Anna Jellen
Kerstin Maier

Der Nullstellensatz in der Diskreten Mathematik

Proseminararbeit

Alpen-Adria-Universität Klagenfurt
Fakultät für Technische Wissenschaften

Betreuer: Ā̄ssoc.Prof. Dipl.-Ing.Dr. Angelika Wiegele
Institut für Mathematik, Universität Klagenfurt

Sommersemester 2016

Abstract

In dieser Proseminararbeit widmen wir uns dem Hilbert'schen Nullstellensatz, der zu den klassischen Theoremen in der Algebraischen Geometrie zählt. Im Fokus steht die Verwendung des Nullstellensatzes zum Beweisen der Unlösbarkeit von kombinatorischen Optimierungsproblemen, wie zum Beispiel der 3-Färbbarkeit eines Graphen.

Zu Beginn werden wir auf Grundbegriffe aus der Graphentheorie eingehen. Danach wird der Nullstellensatz und seine Anwendungen in der Diskreten Optimierung genauer behandelt. Zum Schluss widmen wir uns noch theoretischen Resultaten und dem Beweis des Nullstellensatzes.

Inhaltsverzeichnis

Nullstellensatz

1 Einleitung

Zu Beginn möchten wir auf einige Grundbegriffe in der Graphentheorie und der (Linearen) Algebra eingehen. Dieses Kapitel soll als Nachschlagewerk für die restlichen Kapitel dieser Arbeit dienen. Hierbei werden auch die Begriffe Stable Set, k-Färbbarkeit und Maximaler Schnitt eingeführt, das Finden solcher graphentheoretischen Probleme fällt in die Klasse der NP-vollständigen Probleme. Des Weiteren werden wir in 2 diese drei Probleme in Polynomialdarstellung bringen, was dazu führt, dass wir den Hilbertschen Nullstellensatz darauf anwenden können. Wir werden in dieser Arbeit auf dieses zentrale Resultat der Algebraischen Geometrie eingehen und zeigen, dass sich daraus ein Algorithmus ableiten lässt, der entscheidet, ob die angegebenen Probleme lösbar oder unlösbar sind.

2 Grundbegriffe

2.1 Grundbegriffe aus der (Linearen) Algebra

Definition 2.1 *Es sei H eine Menge mit einer inneren Verknüpfung $\cdot : H \times H \to H$. Es heißt $(H, \cdot)$ eine Halbgruppe, wenn $\forall a, b, c \in H$ gilt [2]:*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Definition 2.2 *Es sei G eine nichtleere Menge mit einer inneren Verknüpfung $\cdot : G \times G \to G$. Es heißt $(G, \cdot)$ eine Gruppe, wenn $\forall a, b, c \in G$ gilt [2]:*

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. $\exists e \in G$ *mit* $e \cdot a = a = a \cdot e$.
3. $\forall a \in G : \exists a' \in G$ *mit* $a' \cdot a = e = a \cdot a'$.

Definition 2.3 *Es sei R eine Menge mit den inneren Verknüpfung $+ : R \times R \to R$ und $\cdot : R \times R \to R$. Es heißt $(R, +, \cdot)$ ein Ring, wenn $\forall a, b, c \in R$ gilt [2]:*

1. $a + b = b + a$.
2. $a + (b + c) = (a + b) + c$.
3. $\exists 0$ *(Nullelement) in* $R : 0 + a = a \quad \forall a \in R$.
4. $\forall a \in R : \exists -a \in R$ *(inverses Element)* $: a + (-a) = 0$.
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
6. $a(b + c) = ab + ac$ *und* $(a + b)c = ac + bc$.

Definition 2.4 *Es sei K eine Menge mit den inneren Verknüpfung $+ : K \times K \to K$ und $\cdot : K \times K \to K$. Es heißt $(K, +, \cdot)$ ein Körper, wenn $\forall a, b, c \in K$ gilt [2]:*

1. $a + b = b + a$.
2. $a + (b + c) = (a + b) + c$.
3. $\exists 0$ *(Nullelement) in* $K : 0 + a = a \quad \forall a \in K$.

4. $\forall a \in K : \exists -a \in K$ *(inverses Element)* $: a + (-a) = 0$.

5. $ab = ba$.

6. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

7. $\exists 1 \neq 0$ *(Einselement) in* $K : 1a = a \quad \forall a \in K$.

8. $\forall a \in K \backslash \{0\} : \quad \exists a^{-1} \in K$ *(inverses Element)* $: aa^{-1} = 1$.

9. $a(b + c) = ab + ac$ *und* $(a + b)c = ac + bc$.

Definition 2.5 *Es sei*

$$R[X] = \{\sum_{i \in \mathbb{N}_0} a_i X^i | a_i \in R \text{ und} a_i = 0 \text{ für fast alle } i \in \mathbb{N}_0\}$$

ein kommutativer Ring mit Einselement 1.
Man nennt R[X] den Polynomring in der Unbestimmten X über R. [2]

Definition 2.6 *Man nennt $K \subseteq E$ einen Teilkörper von E und E einen Erweiterungskörper von K sowie E/K eine Körpererweiterung, wenn K ein Teilring von E und als solcher ein Körper ist, d.h. wenn gilt[2]:*

$$a, b, c \in K, \quad c \neq 0 \quad \Rightarrow \quad a - b, ab, c^{-1} \in K.$$

Definition 2.7 *Es sei L/K eine Körpererweiterung. Ein Element $a \in L$ heißt:*

- *algebraisch über K, wenn es ein von 0 verschiedenes Polynom $P \in K[X]$ gibt mit $P(a) = 0$.*
- *transzendent über K, wenn es nicht algebraisch ist, d.h. für $P \in K[X]$ gilt $P(a) = 0$ nur für das Nullpolynom $P = 0$. [2]*

Definition 2.8 *Der Körper K heißt algebraisch abgeschlossen, wenn jedes nicht konstante Polynom aus K[X] eine Wurzel in K hat. [2]*

Definition 2.9 *Ein Erweiterungskörper von K wird algebraischer Abschluss von K genannt, wenn er algebraisch über K und algebraisch abgeschlossen ist. [2]*

Definition 2.10 *Sei $F = \{f_1, \ldots, f_m\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ eine Menge von Polynomen. Ein Vector $\overline{x} \in \overline{\mathbb{K}^n}$ ist eine Lösung des Systems $f_1 = f_2 = \ldots = f_k = 0$ $(F = 0)$, wenn $f_i(\overline{x}) = 0 \quad \forall i = 1, \ldots, k$.*
Die Varietät $V(f_1, f_2, \ldots, f_k)$ $(V(F))$ ist die Menge aller Lösungen von $F = 0$ in $\overline{\mathbb{K}^n}$.[5]

Definition 2.11 *Die Menge von Polynomen beschreibt ein Ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$, wenn die folgenden Eigenschaften erfüllt sind [5]:*

1. $0 \in I$
2. $f, g \in I \Rightarrow f + g \in I$
3. $f \in I, g \in \mathbb{K}[x_1, \ldots, x_n] \Rightarrow fg \in I$

Sei $F = \{f_1, \ldots, f_m\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$, dann ist

$$\langle F \rangle = \left\{ f = \sum_{i=1}^{k} h_i f_i : \quad f_i \in F, h_i \in \mathbb{K}[x_1, \ldots, x_n] \quad \forall i = 1, \ldots, k \right\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$$

das polynomielle Ideal erzeugt von F in $\mathbb{K}[x_1, \ldots, x_n]$.

2.2 Grundbegriffe der Graphentheorie

Definition 2.12 *Ein Graph G ist ein Paar $G = (V,E)$ disjunkter Mengen mit $E \subseteq V \times V$. Die Elemente von V nennt man Knoten und die Elemente von E Kanten. [1]*

Definition 2.13 *Zwei Knoten $x, y \in V(G)$ sind adjazent in G und heißen Nachbarn von einander, wenn $xy \in E(G)$. [1]*

2.2.1 Stable Set

Definition 2.14 *Paarweise nicht benachbarte Knoten oder Kanten nennt man unabhängig. Eine Teilmenge von V oder E heißt unabhängig, wenn ihre Elemente paarweise nicht benachbart sind. Unabhängige Knotenmengen nennt man auch stabil. [1]*

Definition 2.15 *Ein Stable Set ist eine unabhängige Knotenmenge.*

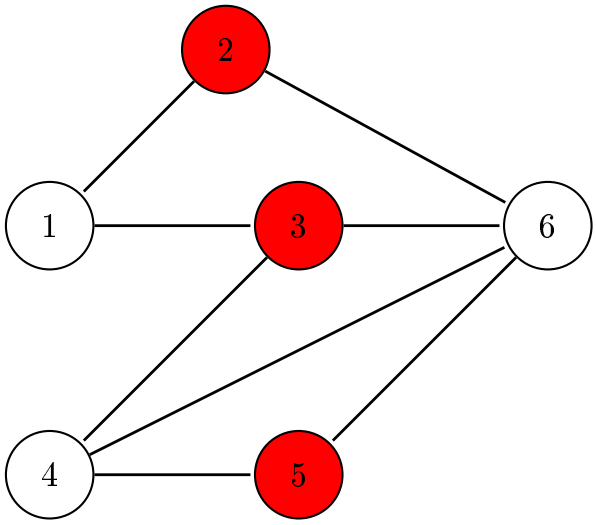

Abbildung 1: Stable Set

2.2.2 k-Färbbarkeit

Definition 2.16 *Die k-Färbung eines Graphen ist eine Abbildung $f : V(G) \to S$ mit $xy \in E(G) : f(x) \neq f(y)$, wobei S Menge der Farben und $|S| = k$. [1, 6]*

2.2.3 Maximaler Schnitt

Definition 2.17 *Eine Menge $\mathcal{A} = \{A_1, \ldots, A_k\}$ disjunkter Teilmengen einer Menge A ist eine Partition von A, wenn $\bigcup \mathcal{A} := \bigcup_{i=1}^{k} A_i = A$ ist und $A_i \neq \emptyset \quad \forall i$. [1]*

Definition 2.18 *Ist V_1, V_2 eine Partition von V, so nennen wir die Menge $E(V_1, V_2)$ aller dieser Partitionen verbindenden Kanten von G einen Schnitt. [1]*

Definition 2.19 *Ein Maximaler Schnitt ist jener Schnitt $F \neq \emptyset$, wo die Summe der Gewichte der verbindenden Kanten maximal ist.*

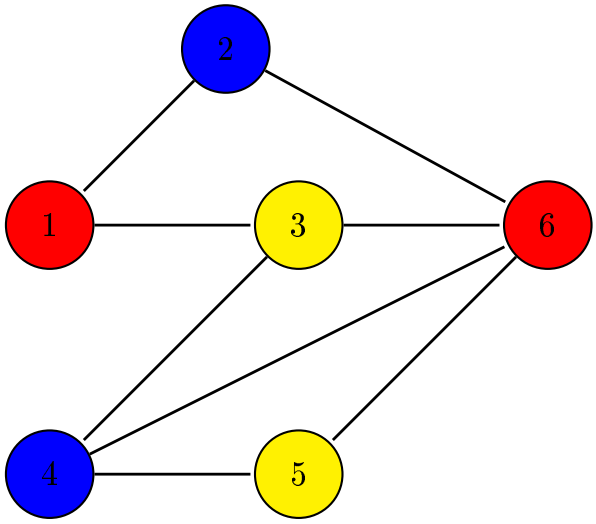

Abbildung 2: 3-Färbung

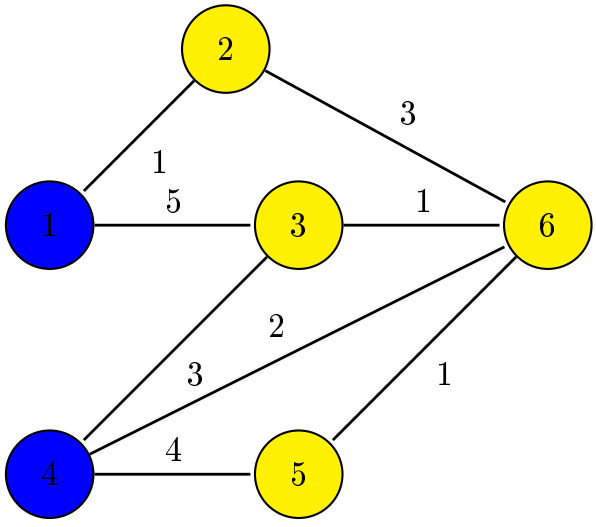

Abbildung 3: Maximaler Schnitt

2.3 Polynomdarstellung kombinatorischer Probleme

2.3.1 Stable Set

Sei $G = (V, E)$ ein Graph. Für ein gegebenes $k \in \mathbb{N}$ betrachten wir folgendes polynomielles System:

$$\begin{aligned} x_i^2 - x_i &= 0 \quad \forall i \in V, \\ x_i x_j &= 0 \quad \forall (i,j) \in E, \\ \sum_{i \in V} x_i &= k. \end{aligned}$$

Dieses System ist genau dann lösbar, wenn G ein Stable Set der Größe k besitzt.

2.3.2 k-Färbbarkeit

Sei $G = (V, E)$ ein Graph. Für ein gegebenes $k \in \mathbb{N}$ betrachten wir folgendes polynomielles System mit $|V| + |E|$ Gleichungen:

$$\begin{aligned} x_i^k - 1 &= 0 \quad \forall i \in V, \\ \sum_{s=0}^{k-1} x_i^{k-1-s} x_j^s &= 0 \quad \forall (i,j) \in E. \end{aligned}$$

Der Graph G ist genau dann k-färbbar, wenn dieses System eine komplexe Lösung besitzt. Des Weiteren gilt, wenn k ungerade , dann ist G genau dann k-färbbar, wenn das System eine Lösung über $\overline{\mathbb{F}_2}$ besitzt. $\overline{\mathbb{F}_2}$ ist der algebraische Abschluss über dem endlichen Körper mit zwei Elementen.

Beweis. Angenommen die Aussage ist wahr über den komplexen Zahlen $\mathbb{C}$.
„ $\Rightarrow$ “ Sei G k-färbbar, ordne jeder Farbe die k-te Einheitswurzel zu. Sei die j-te Farbe $\beta_j = e^{2\Pi j/k}$; substituiere alle x_l mit der zugehörigen Einheitswurzel der Farbe des l-ten Knotens.
Also haben wir eine Lösung des Systems: Die Gleichungen $x_i^k - 1 = 0$ sind trivialerweise erfüllt.
Wir betrachten nun die Kantengleichungen: Wir nehmen eine Kante ij, da x_i und x_j durch Einheitswurzeln substituiert wurden, gilt $x_i^k - x_j^k = 0$. Des Weiteren gilt:

$$x_i^k - x_j^k = (x_i - x_j)(x_i^{k-1} + x_i^{k-2} x_j + x_i^{k-3} x_j^2 + \ldots + x_j^{k-1}) = 0;$$

Durch die Substitution mit unterschiedlichen Einheitswurzeln gilt $x_i - x_j \neq 0$, also muss der andere Faktor, der den Kantengleichungen entspricht, 0 sein.
„ $\Leftarrow$ “ Angenommen die Gleichungen seien erfüllt, d.h. der Lösungspunkt muss aus k-ten Einheitswurzeln bestehen. Den benachbarten Knoten müssen verschiedene Einheitswurzeln zugeordnet werden, da:
Angenommen einem Paar benachbarter Knoten ij wird die selbe Einheitswurzel zugewiesen. Die Gleichung $x_i^{k-1} + x_i^{k-2} x_j + x_i^{k-3} x_j^2 + \ldots + x_j^{k-1} = 0$ wird dann zu $\beta^{k-1} + \beta^{k-1} + \ldots + \beta^{k-1} = k\beta^{k-1} = 0$, jedoch $\beta \neq 0$↯ Es verbleibt zu zeigen, dass das gleiche Argument wie wir oben über die komplexen Zahlen gezeigt haben, auch für $\overline{\mathbb{F}_2}$ gilt. Obwohl $x_i^k - 1$ nur eine Nullstelle über $\mathbb{F}_2$ besitzt, nämlich 1, erhält man über $\overline{\mathbb{F}_2}$ verschiedene Nullstellen $1, \beta_i, \ldots, \beta_{k-1}$ (in diesem Fall keine komplexen Zahlen). Damit gilt das gleiche Argument wie oben. Wir müssen nur bei der Rückrichtung aufpassen, da $k\beta_i^{k-1} \neq 0$ sein muss. Diese Bedingung ist jedoch erfüllt, da k ungerade und durch die Konstruktion β_i^k. □

2.3.3 Maximaler Schnitt

Sei $G = (V, E)$ ein Graph. Wir können die Menge der Schnitte SG von G als 0-1 Inzidenzvektoren darstellen.

$$SG := \{\mathcal{X}^F : F \subseteq E \, ist \, in \, einem \, Schnitt \, von \, G \, enthalten\} \subseteq \{0,1\}^{|E|}.$$

Somit kann der Maximale Schnitt mit den Kantengewichten $w_e \in \mathbb{R}^+$ und $e \in E(G)$ folgend definiert werden:

$$\max\{\sum_{e \in E(G)} w_e x_e : x \in SG\}.$$

Die Vektoren $\mathcal{X}^F$ sind Lösungen des polynomiellen Systems

$$\begin{aligned} x_e^2 - x_e = 0 \quad & \forall e \in E(G), \\ \prod_{e \in T \cap E(G)} x_e = 0 \quad & \forall T \, ungerader \, Kreis \, in \, G \end{aligned}$$

3 Hilberts Nullstellensatz

Zunächst möchten wir auf die allgemeine Problemdarstellung eingehen.
Gegeben: $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$
Gesucht: Lösung x für das System $f_1(x) = 0, f_2(x) = 0, \ldots f_m(x) = 0$ (wird auch geschrieben als $F(x) = 0$)
Ziel ist es eine Lösung zu diesem System zu finden beziehungsweise zu zeigen, dass es keine Lösung gibt.

Bevor wir nun das Theorem für den Hilbertschen Nullstellensatz einführen, möchten wir noch das Fredholm's Alternativtheorem betrachten.

Theorem 3.1 (Fredholm's Alternativtheorem) *Das Lineare Gleichungssystem (LGS) $Ax = b$ besitzt genau dann eine Lösung, wenn ein Vektor y mit der Eigenschaft $y^T A = 0^T$ und $y^T b \neq 0^T$ existiert.*

Der Hilbertsche Nullstellensatz stellt eine strengere und weitreichendere Verallgemeinerung für nichtlineare Polynomialgleichungen dar.

Theorem 3.2 (Hilbert's Nullstellensatz) *Sei $F = \{f_1, \ldots, f_m\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$.*
Die Varietät $\{x \in \overline{\mathbb{K}^n} : f_1(x) = 0, \ldots, f_s(x) = 0\}$ ist genau dann leer, wenn 1 zum Ideal $\langle F \rangle$, das aus F generiert wurde, gehört. Man beachte $1 \in \langle F \rangle$ bedeutet, dass Polynome $\beta_1, \ldots, \beta_m$ im Ring $\mathbb{K}[x_1, \ldots, x_n]$ existieren, sodass $1 = \sum_{i=1}^m \beta_i f_i$. Diese polynomielle Identität ist ein Zertifikat für die Unlösbarkeit von $F(x) = 0$.

Wir können leicht erkennen, dass das Fredholm's Theorem eine lineare Variante des Hilbertschen Nullstellensatzes mit linearen Polynomen und Konstanten β_i's ist.

3.1 Relaxierungen mit Hilfe der Linearen Algebra

Die Hauptidee besteht darin, das gegebene System in eine Reihe Probleme der Linearen Algebra zu relaxieren und dann diese linearen Probleme zu lösen.
Aus dem Hilbertschen Nullstellensatz lässt sich folgendes Korollar ableiten:

Korollar 3.1 *Falls numerische Vektoren $\mu \in \mathbb{K}^m$ existieren, sodass $\sum_{i=1}^m \mu_i f_i = 1 \Rightarrow$ das polynomielle System $F(x) = 0$ ist unlösbar.*

Das Entscheiden, ob ein $\mu \in \mathbb{K}^m$ existiert, sodass $\sum_{i=1}^{m} \mu_i f_i = 1$ ist nur mehr ein Problem der Linearen Algebra über dem Körper $\mathbb{K}$.
Es herrscht ein starker Zusammenspiel zwischen dem System der nichtlinearen Gleichungen $F(x) = 0$, dem Ideal $\langle F \rangle$ und der Linearen Hülle von F über $\mathbb{K}$.

definieren in den Grundbegriffen

Im Folgenden möchten wir auf ein Beispiel eingehen, dass uns zeigt, dass wir nicht immer Unlösbarkeit gezeigt werden kann, auch wenn das System tatsächlich unlösbar ist.

Beispiel 3.1 *Wir betrachten folgende Menge von Polynomen:*

$$F := \{f_1 := x_1^2 - 1, f_2 := 2x_1x_2 + x_3, f_3 := x_1 + x_2, f_4 := x_1 + x_3\}$$

Wir können zeigen, dass das System $F(x) = 0$ unlösbar ist, falls wir ein $\mu \in \mathbb{R}^4$ finden, das die folgende Bedingung erfüllt:

$$\begin{aligned} & \mu_1 f_1 + \mu_2 f_2 + \mu_3 f_3 + \mu_4 f_4 = 1 \\ \Leftrightarrow \quad & \mu_1(x_1^2 - 1) + \mu_2(2x_1x_2 + x_3) + \mu_3(x_1 + x_2) + \mu_4(x_1 + x_3) = 1 \\ \Leftrightarrow \quad & \mu_1 x_1^2 + 2\mu_2 x_1 x_2 + (\mu_2 + \mu_4)x_3 + \mu_3 x_2 + (\mu_3 + \mu_4)x_1 - \mu_1 = 1 \end{aligned}$$

Mit Hilfe von Koeffizientenvergleich erhalten wir das folgende LGS:

$$\begin{array}{lll} -\mu_1 = 1 & \mu_3 + \mu_4 = 0 & \mu_3 = 0 \\ \mu_2 + \mu_4 = 0 & 2\mu_2 = 0 & \mu_1 = 0 \end{array}$$

$F(x) = 0$ ist zwar nicht lösbar, aber da wir für das obere System auch keine Lösung finden, gibt es somit auch keinen Beweis für die Unlösbarkeit von F(x).

Um die Anwendung zu vereinfachen, führen wir nun eine Matrixschreibweise ein. Wir konstruieren die Matrix M_F, wobei die Spalten die Monome und die Zeilen die Polynome des Systems F repräsentieren. Die Einträge der Matrix entsprechen somit den Koeffizienten der Monome des zugehörigen Polynoms. Wir definieren den Vektor $\mu := (\mu_1, \mu_2, \ldots, \mu_m)$ und den Vektor $(\mathbf{0}, 1)^T := (0, \ldots, 0, 1)^T$ mit genau der Anzahl der Monome an Einträgen. Wir können nun das LGS als $\mu M_F = (\mathbf{0}, 1)^T$ schreiben.

Anmerkung 3.1 *Im Fall, dass $F(x) = 0$ ein LGS ist, können wir das Theorem 3.1 anwenden:*

$$F(x) = 0 \text{ unlösbar} \Leftrightarrow \mu M_F = (\boldsymbol{0}, 1)^T \text{ ist lösbar}$$

4 Algorithmus Nullstellensatz in der Linaren Algebra (NulLa)

5 Vergleich mit anderen Algorithmen zur 3-Färbbarkeit

6 Beweis Nullstellensatz

Abbildungsverzeichnis

Literatur

[1] R. Diestel. *Graphentheorie*. Springer, 2006.

[2] C. Karpfinger and K. Meyberg. *Algebra. Gruppen - Ringe - Körper*. Springer, 2013.

[3] J. a. Loera, J. Lee, S. Margulies, and S. Onn. Expressing combinatorial problems by systems of polynomial equations and hilbert's nullstellensatz. *Comb. Probab. Comput.*, 18(4):551–582, 2009. ISSN 0963-5483.

[4] J. a. Loera, J. Lee, P. N. Malkin, and S. Margulies. Computing infeasibility certificates for combinatorial problems through hilbert's nullstellensatz. *Journal of Symbolic Computation*, 2011.

[5] J. a. Loera, J. Lee, R. Hemmecke, and M. Köppe. *Algebraic and Geometric Ideas in the Theory of Discrete Optimization*. Society for Industriell and Applied Mathematics, 2013.

[6] D. B. West. *Introduction to Graph Theory*. Prentice Hall, 2001.