every maximal planar graph, has $\chi(G) \leq 4$, Lemma 4 states that G cannot be uniquely k-colorable for $k \geq 5$.
Let $k = 4$ and consider the following counterexample: Let G be defined as shown in Figure 2.9. Then $|V| = 7$ and $|E| = 15$, whereby the equality

$$|E| = 15 = 3 \cdot 7 - 6 = 3|V| - 6$$

assures maximal planarity of G by Lemma 1, and $\chi(G) = 4$ follows from the subgraph K_4 in the center of the graph. However, both

$$c_1 : V \to \{1, \ldots, 4\}, \quad 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 4, 5 \mapsto 3, 6 \mapsto 2, 7 \mapsto 1$$

and

$$c_2 : V \to \{1, \ldots, 4\}, \quad 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 4, 5 \mapsto 3, 6 \mapsto 2, 7 \mapsto 1$$

are proper 4-colorings of G, and they are distinct since $c_1(1) = c_1(7)$, but $c_2(1) \neq c_2(7)$.

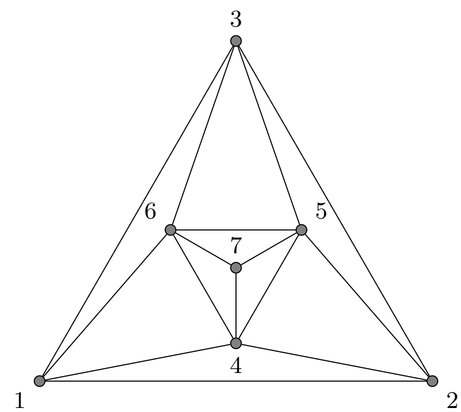


Fig. 2.9: A maximal planar, non-uniquely 4-colorable graph

2.4 The Chromatic Polynomial

The number of distinct proper k-colorings of a graph G can be seen as a function of k and denoted by $P_G(k)$ for $k \in \mathbb{N}_0$. Obviously $P_G(k) = 0 \; \forall \; k < \chi(G)$. A more interesting property is that $P_G(k)$ is indeed a polynomial in k.

Lemma 6. Let $G = (V, E)$ be a graph. Then $P_G(k)$ is a polynomial of degree $|V|$ in k.

Proof [31]. Let $V = \bigcup_{i=1}^{k} V_i$ be a k-partition of V and assume that $p \leq k$ subsets are non-empty. Clearly, there are $k \cdot (k-1) \cdot \ldots \cdot (k-p+1)$ distinct k-colorings of G that result in this particular partition, and this expression is a monic polynomial in k. The total number $P_G(k)$ of k-colorings is the sum of such terms over all possible partitions of V. Since there are only finitely many k-partitions, the sum is also a polynomial.
Note that for $k > n$, there is no valid partition with $p > n$ and exactly one with $p = n$. For this partition, the corresponding summand is a polynomial of degree n, which cannot be cancelled by lower degree terms. This proves the claim. $\square$

Simple examples of chromatic polynomials are $k(k-1)(k-2)$ for a triangle graph or $k(k-1)^{n-1}$ for any tree on n vertices. Moreover, the chromatic polynomial can be computed in polynomial time for various classes of graphs, for instance chordal graphs [41]. A recursive algorithm for general graphs makes use of edge contractions and deletions (see Section 8.2.7).

3. PRELIMINARIES FROM ALGEBRA

[11] is an excellent introduction to the theory of algebraic geometry and contains all prerequisites of this thesis. Most of the contents and the notation of the current chapter is based on this book.

3.1 Polynomial Rings and Ideals

Let $\mathbb{K}$ be a field. The *n-variate polynomial ring* over $\mathbb{K}$ is constructed by adjunction of n distinct (transcendent) elements $x_1, \ldots, x_n$. The resulting ring is denoted by $\mathbb{K}[x_1, \ldots, x_n]$. Note that $\mathbb{K}[x_1, \ldots, x_n]$ is not a field, if $n \geq 1$.
The elements of $\mathbb{K}[x_1, \ldots, x_n]$ are polynomials in $x_1, \ldots, x_n$ with finitely many terms. For a polynomial $p = \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha x^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$, we call $\deg(p) := \max\left(\|\alpha\|_1 : c_\alpha \neq 0\right)$ the *degree* and $\operatorname{len}(p) := |\{\alpha : c_\alpha \neq 0\}|$ the *length* of p. The set $\operatorname{supp}(p) := \{x^\alpha : c_\alpha \neq 0\}$ of non-zero monomials in p is the *support* of p.

Let $(R, +, \cdot)$ be a commutative ring. A subset $I \subseteq R$ is called an *ideal* if I is an additive subgroup of R and $r \cdot x \in I \ \forall\ r \in R, x \in I$. For a set $F \subseteq R$, we call $\langle F \rangle := \left\{\sum_{f \in F} c_f \cdot f : c_f \in R\right\}$ the ideal *generated by* F. If an ideal I can be generated by a finite set, then it is called *finitely generated*. A ring is *noetherian* if every with respect to inclusion strictly ascending chain of ideals is finite, i.e.,

$$\forall\ I_1 \subseteq I_2 \subseteq \ldots\ \exists s \in \mathbb{N} : I_i = I_j\ \forall\ i, j \geq s \quad .$$

For an ideal $I \subseteq R$, we call $\sqrt{I} := \{r \in R :\ \exists k \in \mathbb{N} : r^k \in I\}$ the *radical* of I. I is called *radical* itself if $I = \sqrt{I}$.

For an arbitrary set $F \subseteq \mathbb{K}[x_1, \ldots, x_n]$ of polynomials, we call the set $\mathcal{V}(F) := \{x \in \mathbb{K}^n : f(x) = 0\ \forall\ f \in F\}$ of common zeros the *algebraic variety* of F. Note that $\mathcal{V}(F) = \mathcal{V}(\langle F \rangle)$, such that we can always assume that varieties are taken over ideals.

Remark 5. Apart from $\mathbb{R}$ and $\mathbb{C}$, we will make use of finite fields in order to simplify computations. Since such fields are unique if the number of elements is prime, we denote them by $\mathbb{F}_p$. The isomorphism $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ gives a natural embedding of $\mathbb{F}_p$ into $\mathbb{Z}$.

Theorem 5. Let $R = \mathbb{K}[x_1, \ldots, x_n]$ be the polynomial ring in finitely many variables over a field. Then every ideal $I \subseteq R$ is finitely generated.

Proof . See for example [11]. The idea (which uses terms defined later in this thesis) is to consider the leading ideal $\mathcal{L}(I)$ of I and use Dickson's Lemma (Lemma 7) to show that it is finitely generated by the leading terms of elements $g_1, \ldots, g_s \in I$. Then it is rather straightforward to prove that this generating set itself satisfies $\langle g_1, \ldots, g_s \rangle = I$. $\square$

Remark 6. Theorem 5 is called *Hilbert's basis theorem* in [11]. Another, probably even more famous formulation is that a (univariate) polynomial ring over a noetherian ring is again noetherian. From this statement, Theorem 5 follows immediately by induction over n, where the base case is shown as follows: For $n = 0$, we consider the field $\mathbb{K}$. By definition of a field, the only ideals of $\mathbb{K}$ are $\{0\}$ and $\mathbb{K}$ itself, so every field is trivially noetherian.

Remark 7. An ideal that is generated by monomials, that is, $I = \langle x^{\alpha_i}, 1 \leq i \leq s\} \rangle$, is called a *monomial ideal*. In this case, a polynomial p belongs to I if and only if all monomials in $\text{supp}(p)$ belong to I, and a monomial x^β is in I if and only if $x^{\alpha_i} | x^\beta$ for some generator of I. Therefore, a monomial ideal is defined by the monomials it contains, and its geometry is easily described: It is generated by its $\leq$-minimal elements, and it can be embedded in $\mathbb{Z}^n_{\geq 0}$ as shown in figure 3.1.

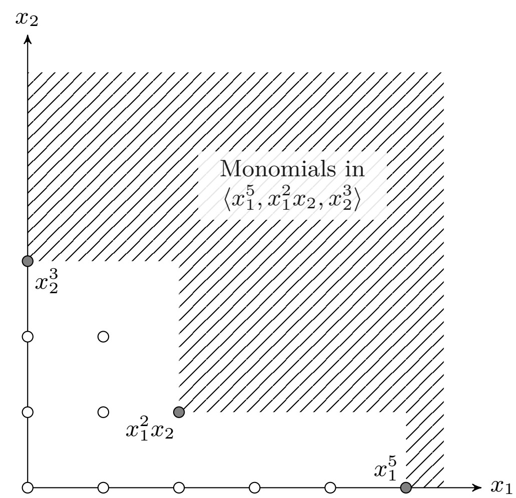


Fig. 3.1: Geometric view on the monomial ideal $\langle x_1^5, x_1^2x_2, x_2^3 \rangle \subseteq \mathbb{K}[x_1, x_2]$

Definition 11. Let $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ be a monomial ideal. Then a monomial $m \in \mathbb{K}[x_1, \dots, x_n]$ with $m \notin I$ is called a *standard monomial* of I. We denote the set of standard monomials of I by $\mathcal{B}_I$.

Remark 8. To avoid going beyond the scope of our thesis, we will not define quotient rings, the dimension of an ideal and other deeper concepts of algebraic geometry. We will, however, need the notion of a zero-dimensional ideal, whose defining property is its finite algebraic variety. A detailed introduction to algebraic geometry is for example given in [20].

3.2 Monomial Orders

When we talk about polynomials, it makes sense to have a canonical way to write them down. In the case of the univariate polynomial ring, this is easy: We order the terms descendingly by their degree, which gives a unique representation of a polynomial in

one variable.
As soon as we work with more than one variable (which will be the case throughout this thesis), the situation is more complicated, since, as we will see in this subsection, there are infinitely many ways to order the monomials. We start by defining what each "proper" term order has to satisfy.

Definition 12. A *term order* (or *monomial order*) on $\mathbb{K}[x_1, \ldots, x_n]$ is any total order $\succ$ on $\mathbb{Z}^n_{\geq 0}$, or equivalently, any total order on the set of monomials $\{x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}\}$, satisfying:

- If $\alpha \succ \beta$, then $\alpha + \gamma \succ \beta + \gamma$, and
- for the constant polynomial 1, $\gamma \succ 1$

for all $\alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}, \gamma \neq 0$.

There are two immediate consequences from this definition: First, if $\succ$ is a term order, then $\alpha + \beta \succ \alpha \; \forall \; \alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, where $\beta \neq 0$, and second, $\succ$ is a well-ordering, that is, every strictly decreasing sequence of monomials is finite. Equivalently, every non-empty set of monomials has a minimal element with respect to $\succ$. The latter is not trivial to see, so we will prove it, using Dickson's lemma.

Lemma 7 (Dickson's lemma)**.** Any set $C \subseteq \mathbb{Z}^n_{\geq 0}$ has only finitely many elements which are minimal with respect to the partial order $\geq$, defined by

$$\alpha \geq \beta \;:\Leftrightarrow\; \alpha_i \geq \beta_i \;\forall\; i \in \{1, \ldots, n\} \quad .$$

Proof. Assume that there is an infinite subset $M \subseteq C$ of minimal elements. We show by induction on the dimension n, that M contains an infinite sequence $m_1 < m_2 < \ldots$, which contradicts the assumption that all elements of M are $\geq$-minimal.

$n = 1$ Let $m_1 := \min_{m \in M}(m)$, $m_2 := \min_{m \in M \setminus \{m_1\}}(m)$, and so on. The order $\geq$ is total on $\mathbb{Z}_{\geq 0}$, thus we are done.

$n \to n+1$ For $m \in \mathbb{Z}^{n+1}_{\geq 0}$, denote by $m' := (m_1, \ldots, m_n)$ the projection of m onto the first n variables, and by $m^* := m_{n+1}$ the remaining component. By induction hypothesis, there is an infinite sequence $m_1, m_2, \ldots \subseteq M$ such that $m'_1 < m'_2 < \ldots$.
Now choose i_1 such that $m^*_{i_1}$ is minimal among the m^*_j for all $j \in \mathbb{Z}_{\geq 0}$, then choose i_2 such that $m^*_{i_2}$ is minimal among the m^*_j for all $j \in \mathbb{Z}_{\geq 0} \setminus \{1, \ldots, i_1\}$, and so forth.
By construction, $m^*_{i_1} < m^*_{i_2} < \ldots$, and moreover $m'_{i_1} < m'_{i_2} < \ldots$, hence $m_{i_1} < m_{i_2} < \ldots$ as claimed.

□

The partial order $\geq$ introduced in this lemma is easily recognized as the divisibility ordering on the monomials in $\mathbb{K}[x_1, \ldots, x_n]$. Now we can prove the consequence from above.

Lemma 8. Any term order on $\mathbb{K}[x_1, \ldots, x_n]$ is a well-ordering.

Proof: [28]. Let $M \subset \mathbb{K}[x_1, \ldots, x_n]$ be a non-empty set of monomials. By Lemma 7, the set M_0 of $\leq$-minimal elements in M is finite, and every $m \in M$ is a multiple of some $m_0 \in M_0$ (not necessarily unique). Let m^* denote the $\succ$-minimal element in M_0. Such an element exists, since $\succ$ is a total order.
Now, if $m \in M$ is an arbitrary monomial, we have that $\exists\ m_0 \in M_0, c \in \mathbb{K}[x_1, \ldots, x_n] :$ $m = c \cdot m_0$, and therefore $m \succ m_0 \succ m^*$, which shows that m^* is in fact $\succ$-minimal in M. □

Proposition 1. There are infinitely many distinct term orders for $\mathbb{K}[x_1, \ldots, x_n]$, if and only if $n > 1$.

Proof. Let $n = 1$. For any term order $\succ$, we have $x \succ 1$, and by successive multiplication with x also $x^{i+1} \succ x^i$ for all $i \in \mathbb{Z}_{\geq 0}$. This fact implies that

$$1 \prec x \prec x^2 \prec \ldots$$

is the unique term order on $\mathbb{K}[x]$.

Let now $n = 2$. For every $w \in \mathbb{N}$, define a term order $\succ_w$ by

$$\begin{aligned} x_1^{\alpha_1} x_2^{\alpha_2} \succ_w x_1^{\beta_1} x_2^{\beta_2} \iff & (w \cdot \alpha_1 + \alpha_2 > w \cdot \beta_1 + \beta_2) \vee \\ & ((w \cdot \alpha_1 + \alpha_2 = w \cdot \beta_1 + \beta_2) \wedge \alpha_1 > \beta_1) \quad . \end{aligned}$$

We will show that this defines a valid term order on $\mathbb{K}[x_1, x_2]$ for all w, and these orderings are pairwise distinct.

- Assume $\alpha \not\succ_w \beta$ and $\beta \not\succ_w \alpha$. Then $w \cdot \alpha_1 + \alpha_2 = w \cdot \beta_1 + \beta_2$ and also $\alpha_1 = \beta_1$, hence $\alpha = \beta$. Consequently, $\succ_w$ is a total order.
- Let $\alpha, \beta, \gamma \in \mathbb{Z}^2_{\geq 0}, \gamma \neq 0$. Then

$$\begin{aligned} \alpha \succ_w \beta \implies & (w \cdot \alpha_1 + \alpha_2 > w \cdot \beta_1 + \beta_2) \vee \\ & ((w \cdot \alpha_1 + \alpha_2 = w \cdot \beta_1 + \beta_2) \wedge \alpha_1 > \beta_1) \\ \implies & (w \cdot (\alpha_1 + \gamma_1) + (\alpha_2 + \gamma_2) > w \cdot (\beta_1 + \gamma_1) + (\beta_2 + \gamma_2) \vee \\ & ((w \cdot (\alpha_1 + \gamma_1) + (\alpha_2 + \gamma_2) = w \cdot (\beta_1 + \gamma_1) + (\beta_2 + \gamma_2)) \\ & \wedge (\alpha_1 + \gamma_1) > (\beta_1 + \gamma_1)) \\ \implies & \alpha + \gamma \succ_w \beta + \gamma \quad . \end{aligned}$$

- $w \cdot \gamma_1 + \gamma_2 > 0 \implies \gamma \succ_w 1$.
- $x_1 \succ_{w'} x_2^w\ \forall\ w' > w$, but $x_1 \prec_{w'} x_2^w\ \forall\ w' \leq w$.

Thus, we have infinitely many distinct monomial orders on $\mathbb{K}[x_1, x_2]$. Since we can always add a new variable whose power serves as a tie-breaker of the existing term order, the claim follows for all $n \geq 2$. □

Remark 9. From any term order $\succ$ on $\mathbb{K}[x_1, \ldots, x_n]$, we obtain in particular a total ordering on the unit monomials $x_1, \ldots, x_n$, which we call *variable order*. Note that if two term orders produce different variable orders, then they cannot be equal, but two term orders whose induced variable orders are equal, can very well be different. In fact, for each variable order there are *infinitely many* distinct monomial orders, which follows from the fact that there are only finitely many (precisely $k!$) variable orders.

Definition 13. Let $p \in \mathbb{K}[x_1, \ldots, x_n]$ be a polynomial. Upon choice of a monomial order $\succ$, we can put the terms of p in descending order, creating a canonical form of p. Let $c_\alpha x^\alpha$ be the highest term in this order, i.e.,

$$p = c_\alpha x^\alpha + \sum_{\alpha \neq \beta \in \mathbb{Z}^n_{\geq 0}} c_\beta x^\beta \text{ and } \alpha \succ \beta \ \forall\ \beta : c_\beta \neq 0 \quad .$$

Then we call $\mathrm{LT}(p) := c_\alpha x^\alpha$ the *leading term*, $\mathrm{LC}(p) := c_\alpha$ the *leading coefficient*, and $\mathrm{LM}(p) := x^\alpha$ the *leading monomial* of p. Moreover, $\mathrm{mdeg}(p) := \alpha$ is the *multi-degree* of p, and $\deg(p) := |\alpha|_1$ is its *total degree*. If there could be confusion about the used term order, it will be indicated by a subscript.

3.2.1 Standard Term Orders

There is an elegant way to describe *any* term order on $\mathbb{K}[x_1, \ldots, x_n]$. However, we will mostly use one of three *standard orders* which are more intuitive to understand than the general scheme. Those standard orders are widely used in computations, for algorithmic examples and for theoretical purposes.

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. The *lexicographic order* $\succ_{\mathrm{Lex}}$ is defined by

$$\alpha \succ_{\mathrm{Lex}} \beta \ \Leftrightarrow\ \exists k : \alpha_k > \beta_k \text{ and } \alpha_i = \beta_i \ \forall i < k \quad ,$$

that is, $\alpha \succ_{\mathrm{Lex}} \beta$ if and only if the leftmost non-zero entry in $\alpha - \beta$ is positive. Equivalently, the higher power of x_1 comes first, ties are broken by the power of x_2, and so on until x_n.

The *graded lexicographic order* $\succ_{\mathrm{GLex}}$ compares the total degree first, and uses $\succ_{\mathrm{Lex}}$ to break ties. Formally,

$$\alpha \succ_{\mathrm{GLex}} \beta \ \Leftrightarrow\ |\alpha|_1 > |\beta|_1 \text{ or } \big(|\alpha|_1 = |\beta|_1 \text{ and } \alpha \succ_{\mathrm{Lex}} \beta\big) \quad .$$

Finally, the *graded reverse lexicographic order* $\succ_{\mathrm{GRevLex}}$ works similarly to $\succ_{\mathrm{GLex}}$, but the tie-breaker is reversed; if the total degrees are equal, then $\alpha \succ_{\mathrm{GRevLex}} \beta$ if and only if the rightmost non-zero entry in $\alpha - \beta$ is negative:

$$\alpha \succ_{\mathrm{GRevLex}} \beta \ \Leftrightarrow\ |\alpha|_1 > |\beta|_1 \text{ or } \big(|\alpha|_1 = |\beta|_1 \text{ and } \alpha \succ_{\mathrm{RevLex}} \beta\big) \quad ,$$

where the auxiliary order $\succ_{\mathrm{RevLex}}$, defined as

$$\alpha \succ_{\mathrm{RevLex}} \beta \ \Leftrightarrow\ \exists k : \alpha_k < \beta_k \text{ and } \alpha_i = \beta_i \ \forall i > k \quad ,$$

is *not* a valid term order, since for instance $1 \succ_{\mathrm{RevLex}} x_1$.

All these monomial orders induce the variable order $x_1 \succ \ldots \succ x_n$ and can therefore also be defined for the rest of the $n!$ variable orders.

Example 3. Following the definition of the standard orders, we see that

$$\begin{array}{ccccccc} x_1^3x_2^2 & \succ_{\text{Lex}} & x_1^3x_2x_3^2 & \succ_{\text{Lex}} & x_1^2x_2^3x_3 & , \\ x_1^3x_2^1x_3^2 & \succ_{\text{GLex}} & x_1^2x_2^3x_3 & \succ_{\text{GLex}} & x_1^3x_2^2 & , \text{ and} \\ x_1^2x_2^3x_3 & \succ_{\text{GRevLex}} & x_1^3x_2x_3^2 & \succ_{\text{GRevLex}} & x_1^3x_2^2 & . \end{array}$$

3.2.2 Matrix Orders

We have seen in Proposition 1 that there are infinitely many term orders on $\mathbb{K}[x_1, \ldots, x_n]$. Is there a construction that generates *all* orders, and in particular the standard orders? Kreuzer and Robbiano [34] showed that such a construction scheme indeed exists. First, we want to avoid a variable order according to which we compare powers of single variables only, but use weights instead. Since for every such weight, this can only give a partial order, it makes sense to break ties using another order.

Definition 14. Let $w \in \mathbb{R}^n$. We call a term order $\succ_w$ a *weight order* with respect to w if

$$\alpha \succ_w \beta \;\Leftrightarrow\; w^T\alpha > w^T\beta \text{ or } \alpha \succ_{\text{Aux}} \beta \quad ,$$

where Aux is an auxiliary term order which serves as a tie-breaker. It is customary to use GRevLex here, but any other term order can also be used.

Iterating the weight vector approach, we take vectors $w_1, \ldots, w_k$ and successively form the scalar product. If we assume $k = n$, then it is possible to choose the weights so that no ties can occur for all comparisons (see Lemma 9). These weight vectors can be written in matrix form, giving name for the matrix order:

Definition 15. Let $M \in \mathbb{R}^{m\times n}$ be a matrix, and let $w_1, \ldots, w_m$ denote the rows of M. We call an order $\succ_M$ on $\mathbb{Z}^n_{\geq 0}$ a *matrix order* with respect to M if

$$\alpha \succ_M \beta \;\Leftrightarrow\; \exists k : w_k\alpha > w_k\beta \text{ and } w_i\alpha = w_i\beta \;\forall i < k \quad .$$

Lemma 9. A matrix order $\succ_M$ is a total order if and only if $\operatorname{rank}(M) = n$.

Proof.

$\Rightarrow$ Let $\operatorname{rank}(M) < n$, and let $x \in \ker(M) \setminus \{0\}$. Then $w_ix = 0\ \forall i$, and therefore neither $\alpha \succ_M \alpha + x$ nor $\alpha \succ_M \alpha + x$ for an arbitrary $\alpha \in \mathbb{Z}^n_{\geq 0}$.

$\Leftarrow$ Assume that $\alpha \not\succ_M \beta$ and $\beta \not\succ_M \alpha$ for some $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}, \alpha \neq \beta$. Then, for all i,

$$w_i\alpha = w_i\beta \;\Rightarrow\; w_i(\alpha - \beta) = 0 \;\Rightarrow\; \alpha - \beta \in \ker(M) \setminus \{0\} \;\Rightarrow\; \operatorname{rank}(M) < n \quad .$$

□

Remark 10. Consider the matrices

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & \cdots & 1 & 1 & 1 \\ 1 & \cdots & 1 & 1 & 0 \\ 1 & \cdots & 1 & 0 & 0 \\ \vdots & \iddots & \iddots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Evidently, $\succ_{M_1} = \succ_{\text{Lex}}$, $\succ_{M_2} = \succ_{\text{GLex}}$ and $\succ_{M_3} = \succ_{\text{GRevLex}}$, as can be seen by looking at the definition of the standard orders. This representation of term orders by matrices is not a coincidence: in fact, *all* possible term orders can be written as matrix orders.

Proposition 2. Let $\succ$ be a term order on $\mathbb{K}[x_1, \ldots, x_n]$. Then there is an $n \times n$-matrix M with real entries such that $\succ_M = \succ$, and the first non-zero entry of each row is positive.

Proof. See [42], Theorem 4. $\square$

Remark 11. The matrix M does not necessarily have to be non-negative; there are valid term orders that have a matrix representation with negative entries. For instance,

$$M_3' = \begin{pmatrix} 1 & \cdots & 1 & 1 & 1 \\ 0 & \cdots & 0 & 0 & -1 \\ 0 & \cdots & 0 & -1 & 0 \\ \vdots & \iddots & \iddots & \vdots & \vdots \\ 0 & -1 & 0 & 0 & 0 \end{pmatrix}$$

is another way to define the GRevLex order, which is closer to the definition above, since in this order, a monomial becomes smaller with respect to the order, if one of the components of the exponent becomes larger.
However, the uppermost non-zero entry in every column has to be positive, ensuring that $x_i \succ 1 \; \forall i$.

Definition 16. Let a term order $\succ$ be fixed. If $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal, then

$$\mathcal{L}(I) := \langle \text{LM}(p) : p \in I \rangle$$

is the *leading ideal* of I with respect to $\succ$.

It will be useful to permute the vertices of a given graph in order to change its Gröbner basis properties in a desired way. Such a permutation can also be modeled by changing the variable order of a term order, while maintaining the weight relations between the variables. The following lemma shows how to obtain a permuted term order from a given order, provided in the general matrix form.

Lemma 10. Let $\sigma \in \mathbb{S}_n$ be a permutation, and $\succ$ a monomial order on $\mathbb{K}[x_1, \ldots, x_n]$. Then there is a monomial order $>$ such that

$$\alpha \succ \beta \iff \sigma_\alpha > \sigma_\beta \quad .$$

In particular, every change in the vertex order of a graph can be represented by a suitable monomial order.

Proof. By Proposition 2, there exists a matrix $M = \begin{pmatrix} m_1 & m_2 & \cdots & m_n \end{pmatrix}^T \in \mathbb{R}^{n \times n}$ such that $\succ \, = \, \succ_M$. Let now $> := \succ_{\sigma(M)}$, where $\sigma(M) = \begin{pmatrix} m_{\sigma(1)} & m_{\sigma(2)} & \cdots & m_{\sigma(n)} \end{pmatrix}^T$. We will show that $>$ has the above property. Let x^α, x^β be monomials. Then

$$\begin{aligned}
x^\alpha \succ x^\beta \quad &\iff \quad x^\alpha \succ_M x^\beta \\
&\iff \quad \exists k : m_k^T \alpha > m_k^T \beta \text{ and } m_i^T \alpha = m_i^T \beta \;\forall i < k \\
&\iff \quad \exists k : m_{\sigma(k)}^T \sigma_\alpha > m_{\sigma(k)}^T \sigma_\beta \text{ and } m_{\sigma(i)}^T \sigma_\alpha = m_{\sigma(i)}^T \sigma_\beta \;\forall i < k \\
&\iff \quad x^{\sigma_\alpha} \succ_{\sigma(M)} x^{\sigma_\beta} \\
&\iff \quad x^{\sigma_\alpha} > x^{\sigma_\beta} \quad .
\end{aligned}$$

□

3.3 Multivariate Polynomial Division

Let $\mathbb{K}[x_1, \ldots, x_n]$ be equipped with a monomial order $\succ$. Given a polynomial p and a finite set of polynomials $f_1, \ldots, f_k$, we want to write p as a combination of the f_i, possibly with a remainder. This generalizes the Euclidean algorithm to both polynomial rings and multiple divisors. The general idea is to find some f_i whose leading term divides $\mathrm{LT}(p)$, multiply it with a suitable coefficient polynomial and subtract the product from p, such that $\mathrm{LT}(p)$ is cancelled. If this is not possible, $\mathrm{LT}(p)$ becomes part of the remainder, and we continue with the next monomial in p. Note that the division process and the result depend on the order of the divisor polynomials, because there is, in general, more than one option in every step.

Theorem 6. Fix a monomial order $\succ$ on $\mathbb{Z}^n_{\geq 0}$ and let $F = (f_1, \ldots, f_k)$ be an ordered k-tuple of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Then every $p \in \mathbb{K}[x_1, \ldots, x_n]$ can be written as

$$p = a_1 f_1 + \cdots + a_k f_k + r \quad ,$$

where $a_i, r \in \mathbb{K}[x_1, \ldots, x_n]$, and either the remainder $r = 0$ or r is a $\mathbb{K}$-linear combination of monomials, none of which is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_k)$. Furthermore, if $a_i f_i \neq 0$, then we have $\mathrm{mdeg}(f) \geq \mathrm{mdeg}(a_i f_i)$.

Proof. See [11], Chapter 2, §3, Theorem 3, where the statement is proven by providing an algorithm (Algorithm 1), which gives, for a polynomial p and a divisor set F, exactly the coefficients and the remainder from the theorem. □

Algorithm 1 Multivariate polynomial division

Input: Dividend $p \in \mathbb{K}[x_1, \ldots, x_n]$, divisors $F = \{f_1, \ldots, f_k\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$
Output: Coefficients and remainder $c_1, \ldots, c_k, r \in \mathbb{K}[x_1, \ldots, x_n]$

```
function POLYNOMIALDIVISION(p, F)
    c_i ← 0 ∀ i
    r ← 0
    while p ≠ 0 do
        i ← 1
        divisionOccured ← false
        while (i ≤ k) ∧ (divisionOccured = false ) do
            if LT(f_i) | LT(p) then
                c_i ← c_i + LT(p)/LT(f_i)
                p ← p − LT(p)/LT(f_i) · f_i
                divisionOccured ← true
            else
                i ← i + 1
            end if
        end while
        if divisionOccured = false then
            r ← r + LT(p)
            p ← p − LT(p)
        end if
    end while
    return c_1, ..., c_k, r
end function
```

Remark 12. We denote the remainder r of multivariate polynomial division of p by F by $r = \overline{p}^F$.

Example 4. Let us consider the polynomial ring in two variables. For $p = x_1x_2^2 + 1$ and $F = \{x_1x_2 + 1, x_2 + 1\}$, the steps are:

$$
\begin{aligned}
\mathrm{LM}(f_1) \,|\, \mathrm{LM}(p) \quad &\Longrightarrow \quad a_1 \leftarrow \frac{\mathrm{LM}(f_1)}{\mathrm{LM}(p)} = x_2,\ p \leftarrow p - a_1 f_1 = -x_2 + 1 \\
\mathrm{LM}(f_2) \,|\, \mathrm{LM}(p) \quad &\Longrightarrow \quad a_2 \leftarrow \frac{\mathrm{LM}(f_2)}{\mathrm{LM}(p)} = -1,\ p \leftarrow p - a_2 f_2 = 2 \\
\mathrm{LM}(f_1), \mathrm{LM}(f_2) \nmid \mathrm{LM}(p) \quad &\Longrightarrow \quad r \leftarrow \mathrm{LT}(p) = 2,\ p \leftarrow p - r = 0
\end{aligned}
$$

and consequently

$$
\begin{array}{ccccccccccc}
p & = & a_1 & \cdot & f_1 & + & a_2 & \cdot & f_2 & + & r \\
 & = & x_2 & \cdot & (x_1x_2 + 1) & + & (-1) & \cdot & (x_2 + 1) & + & 2 \; .
\end{array}
$$

3.4 Gröbner Bases

As mentioned in the previous subsection, the remainder $r = \overline{p}^F$ is not unique for a generic set F of generators for an ideal I. In fact, the situation is even worse: If $p \in I$, there is no guarantee that the division algorithm will write p as a combination of the f_i, that is, $r = 0$. Thus, membership in I cannot directly be shown via multivariate division.

Example 5. We divide $p = xy^2 - x$ by the set $F = \{f_1 = xy + 1, f_2 = y^2 - 1\}$:

$$\begin{aligned}
\mathrm{LM}(f_1) | \mathrm{LM}(p) &\implies a_1 \leftarrow \frac{\mathrm{LM}(f_1)}{\mathrm{LM}(p)} = y,\ p \leftarrow p - a_1 f_1 = -x - y \\
\mathrm{LM}(f_1), \mathrm{LM}(f_2) \nmid \mathrm{LM}(p) &\implies r \leftarrow -x,\ p \leftarrow p - r = -y \\
\mathrm{LM}(f_1), \mathrm{LM}(f_2) \nmid \mathrm{LM}(p) &\implies r \leftarrow r - y = -x - y,\ p \leftarrow p - r = 0
\end{aligned}$$

Hence, the result is

$$\begin{array}{ccccccccccc}
p & = & a_1 & \cdot & f_1 & + & a_2 & \cdot & f_2 & + & r \\
 & = & y & \cdot & (xy+1) & + & 0 & \cdot & (y^2-1) & + & (-x-y)
\end{array}$$

with a non-zero remainder r.
However, the equality

$$xy^2 - x = x(y^2 - 1) = x \cdot f_2$$

shows that $p \in \langle f_1, f_2 \rangle$, although we were not able to prove membership via the division algorithm.

This motivates the need for a set F of generators of an ideal I such that remainders with respect to F are unique. Such a generating set is called a *Gröbner basis* of I.

Definition 17. Fix a monomial order $\succ$, and let $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ be an ideal. A finite set $G = \{g_1, \dots, g_t\}$ is called a *Gröbner basis* of I with respect to $\succ$ if

$$\mathcal{L}(G) = \mathcal{L}(I) \quad .$$

Theorem 7. Let $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ be an ideal. Then there is a Gröbner basis $\mathcal{G}$ of I. Moreover, a Gröbner basis is indeed a basis of I, i.e., $\langle \mathcal{G} \rangle = I$.

Proof. Theorem 5 gives that the ideal $\mathcal{L}(I)$ has a finite generating set of monomials, that is, $\mathcal{L}(I) = \langle m_1, \dots, m_t \rangle$. By definition of a leading ideal, there are polynomials $p_1, \dots, p_t \in I$ such that $\mathrm{LM}(p_i) = m_i\ \forall i$. Therefore, $\mathcal{G} = \{p_1, \dots, p_t\}$ is a Gröbner basis of I.
Let now $\mathcal{G} = \{g_1, \dots, g_t\}$ be a Gröbner basis of I. To show the second claim, we apply Algorithm 1 in the form $\textsc{PolynomialDivision}(p, \mathcal{G})$ for an arbitrary polynomial $p \in I$, and obtain a representation of the form $p = \sum_{i=1}^t c_i g_i + r$. We claim that $r = 0$. Assume $0 \neq r = p - \sum_{i=1}^t c_i g_i \in I$. Then $\mathrm{LT}(r) \in \mathcal{L}(I) = \mathcal{L}(g_1, \dots, g_t)$, and by Remark 7 there is g_i such that $\mathrm{LM}(g_i) | \mathrm{LM}(r)$, which contradicts the properties of a remainder (see Theorem 6). Thus, $r = 0$ and consequently $I \subset \langle \mathcal{G} \rangle$. The opposite inclusion is trivial, since $g_i \in I\ \forall i$. $\square$

Gröbner bases can be characterized in several different ways, each of which reveals important and interesting properties.

Proposition 3. Let $\mathcal{G} = \{g_1, \dots, g_t\}$ be a Gröbner basis for an ideal $I \subseteq \mathbb{K}[x_1, \dots, x_n]$, and let $p \in \mathbb{K}[x_1, \dots, x_n]$ be an arbitrary polynomial. Then there is a unique $r \in \mathbb{K}[x_1, \dots, x_n]$ with the following two properties: No term of r is divisible by any of $\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_t)$ and there is some $g \in I$ such that $p = g + r$.
In particular, r is the remainder on division of p by $\mathcal{G}$ no matter how the elements of $\mathcal{G}$ are listed when using the division algorithm.

Proof [11]. The division algorithm gives $p = \sum_{i=1}^{t} c_i g_i + r$. If we now set $g = p - r = \sum_{i=1}^{t} c_i g_i$, then both properties are satisfied.
To prove uniqueness, assume that there are two such representations $p = g_1 + r_1 = g_2 + r_2$ which satisfy the assumptions. Note that $r_1 - r_2 = g_2 - g_1 \in I$, and therefore $\mathrm{LT}(r_1 - r_2) \in \mathcal{L}(I) = \mathcal{L}(g_1, \dots, g_t)$. Again, as in the proof of theorem 7, there is some g_i with $\mathrm{LM}(g_i) | \mathrm{LM}(r_1 - r_2)$, if $r_1 \neq r_2$. Since the terms of $r_1 - r_2$ each appear in at least one of the remainders, this is a contradiction. We conclude $r_1 = r_2$, and hence the remainder is unique. The last claim follows immediately. □

Lemma 11. If $\mathcal{G}$ is a Gröbner basis for an ideal $I \subseteq \mathbb{K}[x_1, \dots, x_n]$, then

$$p \in I \iff \overline{p}^{\mathcal{G}} = 0 \quad .$$

Proof. By Proposition 3, $r = \overline{p}^{\mathcal{G}}$ is unique. Therefore, if $p \in I$, the validity of $r = 0$ shows the $\Rightarrow$-implication. Conversely, if $p \notin I$, then the remainder clearly cannot be zero. □

Proposition 3 makes clear why Gröbner bases are so useful for ideal computations, for example ideal membership and equality tests. To find a Gröbner basis for a given ideal I, we have to find a set whose leading terms span the leading ideal $\mathcal{L}(I)$. It seems reasonable to start with a generating set G and successively add polynomials whose leading term is not yet in the ideal generated by the leading monomials of G. Such polynomials can be systematically found by combining two existing polynomials in a way that cancels their leading terms. This idea is formalized by the definition of the *S-polynomial* (or *S-pair*) of two polynomials f and g:

$$S(f, g) := \frac{x^\alpha}{\mathrm{LT}(f)} \cdot f - \frac{x^\alpha}{\mathrm{LT}(g)} \cdot g \quad ,$$

where $x^\alpha = \mathrm{lcm}\,(\mathrm{LM}(f), \mathrm{LM}(g))$. The next characterization of Gröbner bases makes use of this notion and shows that it is *sufficient* for a set G to be a Gröbner basis that the S-polynomials of all pairs of polynomials in G vanish. It is due to Buchberger [6] and gives a constructive way to find Gröbner bases.

Theorem 8 (Buchberger's criterion)**.** A finite set $\mathcal{G} = \{g_1, \dots, g_t\}$ is a Gröbner basis for the ideal $\langle g_1, \dots, g_t \rangle$ if and only if

$$\overline{S(g_i, g_j)}^{\mathcal{G}} = 0$$

for all $i, j \in \{1, \dots, t\}$ with $i \neq j$.

Proof. See for example [11], Chapter 2, §6, Theorem 6. □

Remark 13. It can be shown that all properties which we derived for Gröbner bases so far are in fact defining properties: They are equivalent to the leading ideal condition (Definition 17). Thus, a set $\mathcal{G}$ is a Gröbner basis of an ideal I if one (and therefore all) of the following holds:

- $\mathcal{L}(\mathcal{G}) = \mathcal{L}(I)$
- $\overline{S(g_i, g_j)}^{\mathcal{G}} = 0 \;\forall\; i \neq j$
- $p \in I \iff \overline{p}^{\mathcal{G}} = 0$ for all $p \in \mathbb{K}[x_1, \dots, x_n]$
- The remainder of polynomial division by $\mathcal{G}$ is unique.

From the definition of a Gröbner Basis, it is easy to see that for a given ideal I and a Gröbner basis $\mathcal{G}$ of I, every superset $\mathcal{G}' \supset \mathcal{G}$ is a Gröbner Basis of I with respect to the same term order. This motivates two questions: First, we can ask about a *minimal* Gröbner Basis for a specific term order. Does it exist, and if so, is it unique? Second, can we get rid of the choice of a term order? For example, if we build a Gröbner basis for *every* possible term order (obviously such a basis can easily be obtained by taking the union over Gröbner bases for all orders), will this large basis always be finite? These two problems can in fact be answered in a very satisfying manner.
Another interesting question about Gröbner bases addresses their complexity. Since a Gröbner basis is just a set of polynomials, it is natural to take the number of polynomials and their respective complexity, which consists of degree, coefficient size and number of terms, into account. Of these dimensions, we will abandon the coefficient size, since computations can be performed over finite fields to avoid large or fractional coefficients (see Fact 3).

Definition 18. Let $\mathcal{G}$ be a Gröbner basis. The *length* $\mathfrak{l}(\mathcal{G}) := |\mathcal{G}|$ is the number of elements in $\mathcal{G}$. The *degree* $\mathfrak{d}(\mathcal{G}) := \max_{g \in \mathcal{G}}(\deg g)$ is the maximum total degree of an element, and the *support* $\mathfrak{s}(\mathcal{G}) := \max_{g \in \mathcal{G}}(|\operatorname{supp} g|)$ is the largest number of terms in an element of $\mathcal{G}$.
We will call the triple $(\mathfrak{l}(\mathcal{G}), \mathfrak{d}(\mathcal{G}), \mathfrak{s}(\mathcal{G}))$ the *complexity pattern* $\mathfrak{c}(\mathcal{G})$ of $\mathcal{G}$.

The product of these complexity measures gives an upper bound

$$\mathcal{O}\left(\mathfrak{l}(\mathcal{G}) \cdot \mathfrak{d}(\mathcal{G}) \cdot \mathfrak{s}(\mathcal{G})\right)$$

for the total (storage) size of $\mathcal{G}$. However, this upper bound is not strict, since typically a few elements of a Gröbner basis have large degree and a large number of monomials, while most of the other polynomials are small.

Remark 14. The notion of the complexity pattern and its components for a Gröbner basis is not standard and only used in this thesis.

Lemma 12. Let G be a Gröbner basis for an ideal $I \subseteq \mathbb{K}[x_1, \dots, x_n]$. Let $p \in G$ be a polynomial such that $\operatorname{LT}(p) \in \mathcal{L}(G \setminus \{p\})$. Then $G \setminus \{p\}$ is also a Gröbner basis for I.

Proof [11]. By definition of a Gröbner basis, $\mathcal{L}(G) = \mathcal{L}(I)$. Now the assumption is that $\mathrm{LT}(p) \in \mathcal{L}(G \setminus \{p\})$, and therefore $\mathcal{L}(G \setminus \{p\}) = \mathcal{L}(G)$. Thus, $G \setminus \{p\}$ satisfies the condition for being a Gröbner basis for I. $\square$

Definition 19. A Gröbner basis $\mathcal{G}$ of an ideal $\mathcal{I} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is called *reduced* if for all $f, g \in \mathcal{G}, f \neq g$, no monomial in f can be divided by $\mathrm{LM}(g)$, and moreover $\mathrm{LC}(g) = 1\ \forall\ g \in \mathcal{G}$.

Proposition 4. For an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ and a fixed term order $\succ$, the reduced Gröbner basis of I with respect to $\succ$ is unique. We will denote this basis by $\mathcal{G}_{\succ}(I)$.

Proof [11]. Let $\mathcal{G}$ and $\mathcal{G}'$ be two such bases. Clearly, $\mathcal{L}(\mathcal{G}) = \mathcal{L}(I) = \mathcal{L}(\mathcal{G}')$, and the leading monomials of a reduced Gröbner basis are exactly the $\succ$-minimal monomials of this ideal. Therefore, $\mathrm{LM}(\mathcal{G}) = \mathrm{LM}(\mathcal{G}')$, and in particular $|\mathcal{G}| = |\mathcal{G}'|$.
Let now $g' \in \mathcal{G}'$. Then there is some $g \in \mathcal{G}$ such that $\mathrm{LM}(g) = \mathrm{LM}(g')$. Our goal is to show that $g = g'$; then the claim follows. Consider the polynomial $g - g' \in I$, for which $\overline{g - g'}^{\mathcal{G}} = 0$ holds. But by choice of g, the leading terms cancel in the difference, and none of the remaining terms is divisible by any leading term of $\mathcal{G}$ or $\mathcal{G}'$ by assumption that both bases are reduced. Therefore, $\overline{g - g'}^{\mathcal{G}} = g - g'$, which implies $g = g'$. $\square$

Remark 15. The uniqueness of the reduced Gröbner basis of an ideal I justifies the following notion: The length of the reduced basis for a term order $\succ$ is considered a property of the ideal itself and therefore denoted by $\mathfrak{l}_{\succ}(I)$, and analogously for $\mathfrak{d}$ and $\mathfrak{s}$.

To obtain a reduced Gröbner basis from a general one, we can use a reduction algorithm (Algorithm 2), which applies multivariate polynomial division to all elements of the given basis, until the remainders cannot be reduced further.

Algorithm 2 Gröbner basis reduction algorithm

Input: Gröbner basis $G \subseteq \mathbb{K}[x_1, \ldots, x_n]$
Output: Reduced Gröbner basis G' of $\langle G \rangle$

```
function ReduceGröbnerBasis(G)
    G' ← G
    for all g ∈ G' do
        if LT(g) ∈ 𝓛(G' \ {g}) then
            G' ← (G' \ {g})
        end if
    end for
    for all g ∈ G' do
        g' ← ‾g^{G'\{g'}}
        G' ← G' \ {g}
        if g' ≠ 0 then
            G' ← G' ∩ {g'}
        end if
    end for
    return G'
end function
```

Proposition 5. Algorithm 2 returns the reduced Gröbner Basis of the input ideal $\langle G \rangle$, if G was a Gröbner Basis.

Proof. After the first **for**-loop, G' is still a Gröbner basis by Lemma 12, and $\forall\, p \in G'$: $\mathrm{LM}(p) \notin \mathcal{L}(G' \setminus \{p\})$. Such a Gröbner basis is called a *minimal* basis.
We will show that after each iteration of the second **for**-loop, the involved polynomial g is *reduced* for G', i.e., no monomial of g lies in $\mathcal{L}(G' \setminus \{g\})$, and that it remains reduced during the entire process: Note that a reduced element g is also reduced for any other minimal Gröbner basis that contains g and has the same leading ideal, because the definition of a reduced polynomial only depends on the leading terms. We claim that $(G' \setminus \{g\}) \cap \{g'\}$ is again a minimal basis. $\mathrm{LT}(g') = \mathrm{LT}(g)$, since g is in the minimal basis G', and thus $\mathrm{LT}(g)$ always goes to the remainder when we divide by $G' \setminus \{g\}$. In consequence, the leading ideal does not change, which means that $(G' \setminus \{g\}) \cap \{g'\}$ is a Gröbner basis. Reducedness of g' and minimality follow immediately.
After going through all elements in G' and reducing them, we can be sure that every $g \in G'$ is reduced, which is equivalent to G' being a reduced Gröbner basis. □

Corollary 1. Let $\mathcal{G} = \mathcal{G}_{\succ}(I)$ be the reduced Gröbner basis of an ideal I under a fixed term order $\succ$. Then, for every Gröbner basis $\mathcal{G}'$ of I under the same term order, $\mathfrak{l}(\mathcal{G}) \leq \mathfrak{l}(\mathcal{G}')$.

Proof. For input $\mathcal{G}'$, Algorithm 2 yields $\mathcal{G}$ as result. During the algorithm, no new polynomial is added, and therefore $|\mathcal{G}| \leq |\mathcal{G}'|$. □

Reduced Gröbner bases are not necessarily optimal with respect to their complexity pattern. It is easy to find a graph family (see Example 6 below) together with suitable monomial orders, such that the support of the reduced Gröbner bases grows linearly, while other Gröbner bases for the same ideal and the same term order have constant support.
Regarding the degree of a reduced Gröbner basis, it is not obvious if it is minimal among all bases for the same ideal. Of course, if the term order $\succ$ is graded, that is, $w_1 = (1\ 1 \cdots 1)$ in the matrix representation of $\succ$, then the reduction algorithm will never increase the total degree of an element. However, for the Lex order, it can happen that the leading term does not have maximal total degree among the terms of a polynomials. Let, for instance, $p = x_1^2$ and $F = \{x_1^2 + x_2^3 + x_2x_3\}$. Then $\overline{p}^F = -x_2^3 - x_2x_3$, and thus both $\deg(p) = 2 < 4 = \deg(\overline{p}^F)$ and $|\operatorname{supp}(p)| = 1 < 2 = |supp(\overline{p}^F)|$. This means that reduction of p by F, as performed during Algorithm 2, can increase the complexity of the set. However, the set $F \cup \{p\}$ was not a Gröbner basis; thus it is not clear if this can happen for a Gröbner basis input, too, or if the latter prevents the phenomenon.

Definition 20. A finite set $\mathcal{G}$ is called *universal Gröbner basis* of an ideal I if it is a Gröbner basis of I with respect to *any* term order on $\mathbb{K}[x_1, \ldots, x_n]$.
In Corollary 2, we will show that the union

$$\mathcal{G}_{\mathrm{uni}}(I) := \bigcup_{\succ} \mathcal{G}_{\succ}(I)$$

of the reduced Gröbner bases of I for all possible term orders is well-defined for any ideal I and therefore gives a universal Gröbner basis.

3.5 Buchberger's Algorithm

Buchberger's algorithm is a procedure which turns an ideal, given by a finite set of generators, into a Gröbner basis for the same ideal. The simplest implementation of the algorithm (see Algorithm 3) uses Theorem 8 in a very straightforward manner: Start with a generating set $F = \{f_1, \dots, f_s\}$ of the ideal $I = \langle F \rangle$ and take F as an initialization for the prospective Gröbner basis G. Now compute the remainder of the S-polynomial of each pair of elements in G, and add it to G if it is non-zero. Repeat this procedure until all possible S-pairs reduce to 0, since this is equivalent to G being a Gröbner Basis for the ideal it generates, which is exactly I. It is not a priori clear that this is a finite process, but we will see a short argument below.

Algorithm 3 Buchberger's algorithm

Input: $F \subseteq \mathbb{K}[x_1, \dots, x_n]$
Output: Gröbner basis G of $\langle F \rangle$

```
function BUCHBERGER(F)
    G ← F
    repeat
        G' ← G
        for all {p, q} ∈ (G' choose 2) do
            r ← \overline{S(p, q)}^G
            if r ≠ 0 then
                G ← G ∪ {r}
            end if
        end for
    until G = G'
    return G
end function
```

Lemma 13. Buchberger's algorithm terminates after finitely many steps.

Proof [11]. At the end of each step (except the last one), $G' \subsetneq G$. Take some newly added remainder $r \in G \setminus G'$. r is a remainder from division by G', so $m \nmid \mathrm{LT}(r)\ \forall\ m \in \mathcal{L}(G')$, and therefore $\mathrm{LT}(r) \notin \mathcal{L}(G')$. But by construction, $\mathrm{LT}(r) \in \mathcal{L}(G)$, which shows that $\mathcal{L}(G') \subsetneq \mathcal{L}(G)$, and thus the sequence of $\mathcal{L}(G)$ in every step form a strictly ascending chain of monomial ideals in $\mathbb{K}[x_1, \dots, x_n]$.
Now, since the polynomial ring is noetherian, the ideal chain eventually stabilizes, and as soon as this happens, $G' = G$, and the exit criterion for the outer loop is true. $\square$

Remark 16. For general ideals $I \subseteq \mathbb{K}[x_1, \dots, x_n]$, it has been shown that Gröbner bases can become very large. Precisely, [38] gives an upper bound for the degree of a reduced Gröbner basis for an r-dimensional ideal, whose generators have degree bounded by d. The authors show that a Gröbner basis of such an ideal can have degree $\leq 2(\frac{1}{2}d^{n-r}+d)^{2^r}$. For the case of zero-dimensional ideals (which holds for coloring ideals), this bound reduces to $\leq 2(\frac{1}{2}d^n + d)$. In [43], a lower bound of d^n for zero-dimensional ideals is given by a suitable example.

The fact that this bound is exponential in n suggests that Gröbner basis computation is inherently inefficient. However, the restriction to coloring ideals which have a special structure, gives hope to a better upper bound on the degree of the resulting Gröbner bases. On the other hand, a small Gröbner basis does not mean that it can be computed efficiently. In Chapter 5, we show that a polynomial-time algorithm for Gröbner bases of 3-coloring ideals would imply that $\mathcal{P} = \mathcal{NP}$. It could thus be the case that the coloring ideal of an arbitrary graph has a small (e.g. linear-sized) Gröbner basis, but it still takes exponential time to find such a basis in general.

Proposition 6. Let $P \subset \mathbb{K}[x_1, \ldots, x_n]$ be a finite set, and let $p_1, p_2 \in P$ such that

$$\operatorname{lcm}(\mathrm{LM}(p_1), \mathrm{LM}(p_2)) = \mathrm{LM}(p_1) \cdot \mathrm{LM}(p_2) \quad .$$

Then

$$S(p_1, p_2) \rightarrow_P 0 \quad .$$

Proof [11]. Assume without loss of generality that both leading terms of p_1 and p_2 are 1. We separate the two polynomials into $p_1 = \mathrm{LM}(p_1) + r_1$ and $p_2 = \mathrm{LM}(p_2) + r_2$. Now

$$\begin{aligned} S(p_1, p_2) &= \mathrm{LM}(p_2) \cdot p_1 - \mathrm{LM}(p_1) \cdot p_2 \\ &= (p_2 - r_2) \cdot p_1 - (p_1 - r_1) \cdot p_2 \\ &= p_2 p_1 - r_2 p_1 - p_1 p_2 + r_1 p_2 \\ &= r_1 p_2 - r_2 p_1. \end{aligned}$$

Note that $\mathrm{LM}(p_2) \nmid \mathrm{LM}(r_2)$ and therefore $\mathrm{LM}(r_1) \cdot \mathrm{LM}(p_2) \neq \mathrm{LM}(r_2) \cdot \mathrm{LM}(p_1)$, because $\gcd(\mathrm{LM}(p_1), \mathrm{LM}(p_2)) = 1$. Thus, the leading terms of $r_1 p_2$ and $r_2 p_1$ cannot cancel, and $\operatorname{mdeg}(S(p_1, p_2)) = \max(\operatorname{mdeg}(r_1 p_2), \operatorname{mdeg}(r_2 p_1))$. With $p_1, p_2 \in P$, the claim follows. $\square$

Remark 17. Proposition 6 is useful from two points of view: First, it gives a hint on how to speed up Buchberger's algorithm: Before computing an S-pair $S(f, g)$ and reducing it with respect to G, we test f and g for being relatively prime, and if they are, we can directly go to the next pair and skip the (sometimes very costly) polynomial division.
Second, it allows for a direct proof that a given set G is a Gröbner basis: If we can find a term order under which the leading terms of all elements of G are relatively prime, then G is a Gröbner basis under this order.

3.6 The Gröbner Fan

All Gröbner basis techniques so far are based on the choice of a specific term order, which has to be made upfront. As a consequence, it is possible that obtaining a "bad" Gröbner basis, that is, a basis with high complexity or high computational effort, is simply due to a bad choice of monomial order. We want to overcome this drawback by somehow looking at *all* possible term orders, and therefore all possible Gröbner bases, at the same time. Remember that there are, for $n > 1$, infinitely many distinct term orders (Proposition 1). However, we will see that for a given ideal I, the set of leading ideals of I, taken over all term orders, is finite, and so is the set of all Gröbner bases of I. We will introduce the *Gröbner fan* of an ideal and show that it is a powerful tool, both as a theoretical concept and a computational approach, in order to examine Gröbner bases independently of a specific term order. The Gröbner fan is a collection of cones in the positive orthant $\mathbb{R}^n_+$. To understand its properties, we need some definitions that link monomial orders to this orthant.

Definition 21. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. The set

$$\mathrm{Mon}(I) := \{\mathcal{L}_\succ(I) : \succ \text{ is a monomial order on } \mathbb{K}[x_1, \ldots, x_n]\}$$

is called the *collection of leading ideals* of I.

In [39], the collection of leading ideals is denoted by $\mathrm{Mon}^+(I)$, since the authors use $\mathrm{Mon}(I)$ for the more general set of leading ideals with respect to partial orders.

Theorem 9. For any ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$, $\mathrm{Mon}(I)$ is finite.

Proof. See for example [10], Chapter 8, Theorem 4.1. □

In $\mathrm{Mon}(I)$, two reduced Gröbner bases G_1 and G_2 are considered equal if they contain the same polynomials, even if the order of terms *within* the polynomials differs depending on the term order under which G_1 and G_2 are Gröbner bases. This motivates the notation of *marked Gröbner bases*, which do not only contain a set of polynomials, but an indicated leading term for each polynomial. Evidently, for G to be a marked Gröbner basis, there must exist a term order $\succ$ such that the marked leading terms are actually leading terms of their respective polynomials under $\succ$, and at the same time, G has to be a Gröbner basis under $\succ$.

Lemma 14. The set $\mathrm{Mar}(I)$ of marked reduced Gröbner bases of an ideal I is in one-to-one correspondence with $\mathrm{Mon}(I)$.

Proof. See for example [10], Chapter 8, Corollary 4.3. □

Now we are able prove that a universal Gröbner basis, as defined in Definition 20 exists for an arbitrary polynomial ideal.

Corollary 2. $|\mathcal{G}_{\mathrm{uni}}(I)| < \infty$ for every ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$.

Proof. By definition, $\mathcal{G}_{\mathrm{uni}}(I)$ is the union of finite sets. Theorem 9 and Lemma 14 assure that this union is finite, too, which proves the claim. □

Remember that every monomial order on $\mathbb{K}[x_1, \ldots, x_n]$ results from an $(n \times n)$-matrix of weight vectors. It is clear that the first row w_1 of such a matrix necessarily has non-negative entries, in order to satisfy the requirements for a term order. On the other hand, every non-negative vector w can be used as the first weight of a matrix order.
Let now $\mathcal{G}$ be a marked Gröbner basis for an ideal I. Then we can consider the cone $C_\mathcal{G}$ of all $w \in \mathbb{R}^n_+$ such that there is a matrix whose first row is w and which gives exactly the marked leading terms in $\mathcal{G}$. More formally, let $\mathcal{G} = \{g_1, \ldots, g_t\}$, and let $x^{\alpha_i} = \mathrm{LM}(g_i)\ \forall i$. Then

$$C_\mathcal{G} := \left\{w \in \mathbb{R}^n_+ : w \cdot \alpha_i \geq w \cdot \beta \ \forall\ \beta \in \mathrm{supp}(g_i) \quad \forall\ i\right\} \quad .$$

For two marked Gröbner bases of an ideal, the intersection of the cones can be non-empty, since the first row does not entirely define a term order. Moreover, the union of the cones over all elements of $\mathrm{Mar}(I)$ gives the complete non-negative orthant.

Definition 22. The collection

$$\{C_{\mathcal{G}} : \mathcal{G} \in \mathrm{Mar}(I)\}$$

is called the *Gröbner fan* of I.

The Gröbner fan enables the construction of the sets $\mathrm{Mon}(I)$ and $\mathrm{Mar}(I)$: Once we have the set of all cones, we can just take a term order for every cone, and compute the corresponding leading ideal and Gröbner basis.
Fortunately, the Gröbner fan of an ideal I can be computed in a straightforward manner, which is motivated by the property that the union of its cones is $\mathbb{R}^n_+$: Start with an empty set F of cones, and check whether their union is the entire orthant. If so, we are done. If not, choose a vector in the complement of this union, generate the corresponding cone (which is not always unique, since we are only given one weight vector) and add it to F. Now, repeat this procedure until every non-negative weight vector lies in at least one of the cones. The pseudocode for this finite algorithm is given as Algorithm 4.

Algorithm 4 Computing the Gröbner fan

Input: $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$
Output: $F = \{C_{\mathcal{G}} : \mathcal{G} \in \mathrm{Mar}(I)\}$

```
function GröbnerFan(I)
    F ← ∅
    while ⋃_{C∈F} C ≠ ℝ^n_+ do
        Choose w ∈ ℝ^n_+ \ (⋃_{C∈F} C)
        Choose ≻_M with first row w
        𝒢 ← 𝒢_{≻_M}(I)
        F ← F ∪ C_𝒢
    end while
    return F
end function
```

Once the Gröbner fan and the collection of marked Gröbner bases of an ideal are explicitly computed, the ideal can be seen as "decoded" with respect to Gröbner basis theory.

4. GRAPH COLORABILITY AS AN ALGEBRAIC PROBLEM

It is well-known that the colorability problem can be stated in terms of polynomial equations. The case of three colors was first given in [8], and [17] provides the following formulation for general integers k.

4.1 An Equivalent Algebraic Problem Formulation

Proposition 7. Let $G = (V, E)$ be a graph, and let $k \in \mathbb{N}$. G is k-colorable if and only if the polynomial system of equations in $\mathbb{C}[x_1, \ldots, x_n]$

$$x_v^k - 1 = 0 \ \forall\ v \in V \quad \text{and} \quad \sum_{i=0}^{k-1} x_u^{k-1-i} x_v^i = 0 \ \forall\ \{u, v\} \in E$$

has a solution. We will denote this set of polynomials by $\mathcal{F}_G$, and the ideal spanned by its elements by $\mathcal{I}_G$.

Proof.

$\Rightarrow$ Let $c : \{1, \ldots, n\} \to \{1, \ldots, k\}$ be a proper k-coloring. Set $x_i^* := \xi^{c(i)}\ \forall i$, where $\xi := e^{\frac{2\pi i}{k}}$ is the k-th root of unity. Then

- $v_i(x^*) = \left(\xi^{c(i)}\right)^k - 1 = \left(\xi^k\right)^{c(i)} - 1 = 1^k - 1 = 0$ and
- $e_{i,j}(x^*) = \frac{(x_i^*)^k - (x_j^*)^k}{x_i^* - x_j^*} = \frac{0}{x_i^* - x_j^*} = 0$

for all $i \in V$ and $\{i, j\} \in E$. Therefore, $x^* \in \mathcal{V}(\mathcal{I}_G) \neq \emptyset$.

$\Leftarrow$ Let $\mathcal{V}(\mathcal{I}_G)$ be non-empty, and $x^* \in \mathcal{V}(\mathcal{I}_G)$. The equalities $v_i(x^*) = (x_i^*)^k - 1 = 0$ imply that the components of x^* are k-th roots of unity, that is,

$$\forall i\ \exists\ c_i \in \{1, \ldots, k\} \text{ such that } x_i^* = \xi^{c_i} \quad .$$

Define $c : \{1, \ldots, n\} \to \{1, \ldots, k\}$ by $c(i) := c_i$. Then c is a coloring function for G, and

$$\begin{aligned} c_i = c_j \quad &\Rightarrow \quad x_i^* = \xi^{c_i} = \xi^{c_j} = x_j^* \\ &\Rightarrow \quad e_{i,j}(x^*) = \sum_{l=1}^{k} (x_i^*)^k = k \cdot x_i^* \neq 0 \\ &\Rightarrow \quad e_{i,j} \notin \mathcal{I}_G \quad \Rightarrow \quad \{i, j\} \notin E \quad , \end{aligned}$$

which means that c is a proper k-coloring of G.

□

Note that we translate a graph with n vertices and m edges into a set of $n+m$ polynomials over a polynomial ring with n variables. The degree of these polynomials is k for the first and $k-1$ for the second type of polynomials.

Notation. To simplify notation, we call

$$v_i := x_i^k - 1$$

the *vertex polynomial* for the vertex i and

$$e_{u,v} := \sum_{i=0}^{k-1} x_u^{k-1-i} x_v^i$$

the *edge polynomial* for the edge $\{u, v\}$.

Since computations over the field $\mathbb{C}$ are rather expensive, we use that fact that there are "nicer" fields which also possess the crucial property of having k distinct k-th roots of unity. This is, for example, satisfied by the algebraic closure of all finite fields $\mathbb{F}_p$, where p is a prime number which is also relatively prime to k.

Lemma 15. The equation $x^k - 1 = 0$ has k distinct roots over $\overline{\mathbb{F}}_p$, when $p \in \mathbb{P}$ is relatively prime to k.

Proof [37]. The discriminant of a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ is defined to be

$$\operatorname{disc}(f) = \frac{(-1)^{n(n-1)/2}}{a_n} \cdot \operatorname{Res}(f, f') \quad .$$

When the discriminant is non-zero, f does not have multiple roots. In our case, $f(x) = x^k - 1$, and $f'(x) = kx^{k-1}$. The resultant is the determinant of the Sylvester matrix, here $\operatorname{Res}(f, f') = k^k \not\equiv 0 \pmod{p}$, and therefore, the discriminant is non-zero, and all roots of the equation $x^k - 1 = 0$ are distinct. The number of those distinct roots is a consequence of the fundamental theorem of algebra, since $\overline{\mathbb{F}}_p$ is algebraically closed. □

We can now restate the algebraic formulation of graph colorability as follows:

Corollary 3. Let G be a graph, and let $k \in \mathbb{N}$. G is k-colorable if and only if the polynomial system of equations in $\mathbb{F}_p[x_1, \ldots, x_n]$

$$x_v^k - 1 = 0 \;\forall\; v \in V \quad \text{and} \quad \sum_{i=0}^{k-1} x_u^{k-1-i} x_v^i = 0 \;\forall\; \{u, v\} \in E$$

has a solution in $\overline{\mathbb{F}}_p^n$.

Remark 18. The proof of Proposition 7 actually reveals a stronger connection between solvability of $\mathcal{F}_G$ and k-colorings of G: For every coloring, we find exactly one corresponding point in $\mathcal{V}(\mathcal{I}_G)$, and every such point yields a specific proper coloring. In other words, elements of $\mathcal{V}(\mathcal{I}_G)$ and proper k-colorings of G are in bijection; in particular, they have equal cardinality.

Remark 19. Assigning the polynomial ideal $\mathcal{I}_G$ to a graph G gives meaning to the notations $\mathcal{V}_G$, $\mathcal{L}_G$ and $\mathcal{B}_G$, where we see the properties of a coloring ideal as properties of the graph itself. In all cases, it is clear from the context for which k we form the k-coloring ideal.

A useful fact about the numbers that we chose to represent the colors is the *summation formula of roots of unity.*

Lemma 16. Let ξ denote the first k-th root of unity for $k \geq 2$. Then $\{\xi, \xi^2, \ldots, \xi^k\}$ is the set of *all* k-th roots of unity, and their sum is

$$\sum_{i=1}^{k} \xi^i = 0 \quad .$$

Proof.

$$\sum_{i=1}^{k} \xi^i = \frac{1-\xi^k}{1-\xi} = \frac{1-1}{1-\xi} = 0 \quad .$$

□

4.2 Hilbert's Nullstellensatz

Theorem 10 (Weak Nullstellensatz)**.** Let $\mathbb{K}$ be an algebraically closed field and let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal satisfying $V(I) = \emptyset$. Then

$$I = \mathbb{K}[x_1, \ldots, x_n] \quad .$$

Proof. See for example [11], Chapter 4, §1, Theorem 1. □

Lemma 17. Let $P = \{p_1, \ldots, p_k\} \subset \mathbb{K}[x_1, \ldots, x_n]$ be a set of polynomials. Then all $p \in P$ have a common root if and only if the constant polynomial $1 \notin I := \langle p_1, \ldots, p_k \rangle$.

Proof. Assume that $1 \notin I$, and therefore $I \neq \mathbb{K}[x_1, \ldots, x_n]$. Then, by Theorem 10, $V(I) \neq \emptyset$, and every element of $V(I)$ is a common root of the p_i.
Let on the other hand $1 \in I$. Then $\forall\ i \in \{1, \ldots, k\}\ \exists\ c_i \in \mathbb{K}[x_1, \ldots, x_n]$ such that $\sum_{i=1}^{k} c_i p_i = 1$. Assuming that $x \in \mathbb{K}$ is a common root of the p_i leads to the contradiction

$$1 = 1(x) = \left(\sum_{i=1}^{k} c_i p_i \right)(x) = \sum_{i=1}^{k} c_i(x) p_i(x) = 0 \quad .$$

□

A consequence of this lemma is that, in order to test the polynomial system $\mathcal{F}_G$ for a common root, we can form the ideal of all the polynomials and see if 1 is contained in this ideal. And this is exactly the reason why we need to compute a Gröbner basis for $\mathcal{I}_G$ first: Only if we have a Gröbner basis as the set of divisors, we can use multivariate polynomial division to check if $1 \in \mathcal{I}_G$, which would not necessarily give the correct result for the generator set $\mathcal{F}_G$.

Remark 20. For the ideal membership problem, it suffices to compute an arbitrary Gröbner bases of the ideal, since uniqueness of the remainder holds in general. Therefore, it is not required to have a reduced basis for solving the algebraic version of graph coloring.
To answer the question if two given ideals I and J are equal, however, it is necessary to compute the reduced Gröbner bases and check if they contain the exact same elements, or to compute arbitrary bases and test if each element of I lies in J by polynomial division and vice versa.

An interesting property of the Lex order is the shape of the resulting Gröbner bases. As examined in detail in Chapter 3 (*Elimination Theory*) of [11], this monomial order leads to a triangular Gröbner basis form, in the sense that the last polynomial of the basis is univariate, the second last polynomial depends on two variables, and so on. This phenomenon is very useful, since it makes it easy to find an element of the variety by solving the last equation and successively re-substituting the solution into the next polynomial. The monomial order for which the triangular shape of Gröbner bases holds, are called *elimination orders*.

Fact 1. Let $\mathcal{G}$ be a Gröbner basis for an ideal I with respect to an elimination order. Then there is an efficient way to find some $x \in \mathcal{V}(I)$, using $\mathcal{G}$.

Remark 21. Hilbert's Nullstellensatz can also be used to solve combinatorial problems with a different approach: After constructing a set F of polynomials whose common roots encode the solutions of the problem, we can test if $1 \in \langle F \rangle$ by trying to find a polynomial combination of elements in F that add up to 1, as described in the proof of Lemma 17. If this is possible, then there is *no* solution to the combinatorial problem.
The NulLA algorithm [37] makes use of this approach by building a linear system of equations to determine the coefficient polynomials of the equation $\sum c_i p_p = 1$. To do so, a tentative maximum degree d of the coefficients has to be given, and the algorithm can only decide whether or not a *non-solvability certificate* of degree $\leq d$ exists. Hence, only the non-existence of a solution can be shown explicitly by proving a certificate, while solvability cannot be proven directly.
Experimental results show that in most cases, these Nullstellensatz certificates have low degree, which renders NulLA comparable with other algorithms for problems like graph colorability.

4.3 k-Colorings and Standard Monomials of $\mathcal{I}_G$

We would like to strengthen the link between k-colorings of a graph G and the set of standard monomials in the k-coloring ideal of G. It turns out that their cardinalities are equal, but the proof for this fact involves rather profound algebraic concepts. Therefore, we will give some of the steps without proof, while keeping the overall chain of thought complete.
First, we note that the fields we work with, i.e., $\mathbb{C}$ and the finite fields $\mathbb{F}_p$, have the property to be *perfect*, which we don't have to understand in detail (see [5], V, Proposition 5). Second, an ideal I is called *zero-dimensional*, written as $\dim(I) = 0$, if $|\mathcal{V}(I)| < \infty$. As pointed out in Remark 18, the coloring ideal of a graph is zero-dimensional, since the

number of colorings is bounded above by k^n. Third, the set $\mathcal{B}_G$ of standard monomials of the ideal $\mathcal{I}_G$ is a (finite) vector space basis of the quotient ring $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_G$ over $\mathbb{K}$, and therefore $|\mathcal{B}_G| = \dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_G)$ ([10], Theorem 4.3).

Lemma 18 (Seidenberg's Lemma)**.** Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be a zero-dimensional ideal. Suppose that, for every $i \in \{1, \ldots, n\}$, there exists a non-zero polynomial $g_i \in I \cap \mathbb{K}[x_i]$ such that $\gcd(g_i, g_i') = 1$. Then I is a radical ideal.

Proof. See [34], Proposition 3.7.15. □

Theorem 11. Let G be a graph. Then $\mathcal{I}_G$ is a radical ideal.

Proof. For every $i \in \{1, \ldots, n\}$,

$$v_i(x) = x_i^k - 1 \in \mathcal{I}_G \cap \mathbb{K}[x_i]$$

by definition. Since $\mathbb{K}$ is algebraically closed and therefore

$$v_i'(x) = k \cdot x_i^{k-1} \implies \gcd(v_i, v_i') = 1 \quad ,$$

we can apply Lemma 18, which gives the claim. □

Theorem 12. Assume that $\dim(I) = 0$. Then the number of zeros of I in $\mathbb{K}^n$ is less or equal to the vector space dimension $\dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I)$. If $\mathbb{K}$ is perfect and I is radical, then equality holds.

Proof. See [7], Theorem 8.32. □

Corollary 4. The number of proper k-colorings of a graph G equals the number of standard monomials $|\mathcal{B}_G|$.

Proof. As listed above, the prerequisites for Theorem 12, and in particular for the last part, are satisfied, such that $|\mathcal{V}(\mathcal{I}_G)| = |\mathcal{B}_G|$. Together with Remark 18, the claim

$$|\{c : V \to \{1, \ldots, k\} : c \text{ is a proper } k\text{-coloring of } G\}| = |\mathcal{B}_G|$$

follows. □

Remark 22. Note that Corollary 4 implies $k! \mid |\mathcal{B}_G|$, where $\mathcal{B}_G$ is taken with respect to the k-coloring ideal of G.

4.4 General Properties of Gröbner Bases for Coloring Ideals

Lemma 19. Let G be a graph with connected components $G_1, \ldots, G_c$, and fix a term order. If $\mathcal{G}_1, \ldots, \mathcal{G}_c$ are Gröbner bases for the components, then $\mathcal{G} := \bigcup_{i=1}^c \mathcal{G}_i$ is a Gröbner basis for G. If all $\mathcal{G}_i$ are reduced, then $\mathcal{G}$ is also reduced.

Proof. The first claim is shown by the equality

$$\mathcal{L}(\mathcal{I}_G) = \mathcal{L}\left(\sum_{i=1}^{c} \mathcal{I}_{G_i}\right) = \sum_{i=1}^{c} \mathcal{L}(\mathcal{I}_{G_i}) = \sum_{i=1}^{c} \mathcal{L}(\mathcal{G}_i) = \mathcal{L}\left(\sum_{i=1}^{c} \mathcal{G}_i\right) = \mathcal{L}(\mathcal{G}) \quad .$$

Assume now that all $\mathcal{G}_i$ are reduced. Each coloring ideal $\mathcal{I}_{G_i}$ only contains variables which correspond to vertices in G_i, and these are disjoint. Thus, for all $i \in \{1, \dots, c\}$, no term of an element of $\mathcal{G}_i$ is divided by a leading term of an element of $\mathcal{G}_j$, where $i \neq j$, and since $\mathcal{G}_i$ is reduced, the same holds for leading terms in $\mathcal{G}_i$. This suffices to show that $\mathcal{G}$ is reduced. □

Theorem 13. Let G be a k-colorable graph on n vertices. Then for any Gröbner basis $\mathcal{G}$ of $\mathcal{I}_G$,

$$\mathfrak{l}(\mathcal{G}) = |\mathcal{G}| \geq n \quad .$$

Proof. Since the number of solutions for the graph coloring problem is finite, we have

$$|\{\alpha \in \mathbb{N}^n : x^\alpha \notin \mathcal{L}(G)\}| < \infty \quad .$$

Therefore, $\forall i \in \{1, \dots, n\}$ $\exists k \in \mathbb{N}$ such that $x^{k \cdot e_i} \in \mathcal{L}(G)$ (otherwise $\{x^{\mathbb{N} \cdot e_i}\}$ would be an infinite family of monomials which are not in $\mathcal{L}(G)$, a contradiction).
Note that $\mathcal{L}(G)$ is a monomial ideal generated by $\mathrm{LM}(F)$, hence $\forall\, i \in \{1, \dots, n\} \exists f_i \in F$ with $x^{\beta_i} := \mathrm{LM}(f_i) \mid x^{k \cdot e_i}$. That means, $\beta_i \leq k \cdot e_i$. Moreover, $\beta_i \neq 0$ $\forall i$ because $\mathcal{V}(I)$ is non-empty. We see that the f_i are necessarily distinct, and their leading monomials have respective support $\{i\}$. Thus,

$$|\mathcal{G}| \geq |\{f_i : i \in \{1, \dots, n\}\}| = n \quad .$$

□

Example 6. Even in the case of coloring ideals, a reduced Gröbner basis can have worse complexity than a non-reduced basis for the same term order: Consider the graph G as shown in Figure 4.1, together with the standard Lex order. The complexity pattern of the reduced Gröbner basis $\mathcal{G}$ is $(10, 3, 8)$. While its length $\mathfrak{l}(\mathcal{G})$ and degree $\mathfrak{d}(\mathcal{G})$ are minimal, assured by Corollary 1 and Theorem 6, respectively, we find a non-reduced Gröbner basis $\mathcal{G}'$ with respect to the same order, whose complexity pattern is $(10, 3, 3)$. Such a basis is for example given by the vertex and edge polynomials

$$\mathcal{G}' = \{e_{1,3}, e_{2,3}, e_{3,4}, e_{4,5}, e_{5,6}, e_{6,7}, e_{7,10}, e_{8,10}, e_{9,10}, v_{10}\} \quad .$$

Inserting vertices in between the two forks lets the support of the reduced basis grow at the rate $\mathfrak{s}(\mathcal{G}) = n - 2$, whereas $\mathcal{G}'$ can be extended with unchanged support.

Theorem 14. Let G be a k-colorable graph on n vertices, and let $\mathcal{G}$ be a reduced Gröbner basis of $\mathcal{I}_G$. If $u \in \mathcal{G} \cap \mathbb{K}[x_j]$ is a univariate Gröbner Basis element for some j, then u is the vertex polynomial

$$u(x) = u(x_j) = x_j^k - 1 \quad .$$

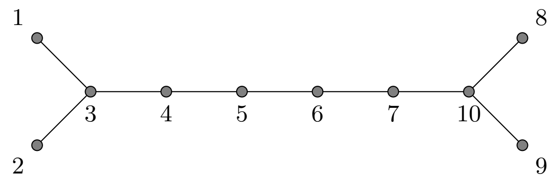


Fig. 4.1: The double fork graph on 10 vertices

Proof. Let u be such a polynomial. Let $c : \{1, \ldots, n\} \to \{1, \ldots, k\}$ be a proper k-coloring of G. Since for every $\sigma \in S_k$, $\sigma(c)$ is a proper k-coloring, we get that

$$\forall i \in \{1, \ldots, n\} \; \exists \text{ a proper } k\text{-coloring } c_i : c_i(j) = i \quad ,$$

in other words, vertex j takes every possible color in at least one proper k-coloring.
Every coloring c defines a point $p = (\xi^{\frac{2i\pi}{k} \cdot c(1)}, \ldots, \xi^{\frac{2i\pi}{k} \cdot c(n)}) \in \mathbb{C}^n$ in $\mathcal{V}_G = \mathcal{V}(\langle \mathcal{G} \rangle)$, that is, $u(p) = 0 \; \forall \; g \in \mathcal{G}$. In particular, $u(\xi^{\frac{2i\pi}{k} \cdot i}) = 0 \; \forall \; i \in \{1, \ldots, n\}$. This shows that $(x_j^k - 1) | u$.
On the other hand, assume that $\deg(u) > k$. Since $x_j^k \in \mathcal{L}(G)$, we have some element $v \in \mathcal{G} : \mathrm{LM}(v) | x_j^k | \mathrm{LM}(u)$, a contradiction to the fact that $\mathcal{G}$ is reduced.
We conclude that $u = x_j^k - 1$ because $\mathbb{K}[x_1, \ldots, x_n]$ is a factorial ring. □

Lemma 20. Let $p \in \mathbb{K}[x_1, \ldots, x_n]$ be a homogeneous polynomial, and let $\succ$ and $>$ be two term orders which induce the same variable order, which is without loss of generality $x_i \succ x_j \; \forall \; i < j$. Then the terms of p are ordered the same way by $\succ$ and $>$.

Proof. Let x^α and x^β be two monomials of p. If $\alpha_1 > \beta_1$, then we can easily see that $x^\alpha \succ x^\beta$: Both monomials can be obtained in the same number of steps by multiplying the initial monomial 1 with a variable. Moreover, in every step we can choose the variable for x^α with a smaller index (and hence higher priority in $\succ$ and $>$) than the one for x^β. By transitivity, $x^\alpha \succ x^\beta$ follows. Conversely, $\alpha_1 < \beta_1$ implies $x^\beta \succ x^\alpha$, and if both first exponents are equal, we continue with the second variable. Therefore, $\succ$ induces the same order on the terms of p as the Lex order, and the same holds for $>$. This finishes the proof. □

Definition 23. Let $p = \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha x^\alpha \in \mathbb{K}[x_1, \ldots, x_n]$. If there exist some $k \in \mathbb{N}$ and $0 \leq i < k$ such that $\deg(x^\alpha) \equiv i \mod k \; \forall \; \alpha : c_\alpha \neq 0$, then we call p *homogeneous (of degree i) modulo k*, denoted by $p \overset{h}{\equiv} i \mod k$.
A set F of polynomials is called homogeneous modulo k if every $f \in F$ is homogeneous of degree i modulo k for some (not necessarily equal) i.

Remark 23. Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$. If both f and g are homogeneous of degree i modulo k and $f + g \neq 0$, then $f + g \overset{h}{\equiv} i \mod k$. Also, if $f \overset{h}{\equiv} i \mod k$ and $g \overset{h}{\equiv} j \mod k$, then $f \cdot g \overset{h}{\equiv} (i + j \mod k) \mod k$. This can be verified by direct calculation.

Proposition 8. Let $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ be homogeneous modulo k, and let $F \subset \mathbb{K}[x_1, \ldots, x_n]$ be a set of polynomials which are homogeneous modulo k. Then

$$S(f, g) \quad \text{and} \quad \overline{S(f, g)}^F$$

are homogeneous modulo k.

Proof. Informally, both the S-pair and the multivariate polynomial division "lift" the involved polynomials to the same degree before performing any other operation. This preserves the homogeneous degree for both addition and multiplication.
More precisely: Let i and j be the degrees of homogeneity modulo k of f and g, respectively. If we set $l := \operatorname{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$ and $d := \deg(l) \mod k$, then $\frac{l}{\mathrm{LM}(f)} \overset{h}{\equiv} (d-i) \mod k$ and $\frac{l}{\mathrm{LM}(g)} \overset{h}{\equiv} (d-j) \mod k$, and therefore

$$S(f,g) = \frac{l}{\mathrm{LM}(f)} \cdot f - \frac{l}{\mathrm{LM}(g)} \cdot g \overset{h}{\equiv} d \mod k \quad ,$$

which is the first claim.
Looking at Algorithm 1, we note that the only operation that could destroy homogeneity modulo k is the assignment $p \leftarrow p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i$. But here the same argument holds: If $p \overset{h}{\equiv} i \mod k$, then $\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \cdot f_i \overset{h}{\equiv} i \mod k$, and thus the homogeneity of p is maintained during this assignment. Since r receives only terms from p, which always have the same degree modulo k, the proof is complete. □

Corollary 5. Gröbner bases of k-coloring ideals are homogeneous modulo k.

Proof. According to Proposition 8, Buchberger's Algorithm (Algorithm 3) and the Gröbner basis reduction algorithm (Algorithm 2) preserve homogeneity modulo k. Thus, it suffices to show that the input polynomials are homogeneous modulo k. But this is trivial, since the degrees of monomials in the vertex polynomials are 0 and k, and the edge polynomials are homogeneous of degree $k-1$. □

Theorem 15. Let G be a k-colorable graph on n vertices, and let $\mathcal{G}$ be a Gröbner basis of $\mathcal{I}_G$. Then $\mathcal{G}$ contains the vertex polynomial $v_i = x_i^k - 1$ for some $i \in \{1, \ldots, n\}$.

Proof. As shown above, $\forall\ i \in \{1, \ldots, n\}\ \exists\ g_i \in \mathcal{G}$ with $\mathrm{LM}(g_i) \mid x_i^k$. Let now $\succ$ be a term order under which $\mathcal{G}$ is a Gröbner basis, and choose i such that $x_j \succ x_i\ \forall\ j \neq i$. We claim that $g_i = x_i^k - 1$. First note that if $\mathrm{LM}(g_i) = x_i^k$, then the claim holds, since g_i cannot contain any other term of degree $\geq k$, because this term would certainly replace x_i^k as the leading term. Moreover, g_i is homogeneous of degree 0 modulo k by Corollary 5, and has therefore the form $g_i = x_i^k + c$ with $c \in \mathbb{K}$. Assuming that $c \neq -1$ and using the fact the $v_i \in \mathcal{I}_G$, we immediately see that $0 \neq c + 1 \in \mathcal{I}_G \Rightarrow \mathcal{I}_G = \mathbb{K}[x_1, \ldots, x_n]$, which contradicts k-colorability of G.
Assume now that $\mathrm{LM}(g_i) = x_i^l$, where $l < k$. Then, again by Corollary 5, every monomial in g_i has degree l, but if there was another monomial of this degree, x_i^l would not be the leading monomial. Therefore, $g_i = x_i^l \Rightarrow 1 = x_i^{k-l} \cdot g_i - v_i \in \mathcal{I}_G$, the same contradiction as above.
We conclude that indeed $\mathrm{LM}(g_i) = x_i^k$, and $g_i = x_i^k - 1$. □

Corollary 6. Let G be a k-colorable graph. Then for any Gröbner basis $\mathcal{G}$ of $\mathcal{I}_G$,

$$\mathfrak{d}(\mathcal{G}) \geq k \quad .$$

Proof. By Theorem 15, $\mathcal{G}$ contains a vertex polynomial, which has degree k. □

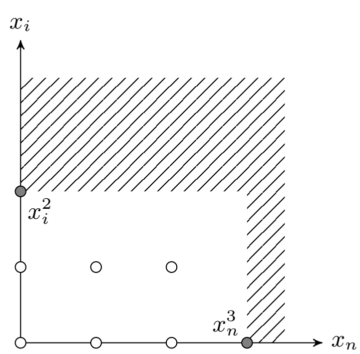
Theorem 16. Every reduced Gröbner basis of a uniquely 3-colorable graph G has $\leq n+6$ elements.

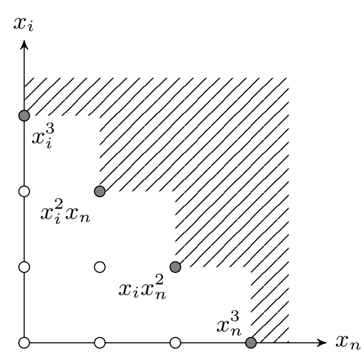
Proof. Lemma 4 assures that $|\{\alpha \in \mathbb{N}^n : x^\alpha \notin \mathcal{L}(G)\}| = 3! = 6$, and the monomials $1, x_n$ and x_n^2 are standard monomials by Theorem 15. Assume that $x_i \in \mathcal{L}(G)\ \forall\ i \in \{1,\ldots,n-1\}$. Then these three monomials would be the only standard monomials, which is not possible. On the other hand, for every i such that $x_i \notin \mathcal{L}(G)$, x_i is a standard monomial. Therefore, we know that

$$2 \leq |\{i \in \{1,\ldots,n\} : x_i \notin \mathcal{L}(G)\}| \leq 4 \quad .$$

Let $\mathcal{G}$ denote an arbitrary reduced Gröbner basis of G for an arbitrary term order. The three cases which we have to consider are:

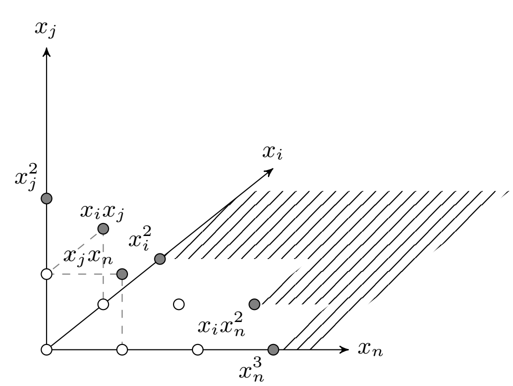
- $\{i \in \{1,\ldots,n\} : x_i \notin \mathcal{L}(G)\} = \{i,n\}$. The geometry of $\mathcal{L}(G)$ has one of the following two forms:



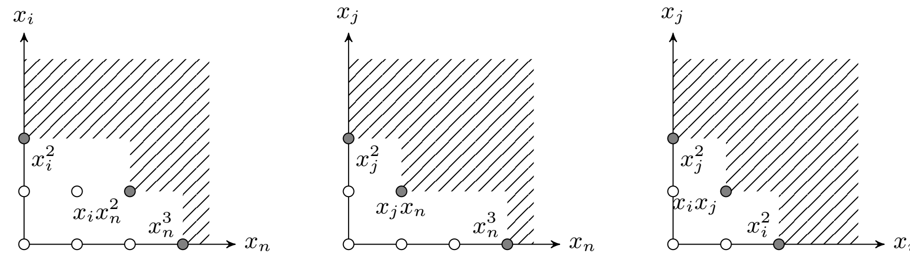


  This two-dimensional projection is the only interesting one, since all monomials which do not lie in the x_i-x_n-plane, are multiples of at least one other variable and therefore in $\mathcal{L}(G)$.
  In the first case, $\mathfrak{l}(\mathcal{G}) = n$, in the second case $\mathfrak{l}(\mathcal{G}) = n+2$.

- $\{i \in \{1,\ldots,n\} : x_i \notin \mathcal{L}(G)\} = \{i,j,n\}$. Now we have to consider a 3-dimensional projection of $\mathbb{Z}^n_{\geq 0}$, which is non-trivial with respect to standard monomials. Up to permutation of x_i and x_j, the position of the 6 standard monomials in this space is unique and looks like this:



with the two-dimensional projections

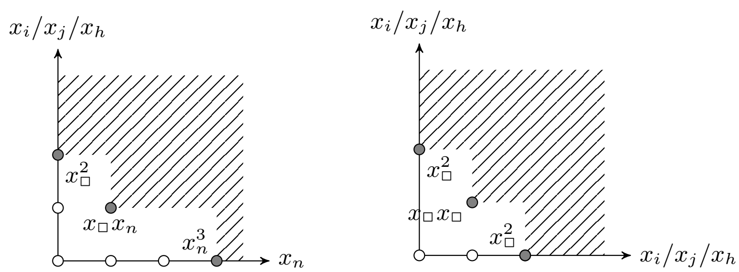


Counting divisibility-minimal elements, we see that $\mathfrak{l}(\mathcal{G}) = n + 3$.

- $\{i \in \{1, \dots, n\} : x_i \notin \mathcal{L}(G)\} = \{i, j, h, n\}$. Although a picture of the (4-dimensional) crucial projection would not reveal the geometry of this monomial ideal, it is fairly easy to imagine: The standard monomials are

$$\mathcal{B}(G) = \{1, x_i, x_j, x_h, x_n, x_n^2\} \quad ,$$

such that all minimal elements of $\mathcal{L}(G)$ are contained in a 2-dimensional coordinate plane and thus have support ≤ 2. There are two types of coordinate planes in this setting, the ones that involve x_n (left figure) and the ones that do not (right figure).



The minimal elements are

$$x_i^2, x_j^2, x_h^2, x_n^3, x_i x_j, x_i x_h, x_i x_n, x_j x_h, x_j x_n, x_h x_n \quad ,$$

and therefore $\mathfrak{l}(\mathcal{G}) = n + 6$.

$\square$

Remark 24. In [32], the authors give a complete description of Gröbner bases for the k-coloring ideals of uniquely k-colorable graphs, using a different approach. They show that, in fact, every reduced Gröbner basis of such a graph has length n. Our reasoning here is independent of this result, and it raises the natural question why only the first configuration in the proof of Theorem 16 can occur.

Theorem 17. Let G be a graph on n vertices, and let $\mathcal{G}$ be an arbitrary Gröbner basis of the 3-coloring ideal $\mathcal{I}_G$. If $\mathcal{G}$ contains a polynomial of degree 1, then G contains a cycle.

Proof. Assume that G is cycle-free. We only need to consider the case that G is a tree: If G is a forest with more than one component, then $\mathcal{G}$ can be partitioned into Gröbner bases of the components (Lemma 19), and at least one of these smaller Gröbner bases contains a polynomial of degree 1.

Using the fact that all trees on n vertices are chromatically equivalent, and their chromatic polynomial is $k(k-1)^{n-1}$, we see that G has exactly $c := 3 \cdot 2^{n-1}$ proper 3-colorings, which is also the number of standard monomials $|\mathcal{B}(G)|$ by Theorem 4. Remember that $x_i^3 \in \mathcal{L}_G$ for all i. Now

$$3 \cdot 2^{n-1} = c = |\mathcal{B}_G| \leq \prod_{i=1}^{n} \min\{p \in \mathbb{N} : x_i^p \in \mathcal{L}_G\} \quad .$$

If $\exists i: \ x_i \in \mathcal{L}_G$, then there has to be some j such that $x_j^3 \notin \mathcal{L}_G$, because the n factors of c have to be distributed among the $n-1$ remaining variables. This contradiction shows the claim. $\square$

5. EXPECTED HARDNESS RESULTS FOR GENERAL GRAPHS

The method examined in this thesis is a radically different approach to a graph theoretic problem from the "conventional" techniques shown in Section 2.2.3. Since we do not perform any operations directly on the input graph, for example enumerating all possible colorings, backtracking or decomposing the graph (techniques which are known to result in exponential-time algorithms), it is not a priori clear what the asymptotic running time of the Gröbner basis approach will be. However, Gröbner basis computations have shown to be very costly in general and for various restrictions on the input, for example zero-dimensional, homogeneous or toric ideals.
We will show that also coloring ideals are hard with respect to their Gröbner bases. But this does not only hold for the Gröbner bases of an exact coloring ideal: Starting at well-known hardness theorems for approximating the 3-coloring problem or finding partial solutions, we will translate the statements into similar approximation results for the computation of Gröbner bases, therefore showing some kind of "robust hardness".

5.1 Buchberger's Algorithm Captures the Hardness of $\mathcal{NP}$

First, we note that the treatment of graph coloring as an algebraic problem, as shown in Section 4.1, carries all the hardness of the problem (see Theorem 2) over to Buchberger's algorithm. In other words, the conversion of a graph G into the polynomial system $\mathcal{F}_G$ and the evaluation of the resulting Gröbner basis $\mathcal{G}$ can be done fast, such that an efficient execution of Buchberger's algorithm would imply that *any* problem in $\mathcal{NP}$ can also be solved efficiently.

Theorem 18. If Buchberger's algorithm runs in polynomial time (in the input size) for 3-coloring ideals, then $\mathcal{P} = \mathcal{NP}$.

Proof. Let $p \in \mathbb{N}$, such that for all graphs $G = (V, E)$ with $|V| = n$, the running time of Algorithm 3 is bounded by $\mathcal{O}(n^p)$. Note that the input size can be as large as $\mathcal{O}(n^2)$ for dense graphs, but this factor can be compensated by choosing $2p$ instead of p.
Then we can easily design a polynomial-time procedure, shown in Algorithm 5, to solve 3Col: Building $\mathcal{I}_G$ from G takes $\mathcal{O}(n^2)$ time, and testing the membership of 1 in $\mathcal{G}$ is polynomial in the storage size of $\mathcal{G}$. Note that, as pointed out in Remark 20, we do not need to compute a reduced Gröbner basis for the membership test. □

In fact, the choice of Buchberger's algorithm in the above proof is arbitrary: Any other algorithm that computes a Gröbner basis $\mathcal{G}(I)$ for a given coloring ideal I has to satisfy the same lower complexity bounds. In particular, any Gröbner basis algorithm that handles general ideals, is necessarily bounded below by a super-polynomial function.

Algorithm 5 An algorithm that solves 3Col using Gröbner bases

Input: $G = (V, E)$

Output: $\begin{cases} \textbf{true} & \text{if } G \text{ is 3-colorable} \\ \textbf{false} & \text{otherwise} \end{cases}$

function 3Col(G)
  $k \leftarrow 3$
  $\succ \leftarrow$ arbitrary term order on $\mathbb{K}[x_1, \ldots, x_n]$
  $I \leftarrow \mathcal{I}_G$
  $\mathcal{G} \leftarrow$ Buchberger(I)
  return $\begin{cases} \textbf{true} & \text{if } \overline{1}^{\mathcal{G}} \neq 0 \\ \textbf{false} & \text{otherwise} \end{cases}$
end function

Corollary 7. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. Unless $\mathcal{P} = \mathcal{NP}$, no Gröbner basis of I can be computed in time bounded by a polynomial in n and the maximal degree of the generating polynomials of I.

Proof. Assume the opposite, and let Gröbner(I) be a polynomially-bounded function that computes a Gröbner basis of a given ideal I. Recall that 3-coloring ideals have polynomial size in n and constant degree 3. Calling Gröbner(I) instead of Buchberger(I) in Algorithm 5 immediately gives a polynomial-time (in the input size) algorithm for 3Col and therefore implies $\mathcal{P} = \mathcal{NP}$ by Theorem 2. □

5.2 Hardness of Suboptimal Solutions

There is a number of hardness results for graph 3-coloring which extend Theorem 2. We will take two of these statements and show how they can be interpreted in the context of Gröbner bases for polynomial ideals.

Theorem 19. It is $\mathcal{NP}$-hard to color a 3-colorable graph with 4 colors. More generally, for every $k \geq 3$ it is $\mathcal{NP}$-hard to color a k-chromatic graph with at most $k + 2\lfloor \frac{k}{3} \rfloor - 1$ colors.

Proof. See [33], Theorem 1 and Corollary 1. Alternatively, a proof of the first statement which does not rely on the PCP theorem can be found in [24], Theorem 1. □

We now translate this approximative result into an analog statement about Gröbner bases. What is the meaning of using additional colors? We can use them to color vertices after the main procedure, such that we only need to find a partial coloring at first. The theorem then states that computation will still be $\mathcal{NP}$-hard. In an algebraic context, that means that we ignore some variables, and only find a Gröbner basis for the rest of the variables. Such a scenario can be modeled by *elimination ideals*:

Definition 24. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. For a set $S \subseteq \{1, \ldots, n\}$, the ideal

$$I_{-S} := \langle I \cap \mathbb{K}[x_i : i \notin S] \rangle$$

is called the *elimination ideal* of I with respect to S.
If S consists of a single element, we also write I_{-i} for $I_{-\{i\}}$.

Each additional color can be assigned to one vertex, or even to an arbitrary stable set of a graph G. A stable set in G translates to a set of variables, none of which appear pairwise in any element of $\mathcal{F}_G$.
Considering the 3-coloring as well as the k-coloring case, and also a single ignored vertex as well as an ignored stable set, we obtain four theorems that deal with Gröbner bases for special subsets of polynomial ideals. In all versions, we assume the term order on $\mathbb{K}[x_1, \ldots, x_n]$ to be an arbitrary, but fixed elimination order. Moreover, we assume that $\mathcal{P} \neq \mathcal{NP}$ (see Remark 2).

Remark 25. Note that, for a set of polynomials $F \subseteq \mathbb{K}[x_1, \ldots, x_n]$,

$$\langle f \in F : f \cap \mathbb{K}[x_i : i \in S] = \emptyset \rangle = \langle F \rangle_{-S} \quad .$$

Thus, it does not matter whether the elimination of S is done before or after forming the ideal.

Theorem 20 (Ideals of maximum degree 3 with one ignored variable)**.**
Let $F \subseteq \mathbb{K}[x_1, \ldots, x_n]$, and fix an elimination order. There is no polynomial-time algorithm that chooses some $i \in \{1, \ldots, n\}$ and computes a Gröbner basis for $\langle F \rangle_{-i}$. This statement holds even if $\deg(F) \leq 3$.

Theorem 21 (Ideals of maximum degree 3 with a set of ignored variables)**.**
Let $F \subseteq \mathbb{K}[x_1, \ldots, x_n]$, and fix an elimination order. There is no polynomial-time algorithm that chooses $S \subseteq \{1, \ldots, n\}$ with

$$(F_{-i})^C \cap (F_{-j})^C = \emptyset \; \forall \; i \neq j \in S \quad ,$$

and computes a Gröbner basis for F_{-S}. This statement holds even if $\deg(F) \leq 3$.

Theorem 22 (Ideals of maximum degree k with $2\lfloor \frac{k}{3} \rfloor - 1$ ignored variables)**.**
Let $F \subseteq \mathbb{K}[x_1, \ldots, x_n]$, and fix an elimination order. There is no polynomial-time algorithm that chooses a set $S \subseteq \{1, \ldots, n\}$ such that $|S| \leq 2\lfloor \frac{k}{3} \rfloor - 1$, and computes a Gröbner basis for F_{-S}. This statement holds even if $\deg(F) \leq k$.

Theorem 23 (Ideals of maximum degree k with $2\lfloor \frac{k}{3} \rfloor - 1$ sets of ignored variables)**.**
Let $F \subseteq \mathbb{K}[x_1, \ldots, x_n]$, and fix an elimination order. There is no polynomial-time algorithm that chooses $S = \bigcup_{q=1}^{s} S_q \subseteq \{1, \ldots, n\}$ with $s \leq 2\lfloor \frac{k}{3} \rfloor - 1$ and

$$(F_{-i})^C \cap (F_{-j})^C = \emptyset \; \forall \; i \neq j \in S_q \; \forall \; q \quad ,$$

and computes a Gröbner basis for F_{-S}. This statement holds even if $\deg(F) \leq k$.

Remark 26. In Theorems 21 and 23, we have to make sure that the choice of S can be done in polynomial time. However, the condition $(F_{-i})^C \cap (F_{-j})^C = \emptyset$ can be verified efficiently, and only $\mathcal{O}(n^2)$ such tests are necessary. Therefore, this is not a problem.

Since the proofs of all four theorems are almost identical, we will only present one of them.

Proof of Theorem 20. Let $G = (V, E)$ be a 3-colorable graph, and assume that a polynomial-time algorithm $\mathcal{A}$ exists which computes a Gröbner bases of $\langle F \rangle_{-i}$. We will give a method to produce a proper 4-coloring of G, contradicting the first statement of Theorem 19 under the assumption that $\mathcal{P} \neq \mathcal{NP}$.
Call $\mathcal{A}(\mathcal{F}_G)$, and note that the input consists of $|V| + |E|$ polynomials with degree ≤ 3 and support ≤ 3. Thus, $\mathcal{F}_G$ has polynomial size in the input size of G, and $\mathcal{A}$ terminates in time which is polynomial in both of these quantities. Assume that the variable which was ignored by $\mathcal{A}$ is i. Since $\langle F \rangle_{-i} = \mathcal{I}_{G|_{V\setminus\{i\}}}$, the Gröbner basis found by $\mathcal{A}$ corresponds to all proper colorings of $G|_{V\setminus\{i\}}$, and according to Lemma 1, one such coloring can be found efficiently. Use the colors $\{1, 2, 3\}$ to color this subgraph, and assign color 4 to the vertex i.
This gives, by construction, a proper 4-coloring of G in polynomial time, which finishes the proof. □

5.3 Obtaining Similar Results from Different Combinatorial Problems

Remember the 3Sat problem from Chapter 2.2.2 and assume that a satisfiable instance is given. Since 3Sat is $\mathcal{NP}$-hard, we cannot expect to obtain a satisfying assignment in polynomial time. Therefore, we explore also suboptimal solutions:

Definition 25. The Max-3Sat problem is the problem of finding the largest number of clauses in a 3Sat instance which are satisfied by a boolean assignment. Formally,

$$\textsc{Max-3Sat}(S) := \max_{x \in \{\mathbf{true}\,,\mathbf{false}\,\}^n} |\{C \in S : C(x) = \mathbf{true}\,\}| \quad .$$

Clearly, we have the equivalence

$$\textsc{Max-3Sat}(S) = k \iff \textsc{3Sat}(S) = \mathbf{true} \quad .$$

The hardness of approximating the optimal solution of Max-3Sat was proven by Håstad and is stated as follows:

Theorem 24. For general 3Sat instances S, it is $\mathcal{NP}$-hard to approximate Max-3Sat(S) within a factor of $\frac{7}{8} + \delta$, where $\delta > 0$.

Proof. See [27], Theorem 6.5. □

We proceed analogously to Section 7: Let $S = \bigwedge_{i=1}^{k} C_i$ be a 3Sat instance over n variables. A system of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ that encodes the solutions of 3Sat(S), is given by

$$\mathcal{F}_S := \{(x_i - 1)(x_i + 1) : 1 \leq i \leq n\} \cup \{l_{v_i^{(1)}} \cdot l_{v_i^{(2)}} \cdot l_{v_i^{(3)}} : 1 \leq i \leq k\} \quad ,$$

where $l_v := \begin{cases} (x_i - 1) & \text{if } v = x_i \\ (x_i + 1) & \text{if } v = \overline{x_i} \end{cases}$ is the *literal polynomial* of a literal v.
Note that $\mathcal{F}_S$ consists of $n+k$ polynomials of maximum degree 3 and maximum support 8, and its encoding is therefore polynomial in the input size of S.

Example 7. Let $n = 3$, $k = 2$ and $S = (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_3)$. Then

$$\begin{aligned}
\mathcal{F}_S &= \{(x_1-1)(x_1+1), (x_2-1)(x_2+1), (x_3-1)(x_3+1), \\
&\quad (x_1-1)(x_2+1)(x_3+1), (x_1-1)(x_2+1)(x_3-1)\} \\
&= \{x_1^2-1, x_2^2-1, x_3^2-1, x_1x_2x_3 + x_1x_2 + x_1x_3 - x_2x_3 + x_1 - x_2 - x_3 - 1, \\
&\quad x_1x_2x_3 - x_1x_2 + x_1x_3 - x_2x_3 - x_1 + x_2 - x_3 + 1\} \quad .
\end{aligned}$$

Proposition 9. The satisfying assignments for S are in bijection with the common roots of $\mathcal{F}_S$.

Proof. Let $x \in \{\textbf{true}, \textbf{false}\}^n$ be an assignment such that $S(x) = \textbf{true}$. Identifying $1 = \textbf{true}$ and $-1 = \textbf{false}$, we see that each variable polynomial is 0. Moreover, since every clause is satisfied by x, the corresponding clause polynomial gives 0 as well.
Let on the other hand $x \in \mathcal{V}(\mathcal{F}_S) \subseteq \mathbb{K}^n$. x satisfies all variable polynomials, hence $x \in \{-1, 1\}^n$. Since $\mathbb{K}$ is an integral domain, at least one of the factors of every clause polynomials is zero, and therefore, the above identification gives that the clause is satisfied by x. $\square$

Thus, Theorem 24 translates into another result about Gröbner bases for a subset of polynomials in $\mathcal{F}_S$.

Theorem 25. Let $F \subseteq \mathbb{K}[x_1, \ldots, x_n]$. For $\delta > 0$, there is no polynomial-time algorithm that chooses $S \subseteq \{1, \ldots, n\}$ with

$$\left| \bigcup_{i \in S} F_{-i}^C \right| \leq \left(\frac{1}{8} - \delta \right) |F| \quad ,$$

and computes a Gröbner basis for F_{-S}. This statement holds even if $\deg(F) \leq 3$.

Proof. Let $\delta > 0$ be fixed, and assume that such a polynomial-time algorithm $\mathcal{A}$ exists. For an arbitrary satisfiable 3Sat instance M with k clauses over n variables, we will produce a truth assignment that satisfies at least $\left(\frac{7}{8} + \delta\right) k$ clauses, which contradicts Theorem 24, if $\mathcal{P} \neq \mathcal{NP}$.
After deleting all variables from the system that do not appear in any clause, apply $\mathcal{A}$ to $\mathcal{F}_M$. The algorithm terminates in time which is polynomial in the input size of M, and the output is a Gröbner basis for F_{-S}, where S is a subset of the variables as defined above. An element in $\mathcal{V}(F_{-S})$ (which can be efficiently found by Lemma 1) translates into a truth assignment, satisfying all clauses that do not contain any variable in S. By construction of $\mathcal{F}_M$, each variable is contained in exactly one variable polynomial and at least one clause polynomial. Therefore, the variables in S appear in $\leq \left(\frac{1}{8} - \delta\right) k$ clause polynomials, and we obtain a $\left(\frac{7}{8} + \delta\right)$-approximation for 3Sat, no matter which values we assign to the variables in S. The procedure is a polynomial-time algorithm, which finishes the proof. $\square$

This approach suggests two new directions in order to strengthen the theorems: First, find an $\mathcal{NP}$-hard problem whose algebraic description is as simple as possible. In this context, simple means that the polynomials are few in the input size and have a simple structure, small degree and small support. Then the conclusion is that even Gröbner bases of these simple polynomial systems are hard to find.
Alternatively, find a problem, for which hardness results of approximations exist. This translates into hardness of finding suboptimal Gröbner bases, for example for a partial system of polynomials, or for polynomials which are similar to the original system.

Remark 27. All our considerations here lead to the conjecture that Gröbner bases cannot be computed efficiently, even if we restrict ourselves to a very limited set of polynomial ideals. However, it is crucial to note that this does *not* preclude a polynomial-sized upper bound for the complexity of a minimum-sized such Gröbner basis. We merely say that there is probably no efficient way to find such a basis for the coloring ideals of general graphs.
To illustrate the difference between these two statements, consider the graph family given in example 8. Its respective Gröbner bases with respect to the Lex order have linear complexity bounds, but this small size is only obtained through the reduction algorithm *after* the termination of Buchberger's algorithm. Accordingly, the computation time rises superlinearly with increasing vertex number n.

Example 8. Consider the polynomial system

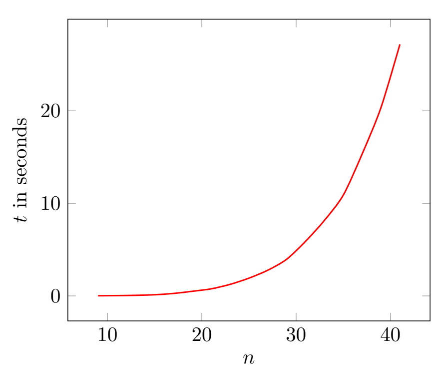
$$\mathcal{F} = \{v_1, \dots, v_n, e_{1,2}, e_{1,3}, \dots, e_{1,n}, e_{2,3}, e_{3,4}, \dots, e_{n-1,n}, e_{2,n}\}$$

for odd $n \geq 3$. We will see in Chapter 6 that this system encodes the wheel graph W_n. Applying Buchberger's algorithm to $\mathcal{F}$ under the Lex order, we get Gröbner bases whose complexity pattern is shown in the first row of Table 5.1. However, running the reduction algorithm on these bases reduces their complexity to the patterns in the second row of the table. Keeping this in mind, it becomes clear why the reduced Gröbner bases only grow linearly, but the computation time seems to rise exponentially with the size of the graph, shown in Figure 5.1.

Tab. 5.1: Complexity of unreduced and reduced Lex bases for $\mathcal{F}$

n	Unreduced complexity	Reduced complexity
3	(10, 3, 3)	(3, 3, 3)
5	(27, 3, 7)	(5, 3, 3)
7	(42, 5, 11)	(7, 3, 3)
9	(57, 5, 28)	(9, 3, 3)
11	(71, 5, 58)	(11, 3, 3)
13	(85, 5, 91)	(13, 3, 3)
15	(99, 5, 132)	(15, 3, 3)

Fig. 5.1: Computation time for Lex bases of W_n



6. EXPLICIT 3-COLORING GRÖBNER BASES FOR SIMPLE GRAPH FAMILIES

The preceding chapter shows that an efficient algorithm to find Gröbner bases for the 3-coloring ideals of general graphs is very unlikely to exist, as well as a closed form that can be efficiently recovered from the graph structure. Therefore, it makes sense to explore special cases, such as simply structured families of graphs, and find patterns which link properties of the graphs and properties of their Gröbner bases. The graphs considered in this chapter are highly structured, and their Gröbner bases mostly contain polynomials which we can relate to substructures in the graphs (see Section 6.1), which allows for extrapolation of algorithmic results for small examples to infinite graph families.

We compute reduced Gröbner bases for the 3-coloring ideal of various families of graphs with a simple structure. Those examples illustrate a variety of interesting properties of Gröbner basis computations for coloring ideals: For instance, the chosen term order can have a huge impact on both computational effort and complexity of the result. However, there are graphs for which all term orders yield the a Gröbner basis of equal complexity. Also, in most cases it is not necessary to choose arbitrary monomial orders to achieve particularly good or bad Gröbner bases, but it suffices to consider the standard orders from Section 3.2.1 and permute the vertices of the graph.

Interesting examples for the connection between the structure of a graph and the corresponding Gröbner bases are the appearance of triangles in general graphs and the concept of dominant paths in tree graphs. We will explain these and other findings by means of the Gröbner bases that we computed for the different graph families. However, as some properties are interesting for all these families, we introduce the concepts at their first appearance and reuse them later without explanation.

6.1 Elementary Subgraph Polynomials

The empirical study of Gröbner bases for 3-coloring ideals reveals that there is a number of polynomials that crop up quite often as Gröbner basis elements, and that can be related to certain substructures of the underlying graph. It is very useful to classify these polynomials, since there are many cases in which the entire Gröbner basis sequence for a family of graphs can be built from polynomials that we can explicitly describe and understand.

For completeness, we will once again include the defining polynomials of the coloring ideal, that is, vertex polynomials and edge polynomials, in this list:

The *vertex polynomial* $v_i := x_i^3 + 1$ ensures the variables to assume values which are third roots of unity.

The *edge polynomial* $e_{i,j} := x_i^2 + x_i x_j + x_j^2$ enforces different colors on connected vertices.

The *path polynomial* $p_{v_1,\ldots,v_s} := x_{v_1}^2 + x_{v_1}x_{v_2} + x_{v_2}x_{v_3} + \ldots + x_{v_{s-1}}x_{v_s} + x_{v_s}^2$ generalizes the edge polynomial by taking the sum $p_{v_1,\ldots,v_s} = \sum_{i=1}^{s-1} e_{v_i,v_{i+1}}$.

The *cycle polynomial* $c_{v_1,\ldots,v_s} := x_{v_1}x_{v_2} + x_{v_2}x_{v_3} + \ldots + x_{v_{s-1}}x_{v_s} + x_{v_s}x_{v_1}$ is the special case of a closed path.

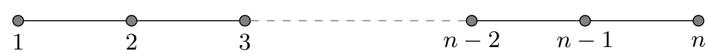
The *triangle polynomial* $t_{i,j,k} := x_i + x_j + x_k$ is a consequence from the summation formula for primitive roots of unity (Lemma 16).

The *diamond polynomial* $d_{i,j} := x_i + x_j$ is the sum of two triangles that share an edge, which forces the two non-shared vertices to take the same color.

Remark 28. Note that all polynomials are specific for 3-coloring ideals, which is particularly why they do not contain any coefficients, and their degree is less or equal to 3.

6.2 Path Graphs

The *path graph* P_n is defined by $V = \{1, \ldots, n\}$ and $E = \{\{i, i+1\} : 1 \leq i < n\}$.



6.2.1 Standard Bases

Showing lower bounds for the Gröbner basis complexity of a given graph is a hard task, since one has to consider all possible term orders, or equivalently, the Gröbner fan (see Section 4) of the graph. The other direction, finding upper bounds, is considerably easier, since it suffices to give an example of a small Gröbner basis. Many graphs (and graph families) have Gröbner bases whose complexity coincides with the general lower bounds derived in Theorems 13 and 15, and Conjecture 2, such that giving an optimal basis basically is a complete solution for the "Gröbner basis problem" of the graph under consideration. Moreover, it is often suitable to use one of the standard term orders, so that we do not have to construct complicated matrix orders to prove the existence of small Gröbner bases.
The standard procedure for this approach is to find Gröbner bases with respect to a certain term order for a sequence of graphs $G_1, G_2, \ldots$ up to a suitable size experimentally, guess the general structure of the (assumed) Gröbner bases $\mathcal{G}_n$, and then prove that these sets are indeed Gröbner bases for the respective graphs. Such a proof typically consists of two parts: Show that the elements in $\mathcal{V}(\mathcal{G}_n)$ are in bijection with the proper colorings of G_n (that is, $\langle \mathcal{G}_n \rangle = \mathcal{I}_{G_n}$), and prove that $\mathcal{G}_n$ is a Gröbner basis for the ideal it generates, by using one of the criteria in Remark 13.
Throughout this chapter, we will assume that the chosen term order induces the variable order $x_1 \succ \ldots \succ x_n$, and use vertex permutations to obtain different variable orders.

Proposition 10. For any term order, the reduced Gröbner basis of P_n is given by

$$\mathcal{G}(P_n) := \{p_{1,\dots,n}, p_{2,\dots,n}, \dots, p_{n-1,n}, v_n\} \quad ,$$

which gives the complexity pattern $\mathfrak{c}(P_n) = (n, 3, n)$.

Proof. Following the proving scheme outlined above, we note that

$$p_{i,\dots,n} = \sum_{j=i}^{n-1} e_{j,j+1} \in \mathcal{I}_{P_n}$$

and thus $\langle \mathcal{G}(P_n) \rangle \subseteq \mathcal{I}_{P_n}$. On the other hand,

$$e_{i,i+1} = p_{i,\dots,n} - p_{i+1,\dots,n} \in \mathcal{G}(P_n)$$

and

$$v_i = v_{i+1} + (x_i + x_{i+1})e_{i,i+1} = \ldots = v_n + \sum_{j=i}^{n-1} (x_j + x_{j+1})e_{j,j+1} \in \mathcal{G}(P_n) \quad ,$$

which shows the equivalence $\mathcal{I}_{P_n} = \langle \mathcal{G}(P_n) \rangle$.
Next, $\mathcal{G}(P_n)$ is a Gröbner basis since the leading terms of its elements are pairwise relatively prime (each is a power of a distinct variable) and therefore all S-pairs vanish (Proposition 6).
The last step is to show that $\mathcal{G}(P_n)$ is reduced. The leading terms of $\mathcal{G}(P_n)$ are squares for all variables $x_1, \dots, x_{n-1}$ and the cube x_n^3. It is evident that no term in any element of $\mathcal{G}(P_n)$ is divided by any of those monomials, which is the definition of a reduced Gröbner basis and therefore finishes the proof. □

Remark 29. The support of this basis is atypically high for such simple graphs, and we will see in Section 6.2.2 below that it can indeed be improved.

6.2.2 Vertex Order

The following example indicates that the vertex order heavily influences the properties of Gröbner bases, and that by cleverly choosing a "good" order, both computational effort and resulting basis complexity can be kept relatively small. The other way round, a "bad" order can result in undesirable results, which is why the vertex order should always be paid attention to when computing Gröbner bases of graphs.

After observation of the Gröbner basis complexity for random vertex orders, we try to systematically find a order of the path graph P_n which gives small or large Gröbner bases with respect to the standard orders: For the first case, we know from Theorems 13 and 6 that the only suboptimal measure of $\mathcal{G}(P_n)$ is its support. The concept of *dominant paths*, explained in Section 6.7.3 at the example of tree graphs, suggests that the support can be decreased by putting high vertices in the center and forming shorter monotone paths. The resulting graph P_n^+, shown in Figure 6.1, gives a Gröbner basis of complexity $\mathfrak{c}(P_n^+) = (n, 3, \lfloor \frac{n}{2} + 2 \rfloor)$.

Fig. 6.1: The path graph P_n^+

In the other direction, we find a graph P_n^-, which is shown in Figure 6.2 and whose Gröbner basis complexity is $\mathfrak{c}(P_n^-) = (2(n-1), \frac{n+1}{2}, 3^{\frac{n-1}{2}})$ for odd n, and $(2(n-1), \frac{n}{2}+1, 2 \cdot F_{n+1})$ for even n. Note that the support here is exponential in the number of vertices.

Fig. 6.2: The path graph P_n^-

The computation times for the Lex bases of P_n, P_n^+ and P_n^- are compared in Figure 6.3, and we see that the result reflects the respective Gröbner basis sizes.

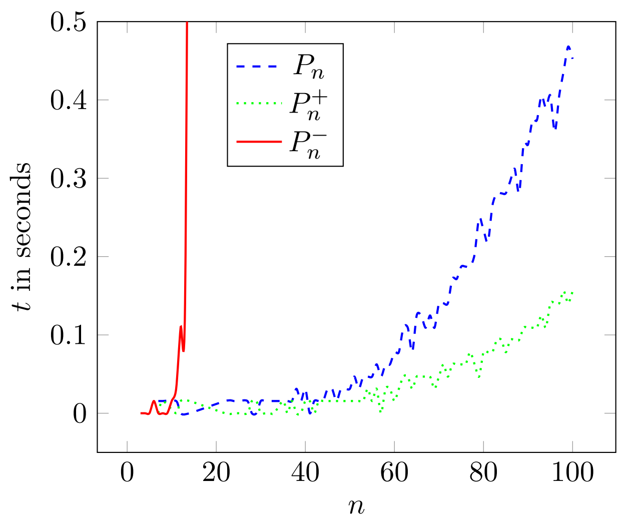


Fig. 6.3: Computation time for the Lex bases of P_n with different vertex orders

Remark 30. Note that the formulae for the Gröbner basis complexities are extrapolations of the experimental results in Tables 6.1 and 6.2. We will provide such extrapolations throughout the chapter.

Tab. 6.1: Complexity of reduced Lex bases for P_n^+

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mathfrak{l}$	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mathfrak{d}$	3	3	3	3	3	3	3	3	3	3	3	3	3	3
$\mathfrak{s}$	3	3	4	4	5	5	6	6	7	7	8	8	9	9

Tab. 6.2: Complexity of reduced Lex bases for P_n^-

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mathfrak{l}$	2	4	5	6	10	12	14	16	18	20	22	24	26	28
$\mathfrak{d}$	3	3	3	3	4	4	5	5	6	6	7	7	8	8
$\mathfrak{s}$	3	4	9	10	27	26	81	68	243	178	729	466	2187	1220

6.2.3 Gröbner Fan

In general, Gröbner bases for coloring ideals depend strongly on the choice of a term order, and their structure becomes unclear very quickly with increasing number of vertices. However, we are in some cases able to understand some (or even all) Gröbner bases in the sense that we can assign elements to substructures in the graph and thus give a meaning to the polynomials that appear in the Gröbner basis.
Apart from the complexity pattern $\mathfrak{c}(\mathcal{G}) = (\mathfrak{l}, \mathfrak{d}, \mathfrak{s})$ we also care about the exact structure of the polynomials in a Gröbner basis. Therefore, we define the *characteristic* $\mathfrak{ch}(\mathcal{G})$ of a given Gröbner basis $\mathcal{G}$ to be the 8-tuple that consists of the number of vertex polynomials, edge polynomials, path polynomials, cycle polynomials, triangle polynomials, diamond polynomials, trivial polynomials, and unknown polynomials, respectively. Clearly, $|\mathfrak{ch}(\mathcal{G})|_1 = \mathfrak{l}(\mathcal{G})$, and if there are no unknown polynomials, then $\mathfrak{d}(\mathcal{G})$ can be read off the characteristic since all other polynomial types have a specific degree. Note that the definition of the characteristic is based on our current understanding of the appearing polynomials, and has to be refined as soon as we are able to classify elements that are considered unknown until now.
The results about Gröbner fans are also purely experimental; they were found by looking at computational results and have not yet been verified theoretically.

The Gröbner fan of the path graph P_n consists of $\frac{(2(n-1))!}{(n-1)!n!}$ distinct Gröbner bases. This number is also called the $(n-1)$th Catalan number $C(n-1)$ (OEIS A000108).
Again, from Lemma 10 we know that any permutation of the vertices of a graph, as done in Section 6.2.2, can be modelled by a monomial order. The Gröbner fan incorporates all possible monomial orders on the underlying polynomial ring, and thus automatically considers P_n^+ and P_n^-, when computed for P_n.
Path graphs reveal an interesting property which does only appear in one other family that we list here: Their Gröbner bases can be of either minimal length *or* minimal support, but not both at the same time. The optimally ordered path graph P_n^+ has a complexity pattern of $\mathfrak{c}(P_n^+) = (n, 3, \lfloor \frac{n}{2} + 2 \rfloor)$, which is the minimal support among all Gröbner bases $\mathcal{G}$ with $\mathfrak{l}(\mathcal{G}) = n$. This basis has the characteristic $\mathfrak{ch}(P_n^+) = (1, 2, n-3, 0, 0, 0, 0, 0)$. However, there exists a basis with complexity pattern $(n+1, 3, 4)$.
In the opposite direction, there exist bases which assume the largest possible values for length, degree and support simultaneously. Their complexity pattern is

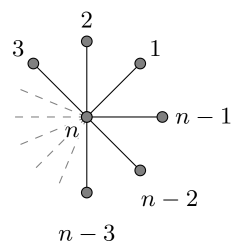
$$\left(2(n-1), \frac{n+1}{2}, \begin{cases} 3^{\frac{n}{2}} & \text{if } n \text{ odd} \\ 4 \cdot 3^{\frac{n-3}{2}} & \text{if } n \text{ even} \end{cases} \right) .$$

The vertex order of P_n^-, together with Lex order, gives both maximal length and degree, but slightly smaller support for even n.

Remark 31. Since path graphs are trees and therefore chordal, Section 7 will give proof that there exists a Gröbner basis for P_n with complexity $(n, 3, 3)$, which, however, is not reduced.

6.3 Star Graphs

The *star graph* S_n is defined by $V = \{1, \ldots, n\}$ and $E = \{\{i, n\} : 1 \leq i < n\}$.



Proposition 11. For all $n \geq 2$, the reduced Gröbner basis $\mathcal{G}(S_n)$ is

$$\mathcal{G}(S_n) := \{e_{1,n}, e_{2,n}, \ldots, e_{n-1,n}, v_n\} \quad .$$

In particular, the Gröbner complexity of S_n is $\mathfrak{c}(S_n) = (n, 3, 3)$.

Proof. Basically repeating the proof of Proposition 10, we note that

$$v_i = v_n + (x_n + x_i)e_{i,n} \in \langle \mathcal{G}(S_n) \rangle \quad .$$

The relation $\mathcal{G}(S_n) \subseteq \mathcal{I}_G$ is immediately clear, and thus $\mathcal{G}(S_n) = \mathcal{I}_G$.
Again, the leading terms of the elements of $\mathcal{G}(S_n)$ are pairwise relatively prime, and therefore $\mathcal{G}(S_n)$ is a Gröbner basis. Moreover, the leading terms are squares for all variables $x_1, \ldots, x_{n-1}$ and the cube x_n^3, which concludes the proof that $\mathcal{G}(S_n)$ is reduced. $\square$

6.3.1 Gröbner Bases for Different Center Vertices

Unlike in the case of path graphs, this particular Gröbner basis for star graphs has optimal complexity. Noting that all vertex permutations that leave the center unchanged are trivial, we expect to find Gröbner bases with a different structure only by choosing another center vertex. Table 6.3 shows how the complexity pattern changes with the center v. While for $v = 1$, the length of the basis is $\frac{n(n-1)}{2} + 1$, it drops with increasing center vertex and reaches n for $v = n$.
The result suggests that vertices with high degree should have low priority in the variable order, in order to obtain small Gröbner bases. We will test this heuristic for general trees in Section 6.7.2.

Tab. 6.3: Complexity of reduced standard bases for S_n for different center vertices

$n\backslash c$	1	2	3	$\cdots$	$n-2$	$n-1$	n
3	$(4,3,4)$	$(3,3,4)$	$(3,3,3)$		$(4,3,4)$	$(3,3,4)$	$(3,3,3)$
4	$(7,3,6)$	$(5,3,4)$	$(4,3,4)$		$(5,3,4)$	$(4,3,4)$	$(4,3,3)$
5	$(11,3,6)$	$(8,3,6)$	$(6,3,4)$		$(6,3,4)$	$(5,3,4)$	$(5,3,3)$
6	$(16,3,6)$	$(12,3,6)$	$(9,3,6)$		$(7,3,4)$	$(6,3,4)$	$(6,3,3)$
7	$(22,3,6)$	$(17,3,6)$	$(13,3,6)$		$(8,3,4)$	$(7,3,4)$	$(7,3,3)$
8	$(29,3,6)$	$(23,3,6)$	$(18,3,6)$		$(9,3,4)$	$(8,3,4)$	$(8,3,3)$
9	$(37,3,6)$	$(30,3,6)$	$(24,3,6)$		$(10,3,4)$	$(9,3,4)$	$(9,3,3)$
10	$(46,3,6)$	$(38,3,6)$	$(31,3,6)$		$(11,3,4)$	$(10,3,4)$	$(10,3,3)$
11	$(56,3,6)$	$(47,3,6)$	$(39,3,6)$		$(12,3,4)$	$(11,3,4)$	$(11,3,3)$
12	$(67,3,6)$	$(57,3,6)$	$(48,3,6)$		$(13,3,4)$	$(12,3,4)$	$(12,3,3)$

6.3.2 Gröbner Fan

The Gröbner fan of the star graph S_n consists of $\sum_{k=0}^{n-1} \frac{(n-1)!}{k!}$ distinct Gröbner bases (OEIS A000522).

We have seen above that a minimum-complexity basis is given by any of the standard bases of S_n, which justifies the notation $S_n = S_n^+$. The experimental results for this vertex order (which, of course, coincide with the theoretical findings) are shown the last column of Table 6.3. Apart from the characteristic $\mathfrak{ch}(S_n^+) = (1, n-1, 0, 0, 0, 0, 0, 0)$ of this basis, there is another minimum-length basis $\mathcal{G}$ with $\mathfrak{c}(\mathcal{G}) = (n, 3, 4)$ and $\mathfrak{ch}(\mathcal{G}) = (1, 1, n-2, 0, 0, 0, 0, 0)$, which is not generated by a standard order.

The badly ordered star with center vertex 1, also denoted as S_n^-, results in a Gröbner basis with complexity pattern $\mathfrak{c}(S_n^-) = \left(\frac{n(n-1)}{2} + 1, 3, 6\right)$ for $n \geq 4$, as can be seen in the first column of the same table. This complexity is the maximum length, degree and support of all bases in the Gröbner fan.

Therefore, these two vertex orderings represent the best and worst case with respect to Gröbner bases for the star graph.

6.3.3 Extended Stars

The family of star graphs can be generalized to *extended stars*, whose rays have length $k \geq 1$. The extended star graph $S_{n,k}$, shown in Figure 6.4, consists of $nk+1$ vertices, and its center is the vertex n. As above, we also consider the "badly ordered" extended star $S_{n,k}^-$, which we expect to have a large Gröbner basis, as opposed to the normal order, which exhibits a complexity of $(nk+1, 3, k+2)$. The correctness of this supposition can be seen in Table 6.4, where an empty cell means that MACAULAY2 ran out of memory during the computation. This family shows the worst Gröbner basis behaviour of all graphs we considered, compared to their size.

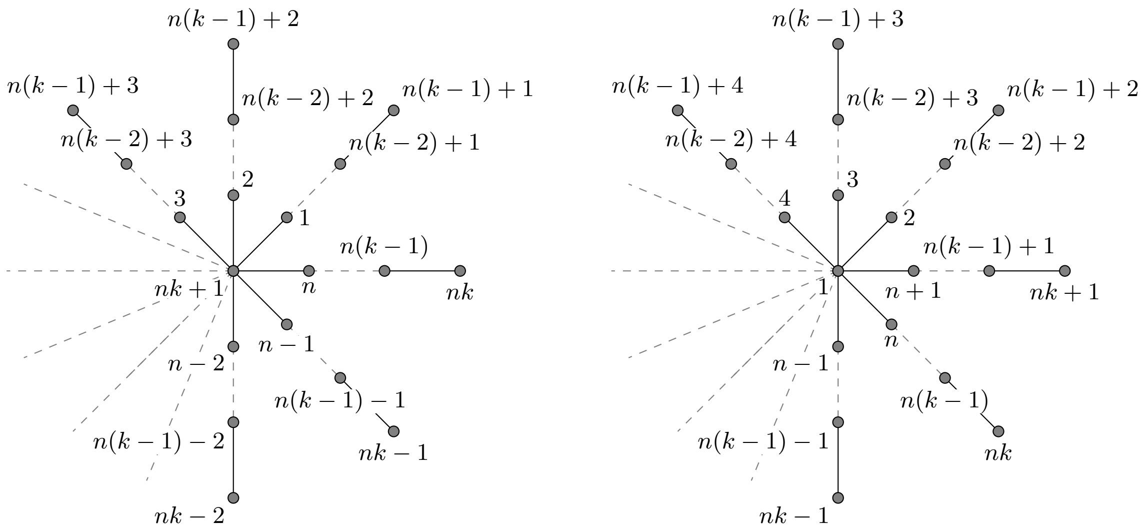


Fig. 6.4: The extended stars $S_{n,k}$ and $S^-_{n,k}$

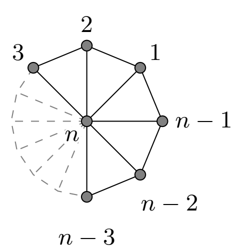
Tab. 6.4: Complexity of reduced standard bases for $S_{n,k}$ and $S^-_{n,k}$

$n\backslash G$	$S_{3,k}$	$S^-_{3,k}$	$S_{4,k}$	$S^-_{4,k}$	$S_{5,k}$	$S^-_{5,k}$
1	$(4,3,3)$	$(7,3,6)$	$(5,3,3)$	$(11,3,6)$	$(6,3,3)$	$(16,3,6)$
2	$(7,3,4)$	$(15,5,28)$	$(9,3,4)$	$(28,6,72)$	$(11,3,4)$	$(28,6,72)$
3	$(10,3,5)$	$(30,7,162)$	$(13,3,5)$	$(71,9,648)$	$(16,3,5)$	$(141,10,2592)$
4	$(13,3,6)$	$(58,9,1118)$	$(17,3,6)$		$(21,3,6)$	
5	$(16,3,7)$		$(21,3,7)$		$(26,3,7)$	
6	$(19,3,8)$		$(25,3,8)$		$(31,3,8)$	

6.4 Wheel Graphs

The *wheel graph* W_n is defined by $V = \{1, \ldots, n\}$ and

$$E = \{\{i,n\} : 1 \le i < n\} \cup \{\{i,i+1\} : 1 \le i < n-1\} \cup \{\{1,n-1\}\}$$



Proposition 12. For all odd $n \ge 3$, the reduced Gröbner basis $\mathcal{G}(W_n)$ is

$$\mathcal{G}(W_n) := \{t_{1,n-1,n}, t_{3,n-1,n}, \ldots, t_{n-2,n-1,n}, d_{2,n-1}, d_{4,n-1}, \ldots, d_{n-3,n-1}, e_{n-1,n}, v_n\} \quad .$$

In particular, the Gröbner complexity of W_n is $\mathfrak{c}(W_n) = (n, 3, 3)$.

Proof. Again, we see by direct (and lengthy) computation that every polynomial in $\mathcal{G}(W_n)$ lies in $\mathcal{I}_G$, and every vertex and edge polynomial is in $\langle \mathcal{G}(W_n) \rangle$. The leading terms of the elements of $\mathcal{G}(W_n)$ are pairwise relatively prime, and therefore $\mathcal{G}(W_n)$ is a Gröbner basis. Moreover, the leading terms are linear for all variables $x_1, \dots, x_{n-2}$, the square x_{n-1}^2 and the cube x_n^3. Hence, no term of any element is divided by a leading monomial, which concludes the proof that $\mathcal{G}(W_n)$ is reduced. $\square$

Lemma 21. For $n \geq 5$, W_n is *not* chordal.

Proof. It is easy to see that the subgraph induced by $V \setminus \{1\}$ is an $(n-1)$-cycle, which implies the claim. $\square$

6.4.1 Gröbner Fan

Since odd wheels are not 3-colorable (they contain a 4-clique), we need to distinguish two cases: For even n, the Gröbner bases $\{1\}$ is trivially unique with complexity $(1, 0, 1)$ and characteristic $\mathfrak{ch}(W_n) = (0, 0, 0, 0, 0, 0, 1, 0)$.
In the more interesting case $2 \nmid n$, the number of Gröbner bases in the Gröbner fan of W_n is $\frac{(n+3)(n-1)}{2}$, all of which have the same complexity $\mathfrak{c}(W_n) = (n, 3, 3)$. The characteristic is also unique; we have

$$\mathfrak{ch}(W_n) = \left(1, 1, 0, 0, \frac{n-1}{2}, \frac{n-3}{2}, 0, 0\right) \quad .$$

6.5 Complete Tripartite Graphs

The *complete tripartite graph* $K_{k,m,n} = (V, E)$ with $k, m, n \in \mathbb{N}_0$ (see Figure 6.5) is defined by

$$V = V_1 \cup V_2 \cup V_3 := \{1, \dots, k\} \cup \{k+1, \dots, k+m\} \cup \{k+m+1, \dots, k+m+n\}$$

and

$$E = \{\{i, j\} : i \in V_1, j \in V_2\} \cup \{\{i, j\} : i \in V_1, j \in V_3\} \cup \{\{i, j\} : i \in V_2, j \in V_3\} \quad .$$

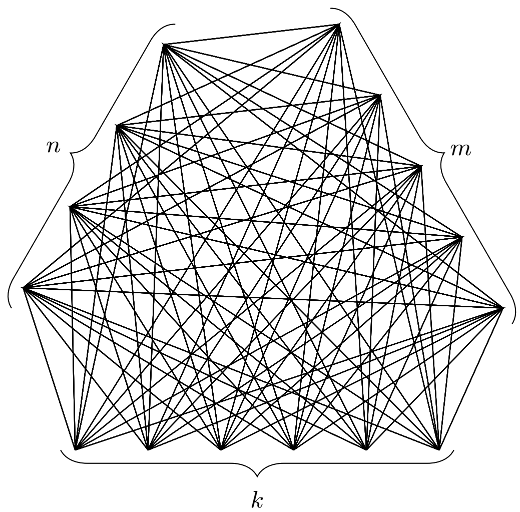


Fig. 6.5: The complete tripartite graph $K_{k,m,n}$

Lemma 22. For all $k, m, n \in \mathbb{N}_0$, $K_{k,m,n}$ is 3-colorable, and if at least two of the parameters are ≥ 2, it is *not* chordal, but still perfect. Moreover, $K_{k,m,n}$ is uniquely 3-colorable.

Proof. The first and the last property are trivial. Let without loss of generality $k, m \geq 2$, then obviously $\{1, 2\} \subset V_1$ and $\{k+1, k+2\} \subset V_2$, and therefore the 4-cycle

$$1 \to k+1 \to 2 \to k+2 \to 1$$

has no chord.
To prove perfectness, note that a graph is perfect if and only if its complement is perfect (see for example [14], Theorem 5.5.4). But the complement of the $K_{k,m,n}$ is the disjoint union of the three smaller graphs K_k, K_m, and K_n, which are chordal and therefore perfect. □

6.5.1 Standard Bases

Proposition 13. For all $k, m, n \geq 1$, the reduced Gröbner basis $\mathcal{G}(K_{k,m,n})$ is

$$\begin{aligned} \mathcal{G}(K_{k,m,n}) \quad := \quad & \{t_{1,k+m,k+m+n}, t_{2,k+m,k+m+n}, \ldots, t_{k,k+m,k+m+n}, \\ & d_{k+1,k+m}, d_{k+2,k+m}, \ldots, d_{k+m-1,k+m}, \\ & d_{k+m+1,k+m+n}, d_{k+m+2,k+m+n}, \ldots, d_{k+m+n-1,k+m+n}, \\ & e_{k+m,k+m+n}, v_{k+m+n}\} \quad . \end{aligned}$$

In particular, the Gröbner complexity of this graph is $\mathfrak{c}(K_{k,m,n}) = (n, 3, 3)$.

Proof. The proof is the same as in Proposition 12. □

In particular, the complete tripartite graph form a non-chordal family of graphs which possess an n-sized Gröbner basis.

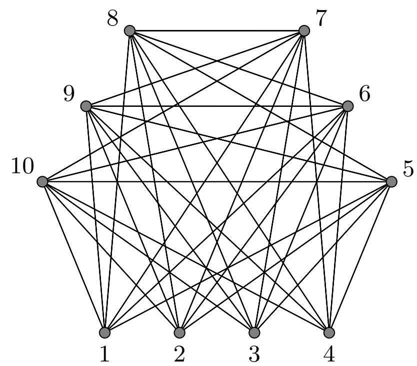


Fig. 6.6: The complete tripartite graph $K_{4,3,3}$

Example 9. The Lex basis with ascending vertex order of the $K_{4,3,3}$ (see figure 6.6) is

$$\begin{aligned}
\{x_1 + x_7 + x_{10}, &\qquad & \{t_{1,7,10},\\
x_2 + x_7 + x_{10}, && t_{2,7,10},\\
x_3 + x_7 + x_{10}, && t_{3,7,10},\\
x_4 + x_7 + x_{10}, && t_{4,7,10},\\
x_5 + x_7, &\quad = \quad& d_{5,7},\\
x_6 + x_7, && d_{6,7},\\
x_7^2 + x_7x_{10} + x_{10}^2, && e_{7,10},\\
x_8 + x_{10}, && d_{8,10},\\
x_9 + x_{10}, && d_{9,10},\\
x_{10}^3 + 1\} && v_{10}\} \quad .
\end{aligned}$$

6.5.2 Gröbner Fan

The Gröbner fan of a complete tripartite graph $K_{k,m,n}$ consists of $2(km + kn + mn)$ distinct Gröbner bases. This family of graphs has the unique complexity pattern

$$\mathfrak{c}(K_{k,m,n}) = (k + n + m, 3, 3) \quad ,$$

and moreover, all its Gröbner bases have one of three characteristics:

$$\begin{aligned}
\mathfrak{ch}(K_{k,m,n}) \quad \in \{ \quad & (1, 1, 0, 0, k, m + n - 2, 0, 0),\\
& (1, 1, 0, 0, m, k + n - 2, 0, 0),\\
& (1, 1, 0, 0, n, k + m - 2, 0, 0) \quad \} \; .
\end{aligned}$$

6.6 Random Tripartite Graphs

We generate graphs according to the model proposed by Gilbert in [22]. For a graph G, let $G(p)$ denote the graph obtained by taking the same vertex set, and every edge of G appearing independently with probability $p \in [0, 1]$. Since we mostly rely on 3-colorability of a graph (otherwise the resulting basis would be trivial), the underlying graph is always a complete tripartite graph of random size: We build the graph by first choosing three partition sizes, each uniformly and independently drawn between integer bounds l and u, where $l, u \in \mathbb{N}$ and often $l = 1$, followed by inserting edges independently with probability p. Choosing $p = 0$ results in an empty graph, while $p = 1$ always gives a complete tripartite graph.

6.6.1 Triangle polynomials

For 3-coloring, triangles are shown in experiments to be very "nice" substructures in a graph, in the sense that graphs which contain many triangles tend to have small and fast computable Gröbner bases. This computational finding can be justified theoretically by looking at the coloring ideal and Gröbner basis computation.
A triangle $\{i, j, k\}$ in a graph G forces its three vertices to take different colors; therefore,

$$\{x_i, x_j, x_k\} = \{\xi, \xi^2, \xi^3\}, \quad \text{where } \xi = \xi_3$$

for every proper coloring, and from the summation formula for roots of unity (see [**?**]) we get that $x_i + x_j + x_k = 0$. This is exactly the triangle polynomial from Section 6.1 above, hence $t_{i,j,k} \in \mathcal{I}_G$. If we now without loss of generality assume that $x_i \succ x_j \succ x_k$ in the chosen term order, then it is clear that an arbitrary Gröbner basis of G with respect to $\succ$ contains an element g with $\mathrm{LM}(g) = x_i$, provided that $\chi(G) \leq 3$, because in this case $1 \notin \mathcal{I}_G$.
Let $\mathcal{G}$ be a reduced Gröbner basis of G. According to Definition 19, no term in any element of $\mathcal{G}$ divides x_i; therefore, this variable does not show up in $\mathcal{G}$ except in the polynomial whose leading term it is (which may or may not be $t_{i,j,k}$). We see that a triangle practically removes the variable connected to the largest of its three vertices (with respect to $\succ$) from a Gröbner basis. This phenomenon can be loosely explained by the fact that it suffices to know the colors of two vertices of the triangle; then the third color is already determined.

6.6.2 Speed-Up by Adding Triangle Polynomials

To test the effect of heuristics for Gröbner basis computations, we apply the heuristic methods to randomly generated graphs and evaluate the results, e.g. computation time or Gröbner basis size, for the original and the modified input. A large gap between the two inputs then suggests that the method is working well for the graphs under consideration.

Let us have a look at the probability for a triangle in a random graph: $K_{k,m,n}$ contains kmn distinct triangles, and in the Gilbert model, each of them occurs with probability p^3. Thus,

$$\mathbb{P}\left(K_{k,m,n}(p) \text{ contains at least one triangle}\right) = 1 - \left(1 - p^3\right)^{kmn} \quad .$$

For the expected number of triangles we have

$$\mathbb{E}\left[\left|\{\text{triangles in } K_{k,m,n}(p)\}\right|\right] = kmn \cdot p^3 \quad .$$

These functions, together with experimental data over a sample set of 10000 $K_{5,5,5}(p)$ graphs, are shown in Figure 6.7.

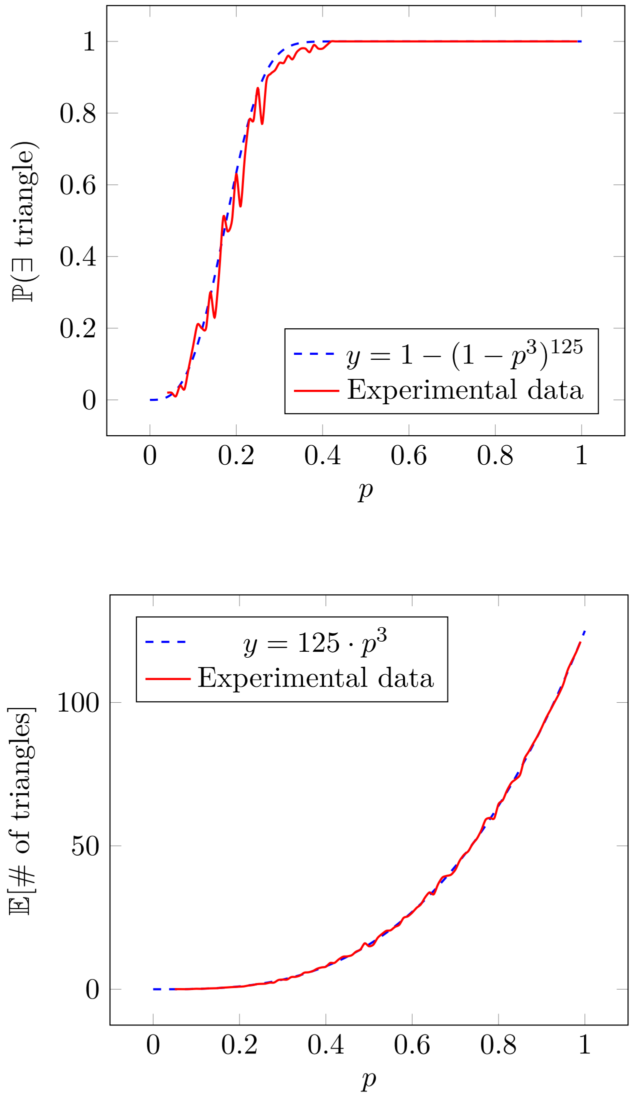


Fig. 6.7: Triangles in the random graph $K_{5,5,5}(p)$

Consequently, we expect a drastic effect for values of p close to 1, while for small p ($p < 0.2$), the speed-up should not be noticeable.

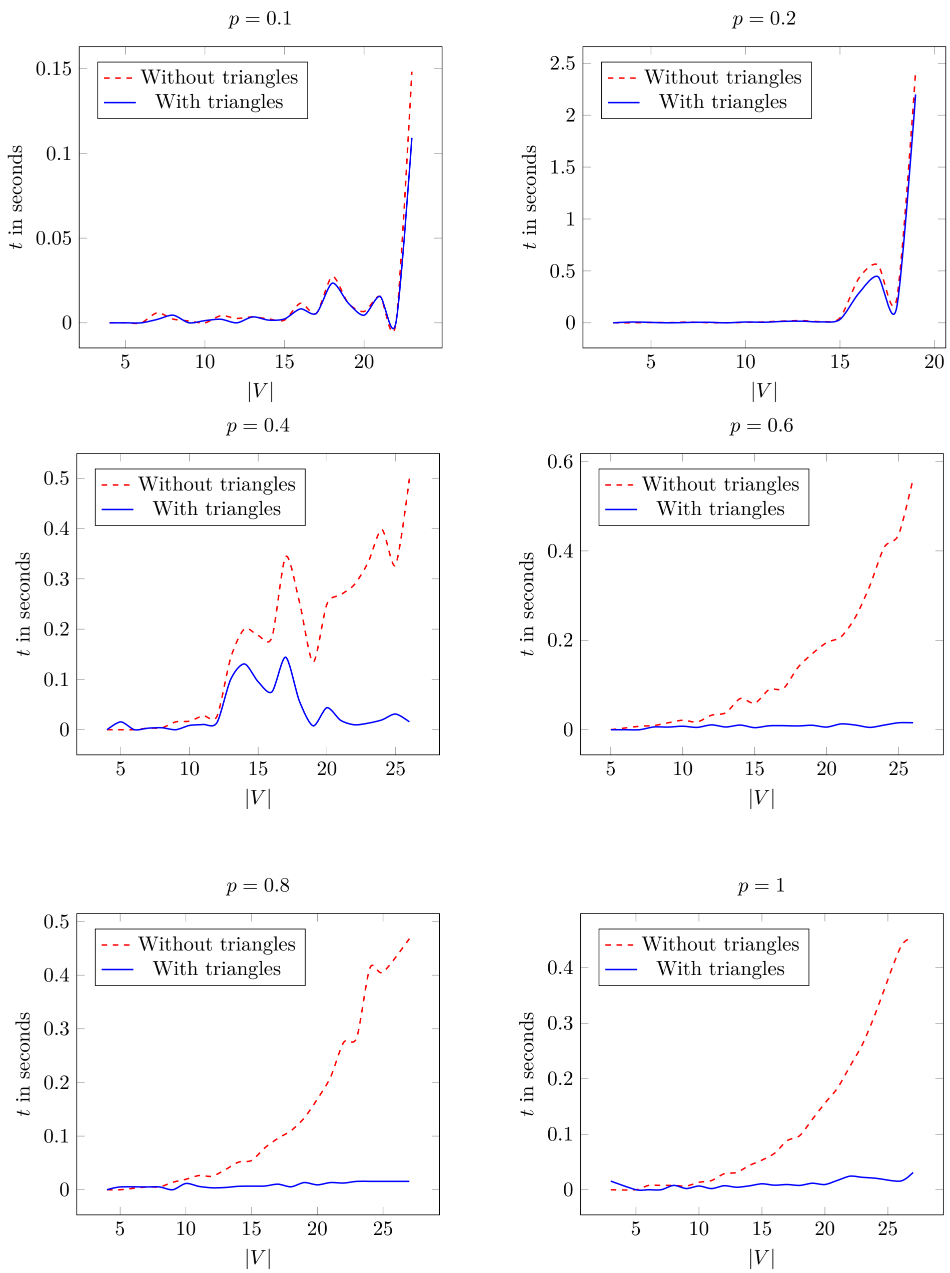


Fig. 6.8: Gröbner basis computation times for random graphs $K_{k,m,n}(p)$ with and without triangle polynomials

Figure 6.8 shows the average Gröbner basis computation time with and without triangle polynomials for several values of p. The results coincide closely with our above reasoning; for $p = 1$, that is, complete tripartite graphs, the speed-up factor is around 20.

Of course, the necessary preprocessing to find all triangles in G takes time, too. Algorithm 6 returns a complete list of triangles in $\mathcal{O}(n^3)$ time, which can be neglected in any Gröbner basis computation of practical size. With little effort, the algorithm can be adapted to list diamonds in G as well, which admittedly has only a small effect, and only for very dense graphs.

Algorithm 6 Detecting triangles in a graph

Input: Graph $G = (V, E)$
Output: List L of all triangles in G

```
function ListTriangles(G)
    L ← ∅
    for all {u, v} ∈ E do
        for all w ∈ (N(u) ∩ N(v) ∩ {w ∈ V : u < v < w}) do
            L ← L ∪ {{u, v, w}}
        end for
    end for
    return L
end function
```

6.7 Tree Graphs

6.7.1 Negative Examples

Randomly generated tree graphs exhibit a very high range of Gröbner basis complexities with respect to standard orders: Some trees have almost optimally-sized bases, while they are large and unstructured for other trees.

Example 10. Consider the two graphs T_1 and T_2 shown in Figure 6.9. The Lex bases with respect to the given vertex orders have complexity $\mathfrak{c}(T_1) = (42, 7, 138)$ and $\mathfrak{c}(T_2) = (24, 5, 68)$, which does not at all correspond to the size and structure of the graphs.

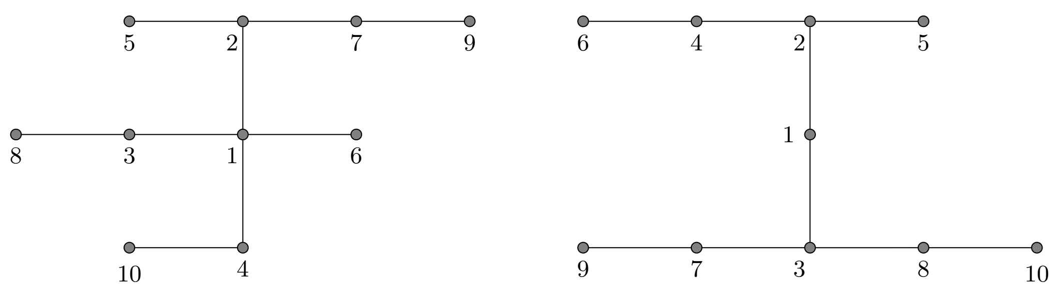


Fig. 6.9: Trees T_1, T_2 with bad vertex orders

Experiments with random trees and their standard Gröbner bases indicate that large and unstructured bases occur for graphs which have low vertex numbers in the center and high numbers as leaves, while low leaf vertices and high center vertices correlate with small and clear Gröbner bases.

6.7.2 Vertex Reordering

Intuitively, we assume that it should be helpful to permute the vertices in a way that places high numbers in the center of the graph. Applying our reasoning to experimental graphs, we find that a quite efficient vertex ordering is defined by

$$\deg u > \deg v \implies u > v \iff x_v \succ x_u \quad .$$

By this criterion, vertices with high degree are assigned to "small" monomials with respect to $\succ$, which only appear infrequently in the leading terms of the Gröbner basis elements.
Algorithm 7 permutes the vertex labels of a given graph to the optimal order, which allows us to use the "normal" monomial orders Lex, GLex and GRevLex with the variable order $x_1 \succ x_2 \succ \ldots \succ x_n$. Note that the algorithm can be refined by investigating which choice of a vertex in the set $\arg\min_{v \in R}(\deg v)$ of remaining minimal-degree vertices is the best. One idea here would be to create long ascending paths towards the center of the graph instead of up-and-down paths.

Algorithm 7 Re-ordering the vertices to obtain smaller Gröbner bases

Input: Graph $G = (V, E)$
Output: Permutation of G with $\deg u > \deg v \implies u > v$ for all $u, v \in V$

```
function ReorderVertices(G)
    R ← V
    i ← 1
    while R ≠ ∅ do
        Choose v ∈ arg min_{v∈R}(deg v)
        σ(v) = i
        i ← i + 1
        R ← R \ {v}
    end while
    return G' := (V, σ(E))
end function
```

Remark 32. Algorithm 7, run on S_n with an arbitrary center vertex, yields the optimal order S_n^+.

Example 11. If we run Algorithm 7 on the two tree graphs from Example 10, we obtain the vertex order shown in Figure 6.10, and the Gröbner basis complexity reduces to $\mathfrak{c}(T_1^+) = (10, 3, 5)$ and $\mathfrak{c}(T_2^+) = (11, 3, 4)$.

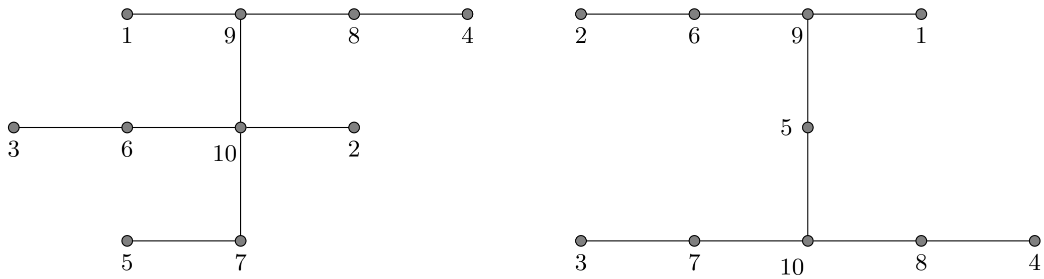


Fig. 6.10: Trees T_1^+, T_2^+ with good vertex orders

To give an impression of the effect of vertex reordering on computational effort and complexity of the result, we show a comparison for a set of 200 randomly generated tree graph of size $5 \leq n \leq 20$ in Figure 6.11.

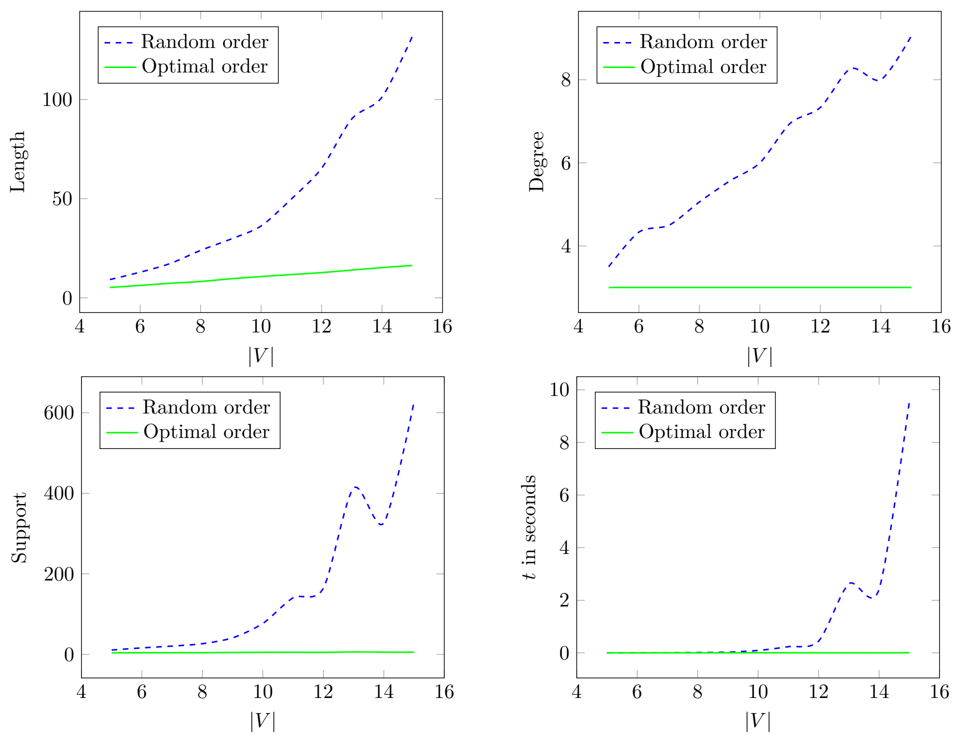


Fig. 6.11: Complexity of tree Gröbner bases for random and optimal vertex order

6.7.3 Dominant Paths

We try to understand the structure of Gröbner bases by looking at the Lex bases of optimally ordered trees, as generated by Algorithm 7. The two examples in Figure 6.12 have the Gröbner bases

$$\mathcal{G}_3 = \mathcal{G}(\mathcal{I}_{T_3}) = \{e_{1,10}, e_{2,10}, e_{3,10}, p_{4,9,10}, p_{5,9,10}, e_{6,8}, p_{7,9,10}, p_{8,7,9,10}, v_8, e_{9,10}, v_{10}\}$$

and

$$\mathcal{G}_4 = \mathcal{G}(\mathcal{I}_{T_4}) = \{e_{1,10}, e_{2,10}, e_{3,8}, e_{4,9}, e_{5,9}, e_{6,10}, p_{8,6,10}, e_{7,10}, p_{9,7,10}, v_8, v_9, v_{10}\} \quad .$$

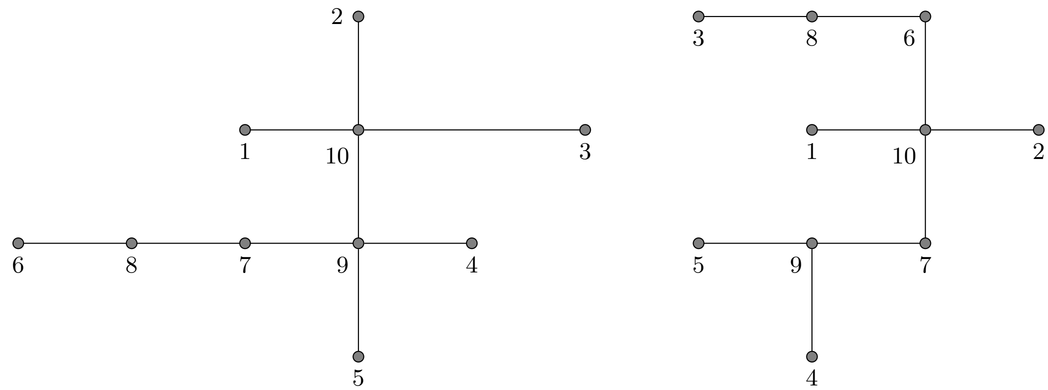


Fig. 6.12: Optimally ordered trees T_3, T_4 with classifiable standard bases

A first observation is that all polynomials are elementary as defined in Section 6.1, which is not always the case. However, around 70% of optimally ordered trees show this kind of Gröbner bases, and we conjecture that there is always a vertex order which satisfies the degree condition from the re-ordering algorithm, and under which all polynomials in the Gröbner basis are classifiable.

Next, we notice that a vertex polynomial v_i appears in the Gröbner basis if and only if $i > j \; \forall \; j \in \mathcal{N}(i)$, that is, if i has the highest number among its neighborhood. These vertices are v_8 and v_{10} for T_3, and v_8, v_9 and v_{10} for T_4. This can, in general, be explained by looking at the generator system $\mathcal{F}_G$: If there is some $j \in \mathcal{N}(i)$ with $j > i$, then the leading term of the edge polynomial $e_{i,j}$ is x_i^2, which divides $x_i^3 = \mathrm{LM}(v_i)$. Therefore, the vertex polynomial is reduced by an edge polynomial and cannot be part of the Gröbner basis. The other direction is not that clear, and it turns out that for graphs containing cycles, not all maximal vertices are part of the Gröbner basis. However, this observation is supported by Lemma 15 which states that the vertex polynomial v_n is part of every Gröbner basis of a graph on n vertices.

Finally, the paths of length ≥ 2 (here we treat edges as paths) in $\mathcal{G}$ lead from arbitrary vertices to local maxima: For example, the path polynomial $p_{8,7,9,10}$ in $\mathcal{G}_3$ encodes the path from vertex 8, which is locally maximal, down to vertex 7, and then up to 9 and 10, where it stops. In fact, there is such a path from every vertex of the graph. Sometimes, it degenerates to an edge or even to a vertex, but it exists for all $v \in V$.

This leads to the notion of a *dominant path* $(v_1, \ldots, v_k)$, which is defined for every starting vertex of a tree graph and can be constructed by the following steps:

1. Start from an arbitrary vertex i, i.e., $v_1 := i$, and set the counter $l := 1$.

2. Go to the highest neighbor of the current vertex: $v_{l+1} := \max_i \big(i \in \mathcal{N}(v_l)\big)$. If $v_{l+1} < v_l$, repeat Step 2, otherwise go to Step 3. In both cases, increase l by 1.

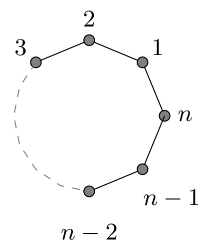
3. If v_l is locally maximal, go to Step 4. Otherwise, go to the highest neighbor of v_l as above and repeat Step 3, again increasing l by 1.

4. Check if the path starts at a lower point than it ends. If not, discard it.

Together with the vertex polynomials of locally maximal vertices, the dominant paths give a set of polynomials which we find in the standard Gröbner bases of tree graphs. They mostly appear in other graphs as well, but can sometimes be reduced by other structures like triangles, such that the theory becomes much more subtle in general.

6.8 Cycle Graphs

The *cycle graph* C_n is defined by $V = \{1, \dots, n\}$ and $E = \{\{i, i+1\} : 1 \le i < n\} \cup \{\{1, n\}\}$.



Cycle graphs are the most basic examples of non-chordal graphs, and also the simplest examples of graphs which do not possess an n-sized Gröbner basis. Their bases contain polynomials that do not seem to have a plain structure, and there is no Gröbner basis of a cycle graph which only consists of polynomials which we can classify, apart from small exceptions like the triangle graph.

6.8.1 Standard Bases

An interesting observation is that the Gröbner bases with respect to the standard orders contain something like a generalization of path polynomials, which have higher degree and whose structure indicates that they represent chords of the cycle.

Example 12. The following are Lex bases with respect to the ascending vertex order, as shown in the definition of cycle graphs.

$$\begin{aligned}
\mathcal{G}(C_4) &= \{x_1^2 + x_1x_4 + x_4^2, x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1, x_2^2 + x_2x_3 + x_3x_4 + x_4^2, \\
&\quad x_3^2 + x_3x_4 + x_4^2, x_4^3 + 1\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{G}(C_5) &= \{x_1^2 + x_1x_5 + x_5^2, x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1, x_1x_3 + x_1x_4 + \\
&\quad + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_5 + x_4x_5 + x_5^2, x_2^2 + x_2x_3 + x_3x_4 + \\
&\quad + x_4x_5 + x_5^2, x_3^2 + x_3x_4 + x_4x_5 + x_5^2, x_4^2 + x_4x_5 + x_5^2, x_5^3 + 1\}
\end{aligned}$$

$$\begin{aligned}
\mathcal{G}(C_6) &= \{x_1^2 + x_1x_6 + x_6^2, x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_1, \\
&\quad x_1x_3x_4 + x_1x_3x_6 + x_1x_4x_5 + x_1x_5x_6 + x_2x_3x_4 + x_2x_3x_6 + x_2x_4x_5 + \\
&\quad + x_2x_5x_6 + x_3x_4x_6 + x_3x_6^2 + x_4x_5x_6 + x_5x_6^2, x_2^2 + x_2x_3 + x_3x_4 + \\
&\quad + x_4x_5 + x_5x_6 + x_6^2, x_3^2 + x_3x_4 + x_4x_5 + x_5x_6 + x_6^2, x_4^2 + x_4x_5 + \\
&\quad + x_5x_6 + x_6^2, x_5^2 + x_5x_6 + x_6^2, x_6^3 + 1\}
\end{aligned}$$

We see that the dominant paths, starting from all vertices, appear in these bases, and that they contain one messy polynomial. These unclassifiable polynomials become more for larger graphs, and without them, we would just have an $(n+1)$-sized basis of characteristic $(1, 2, n-3, 1, 0, 0, 0, 0)$.

Despite their unclear structure, these Gröbner bases have a complexity pattern which allows for a simple description. Since $\chi(C_n) = 2$ for even n and $\chi(C_n) = 3$ for odd n, it is not surprising that the Gröbner bases structurally differ for these two cases. We obtain for $n \geq 6$

$$\mathfrak{c}(C_n) = \begin{cases} \left(\frac{3}{2}n - 1, \frac{n}{2}, 4 \cdot 3^{\frac{n}{2}-1}\right) & \text{for } n \text{ even} \\ \left(\frac{3n-1}{2}, \frac{n-1}{2}, 3^{\frac{n-1}{2}}\right) & \text{for } n \text{ odd} \end{cases},$$

which is exponentially large in the input size of C_n for all n.

Tab. 6.5: Complexity of reduced Lex bases for C_n

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mathfrak{l}$	2	3	5	7	8	10	11	13	14	16	17	19	20	22
$\mathfrak{d}$	3	3	3	3	3	3	4	4	5	5	6	6	7	7
$\mathfrak{s}$	3	3	4	9	12	27	36	81	108	243	324	729	972	2187

6.8.2 Gröbner Fan

The number of distinct bases in the Gröbner fan of a cycle graph does not seem to be a known sequence; the OEIS does not find any matching for the numbers in the first row of Table 6.6. Moreover, we encounter the same phenomenon as for path graphs: A Gröbner basis can have either minimal length or minimal support, but not both. The standard bases from Table 6.5 have small length, but their support grows very fast.

Tab. 6.6: Complexity measures in the Gröbner fan of C_n

n	3	4	5	6	7	8
Number of bases	6	12	60	228	854	3208
Minimal length	3	5	7	8	10	11
Minimal degree	3	3	3	3	3	3
Minimal support	3	4	8	9	21	10
Minimal-length basis	$(3, 3, 3)$	$(5, 3, 4)$	$(7, 3, 8)$	$(8, 3, 12)$	$(10, 3, 22)$	$(11, 4, 32)$

Based on the results in Tables 6.5 and 6.6, from which we suppose that the monotone vertex order and the standard bases give a minimum-length basis, we conjecture:

Conjecture 1. For the cycle graph C_n, a minimum-length Gröbner basis consists of $\left\lfloor \frac{3n-1}{2} \right\rfloor$ elements.

A stronger conjecture would be that for arbitrary graph families $G_n = (V_n, E_n)$ with $|V_n| = n$, there is a sequence of Gröbner bases $(\mathcal{G}_n)$ for $(\mathcal{I}_{G_n})$, such that $\mathfrak{l}(\mathcal{G}_n) = \mathcal{O}(n)$. The reasoning behind this conjecture is the following: We know that chordal graphs have short Gröbner bases, and the only forbidden subgraph in a chordal graph is a long induced cycle. Therefore, each graph can be seen as a combination of a chordal graph and multiple cycles, and both families allow for linear-sized bases.

6.9 Iterated Octahedral Graphs

The family of iterated octahedral graphs, as defined in Section 2.3.1, is an example of maximal planar, but 3-colorable graphs. As such, the proper 3-coloring is unique (Lemma 5), and [32] showed that the Gröbner bases of uniquely colorable graphs are equal for all term orders which induce the same variable order (see also Remark 24).
The Lex basis of O_{3n} for the vertex order shown in Figure 2.5 consists of one vertex polynomial, one edge polynomial, n triangle polynomials and $2(n-1)$ diamond polynomials.

6.9.1 Gröbner Fan

We can reproduce the result about uniqueness of the Gröbner basis by looking at the Gröbner fan of the iterated octahedral graph O_{3n}: It consists of $6n^2$ distinct Gröbner bases. This family of graphs has the Gröbner basis characteristic

$$\mathfrak{ch}(O_{3n}) = (1, 1, 0, 0, n, 2(n-1), 0, 0) \quad ;$$

in particular, its complexity pattern $\mathfrak{c}(O_{3n}) = (3n, 3, 3)$ is unique.

7. A POLYNOMIAL-TIME ALGORITHM FOR THE GRÖBNER BASES OF CHORDAL GRAPHS

In this section, we will develop an algorithm that computes a Gröbner basis for the k-coloring ideal of a given chordal graph in polynomial time. It is known that the chromatic number of a chordal graph can be calculated in linear time $\mathcal{O}(|V|+|E|)$ ([26], Theorem 4.17), but a Gröbner basis provides more information than just a coloring, for instance the number of distinct proper colorings, and, in case of an elimination order, an efficient way to produce such a coloring.
We start by examining some properties and notation concerning chordal graphs, which we will use when describing the algorithm.

7.1 Preliminaries

Recall from Section 2.3.2 that a graph is chordal if it does not contain an induced cycle of length more than 3, i.e., every cycle which is not a triangle contains a chord. There are some other characterizations of chordal graphs, which turn out to be useful from an algorithmic viewpoint. The first one uses an operation called *pasting*: Let G be a graph, and let G_1, G_2 be induced subgraphs of G, such that $G = G_1 \cup G_2$. If $S = G_1 \cap G_2$, then we say that G arises from G_1 and G_2 by pasting them together along S.

Proposition 14. A graph is chordal if and only if it can be constructed recursively by pasting along complete subgraphs, starting from complete graphs.

Proof. See for example [14], Proposition 5.5.1. □

The second characterization is recursive and depends on the notion of a *simplicial vertex*, which is defined as a vertex whose neighbors form a clique. A graph is *recursively simplicial* if it contains a simplicial vertex v which can be removed such that the remaining subgraph is again recursively simplicial.

Theorem 26. A graph is chordal if and only if it is recursively simplicial.

Proof. We prove that recursive simpliciality is equivalent to constructability by pasting along complete subgraphs, starting from complete graphs. We call this latter property being *pastable*.
Let G be recursively simplicial with n vertices. By definition, we can find a simplicial vertex v_{n-1} whose neighborhood is a clique C_{n-1}. Denoting $G_{n-1} := G - v_{n-1}$ and repeating this procedure, we end up with a sequence $G = G_n, \ldots, G_1 = (\{1\}, \emptyset)$, a sequence of cliques $C_{n-1}, \ldots, C_1$, and a sequence of vertices $v_{n-1}, \ldots, v_1$.
Going in the other direction, we introduce the notation

$$G^{+C} := \big(V \cup \{n+1\}, E \cup \{\{j, n+1\} : j \in C\}\big) \quad ,$$

such that our sequence satisfies $G_{i+1} = G_i^{+C_i}\ \forall\ i \in \{1, \ldots, n-1\}$.
Noting that the operation $G \to G^{+C}$, where C is a clique, is exactly pasting along complete subgraphs for $G_1 = G$ and $G_2 = C \cup \{n+1\}$, we see immediately that G is pastable, starting from the complete graph K_1.

Let, on the other hand, G be pastable (and thus, G is chordal). We argue by induction on n, the number of vertices in G. Consider the last pasting operation, i.e., $G = G_1 \cup G_2$, and $S := G_1 \cap G_2$. Choose an arbitrary vertex $v \in G_2$. Since G_2 is complete, v is simplicial in G. Deleting v from G results in a chordal graph G', since deleting a vertex cannot induce a hole. Therefore, $G - v$ has $n-1$ vertices and is pastable, so we can again find a simplicial vertex. We conclude that G is recursively simplicial. $\square$

A third characterizing property of chordal graphs is the *perfect elimination ordering.*

7.2 Perfect Elimination Orderings

Most efficient algorithms for graph problems on chordal graphs rely on a special ordering of the vertices, as pointed out for example in [26], Chapter 4, which gives a thorough introduction to the algorithmic aspects of chordal graphs (which are called *triangulated* in this book).

Definition 26. Let $G = (V, E)$ be a graph, and let $V = \{1, \ldots, n\}$. The vertex order is called a *perfect elimination ordering* if $\mathcal{N}(v) \cap \{1, \ldots, v-1\}$ is a complete graph for all $v \in V$.

It is intuitively clear that the order of removing or adding vertices in Theorem 26 is a perfect elimination order. We will give a rigorous proof which actually shows both directions.

Lemma 23. A vertex order on a graph G is a perfect elimination order if and only if it can be used to show that G is recursively simplicial.

Proof.

$\Rightarrow$ Assume that $v_1, \ldots, v_n$ are ordered in a perfect elimination order, that is, $v_i = i\ \forall\ i$. Then $\mathcal{N}(n) \cap \{1, \ldots, n-1\} = \mathcal{N}(n)$ is a clique, and after removing n from G, the remaining order is still a perfect elimination order. Induction gives the claim.

$\Leftarrow$ Let $v_n, \ldots, v_1$ be the order of removal in a recursively simplicial graph. The vertices that v_i is attached to during the $+C$-operation form a complete graph in G_i, which is exactly the subgraph induced by $\{1, \ldots, i-1\}$. Thus $\mathcal{N}(i) \cap \{1, \ldots, i-1\}$ is a clique for all $i \in V$.

$\square$

From this lemma, we immediately get another characterization for chordal graphs.

Corollary 8. A graph is chordal if and only if it has a perfect elimination ordering.

Keeping this in mind, it is not surprising that an algorithm that recursively builds a chordal graph and a corresponding Gröbner basis runs in polynomial time.

Remark 33. From what we did so far, it has become clear that the ordering of the vertices, and therefore the ordering of the variables in the algebraic problem formulation, is very important to guarantee the correctness of the results below. However, it turns out that the *exact* term order does not matter, as long as the variable order is fixed (see Remark 9). We can therefore just assume that the Lex order (with permuted vertices) is used throughout this section, since it is the most intuitive order for the reader to retrace the calculations.

7.3 The Augmenting Polynomial

The algorithm will decompose a given graph in a perfect elimination order and build it back up, while adding a suitable polynomial for each new vertex. Such a polynomial has to ensure that the variety, defined by the new ideal, exactly contains the proper colorings of the augmented graph.
We start by introducing two families of symmetric polynomials.

Definition 27. The *k-th elementary symmetric polynomial* $\sigma_k(x_1, \ldots, x_n)$ over n variables is

$$\sigma_k(x_1, \ldots, x_n) := \sum_{1 \le j_1 < \cdots < j_k \le n} x_{j_1} \cdots x_{j_k} \quad .$$

The *k-th complete homogeneous symmetric polynomial* $S_k(x_1, \ldots, x_n)$ over n variables is

$$S_k(x_1, \ldots, x_n) := \sum_{1 \le j_1 \le \cdots \le j_k \le n} x_{j_1} \cdots x_{j_k} \quad .$$

Note that both polynomials are degree-k-homogeneous, but σ_k is by definition square-free, while S_k can contain higher powers of a variable.

Lemma 24. Let G be a chordal graph on n vertices. For any $k, r \in \mathbb{N}$, where $k > r$, and for any partial assignment $\{x_{c_1} = \xi_1, \ldots, x_{c_r} = \xi_r\}$ of r distinct k-th roots of unity to variables in $\mathbb{K}[x_1, \ldots, x_n]$, there is a polynomial $p \in \mathbb{K}[x_1, \ldots, x_{n+1}]$ which is homogeneous of degree $k - r$, such that

$$p(x_1, \ldots, x_{n+1}) = 0 \iff x_{n+1} \in R_k \setminus \{\xi_1, \ldots, \xi_r\} \quad ,$$

i.e., the solutions of x_{n+1} in p are exactly the $k - r$ other roots of unity.

Proof. Without loss of generality, assume that $c_i = i \; \forall i \in \{1, \ldots, r\}$, and set $x := x_{n+1}$. We show that the complete homogeneous symmetric polynomial $p := S_{k-r}(x_1, \ldots, x_r, x)$ is the polynomial we are looking for.
First, note that it suffices to prove that

$$S_{k-r}(x_1, \ldots, x_r, x) \cdot (x - x_1) \cdots (x - x_r) = x^k - 1 \quad .$$

Then the claim follows with the following argument: Let $x \in R_k \setminus \{\xi_1, \ldots, \xi_r\}$. The equality therefore becomes

$$S_{k-r}(x_1, \ldots, x_r, x) \cdot \underbrace{(x - x_1)}_{\neq 0} \cdots \underbrace{(x - x_r)}_{\neq 0} = \underbrace{x^k - 1}_{=0} \implies S_{k-r}(x_1, \ldots, x_r, x) = 0 \quad .$$

Hence, we have found $k-r$ distinct roots of a $(k-r)$-dimensional univariate polynomial, and this ensures that there are no other roots of p.
Now, consider the degree d-homogeneous polynomial $\sigma_i(x_1,\ldots,x_r)S_{d-i}(x_1,\ldots,x_r)$. For every monomial x^α with $|\alpha| = d$ and $|\operatorname{supp}(\alpha)| = m$, its coefficient is the number of square-free factors of degree i, that is, $\binom{m}{i}$.
Summing up these coefficients over d with alternating signs gives that the coefficient of x^α in

$$\sum_{i=0}^{d}(-1)^{d-i}\sigma_i(x_1,\ldots,x_r)S_{d-i}(x_1,\ldots,x_r)$$

is

$$\sum_{i=0}^{m}(-1)^{d-i}\binom{m}{i} = 0 \quad .$$

Therefore,

$$\sum_{i=0}^{d}(-1)^{d-i}\sigma_i(x_1,\ldots,x_r)S_{d-i}(x_1,\ldots,x_r) = 0 \;\forall\; d \in \{0,\ldots,k-1\} \quad .$$

Using the specific values of the partial assignment for $x_1,\ldots,x_r$, we see moreover that

$$\sum_{i=0}^{d}\sigma_i(x_1,\ldots,x_r)\sigma_{d-i}(x_{r+1},\ldots,x_k) = 0 \;\forall\; d \in \{1,\ldots,k-1\} \quad .$$

Equating these sums for $d=1$ and using the fact that $\sigma_0(x_{r+1},\ldots,x_k) = 1 = S_0(x_1,\ldots,x_r)$ gives

$$(-1)^d\sigma_d(x_1,\ldots,x_r) = S_d(x_{r+1},\ldots,x_k)$$

for the case $d=1$.
Now we increase d by 1 and insert the last equation to yield the same equality for $d=2$, and so on up to $d=k-1$. In total, we conclude

$$\begin{aligned}
S_{k-r}(x_1,\ldots,x_r,x)\cdot\prod_{i=1}^{r}(x-x_i) &= \sum_{d=0}^{k-r}S_d(x_1,\ldots,x_r)x^{k-r-d}\cdot\prod_{i=1}^{r}(x-x_i)\\
&= \sum_{d=0}^{k-r}(-1)^d\sigma_d(x_{r+1},\ldots,x_k)x^{k-r-d}\cdot\prod_{i=1}^{r}(x-x_i)\\
&= \prod_{i=r+1}^{k}(x-x_i)\cdot\prod_{i=1}^{r}(x-x_i)\\
&= \prod_{i=1}^{k}(x-x_i)\\
&= x^k-1 \quad ,
\end{aligned}$$

which is what we claimed. □

7.4 The Algorithm

Our somewhat naive implementation is intuitively understandable: It successively tests vertices for simpliciality (using Algorithm 9) and removes hits in order to obtain a perfect elimination order. At the same time, it adds new polynomials to a set which, at the end, is exactly the Gröbner basis we are looking for.

Algorithm 8 Gröbner basis of a chordal graph

```
Input: Chordal graph G = (V, E), coloring number k
Output: Gröbner basis 𝒢 of size |V|
  function BuildGröbnerBasis(G, k)
      n ← |V|
      G_n ← G
      𝒢 ← {v_n}
      for all i ∈ {n − 1, . . . , 1} do
          for all v ∈ V_{i+1} do
              if IsSimplicial(v) then
                  v_i ← v
                  C_i ← 𝒩(v)
                  G_i ← G_{i+1} − v
                  𝒢 ← 𝒢 ∪ {S_{k−|C_i|}(C_i, v_i)}
                  exit for
              end if
          end for
      end for
      return 𝒢
  end function
```

Algorithm 9 Testing a vertex for simpliciality

```
Input: Graph G = (V, E), vertex v ∈ V
Output: true if v is simplicial in G, else false
  function IsSimplicial(G, v)
      d ← deg(v)
      for all n ∈ 𝒩(v) do
          if |𝒩(v) ∩ 𝒩(n)| < d − 1 then
              return false
          end if
      end for
      return true
  end function
```

7.4.1 Correctness

Lemma 25. Let G be a graph on n vertices, and let $\succ$ be a term order. Let $C = \{c_1, \ldots, c_r\}$ be an r-clique in G, and choose a Gröbner basis $\mathcal{G}$ of $\mathcal{I}_G$. Then, with

$p = S_{k-r}(x_{c_1}, \dots, x_{c_r}, x_{n+1})$,

$$\langle \mathcal{G}, p\rangle = \langle \mathcal{G}, v_{n+1}, e_{c_1,n+1}, \dots, e_{c_r,n+1}\rangle = \mathcal{I}_{G+C} \quad .$$

Proof. We show that $\langle \mathcal{G}, p\rangle$ is a radical ideal, and that both ideals generate the same variety. Then the claim follows from the bijection between varieties and radical ideals.

- Since $p = \prod_{i=r+1}^{k}(x - x_i)$ is square-free, we know that $\langle p\rangle$ is a radical ideal. The same holds for $\langle \mathcal{G}\rangle$ as the coloring ideal of a graph. But then

  $$\mathrm{rad}(\langle \mathcal{G}, p\rangle) = \mathrm{rad}(\langle \mathcal{G}\rangle \cap \langle p\rangle) = \mathrm{rad}(\langle \mathcal{G}\rangle) \cap \mathrm{rad}(\langle p\rangle) = \langle \mathcal{G}\rangle \cap \langle p\rangle = \langle \mathcal{G}, p\rangle$$

  as claimed.

- Let $x = (x_1, \dots, x_{n+1}) \in \langle \mathcal{G}, p\rangle$. By definition, x_{n+1} is a k-th root of unity, and therefore $v_{n+1} = 0$. Moreover, $x_{n+1} \neq x_{c_i} \ \forall\ i \in \{1, \dots, r\}$, which implies that $e_{c_i,n+1} = 0$. In sum, $x \in \mathcal{I}_{G+C}$.

  Let now $x = (x_1, \dots, x_{n+1}) \in \mathcal{I}_{G+C}$. Then the generator polynomials v_{n+1}, $e_{c_1,n+1}$, …, $e_{c_r,n+1}$ ensure that $x_{n+1} \in R_k \setminus \{x_{c_1}, \dots, x_{c_r}\}$, hence $p(x) = 0$ and $x \in \langle \mathcal{G}, p\rangle$.

□

Lemma 26. For every Gröbner basis $\mathcal{G}$ of $\mathcal{I}_G$ with respect to $\succ$, $\mathcal{G} \cup \{p\}$ is a Gröbner basis of $\mathcal{I}_{G+C}$ with respect to an extended term order $\succ'$, where p is again defined as in Lemma 24.

Proof. Lemma 25 shows that $\langle \mathcal{G}, p\rangle = \mathcal{I}_{G+C}$. Hence, it is left to show that all S-polynomials in $\mathcal{G} \cup \{p\}$ reduce to 0. We only have to consider S-pairs that involve the new polynomial p.
By definition of $\succ'$, we have that $\mathrm{LM}_{\succ'}(p) = x_{n+1}^{k-r}$, which is relatively prime to all $g \in \mathcal{G}$, since x_{n+1} does not appear in this basis. Therefore,

$$S(g, p) \to_{\mathcal{G}\cup\{p\}} 0 \quad \forall g \in \mathcal{G}$$

by Lemma 6.
This is sufficient for $\mathcal{G}' := \mathcal{G} \cup \{p\}$ to be a Gröbner Basis. □

Theorem 27. Upon termination of BuildGröbnerBasis(G), the set $\mathcal{G}$ is a Gröbner basis for $\mathcal{I}_G$ under the Lex order, where the vertices are ordered in the perfect elimination order that was established in the algorithm.

Proof. Note that $\{p_1 := v_n\}$ is a Gröbner basis for G_1. By Lemma 26, this basis can be extended in $n-1$ steps by adding p_i as constructed in the algorithm. Therefore, $\mathcal{G} = \{p_1, \dots, p_n\}$ is a Gröbner basis of $G_n = G$ with respect to the extended vertex order, which concludes the proof. □

7.4.2 Complexity of the Resulting Gröbner Basis

As we have seen above, exactly one polynomial is added to $\mathcal{G}$ for every vertex of G. But what is the degree and length of these polynomials?
From the definition of $p := S_k(x_1, \ldots, x_n)$, we see that $\mathrm{len}(p) = \binom{k+n-1}{n-1}$ and $\deg(p) = k$. Therefore, we add polynomials S_i with $\mathrm{len}(S_i) = \binom{k}{|C_i|}$ and $\deg(S_i) = k - |C_i|$. Note that, for a fixed number k of colors, both numbers are polynomials.

7.4.3 Running Time

The function IsSimplicial consists of an outer loop with exactly n iterations, in each of which the intersection of two subsets of V is formed. Such an intersection can be computed in linear time, therefore the function runs in time $\mathcal{O}(n^2)$.
In the main function BuildGröbnerBasis, the two nested **for**-loops are traversed $\mathcal{O}(n)$ times each, and every time IsSimplicial is called. The main part of the **if**-case is the assignment of B. Building the polynomial $S_{k-|C_i|}(C_i, v_i)$ takes $(k-r) \cdot \binom{k}{r}$ steps, which is clearly in $\mathcal{O}(k \cdot k!)$. The remaining statements in the loop have running time $\mathcal{O}(n^2)$.
Putting the pieces together, we obtain a total running time of

$$\mathcal{O}\left(n^2(k \cdot k! + n^2)\right) \quad ,$$

which is polynomial in n for fixed k.

Remark 34. In particular, we get an $\mathcal{O}(n^4)$-algorithm for 3-coloring chordal graphs, and it produces a Gröbner basis with polynomials of length up to $(k-1)(k-1)! = 4$.

It is evident that our implementation is not optimal with respect to running time. For instance, finding a simplicial vertex can be done in linear time (see for example [26]), and there is even a linear-time procedure that establishes a perfect elimination order on G. Nevertheless, our algorithm shows that k-colorability for chordal graph is polynomial-time solvable, and it reproduces the theoretical steps closely enough to be understood in a straight-forward manner.

7.5 The Case of Non-Colorability

What happens in the process of the algorithm if G is not k-colorable? Intuitively, we would expect the constant polynomial 1 to appear somewhere in the set $\mathcal{G}$.
The correctness of this intuition can be shown formally: Assume that $\chi(G) = \chi > k$, and we try to find a Gröbner basis for the k-coloring ideal of G. Since G is chordal, it is also perfect, and thus has a χ-clique $\{v_1, \ldots, v_\chi\}$. We assume without loss of generality that these vertices are ordered ascendingly with respect to the perfect elimination order from the algorithm.
In the step where v_{k+1} is removed from the graph, we have $|\mathcal{N}(v_{k+1}) \cap \{1, \ldots, v_{k+1}-1\}| = k$, and therefore, we add the complete polynomial of degree 0

$$S_{k-k}(x_{v_1}, \ldots, x_{v_k}, x_{v_{k+1}}) = 1 \quad .$$

Hence, BuildGröbnerBasis detects non-colorability on the fly. This observation suggests the following simple improvement on the algorithm: If we find a simplicial vertex of degree $\geq k$, then we can stop immediately and return the trivial Gröbner basis $\mathcal{G} = \{1\}$. On the other hand, we can be sure that if there is no such forbidden vertex, then G is k-colorable.

7.6 Example: Tree Graphs

We want to illustrate our method by 2- and 3-coloring tree graphs. Note that these graphs are trivially chordal, and their maximum cliques have size 1. When deconstructing a tree in a perfect elimination order, we can always pick a leaf, such that the remaining graph is still a tree.

7.6.1 2-Coloring

It is known that trees, as a subclass of bipartite graphs, are 2-colorable and have exactly two distinct 2-colorings. We want to recover this result from the arguments above. Remember that each vertex of a tree T is assigned a square root of unity, that is, either 1 or -1. Since $k = 2$ and $|C_i| = 1$, the polynomials S_i have the form $S_{2-1}(x_i, x_j) = x_i + x_j$. Together with the vertex polynomial $v_n(x) = x_n^2 - 1$, we obtain the Gröbner basis

$$\mathcal{G} = \{x_1 + x_2, x_2 + x_3, \ldots, x_{n-1} + x_n, x_n^2 - 1\} \quad .$$

The 2-colorability of T follows from the fact that none of these polynomials is 1, and the number of proper 2-colorings can be read off the initial ideal of $\mathcal{G}$: The leading terms of elements in $\mathcal{G}$ are x_i, $1 \leq i < n$, and x_n^2. Therefore, the two-element set $\mathcal{B}_T = \{1, x_n\}$ is the set of standard monomials, that is, a basis of $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_T$, and the claim is shown.

7.6.2 3-Coloring

For $k = 3$, we use powers of $\xi := \xi_3 = e^{\frac{2\pi \cdot i}{3}}$ to represent the colors. The S_i now have the pattern $S_{3-1}(x_i, x_j) = x_i^2 + x_i x_j + x_j^2$, which coincides with the edge polynomials $e_{i,j}$. Therefore, the Gröbner basis has the form

$$\mathcal{G} = \{x_1^2 + x_1 x_2 + x_2^2, x_2^2 + x_2 x_3 + x_3^2, \ldots, x_{n-1}^2 + x_{n-1} x_n + x_n^2, x_n^3 - 1\} \quad .$$

As above, 3-colorability is an immediate consequence of the constant polynomial 1 not being part of this set. However, the number of distinct 3-colorings is different: The leading terms of elements in $\mathcal{G}$ are $x_i^2 \ \forall \ i \in \{1, \ldots, n-1\}$ and x_n^3. This gives the basis

$$\mathcal{B}_T = \left\{ x^\alpha : \alpha \in \left(\{0,1\}^{n-1} \times \{0,1,2\} \right) \cap \mathbb{Z}^n \right\}$$

of $\mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}_T$, and the number of colorings is therefore $3 \cdot 2^{n-1}$.

8. CONCLUSIONS, OPEN PROBLEMS AND FUTURE DIRECTIONS

8.1 Counterexamples for Natural Conjectures

8.1.1 Graphs of Small Treewidth

Some combinatorial problems on graphs can be solved using *tree decompositions* of a graph G. The approach is efficient if the decomposition of G has only small vertex sets, that is, if the *treewidth* of G (as defined e.g. in [14], p. 321) is small. This suggests that graph families of constant treewidth have small Gröbner bases, too.
This conjecture is disproved by the cycle graphs C_n, whose treewidth is 2 for all n. An optimal tree decomposition of C_n is given in Figure 8.1.

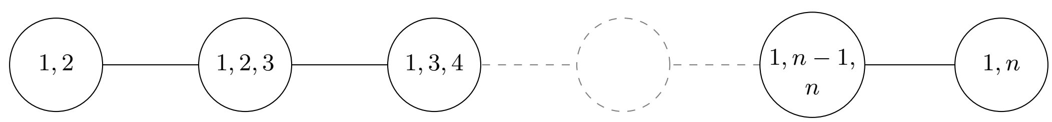


Fig. 8.1: Optimal tree decomposition of C_n

8.1.2 n-sized Bases for Perfect Graphs

It has been shown that many combinatorial problems, among them k-coloring, can be solved in polynomial time not only for chordal graphs, but also for the strictly larger class of perfect graphs (see Section 2.3.2).
Therefore, it is a natural question to ask whether the complexity result about n-sized Gröbner bases which we derived above for chordal graphs can be extended to perfect graphs. Unfortunately, the answer is no, since already even cycles (which are evidently perfect, since their clique number and chromatic number are both 2) reveal rather nasty Gröbner basis structures. Although we cannot show rigorously what the minimal Gröbner basis for a cycle C_{2n} is, computation of the Gröbner fan for small n gives proof that there is no Gröbner basis of size n (see Section 6.8.2). The growth of the support of minimal bases, shown in this section, even leads to the conjecture that there exists no polynomial-time algorithm which computes a (polynomial-size) Gröbner basis for a given perfect graph.

8.1.3 Triangle-Coverable Graphs

Triangles are known to be "nice" substructures in a graph: They both reduce the complexity of Gröbner bases (Section 6.6.1) and the time for their computation (Section 6.6.2). This leads to the conjecture that the Gröbner bases of graphs, whose vertex set can be covered with triangles, show nice properties or have small size. Here, triangle-coverability is defined as the property that every $v \in V$ is part of a triangle, i.e.,

$$\forall\ v \in V\ \exists w_1, w_2 \in \mathcal{N}(v), w_1 \neq w_2 :\ \mathcal{N}(w_1) \cap \mathcal{N}(w_2) \neq \emptyset \quad .$$

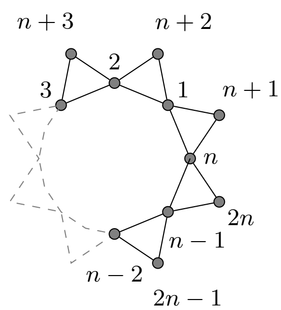


Fig. 8.2: The triangle-coverable sun graph S_{2n}

A counterexample of this assumption is given by a straightforward construction, resulting in so-called *sun graphs* (Figure 8.2): We take an n-cycle and add a triangle to every edge, using the edge as the base. The graph S_{2n}, obtained by this process, has $2n$ vertices and $3n$ edges, and it is clearly covered by the n triangles it contains.
Figure 8.3 shows that the length of the standard bases is only slightly above $2n$, but their support grows fast. We tried to compute the Gröbner fan of S_{2n} for some n, but Macaulay2 runs out of memory already for $n = 5$. Table 8.1 shows the Gröbner fan complexity for S_4, S_6 and S_8.

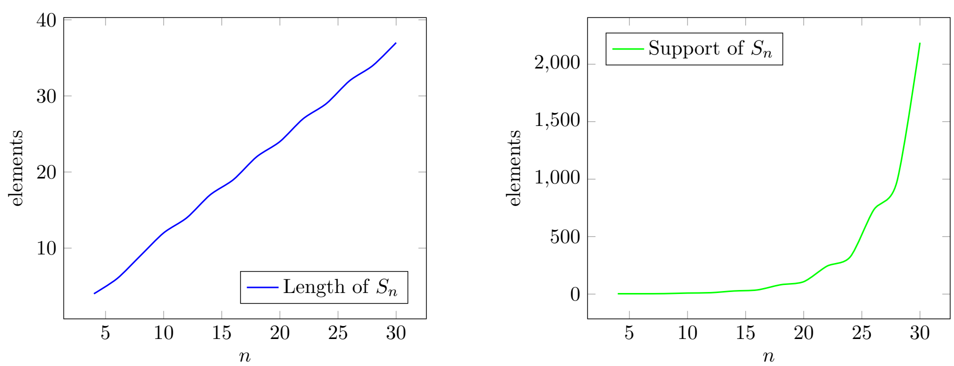


Fig. 8.3: Length and support of the Lex bases of S_n

Tab. 8.1: Complexity measures in the Gröbner fan of S_n

n	4	6	8
Number of bases	6	12	60
Minimal length	3	5	7
Minimal degree	3	3	3
Minimal support	3	4	8
Minimal-length basis	$(3,3,3)$	$(5,3,4)$	$(7,3,8)$

8.2 Open Questions for Future Research

8.2.1 The Power of Standard Bases

In many cases, considering the three standard bases for different vertex orders suffices to show upper and lower bounds on the Gröbner basis complexity of graphs. Moreover, Lex, GLex and GRevLex order only differ in few and unstructured cases throughout our examples.

Do these orders always give best and worst Gröbner bases? The other way round, is there a family of graphs for which the standard orders are not optimal? If so, how can such graphs be found? For which graphs are the standard bases with respect to the same vertex order equal?

8.2.2 Proving All Experimental Results

A large amount of our results are observations and extrapolations of experiments, and in particular complexity statements for infinite families of graphs are not rigorously proven for all $n \in \mathbb{N}$. Exceptions are graphs whose Gröbner bases can completely classified, such that a tentative description of the n-th Gröbner basis can be found and then proved.

Is there a way to prove Gröbner basis complexities, without knowing the specific basis? Does the same hold for Gröbner fans?

8.2.3 Polynomial-Time Algorithms for Larger Classes of Graphs

Can we find an algorithm that computes a Gröbner basis of a given graph in polynomial time, if G comes from a larger class than chordal graphs? If so, what complexity do the resulting bases have?

8.2.4 Minimal Elimination Orders

The key fact for the result in Chapter 7 was the existence of perfect elimination orders for chordal graphs. [15] defines a related concept, which exists for general graphs G: The *minimal elimination order*. It is basically constructed as a perfect elimination order for a chordal graph G' which arises from adding a minimal number of edges to G.

Does a heuristic built on this concept give particularly small Gröbner bases? Can we *give a better bound for the complexity of Gröbner bases by using minimal elimination orders?*

8.2.5 Minimal Support of Gröbner Bases

It is known that a Gröbner basis $\mathcal{G}$ of an ideal I is binomial if and only if I is a binomial ideal. Therefore, I being *not* binomial is a sufficient condition for $\mathfrak{s}(\mathcal{G}) \geq 3$. Since experiments indicate that k-coloring ideals of non-empty graphs are not binomial for all $k \geq 3$, we conjecture:

Conjecture 2. Let $G = (V, E)$ be a k-colorable graph, $k \geq 3$. If $E \neq \emptyset$, then $\mathcal{I}_G$ is *not* a binomial ideal. Therefore, $\mathfrak{s}(\mathcal{G}) \geq 3$ for an arbitrary Gröbner basis $\mathcal{G}$ of G.

Can we prove that?

8.2.6 Fan Complexity Bounds

We have seen in Chapter 6 that the Gröbner fans of some families of graphs have very close lower and upper complexity bounds. For example, all Gröbner bases of the complete tripartite graph $K_{k,m,n}$ have the same complexity pattern $(k + m + n, 3, 3)$. For complete tripartite graphs, this property can in fact be seen by a Theorem in [32] (see Remark 24), since the graphs of this family are uniquely 3-colorable.

Can we give complexity bounds for all Gröbner bases of certain graph families?

8.2.7 Edge Contraction and Deletion

The theory of graph minors, which has been proven an extremely useful tool in graph theory, mainly relies on two operations, performed on a given graph: Edge contraction and edge deletion. These operations can be seen as functions that map a graph to another graph with a slightly different vertex and edge set. Formally, the contraction and deletion operators, $C_{u,v}(G)$ and $D_{u,v}(G)$ for an input graph $G = (V, E)$, are defined as follows:

$$C_{u,v} : \mathbb{G}_n \rightarrow \mathbb{G}_{n-1}, \quad C_{u,v}(G) = (V \setminus \{v\}, E_{u=v})$$

and

$$D_{u,v} : \mathbb{G}_n \rightarrow \mathbb{G}_n, \quad D_{u,v}(G) = (V, E \setminus \{u, v\}) \quad ,$$

where $\mathbb{G}_n$ is the set of all graphs on n vertices.
The significance of these two operators for graph theory, and in particular for the graph coloring problem, is illustrated by the deletion-contraction algorithm (see [31], Chapter 1.3), a recursive procedure that computes the chromatic polynomial (Section 2.4) of a graph using the following identity:

$$P(G, k) = P(D_{u,v}(G), k) - P(C_{u,v}(G), k) \quad \forall \ \{u, v\} \in E \quad .$$

Using the fact that both terms on the right hand side use graphs with fewer vertices or edges, it is easily seen that this recurrence terminates in a set of empty graphs, whose chromatic polynomial can be explicitly stated as $P(\overline{K}_n, k) = k^n$.

It is natural to ask about the connection between Gröbner bases and deletion/contraction: It seems reasonable to assume that a Gröbner basis of a graph G can be deducted from the bases of its transforms $D_{u,v}(G)$ and $C_{u,v}(G)$, taken with respect to the same term order.

Can we formalize this idea, resulting in a recursive formula for Gröbner bases? In particular, how do we deal with the fact that deletion and contraction can change the chromatic number of the graph?

8.2.8 Generalizing Dominant Paths

Our understanding of the phenomenon encountered in Section 6.7.3 is limited to tree graphs and path polynomials. While dominant paths do not necessarily appear in graphs with cycles, there are other substructures which can be found in the Gröbner bases of such graphs, for example cycle, triangle or diamond polynomials. However, based on observations on randomly generated graphs, the emergence of these polynomials seems to depend on different factors and cannot be explained as clearly and simply as the dominant paths. Also, the fact that dominant paths "dominate" other paths and vertices, and in turn are dominated by triangles, suggests that there exists some sort of hierarchy of polynomials which push each other put of a Gröbner basis.

Can we extend this approach to general graphs or at least to some classes of graphs with cycles? Is there a comprehensive theory that exactly explains which polynomials appear in a certain basis, not just based on heuristics? What is the computational effect from adding expected polynomials to the generating system $\mathcal{F}_G$ of a coloring ideal?

BIBLIOGRAPHY

[1] S. Arora, B. Barak. *Computational Complexity: A Modern Approach*, Cambridge University Press, 2009.

[2] K. Appel, W. Haken. *Every Planar Map is Four Colorable*, Illinois Journal of Mathematics 21:429–567, 1977.

[3] P. Bartlett. *Undirected Graphical Models: Chordal Graphs, Decomposable Graphs, Junction Trees, and Factorizations.* Lecture notes (http://www.stat.berkeley.edu/ bartlett/courses/241A-spring2007/graphnotes.pdf), 2003.

[4] C. Berge. *Perfect graphs*, In Six Papers on Graph Theory:1–21. Indian Statistical Institute, Calcutta, 1963.

[5] N. Bourbaki. *Algèbre. Chapitres 4 à 7*, Springer, 2007.

[6] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.* PhD thesis, 1965.

[7] T. Becker, V. Weispfenning. *Gröbner Bases. A Computational Approach to Commutative Algebra*, Springer, 1993.

[8] D. Bayer. *The Division Algorithm and the Hilbert Scheme.* PhD thesis, 1982.

[9] C.-Y. Chao, Z. Chen. *On uniquely 3-colorable graphs*, In Discrete Math. 112, 1–3:21–27, 1993.

[10] D. Cox, J. Little, D. O'Shea. *Using Algebraic Geometry*, Second Edition, Springer, 2005.

[11] D. Cox, J. Little, D. O'Shea. *Ideals, Varieties, and Algorithms*, Third Edition, Springer, 2007.

[12] G. Chartrand, P. Zhang. *Chromatic Graph Theory*, Chapman & Hall, 2008.

[13] E. Dahlhaus. *Minimal elimination ordering for graphs of bounded degree.* Discrete Applied Mathematics 116:127–143, 2002.

[14] R. Diestel. *Graph Theory.* Third Edition, Springer, 2005.

[15] E. Dahlhaus, M. Karpinski. *An Efficient Parallel Algorithm for the Minimal Elimination Ordering (MEO) of an Arbitrary Graph.* In Theor. Comput. Sci. 134:493–528, 1994.

[16] J. De Loera, J. Lee, S. Margulies, S. Onn. *Expressing combinatorial optimization problems by systems of polynomial equations and the nullstellensatz.* Journal of Combinatorics, Probability and Computing, 2008.

[17] J. De Loera, P. Malkin, P. Parrilo. *Computation with Polynomial Equations and Inequalities Arising in Combinatorial Optimization.* Mixed Integer Nonlinear Programming, The IMA Volumes in Mathematics and its Applications 154, 2012.

[18] G.A. Dirac. *On rigid circuit graphs.* 1961.

[19] D. D'souza, P. Shankar. *Modern Applications of Automata Theory.* World Scientific Publishing Co., Inc., 2011.

[20] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Math., vol. 150, Springer-Verlag, 1995.

[21] B. Felszeghy. *Gröbner theory of zero dimensional ideals with a view toward combinatorics.* PhD thesis, 2007.

[22] E.N. Gilbert. *Random Graphs*, The Annals of Mathematical Statistics 30, no. 4:1141–1144, 1959.

[23] M. R. Garey, D. S. Johnson, L. Stockmeyer. *Some simplified $\mathcal{NP}$-complete problems*, In Proceedings of the sixth annual ACM symposium on Theory of computing (STOC '74):47–63, 1974.

[24] V. Guruswami, S. Khanna. *On the Hardness of 4-Coloring a 3-Colorable Graph*, In Proceedings of the 15th Annual IEEE Conference on Computational Complexity (COCO '00). IEEE Computer Society, Washington, DC, USA, 2000.

[25] M. Grötschel, L. Lovasz, A. Schrijver. *Geometric Algorithms and Combinatorial Optimization*, Springer, 1988.

[26] M. Golumbic. *Algorithmic Graph Theory and Perfect Graphs*, Annals of Discrete Mathematics, Vol 57, North-Holland Publishing Co., 2004.

[27] J. Håstad. *Some optimal inapproximability results*, In Proceedings of the twenty-ninth annual ACM symposium on Theory of computing (STOC '97):1–10. ACM, New York, NY, USA, 1997.

[28] S. Hougardy. *Classes of Perfect Graphs*, Discrete Mathematics 306:2529–2571, 2006.

[29] M. Hoechster. *Math 615: Lecture of January 10, 2007*, Lecture notes (http://www.math.lsa.umich.edu/ hochster/615W07/L01.10.pdf), 2007.

[30] A. Hertz, M. Plumettaz, N. Zufferey. *Variable Space Search for Graph Coloring*, Discrete Applied Mathematics, 156(13):2551–2560, 2008.

[31] T. Hubai. *The chromatic polynomial*, Master's Thesis (https://www.cs.elte.hu/blobs/diplomamunkak/mat/2009/hubai_tamas.pdf), 2009.

[32] C. Hillar, T. Windfeldt. *Algebraic characterization of uniquely vertex colorable graphs*, Journal of Combinatorial Theory, Series B 98:400–414, 2008.

[33] S. Khanna, N. Linial, S. Safra. *On the hardness of approximating the chromatic number*, In Proceedings of the 2nd Israel Symposium on Theory and Computing Systems, ISTCS:250–260, IEEE Computer Society Press, 1993.

[34] M. Kreuzer, L. Robbiano. *Computational Commutative Algebra 1*, Springer, 2008.

[35] J. Kleinberg, E. Tardos. *Algorithm Design*. Addison-Wesley Longman Publishing Co., Inc., 2005.

[36] R. Lewis, J. Thompson, C. Mumford, J. Gillard. *A Wide-Ranging Computational Comparison of High-Performance Graph Colouring Algorithms*, Comput. Oper. Res. 39, 9, 2012.

[37] S. Margulies. *Computer Algebra, Combinatorics, and Complexity: Hilbert's Nullstellensatz and $\mathcal{NP}$-complete Problems.* PhD thesis, 2008.

[38] E.W. Mayr, S. Ritscher. *Degree bounds for Gröbner bases of low-dimensional polynomial ideals*, In Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation (ISSAC '10):21–27, New York, 2010.

[39] T. Mora, L. Robbiano. *The Gröbner fan of an ideal*, J. Symb. Comput. 6, 2–3:183–208, 1988.

[40] I. Méndez-Díaz, P. Zabala. *A branch-and-cut algorithm for graph coloring*, Discrete Appl. Math. 154, 5:826–847, 2006.

[41] J. Naor, M. Naor, A. Schaffer. *Fast parallel algorithms for chordal graphs*, In Proceedings of the nineteenth annual ACM symposium on Theory of computing (STOC '87):355–364. ACM, New York, 1987.

[42] A. Ovchinnikov, A. Zobnin. *Classification and Applications of Monomial Orderings and the Properties of Differential Orderings*, Proceedings of the Fifth International Workshop on Computer Algebra in Scientific Computing, Yalta, Ukraine, 2002.

[43] S. Ritschel. *Degree Bounds for Zero-dimensional Gröbner Bases*, Master's Thesis (http://repository.lib.ncsu.edu/ir/bitstream/1840.16/281/1/etd.pdf), 2009.

[44] L. Robbiano. *Term Ordering on the Polynomial Ring*, 1985.