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 graphentheoretischer 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 Nullstelle 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 Komplexitätstheorie

Definition 2.12 *Eine Turning-Maschine ist gegeben durch ein 7-Tupel* $M = (Z, \Sigma, \Gamma, \delta, z_0, \square, E)$.

- Z *die endliche Zustandsmenge,*
- Σ *das Eingabeband,*
- $\Sigma \subset \Gamma$ *das Arbeitsalphabet,*
- $\delta : Z \times \Gamma \to Z \times \Gamma \times \{L, R, N\}$ *die Überführungsfunktion,*
- $z_0 \in Z$ *der Startzustand,*
- $\square \in \Gamma - \Sigma$ *das Blank-Zeichen und*
- $E \subseteq Z$ *die Menge der Endzustände.*

Definition 2.13 *P ist die Klasse der Entscheidungsprobleme, die in polynomieller Zeit durch eine Turing-Maschine entscheidbar sind.*

Definition 2.14 *NP ist die Klasse der Entscheidungsprobleme, die in polynomieller Zeit durch eine nichtdeterministische Turing-Maschine entscheidbar sind, so dass:*

- *wenigstens ein Berechnungspfad akzeptiert wird, wenn die Antwort „ja“ ist und*
- *kein Berechnungspfad akzeptiert wird, wenn die Antwort „nein“ ist.*

Definition 2.15 *Die Klasse #P besteht aus Funktionen f, so dass für eine polynomiell-zeitbeschränkte nichtdeterministische Turing-Maschine M, f(x) ist die Anzahl akzeptierender Berechnungen von M(x) ist.*

2.3 Grundbegriffe der Graphentheorie

Definition 2.16 *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 2.17 *Zwei Knoten* $x, y \in V(G)$ *sind adjazent in G und heißen Nachbarn von einander, wenn* $xy \in E(G)$. *[1]*

Stable Set

Definition 2.18 *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 2.19 *Ein Stable Set ist eine unabhängige Knotenmenge.* $\alpha(G)$ *ist die maximale Größe eines Stable Sets vom Graph G.*

k-Färbbarkeit

Definition 2.20 *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]*

chromatische Zahl

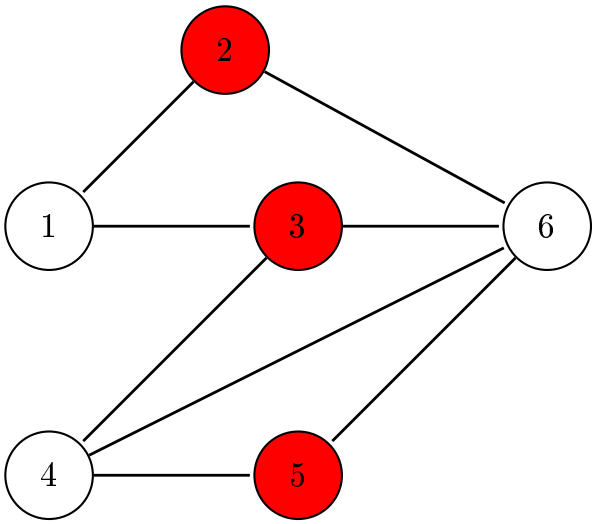

Abbildung 1: Stable Set

Maximaler Schnitt

Definition 2.21 *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 2.22 *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 2.23 *Ein Maximaler Schnitt ist jener Schnitt $F \neq \emptyset$, wo die Summe der Gewichte der verbindenden Kanten maximal ist.*

2.4 Polynomdarstellung kombinatorischer Probleme

Stable Set

Lemma 2.1 *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.

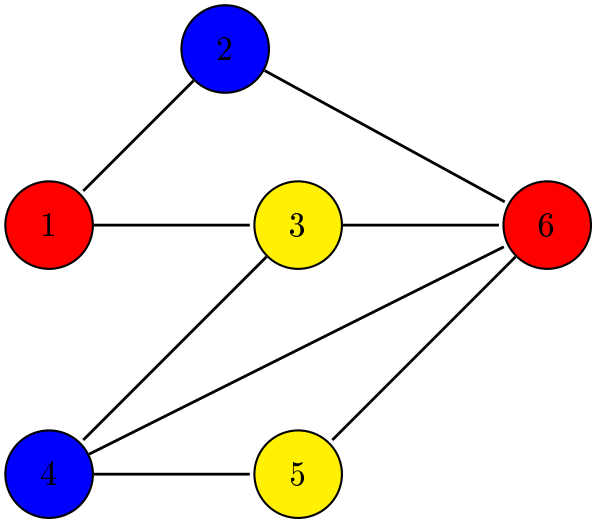

Abbildung 2: 3-Färbung

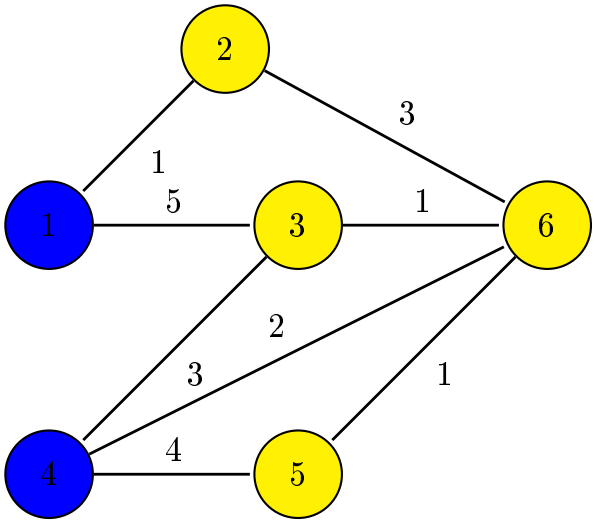

Abbildung 3: Maximaler Schnitt

k-Färbbarkeit

Lemma 2.2 *Sei $G = (V, E)$ ein Graph. Für ein gegebenes $k \in \mathbb{N}$ betrachten wir folgendes polynomielles System mit $|V| + |E|$ Gleichungen:*

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

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. □

Maximaler Schnitt

Lemma 2.3 *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

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

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 Nachweis 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 starkes 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:*

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

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:

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

$F(x) = 0$ 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:*

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

Beispiel 3.2 *Die Matrix M_F zum Beispiel 3.1 sieht folgendermaßen aus:*

$$M_F := \begin{array}{c} \\ \mu_1 \\ \mu_2 \\ \mu_3 \\ \mu_4 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x_1 & x_2 & x_3 & x_1x_2 & x_1^2 \end{array} \\ \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

Leider, wie wir bereits im Beispiel 3.1 gesehen haben, können wir keine Aussage über die Lösbarkeit von $F(x) = 0$ treffen, wenn $\mu M_F = (\mathbf{0}, 1)^T$ unlösbar. Es besteht jedoch weiterhin die Möglichkeit, auf die Unlösbarkeit von $F(x) = 0$ zu kommen. Der Hilbertsche Nullstellensatz sagt aus, dass durch eine Erweiterung von F durch Polynome vom Ideal von F, das System $\mu M_F = (\mathbf{0}, 1)^T$ lösbar werden kann. Dies erkennt man anhand folgendem Beispiel:

Beispiel 3.3 *Das erweiterte System für F aus dem Beispiel 3.1 könnte folgendermaßen aussehen:*

$$F' = \{f_1, f_2, f_3, f_4, x_2f_1, x_1f_2, x_1f_3, x_1f_4\}$$

Das neue lineare System lässt sich nach dem Koeffizientenvergleich darstellen als:

$$\begin{array}{rrr} -\mu_1 = 1 & \mu_3 + \mu_4 = 0 & \mu_3 - \mu_5 = 0 \\ \mu_2 + \mu_4 = 0 & 2\mu_2 + \mu_7 = 0 & \mu_1 + \mu_7 + \mu_8 = 0 \\ \mu_6 + \mu_8 = 0 & \mu_5 + 2\mu_6 = 0 & \end{array}$$

Da dieses System die Lösung $\mu = (-1, -\frac{2}{3}, -\frac{2}{3}, \frac{2}{3}, -\frac{2}{3}, \frac{1}{3}, \frac{4}{3}, -\frac{1}{3})$ *besitzt, können wir folgern, dass das nichtlineare System* $F(x) = 0$ *unlösbar ist.*

4 Algorithmus Nullstellensatz in der Linearen Algebra (NulLa)

Im Folgenden stellen wir einen Algorithmus vor, welcher entscheidet, ob $F(x) = 0$ eine Lösung in $\overline{\mathbb{K}}$ besitzt oder nicht. Die Grundidee des Algorithmus liegt darin, dass überprüft wird, ob $\mu M_F = (\mathbf{0}, 1)^T$ lösbar ist. Das ist genau dann der Fall, wenn $1 \in span_{\mathbb{K}}(F)$. Falls das System nicht lösbar ist wird F mit Polynomen aus $\langle F \rangle$, der Form $x_i f$ für alle x_i und für alle $f \in F$, erweitert und erneut überprüft. Aufgrund der Resultate des Nullstellensatzes wissen wir, dass der Algorithmus terminieren muss, wenn $F(x) = 0$ unlösbar ist. Außerdem erhalten wir auch eine obere Schranke D: Wenn $F(x) = 0$ ist unlösbar, dann wissen wir, dass ein Polynom existiert für das folgendes gilt:

$$\sum_i \beta_i f_i = 1, \qquad deg(\beta_i) \leq D$$

Daraus folgt, dass dieses Polynom einen Maximalgrad von $deg(F) + D$ besitzt.
Das nachfolgende Lemma wird zeigen, dass dieses D eine obere Schranke der Iterationen für unseren Algorithmus bildet.

Lemma 4.1 *Sei* $\mathbb{K}$ *ein Körper und* $f_1, \ldots, f_k$ *Polynome aus* $\mathbb{K}[x_1, \ldots, x_n]$ *mit Graden* $d_1 \geq d_2 \geq \ldots \geq d_k \geq 2$. *Falls diese Polynome keine gemeinsame Nullstelle über* $\overline{\mathbb{K}}$ *besitzen, dann existieren* $g_1, \ldots, g_k$ *in* $\mathbb{K}[x_1, \ldots, x_n]$, *sodass* $\sum_{i=1}^{k} g_i f_i = 1, deg(g_i f_i) \leq D$. D *setzt sich wie folgt zusammen:*

$$D = \begin{cases} d_1 \cdots d_k, & \text{falls } k \leq n, \\ d_1 \cdots d_{n-1} d_k, & \text{falls } k > n > 1, \\ d_1 + d_k - 1, & \text{falls } k > n = 1 \end{cases} \tag{1}$$

Diese Abschätzung für D *gilt für beliebige Polynome.*

Mithilfe des obigen Lemmas können wir nun unseren Algorithmus folgend aufschreiben:

Algorithm 1: NulLA Algorithmus

```
1 function NulLA (F, D);
  Input  : Eine endliche Ausgangsmenge von Polynomen F ⊆ K[x_1, ..., x_n] und die maximale
           Anzahl an Iterationen D
  Output: LÖSBAR, wenn F(x) = 0 ist lösbar über K̄, sonst KEINE LÖSUNG
2 for k = 0, 1, ..., D do
3 |  if 1 ∈ span_K(F) then
4 |  |  return KEINE LÖSUNG;
5 |  else
6 |  |  return Ersetze span_K(F) durch (span_K(F))^+ (hinzufügen der Polynome x_i F zur Menge F);
7 |  end
8 end
9 return LÖSBAR
```

Falls $F(x) = 0$ unlösbar, findet der Algorithmus einen Nachweis dafür nach höchstens D Iterationen.
Die tatsächliche Anzahl an Iterationen r, die der Algorithmus benötigt, definieren wir nun als Rang von NulLA. Für ein unlösbares System $F(x) = 0$ ergibt sich nun ein Nachweis $\sum_i \beta_i f_i = 1$ vom Grad $r + deg(F)$. Allerdings sehen wir durch Lemma 4.1, dass die Schranke D exponentielles Wachstum aufweist. Bessere Schranken existieren jedoch für bestimmte kombinatorische Problemstellungen, wie z.B. auch jene, die wir

im Abschnitt 2.4 vorgestellt haben. Anhand des folgenden Korollars sehen wir, dass für diese Probleme eine merkbar bessere Schranke gegenüber der Exponentiellen aus 4.1 erhalten.

Korollar 4.1 *Für gegebene Polynome $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, wobei $\mathbb{K}$ ein algebraisch abgeschlossener Körper ist und $d = \max\{deg(f_i)\}$, falls $f_1, \ldots, f_s$ keine gemeinsame Nullstelle besitzen (auch nicht im Unendlichen), dann gilt $1 = \sum_{i=1}^{s} \beta_i f_i$ mit $deg(\beta_i) \leq n(d-1)$.*

Dadurch erhalten wir eine obere Schranke von $2n$ bzw. n für das 3-Färbbarkeitsproblem bzw. Stable Set-Problem.

Das folgende Lemma trifft eine Aussage über die Laufzeit des Algorithmus:

Lemma 4.2 *Sei $d \in \mathbb{Z}_+$ fix und $F = \{f_1, \ldots, f_m\}$ eine Menge von Polynomen aus $\mathbb{K}[x_1, \ldots, x_n]$. Wenn die Bedingungen von NulLA erfüllt sind, dann gilt: Die ersten d Iterationen können in polynomieller Zeit der Größe des Inputs F durchgeführt werden.*

Obwohl wir nun theoretisch eine polynomielle Laufzeit des Algorithmus gezeigt haben, kann es trotzdem noch Probleme in der praktischen Umsetzung geben. Dies liegt im schnellen Wachstum der Matrizen, die die linearen Systeme repräsentieren, von $O(n^n)$. Glücklicherweise gibt es praktische Resultate, die zeigen, dass das Wachstum des Rangs von NulLA für das Färbbarkeitsproblem oft sehr langsam ist. Dadurch können wir den Algorithmus auch auf große Graphen anwenden, wie wir im folgenden Kapitel sehen werden. [5]

4.1 3-Färbbarkeit und NulLA

In diesem Kapitel werden wir unseren Algorithmus verwenden, um zu zeigen, dass ein Graph nicht 3-färbbar ist. Wie wir bereits mit Hilfe des Lemmas 2.2 gezeigt haben, ist ein Graph genau dann 3-färbbar, wenn das folgende System eine Lösung über $\overline{\mathbb{F}_2}$ besitzt:

$$\begin{aligned} x_i^3 + 1 &= 0, \qquad \forall i \in V(G) \\ x_i^2 + x_i x_j + x_j^2 &= 0, \qquad \forall i, j \in E(G) \end{aligned} \tag{$*$}$$

Nun können wir ein Korollar zur nicht 3-Färbbarkeit aufstellen.

Korollar 4.2 *Ein Graph ist nicht 3-färbbar $\Leftrightarrow \sum_i \beta_i f_i = 1$, für $\beta_i \in \mathbb{F}_2[x_1, \ldots, x_n]$ und $f_i \in \mathbb{F}_2[x_1, \ldots, x_n]$ wie in Lemma 2.2 definiert.*

Dieses Korollar ermöglicht uns das Operieren über dem Körper $\mathbb{F}_2$, was für praktische Anwendungen sehr zeiteffizient ist. [4]

Jedoch ist dies nicht für alle Graphen möglich, die nicht 3-Färbbarkeit in angemessener Zeit zu bestimmen, was uns das folgende Lemma zeigt [3]:

Lemma 4.3 *Angenommen $P \neq NP$, dann muss es eine unendlich große Menge von Graphen geben, für welche der Grad des Polynoms zum Nachweis der nicht 3-Färbbarkeit in Abhängigkeit der Anzahl der Knoten und Kanten im Graphen unendlich anwachsen kann.*

Die nächsten Resultate zeigen uns, für welche Graphen es möglich ist, einen Nachweis für nicht 3-Färbbarkeit mit NulLA und $D = 1$ zu erbringen.

Definition 4.1 *Der NulLa kann einen Nachweis der Unlösbarkeit für $(*)$ innerhalb der Schranke $D = 1$ erbringen, genau dann wenn Koeffizienten $a_i, a_{ij}, b_{ij}, b_{ijk} \in \mathbb{F}$ existieren, sodass:*

$$\sum_{i \in V} \left(a_i + \sum_{j \in V} a_{ij} x_j \right) (x_i^3 + 1) + \sum_{\{i,j\} \in E} \left(b_{ij} + \sum_{k \in V} b_{ijk} x_k \right) (x_i^2 + x_i x_j + x_j^2) = 1$$

Nun kommen wir zur kombinatorischen Beschreibung unseres Problems. Wir gehen von einem einfachen ungerichteten Graphen $G = (V, E)$ aus. Nun sei $Arcs(G)$ die Menge die für jede ungerichteten Kante $\{i, j\} \in E(G)$ zwei gerichtete Kanten $(i, j), (j, i)$ enthält:

$$Arcs(G) = \{(i, j) : i, j \in V(G), und \{i, j\} \in E(G)\}.$$

Mit Hilfe dieser Menge können wir nun zwei Strukturen für Teilgraphen definieren.

Definition 4.2 *1.* ***orientiertes partielles Dreieck:***
Gegeben: $\{(i, j), (j, k)\} \subseteq Arcs(G)$ *und auch* $(k, i) \in Arcs(G)$. *Dies induziert einen Kreis der Länge 3 in G, deshalb schreiben wir auch* (i, j, k).

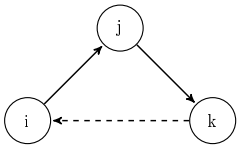

Abbildung 4: orientiertes partielles Dreieck

2. ***orientiertes ? Viereck:***
Gegeben: $\{(i, j), (j, k), (k, l), (l, i)\} \subseteq Arcs(G)$ *und* $(i, k), (j, l) \notin Arcs(G)$. *Dies induziert einen Kreis der Länge 4 in G, deshalb schreiben wir auch* (i, j, k, l).

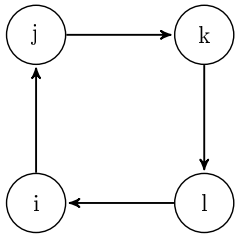

Abbildung 5: orientiertes Viereck

3. ***ungerades Rad:***
Gegeben: Knoten $1, \ldots, n($ $n \in \mathbb{N}_G)$, *wobei Knoten 1 adjazent zu allen anderen Knoten ist und Knoten* $i = 2, \ldots, n$ *adjazent zu Knoten* $1, i - 1, i + 1$.

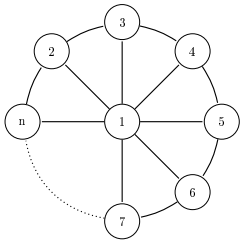

Abbildung 6: ungerades Rad

Theorem 4.1 *Für einen einfachen ungerichteten Graph* $G = (V, E)$ *sind folgende Aussagen äquivalent:*

1. *Für folgendes polynomielle System über $\mathbb{F}_2$ bringt NulLA einen Nachweis für die nicht 3-Färbbarkeit in D=1*

$$J_G = \{x_i^3 + 1 = 0, x_i^2 + x_i x_j + x_j^2 = 0 : i \in V(G), \{i,j\} \in E(G)\}$$

2. *Es existiert eine Menge C von orientierten partiellen Dreiecken und orientierten ? Vierecken aus $Arcs(G)$, sodass*

   a) $\left|C_{(i,j)}\right| + \left|C_{(j,i)}\right| \equiv 0 \mod 2 \quad \forall \{i,j\} \in E$

   b) $\sum_{(i,j) \in Arcs(G), i<j} \left|C_{(i,j)}\right| \equiv 1 \mod 2$

   wobei $C_{(i,j)}$ die Menge der Kreise in C, welche $(i,j) \in Arcs(G)$ enthalten, beschreibt.

Solche Graphen sind nicht 3-färbbar und dies kann in polynomieller Zeit bestimmt werden

In diesem Theorem stellt C eine Kantenüberdeckung mit gerichteten Kanten vom ungerichteten Graphen G dar. Die Bedingung a) sagt aus, dass jede Kante in G von einer geraden Anzahl an gerichteten Kanten aus C überdeckt. Bedingung b) liefert eine Aussage für den Graphen $\widehat{G}$, welcher eine gerichtete Version von G ist, wobei die Richtungen von der Ordnung der Knoten $1 < 2 < \ldots < n$ bestimmt wird. Die Anzahl der Kanten in $\widehat{G}$, die sich auch in C befinden, ist ungerade. Wenn wir nun die Kreise der Länge 3 und der Länge 4 in G betrachten, die den partiellen gerichteten Dreiecken und gerichteten Vierecken entsprechen, so erzeugen diese eine Kantenüberdeckung eines nicht 3-färbbaren Teilgraphen von G. Falls ein Graph nun einen nicht 3-färbbaren Teilgraphen enthält, und es für diesen Graphen einen Nachweis für die nicht 3-Färbbarkeit in $D = 1$ gibt, dann gibt es den auch für G.
Die Klasse der Graphen mit dieser Eigenschaft, beinhaltet auch alle Graphen, die ein ungerades Rad enthalten.

Korollar 4.3 *Falls ein Graph $G = (V, E)$ ein ungerades Rad als Teilgraph enthält, so gibt es einen Nachweis für nicht 3-Färbbarkeit mit $D = 1$.*

Beweis. G enthält ein ungerades Grad, wie in Punkt 3 der Definition 4.2 beschrieben, und sei C die Menge der partiellen Dreiecke:

$$C := \{(i, 1, i+1) : 2 \leq i \leq n-1\} \cup \{(n, 1, 2)\}.$$

Wie wir in 6 sehen können, wird jede Kante genau nullmal oder zweimal von partiellen gerichteten Dreiecken von C überdeckt und damit wird Bedingung a) von Theorem 4.1 erfüllt. Außerdem gilt für jede Kante $(1, i) \in Arcs(G)$, dass sie genau einmal von einem partiellen gerichteten Dreieck aus C abgedeckt wird und die Anzahl der Kanten $(1, i)$ ist ungerade. Dadurch erfüllt C auch die Bedingung b) unseres Theorems. □

Ein weiteres nichttriviales Beispiel für den Nachweis der nicht 3-Färbbarkeit des NulLa mit $D = 1$ stellt der Grötzsch Graph dar.

Graph

Beispiel 4.1 *Der Grötzsch Graph enthält wie man sehen kann, keine Kreise der Länge 3. Jedoch enthält er folgende Menge von orientierten Vierecken:*

$$C := \{(1,2,3,7), (2,3,4,8), (3,4,5,9), (4,5,1,10), (1,10,11,7), (2,6,11,8), (3,7,11,9), (4,8,11,10), (5,9,11,6)\}.$$

Auch hier liefert wieder unser Theorem 4.1 die Aussage dafür, dass für diesen Graphen die nicht 3-Färbbarkeit mit $D = 1$ gezeigt werden kann. Jede Kante von G wird genau von zwei Vierecken aus C überdeckt und somit ist Bedingung a) erfüllt. Außerdem kann man durch Abzählen erkennen, dass auch Bedingung b) erfüllt ist.

$$
\begin{array}{ll}
x_i^2 x_j + x_i x_j^2 + 1 & \forall \{i,j\} \in E, \\
x_i x_j^2 + x_j x_k^2 & \forall (i,j),(j,k),(k,i) \in Arcs(G), \\
x_i x_j^2 + x_j x_k^2 + x_k x_l^2 + x_l x_i^2 & \forall (i,j),(j,k),(k,l),(l,i) \in Arcs(G), \\
 & (i,k),(j,l) \notin Arcs(G).
\end{array}
$$

Um das Theorem 4.1 zu beweisen, benötigen wir 2 Lemmas. Als Vorbereitung dafür, definieren wir zuerst die Menge H. Als erstes vereinfachen wir das Polynom zum Nachweis für die nicht 3-Färbbarkeit (siehe Definition 4.1). Nach Ausmultiplizieren der linken Seite können wir sehen, dass der einzige Koeffizient für den Term $x_j x_i^3$ a_{ij} ist. Daraus folgt, dass $a_{ij} = 0 \forall i,j \in V(G)$. Das gleiche Argument gilt auch für den einzigen Koeffizienten b_{ij} von $x_i x_j$. Dadurch erhält man folgende Vereinfachung:

$$
\sum_{i \in V} a_i (x_i^3 + 1) + \sum_{\{i,j\} \in E} \left(\sum_{k \in V} b_{ijk} x_k \right) (x_i^2 + x_i x_j + x_j^2) = 1
$$

Nun betrachten wir die Menge der Polynome in F:

$$
\begin{array}{ll}
x_i^3 + 1 & \forall i \in V, \\
x_k (x_i^2 + x_i x_j + x_j^2) & \forall \{i,j\} \in E, k \in V.
\end{array}
$$

Die Elemente von F sind jene Polynome, die einen Nachweis der Unlösbarkeit mit rang 1 darstellen. Ein solcher Nachweis kann nur erbracht werden, genau dann wenn das konstante Polynom 1 in der linearen Hülle von F enthalten ist: $1 \in \langle F \rangle_{\mathbb{F}_2}$, wobei $\langle F \rangle_{\mathbb{F}_2}$ Vektorraum über $\mathbb{F}_2$, der durch die Polynome von F generiert wird. Nun vereinfachen wir die Menge F und definieren sie als unsere Menge H:

Wenn wir die Monome $x_i x_j^2$ als gerichtete Kanten (i,j) betrachten, beschreiben die Polynome in der zweiten Zeile unsere orientierten partiellen Dreiecke und jene in Zeile drei die orientierten Vierecke. Das erste Lemma, welches wir zum Beweis für unser Theorem benötigen, sagt aus, dass wir H anstatt von F verwenden können.

Lemma 4.4 $1 \in \langle F \rangle_{\mathbb{F}_2} \Leftrightarrow 1 \in \langle H \rangle_{\mathbb{F}_2}$

Im folgenden Lemma wird beschrieben, dass sowohl die Bedingungen von Theorem 4.1 als auch die Bedingung $1 \in \langle H \rangle_{\mathbb{F}_2}$ zum Nachweis der nicht 3-Färbbarkeit genügen.

Lemma 4.5 *Es existiert eine Menge C von gerichteten partiellen Dreiecken und orientierten Vierecken, die die Bedingungen a) und b) des Theorems 4.1 erfüllen* $\Leftrightarrow 1 \in \langle H \rangle_{\mathbb{F}_2}$

Aus der Kombination dieser beiden Lemmas sehen wir nun, dass sie einen Beweis für Theorem 4.1 bilden. Für die beiden Beweise verweisen wir auf [5]. Das die Entscheidung, ob solche Graphen nicht 3-färbbar sind, in polynomieller Zeit erfolgt, zeigt uns Lemma 4.2.

4.2 Stable Sets und NulLA

Als erstes möchten wir ein paar Begriffe zum besseren Verständnis des folgenden Kapitels erklären.
Wir nennen eine Menge, die alle Stable Sets der Größe i eines Graphen G enthält, S_i. Die Elemente von S_i sind I und ein $I \in S_i$ besteht aus Knoten $\{c_1, c_2, \ldots, c_i\}$. In der Polynomdarstellung bezeichnet nun ein Monom x_I nun das Stable Set $I \in S_i$, mit $x_I := x_{c_1} x_{c_2} \cdots x_{c_i}$.
Außerdem sei $S_0 := \emptyset$ und $x_\emptyset = 1$. Zwei weitere Bedingungen sind:

- Für $I \cup k \in S_{i+1}$ gilt, dass $I \cap k = \emptyset$ und $x_I x_k$ ein quadratfreies Monom eines Stable Sets ist vom Grad $i+1$.

- Für $I \cup k \notin S_{i+1}$ gilt, dass $I \cap k = \emptyset$ und $x_I x_k$ ein quadratfreies Monom eines Nonstable Sets ist vom Grad $i+1$, da $I \cup k$ zumindest eine Kante $\{k, c_j\}$ enthält. $min_k(I)$ bezeichnet hier das kleinste $c_j \in I$ für das gilt: $\{k, c_j\} \in E(G)$.

Außerdem definieren wir noch P_i und L_i, die für die spätere Notation auch wichtig sind:

$$P_i := \sum_{I \in S_i} x_I, \qquad with P_0 := 1,$$
$$L_i := \frac{iL_{i-1}}{\alpha(G) + r - i}, \qquad with L_0 := \frac{1}{\alpha(G) + r}.$$

Definition 4.3 *Ein Graph besitzt kein Stable Set der Größe $\geq \alpha(G)$, wenn es eine Lösung für das folgende System gibt:*

$$1 = A\left(-(\alpha(G) + r) + \sum_{i=1}^{n} x_i\right) + \sum_{k \in V(G)} Q_k(x_k^2 - x_k) + \sum_{\{u,v\} \in E(G)} Q_{uv}(x_u x_v) \qquad r \geq 1.$$

Theorem 4.2 *Für einen Graph G existiert ein Nachweis des Nullstellensatzes mit Grad $\alpha(G)$, für die Nichtexistenz eines Stable Sets, der Größe $\alpha(G) + r (r \geq 1)$, sodass die Definition 4.3 erfüllt ist, wobei*

$$A = -\sum_{i=0}^{\alpha(G)} L_i P_i,$$
$$Q_{uv} = \sum_{i=1}^{\alpha(G)} \left(\sum_{\substack{I \in S_i : I \cup v \notin S_{i+1} and \\ min_v(I) = u}} L_{i+1} x_{I \setminus u} \right), and$$
$$Q_k = \sum_{i=1}^{\alpha(G)} \left(\sum_{I \in S_i : I \cup k \in S_{i+1}} L_{i+1} x_I \right).$$

Beweis. In unserem Beweis werden wir lediglich zeigen, dass die Gleichung aus Definition 4.3 gilt. Dazu setzen wir zuerst B, C, D folgendermaßen: $\underbrace{blabla}_{blub}$

$$1 = A \underbrace{\left(-(\alpha(G) + r) + \sum_{i=1}^{n} x_i\right)}_{B} + \underbrace{\sum_{k \in V(G)} Q_k(x_k^2 - x_k)}_{D} + \underbrace{\sum_{\{u,v\} \in E(G)} Q_{uv}(x_u x_v)}_{C}$$

Was man nun leicht erkennen kann, ist:

$$-L_0 P_0 \left(-(\alpha(G) + r)\right) = -\frac{1}{\alpha(G) + r} \left(-(\alpha(G) + r)\right) = 1.$$

Es bleibt zu zeigen, dass jeder Koeffizient jedes Monoms der Gleichung gleich 0 wird. Zunächst zeigen wir, dass jedes Monom in A, Q_k, Q_{uv} ein Stable Set ist und dann, dass Stable Set Monome in Q_k keine Monome der Form x_k und Stable Set Monome in Q_{uv} keine Monome der Form x_u bzw. x_v enthalten. Dies gelingt uns, indem wir zeigen, dass das System $AB + C + D$ nur drei Typen von Monomen auftreten. Nämlich: Quadratfreie Stable Set Monome, quadratfreie Nonstabel Set Monome und Stable Set Monome mit genau einer quadratischen Variable.

- **Quadratfreies Stable Set:** Sei $I = \{c_1, \ldots, c_m\}$ ein Stable Set der Größe m. Das Monom x_I kann nun in AB auf zwei Weisen erzeugt werden:

  - $x_{I \setminus c_k} x_{c_k}$ wird m-mal gebildet, für jedes c_k einmal, oder
  - $x_I \left(-(\alpha(G) + r)\right)$.

  Also ergibt sich der Koeffizient für x_I in AB als:

$$-mL_{m-1} - L_m \left(-(\alpha(G) + r)\right) = -m\frac{L_m(\alpha(G) + r - m)}{m} + L_m(\alpha(G) + r) = mL_m.$$

  Der Koeffizient für x_I in C existiert nicht, da x_I ein Monom eines Stable Sets ist.
  In D wird das Monom x_I erzeugt durch $x_{I \setminus c_k} - x_{c_k}$, daraus ergibt sich der Koeffizient $-mL_m$. Gesamt folgt das Ergebnis:

$$\underbrace{mL_{m-1}}_{from AB} \underbrace{-mL_m}_{from D} = 0.$$

- **Quadratfreies Nonstable Set:** Sei $I = \{c_1, \ldots, c_m\}$ ein Stable Set der Größe m und $x_I x_v$ ein Monom mit $u = min_v I$, wobei $\{u, v\} \in E(G)$.
  Es existieren $\binom{m+1}{m}$ Teilmengen von $c_1, \ldots, c_m$ und M sei die Anzahl der Stable Sets dieser Teilmengen. Jedes dieser M Stable Sets kommt in einem Monom in A vor. Also kommt das Monom $x_I xv$ M-mal in AB vor mit dem Koeffizienten $-ML_m$.
  $x_I x_V$ kommt nicht in D vor, da es ein Nonstable Set ist.
  Jedoch kommt $x_I x_v$ genau M-mal in C mit dem Koeffizienten ML_m vor. Es ergibtt sich:

$$\underbrace{-ML_m}_{from AB} + \underbrace{ML_m}_{from C} = 0.$$

- **Stable Set mit einer quadratischen Variable:** Sei $I = \{c_1, \ldots, c_m\}$ ein Stable Set der Größe m und das zugehörige Monom $x_{I \setminus k} x_k^2$.
  In AB wird dieses Monom direkt als Produkt von $x_I x_k$ mit Koeffizient $-L_m$ erzeugt.
  In C kommt es nicht vor, da es keine Kante enthält.
  In D wird es aus $x_{I \setminus k} x_k^2$ erzeugt mit Koeffizient L_m. Daraus ergibt sich:

$$\underbrace{-L_m}_{from AB} + \underbrace{L_m}_{from D} = 0.$$

Da der konstante Term in $AB + C + D$ gleich 1 ist und die Koeffizienten für alle anderen Monome gleich 0 sind, ergibt sich, dass die Gleichung ein Nachweis für Stable Sets ist mit Grad $\alpha(G)$. □

Um diesen Satz zu veranschaulichen möchten wir nun ein kleines Beispiel geben:

Beispiel 4.2 *Wir betrachten den Turán Graph $T(5,3)$, dieser hat eine chromatische Zahl von $\alpha(T(5,3)) = 2$.*

Bild einfügen

Wenn wir nun auf ein Stable Set der Größe 3 testen, erhalten wir mit unserem Algorithmus folgenden

Nachweis:

$$
\begin{aligned}
1 = &\left(\frac{1}{3}x_4 + \frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_3 + \left(\frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_4 + \left(\frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_5 + \left(\frac{1}{3}x_4 + \frac{1}{3}\right)x_2x_3 \\
&+ \left(\frac{1}{3}\right)x_2x_4 + \left(\frac{1}{3}\right)x_2x_5 + \left(\frac{1}{3}x_4 + \frac{1}{3}\right)x_3x_5 + \left(\frac{1}{3}\right)x_4x_5 \\
&+ \left(\frac{1}{3}x_2 + \frac{1}{6}\right)(x_1^2 - x_1) + \left(\frac{1}{3}x_1 + \frac{1}{6}\right)(x_2^2 - x_2) + \left(\frac{1}{3}x_4 + \frac{1}{6}\right)(x_3^2 - x_3) + \left(\frac{1}{3}x_3 + \frac{1}{6}\right)(x_4^2 - x_4) \\
&+ \left(\frac{1}{6}\right)(x_5^2 - x_5) + \underbrace{\left(-\frac{1}{3}(x_1x_2 + x_3x_4) - \frac{1}{6}(x_1 + x_2 + x_3 + x_4 + x_5) - \frac{1}{3}\right)}_{\textit{Stable Set Polynom}}(x_1 + x_2 + x_3 + x_4 + x_5 - 3)
\end{aligned}
$$

Man kann gut erkennen, dass der Koeffizient für das Stable Set Polynom für jedes Stable Set in $T(5,3)$ genau ein Monom enthält. Wenn wir z.B. den Term $\frac{1}{3}x_1x_2$ betrachten, sehen wir, dass dieser zum Stable Set $\{1,2\}$ gehört. Außerdem stellt jedes Monomin jedem Koeffizient ein Stable Set in $T(5,3)$ dar.

Nun folgen noch theoretische Resultate zur Größe der Nullstellen Nachweise.

Theorem 4.3 *Für einen Graph G liefert der Nullstellensatz einen Nachweis für die Nichtexistenz eines Stable Sets, das größer als $\alpha(G)$ ist, mit einem Grad der zumindest $\alpha(G)$ ist.*

Korollar 4.4 *Für einen Graph G liefert der Nullstellensatz einen Nachweis für die Nichtexistenz eines Stable Sets, das größer als $\alpha(G)$ ist, welcher zumindest ein Monom für jedes Stable Set in G enthält.*

Aus diesen beiden Resultaten können wir nun folgendes Theorem folgern:

Theorem 4.4 *Für einen Graph G liefert der Nullstellensatz einen Nachweis für die Nichtexistenz eines Stable Sets, das größer als $\alpha(G)$ ist, welcher einen Grad von $\alpha(G)$ besitzt und außerdem zumindest einen Term für jedes Stable Set in G enthält.*

Dieses Theorem gibt uns also eine untere Schranke für den Grad und Anzahl der Terme eines Nachweises für die Nichtexistenz eines Stable Sets nach dem Nullstellensatz. Weiters gibt es eine allgemeinere Aussage für die Komplexität:

Korollar 4.5 *Es existiert eine unendlich große Menge von Graphen G_n mit n Knoten, so dass der minimale Grad eines Nachweises mit dem Nullstellensatz linear anwächst und gleichzeitig die Anzahl der Terme der Koeffizienten Polynome des Nachweises exponentiell in n anwächst.*

Zum Schluss können wir zusammenfassen, dass die Polynome, die zum Verifizieren des Nullstellensatzes dienen, sehr dicht sind, da alle quadratfreien Monome, welche Stable Sets darstellen, in ihnen vorkommen. Das stellt jedoch ein großes Hindernis für die Berechnung dar. In diesem Fall ist es so, dass die Berechnung von Hilberts Nullstellensatz zumindest so schwer ist wie das Zählen aller möglichen Stable Sets eines Graphen. Dieses Problem ist also bereits für Graphen mit geringen Knotengrad $\#P$-vollständig.

#P,NP,P definieren: @Kerstin: hab ich gemacht - weiß nicht ob das Paper, das ich verwendet habe gut ist! Bitte anschauen

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.