Freie Universität Berlin

Fachbereich Mathematik und Informatik

Bachelorarbeit

Der kombinatorische Nullstellensatz und seine Anwendungen

Eingereicht von: Olaf Parczyk (4365433)

Eingreicht am: 18. Dezember 2012

Betreuer: Prof. Dr. Tibor Szabó und Dr. Yury Person

Inhaltsverzeichnis

Zusammenfassung

In der Mathematik gibt es viele Methoden, die sich der Hilfe von Polynomen bedienen. Neben Dimensionsargumenten, kann die Lösung auch von Nullstellen oder Nicht-Nullstellen abhängen. Diese Techniken haben Anwendungen in den verschiedensten Gebieten der Mathematik. In dieser Arbeit wird der sogenannte kombinatorische Nullstellensatz behandelt, eine algebraische Methode, die eine Nicht-Nullstelle für Polynome mit führendem Koeffizienten ungleich Null auf ausreichend großen Mengen garantiert. Es werden zwei zentrale Theoreme vorgestellt und deren Anwendungen in der Zahlentheorie, Kombinatorik, Graphentheorie und Algebra diskutiert. Das Ziel dabei ist die Vielseitigkeit und Stärke der angewandten Methode herauszuarbeiten. Zum Abschluß wird auf das korrespondierende algorithmische Problem und einige Erweiterungen eingegangen.

1 Der kombinatorische Nullstellensatz

1.1 Einleitung

In der diskreten Mathematik spielen algebraische Methoden und Polynome eine wichtige Rolle. Es ist wohl bekannt, dass ein nichttriviales Polynom n-ten Grades keine $n+1$ Nullstellen besitzen kann. Diese Aussage lässt sich einfach auf mehrere Variablen verallgemeinern, wie Lemma 1.4 zeigt. Es geht aber besser: Selbst wenn der Grad des Polynoms in den einzelnen Variablen größer ist als die Anzahl der Punkte, kann unter bestimmten Voraussetzungen das Polynom nicht komplett darauf Null werden.

Dies wurde zum Beispiel von Alon und Tarsi [11, 10] herausgearbeitet (vergleiche Abschnitt 4.2 und 5.1). Sie modellierten die Problemstellungen als Polynome, deren Lösung an das Nichtverschwinden über bestimmten Mengen geknüpft war. Mit Hilfe von Multilinearisierung reduzierten sie den Grad der Polynome so lange bis der einfache Fall wieder anwendbar war und somit eine Lösung vorlag.

In weiteren Publikationen von Alon [5, 4, 3] wurde diese Vorgehensweise immer wieder eingesetzt. Alon, Nathanson und Rusza [8, 9] fassten diese Technik zur sogenannten Polynommethode, Theorem 1.7, zusammen. Neben Theorem 2.1 lassen sich weitere Anwendungen des kombinatorischen Nullstellensatzes auch mit dieser Methode beweisen.

Erst 1995 formulierte Alon [1] die beiden Theoreme, um die es nun gehen soll und bezeichnete sie als den kombinatorischen Nullstellensatz. Namensgebend waren dabei die Parallelen zum Nullstellensatz von Hilbert, einem wichtigen Theorem der algebraischen Geometrie.

In den nächsten beiden Abschnitten werden die zentralen Theoreme und deren Beweise vorgestellt und exemplarisch in deren Gebrauch eingeführt. Im weiteren Verlauf der Arbeit geht es darum die Stärke und Vielseitigkeit dieser Theoreme herauszuarbeiten. Dazu werden wir Anwendungen aus verschiedenen Gebieten vorstellen. In der Zahlentheorie widmen wir uns einigen Vermutungen über beschränkte Summen von Mengen. Die Kombinatorik bietet uns zwei sehr anschauliche Problemstellungen. Aus der Graphentheorie gibt es Theoreme über Untergraphen und eine interessante Variante der Graphenfärbung. Nach zwei algebraischen Anwendungen gehen wir dann auf die Suche nach einem effizienten Algorithmus. Zum Schluß analysieren wir einige Erweiterungen des kombinatorischen Nullstellensatzes mit Beispielen aus der Geometrie und schließen mit Bemerkungen und Ausblicken.

Das Ziel dieser Arbeit ist es, einen guten Überblick über den kombinatorischen Nullstellensatz und dessen vielseitige Anwendungsmöglichkeiten zu verschaffen. Dabei stellen wir die Beweise möglichst ausführlich dar und geben Anreize weiter in die Themen einzusteigen. Als Grundlage dient die Arbeit von Alon [1], wir stellen aber weitestgehend neuere Resultate vor und betrachten neuere Entwicklungen auf den Gebieten.

Zur besseren Lesbarkeit vereinbaren wir noch einige Koventionen: Im folgenden ist $\mathbb{F}$ immer ein Körper, R ein Ring mit Eins und $\mathbb{N} = \{0, 1, 2, \dots\}$. Als Kurzform für Vektoren nutzen wir $\mathbf{s} = (s_1, \dots, s_n)$. Wir betrachten Elemente f bzw. $f(x_1, \dots, x_n)$ aus dem Polynomring $R[x_1, \dots, x_n]$ über n Variablen. Ein Polynom f lässt sich als Linearkombination von Monomen schreiben $f(x_1, \dots, x_n) = \sum_{\mathbf{i}=(i_1,\dots,i_n)\in\mathbb{N}^n} a_{\mathbf{i}} x_1^{i_1} \dots x_n^{i_n}$ mit $a_{\mathbf{i}} \in R$.

Der total Grad ist definiert als $\deg(f) := \max\{\sum_{k=1}^{n} i_k : \mathbf{i} \in \mathbb{N}^n \text{ und } a_{\mathbf{i}} \neq 0\}$ und der Grad in einer Variablen x_j ist $\deg_j(f) := \max\{k : \exists\, \mathbf{i} \in \mathbb{N}^n \text{ mit } i_j = k \text{ und } a_{\mathbf{i}} \neq 0\}$.

1.2 Die Theoreme

Theorem 1.1. *Sei $f \in \mathbb{F}[x_1, \ldots, x_n]$. Für nichtleere Teilmengen $S_1, \ldots, S_n$ von $\mathbb{F}$ definieren wir $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. Wenn f über den gemeinsamen Nullstellen von g_i verschwindet, also $f(s_1, \ldots, s_n) = 0$ für alle $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, dann existieren Polynome $h_1, \ldots, h_n \in R[x_1, \ldots, x_n]$ mit*

$$f = \sum_{i=1}^{n} h_i g_i,$$

wobei $deg(h_i) \leq deg(f) - deg(g_i)$ und R der kleinste Unterring von $\mathbb{F}$ ist, so dass $f, g_1, \ldots, g_n \in R[x_1, \ldots, x_n]$.

Im vergleich dazu der Hilbertsche Nullstellensatz:

Theorem 1.2. *Sei $\mathbb{F}$ ein algebraisch abgeschlossener Körper und $f, g_1, \ldots, g_n$ Polynome in $\mathbb{F}[x_1, \ldots, x_n]$, wobei f über den gemeinsamen Nullstellen von $g_1, \ldots, g_n$ verschwindet, dann gibt es ein $k \in \mathbb{N}$ und Polybome $h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$, so dass*

$$f^k = \sum_{i=1}^{n} h_i g_i$$

Der gravierende Unterschied liegt also in der freien Wahl der g_i und der algebraischen Abgeschlossenheit. Aus dem ersten Theorem lässt sich das Folgende direkt ableiten.

Theorem 1.3. *Sei $f \in \mathbb{F}[x_1, \ldots, x_n]$. Angenommen der Grad von f ist $\sum_{i=1}^{n} t_i$, mit $t_i \in \mathbb{N}$, und der Koeffizient vor $\prod_{i=1}^{n} x_i^{t_i}$ ist nicht Null. Für Teilmengen $S_1, \ldots, S_n$ von $\mathbb{F}$ mit $|S_i| \geq t_i + 1$ gibt es dann $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ mit*

$$f(s_1, \ldots, s_n) \neq 0.$$

Diese Theoreme werden als kombinatorischer Nullstellensatz bezeichnet. Zum Beweis verallgemeinern wir die Aussage, dass ein Polynom n-ten Grades, welches nicht das Nullpolynom ist, höchstens n Nullstellen hat, auf mehrere Variablen.

Lemma 1.4. *Sei $f \in \mathbb{F}[x_1, \ldots, x_n]$. Für alle i sei $\deg_i(f) \leq t_i$ und $S_i \subseteq \mathbb{F}$ mit $|S_i| \geq t_i + 1$. Wenn $f(s_1, \ldots, s_n) = 0$ für alle $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, dann $f \equiv 0$.*

Beweis. Für $n = 1$ entspricht die Aussage dem oben beschriebenen Fall. Angenommen die Aussage gilt für $n-1$ mit $n \geq 2$, dann zeigen wir die Aussage für n und das Lemma folgt nach vollständiger Induktion.

Betrachte f als Polynom in x_n

$$f = \sum_{i=1}^{t_n} f_i(x_1, \ldots, x_{n-1}) x_n^i$$

mit $deg_{x_j}(f_i) \leq t_j$. Setzen wir hier $(s_1, \ldots, s_{n-1}) \in S_1 \times \cdots \times S_{n-1}$ ein, so erhalten wir ein Polynom, dass für alle $s_n \in S_n$ Null wird und damit das Nullpolynom ($|S_n| \geq t_n + 1$). Daraus folgt $f_i(s_1, \ldots, s_{n-1}) = 0$, nach Induktionsvorrausetzung sind dann alle $f_i \equiv 0$ und damit $f \equiv 0$. □

Beweis von Theorem 1.1. Definiere $t_i = |S_i| - 1$. Nach Vorraussetzung gilt

$$f(s_1, \ldots, s_n) = 0 \text{ für alle } (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n. \tag{1}$$

Außerdem gilt $g_i(x_i) = 0$ für $x_i \in S_i$ und wenn wir das Produkt weiter ausschreiben $g_i(x_i) = \prod_{s \in S_i}(x_i - s) = x_i^{t_i+1} - \sum_{j=0}^{t_i} g_{ij} x_i^j$ haben wir

$$x_i^{t_i+1} = \sum_{j=0}^{t_i} g_{ij} x_i^j \text{ für alle } x_i \in S_i. \tag{2}$$

Betrachten wir f als Linearkombination von Monomen und ein Monom der Form $x_i^{t_i+1} h_i$, dann gilt $deg(h_i) \leq deg(f) - (t_i + 1)$. Wir verringern den Exponenten von x_i durch Einsetzen von (2), welches dem Subtrahieren von $g_i h_i$ entspricht.

$$x_i^{t_i+1} h_i \underset{x_i \in S_i}{\overset{(2)}{=}} \left(\sum_{j=0}^{t_i} g_{ij} x_i^j \right) h_i = \left(x_i^{t_i+1} - g_i \right) h_i = x_i^{t_i+1} h_i - g_i h_i$$

Durch wiederholtes Anwenden erhalten wir das Polynom $\tilde{f}$, welches in x_i Grad höchstens t_i hat und in jedem Schritt ein h_i, welche wir für jedes i akkumulieren. $\tilde{f}$ entsteht also aus f durch das Subtrahieren von Produkten der Form $g_i h_i$, kurz $\tilde{f} = f - \sum_{i=1}^{n} g_i h_i$, wobei $deg(h_i) \leq deg(f) - deg(g_i)$. Die Koeffizienten von h_i liegen in dem kleinsten Ring R, der die Koeffizienten von f und $g_1, \ldots, g_n$ enthält, also $h_i \in R[x_1, \ldots, x_n]$.

Darüber hinaus gilt $\tilde{f}(s_1, \ldots, s_n) \overset{(2)}{=} f(s_1, \ldots, s_n) \overset{(1)}{=} 0$ für $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$. Da $|S_i| = t_i + 1$ und damit größer als der Grad von f in x_i greift Lemma 1.4 und $\tilde{f} \equiv 0$. Daraus folgt direkt $f = \sum_{i=1}^{n} h_i g_i$. □

Beweis von Theorem 1.3. Erstmal können wir annehmen, dass $|S_i| = t_i + 1$ und definieren $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. Nehmen wir weiterhin an, dass die Aussage falsch ist, also $f(s_1, \ldots, s_n) = 0$ für alle $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, dann folgt mit Theorem 1.1 die Existenz von $h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$ mit $deg(h_i) \leq deg(f) - deg(g_i)$, so dass

$$f = \sum_{i=1}^{n} h_i g_i.$$

Der Grad von jedem $h_i g_i = h_i \prod_{s \in S_i}(x_i - s)$ ist höchstens $deg(f) = \sum_{i=1}^{n} t_i$ und ein Monom hat genau dann Grad $deg(f)$, wenn es durch $x_i^{t_i+1}$ teilbar ist, da $|S_i| = t_i + 1$. Also muss der Koeffizient vor $\prod_{i=1}^{n} x_i^{t_i}$ in $\sum_{i=1}^{n} h_i g_i$ Null sein. Nach Voraussetzung ist der Koeffizient vor $\prod_{i=1}^{n} x_i^{t_i}$ in f allerdings ungleich Null, ein Widerspruch. □

1.3 Erste Beispiele

Eine erste einfache Anwendung ist das Cauchy-Davenport Theorem, welches selber etliche Anwendungen in der Zahlentheorie hat, und durch das der Gebrauch des kombinatorischen Nullstellensatzes vorgestellt werden soll.

Theorem 1.5. *Sei p eine Primzahl und A,B zwei nichtleere Teilmengen von $\mathbb{F}_p$. Die Minkowski-Summe von A und B ist definiert als $A+B := \{a+b : a \in A, b \in B\}$. Dann gilt*

$$|A+B| \geq min\{p, |A|+|B|-1\}.$$

Um Theorem 1.3 zu benutzen, benötigen wir ein Polynom f, welches das Problem modelliert, ein Monom maximalen Grades mit Koeffizienten ungleich Null in f und passende Mengen $S_1, \ldots, S_n$. Die Schwierigkeit liegt meistens darin alle Bedingungen gleichzeitig zu erfüllen, denn die Größe der Mengen muss zum Polynom und dem Monom passen. Im folgenden Beweis heben wir diese Schritte hervor.

Beweis. Für $|A|+|B| > p$ ist $|A \cap B| > 0$ und damit auch $|A \cap (\{z\}-B)| > 0$ für beliebiges $z \in \mathbb{F}_p$. Deshalb existiert $a \in A$, $b \in B$ mit $a = z - b$, zusammen $a+b = z \in A+B$ und damit $A+B = \mathbb{F}_p$, also $|A+B| = p$.

Für $|A|+|B| \leq p$ nehmen wir an, dass $|A+B| \leq |A|+|B|-2$. Dann existiert eine Menge C mit $A+B \subset C$ und $|C| = |A|+|B|-2$. Wir definieren unser Polynom $f \in \mathbb{F}_p[x,y]$ durch $f(x,y) = \prod_{c \in C}(x+y-c)$, denn dann gilt

$$f(a,b) = 0 \text{ für alle } a \in A, b \in B. \tag{3}$$

Mit $t_1 = |A|-1$, $t_2 = |B|-1$ ist der Koeffizient vor $x^{t_1}y^{t_2}$ in f der Binomialkoeffizient $\binom{(|A|+|B|-2}{|A|-1)}$ und damit ungleich Null, da $|A|+|B|-2 < p$. Für $n = 2$ und die Mengen $S_1 = A$, $S_2 = B$ greift jetzt Theorem 1.3, es existieren also $a \in A$, $b \in B$ mit $f(a,b) \neq 0$ im Widerspruch zu (3). Also war die Annahme falsch und es gilt auch im zweiten Fall $|A+B| \geq |A|+|B|-1$ □

Als nächstes schauen wir uns ein geometrisches Resultat von Alon und Füredei [5] an, welches dort mit der Methode aus [3], einem Vorläufer der Polynommethode bewiesen wurde.

Theorem 1.6. *Seien $H_1, H_2, \ldots, H_m$ eine Familie von Hyperebenen in $\mathbb{R}^n$, die alle Ecken des Würfels $\{0,1\}^n$ enthalten bis auf eine. Dann ist $m \geq n$.*

Beweis. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass die nicht enthaltene Ecke der Nullvektor ist. Sei $\langle \mathbf{a}_i, \mathbf{x} \rangle = \mathbf{b}_i$ die Gleichung, die H_i beschreibt, wobei $\mathbf{x} = (x_1, \ldots, x_n)$ und $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{j=1}^{n} a_i b_j$ das übliche innere Produkt zwischen den Vektoren $\mathbf{a}$ und $\mathbf{b}$ ist. Wir halten fest, dass $\mathbf{b}_i \neq 0$ für alle i, da H_i nicht den Ursprung enthält. Wir nehmen an die Behauptung sei falsch, also $m < n$, und betrachten das Polynom

$$f(\mathbf{x}) = (-1)^{n+m+1} \prod_{j=1}^{m} b_j \prod_{i=1}^{n}(x_i - 1) - \prod_{i=1}^{m}[\langle \mathbf{a}_i, \mathbf{x} \rangle - b_i].$$

Der Grad dieses Polynoms ist n und der Koeffizient vor $\prod_{i=1}^{n} x_i$ ist

$$(-1)^{n+m+1} \prod_{j=1}^{m} b_j \neq 0.$$

Für Mengen $S_i = \{0, 1\}$ und $t_i = 1$ gibt es nach Theorem 1.3 einen Punkt $\mathbf{s} \in \{0, 1\}^n$ für den f nicht Null ist. Dieser Punkt kann nicht der Nullvektor sein, da sich dort die beiden Summanden aufheben und f Null wird. Es handelt sich also um eine andere Ecke des Würfels. In diesem Fall ist aber $\langle \mathbf{a}_i, \mathbf{x} \rangle - \mathbf{b}_i = 0$ für ein i und somit ist f an dieser Stelle Null, ein Widerspruch. Die Annahme war somit falsch und wir erhalten $m \geq n$. □

Zum Abschluß dieser Einführung kommen wir zur bereits erwähnten Polynomialmethode [9], welche sich auch direkt aus Theorem 1.3 ableiten lässt. Für ein Polynom $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ und Mengen $S_1, \ldots S_n \subset \mathbb{F}_p$ definieren wir

$$\oplus_f \sum_{i=1}^{n} S_i = \{s_0 + \cdots + s_n : s_i \in S_i, f(s_1, \ldots, s_n) \neq 0\}$$

Theorem 1.7. *Sei p eine Primzahl, $f \in \mathbb{F}_p[x_1, \ldots, x_n]$, $S_i \subseteq \mathbb{F}_p$ mit $|S_i| = t_i + 1$ und $m = \sum_{i=1}^{n} t_i - deg(f)$, wobei $t_i \in \mathbb{N}$. Wenn der Koeffizient vor $\prod_{i=1}^{n} x_i^{t_i}$ in*

$$(x_1 + \cdots + x_n)^m f(x_1, \ldots x_n)$$

ungleich Null in $\mathbb{F}_p$ ist, dann

$$|\oplus_f \sum_{i=1}^{n} S_i| \geq m + 1$$

und automatisch $m < p$.

Beweis. Angenommen das Resultat ist falsch. Sei also E eine Multimenge mit m Elementen aus $\mathbb{F}_p$, die $\oplus_f \sum_{i=1}^{n} S_i$ enthält und definiere $Q(x_1, \ldots, x_n)$ als

$$Q(x_1, \ldots, x_n) = f(x_1, \ldots x_n) \prod_{e \in E} (x_1 + \cdots + x_n - e).$$

Da für $(x_1, \ldots, x_n) \in S_1 \times \cdots \times S_n$ entweder $(x_1 + \cdots + x_n) \in \oplus_f \sum_{i=1}^{n} S_i \subset E$ oder $f(x_1, \ldots, x_n) = 0$ gilt, erhalten wir

$$Q(x_1, \ldots, x_n) = 0 \text{ für alle } (x_1, \ldots, x_n) \in S_1 \times \cdots \times S_n. \tag{4}$$

Außerdem besitzt sowohl das Polynom Q, wie auch $(x_1 + \cdots + x_n)^m f(x_1, \ldots x_n)$ den Grad $m + \deg(f) = \sum_{i=1}^{n} t_i$ und damit ist der Koeffizient vor dem Monom $\prod_{i=1}^{n} t_i$ in beiden identisch, also nach Voraussetzung nicht Null. Mit Theorem 1.3 gibt es dann $(x_1, \ldots, x_n) \in S_1 \times \cdots \times S_n$, so dass $Q(x_1, \ldots, x_n) \neq 0$ im Widerspruch zu (4). □

Umgekehrt findet man Theorem 1.3 in der Polynomialmethode zumindest für $\mathbb{F} = \mathbb{F}_p$ einfach wieder. Dafür genügt es einzusehen, dass mit den Vorraussetzungen von Theorem 1.3 $\deg(f) = \sum_{i=1}^n t_i$, also $m = 0$, der Koeffizient vor $\prod_{i=1}^n x_i^{t_i}$ in $f(x_1, \ldots, x_n)$ bzw. $(x_1 + \cdots + x_n)^0 f(x_1, \ldots, x_n)$ nicht Null ist in $\mathbb{F}_p$. Außerdem gilt $|\oplus_f \sum_{i=1}^n S_i| \geq m+1 = 1$, womit $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ mit $f(s_1, \ldots, s_n) \neq 0$ existiert. Der nächste Korollar ist eine direkte Folgerung aus der Polynomialmethode, mit dem Nullstellensatz wäre dies aufwendiger zu zeigen.

Korollar 1.8. *Für $A, B \subset \mathbb{F}_p$ mit p Primzahl und $|A| \neq |B|$ ist*

$$|\{a + b : a \in A, b \in B, ab \neq 1\}| \geq min\{p, |A| + |B| - 3\}.$$

Beweis. Wir wenden Theorem 1.7 mit $n = 2$, $f(x, y) = xy - 1$, $S_1 = A$, $S_2 = B$ und $m = |A| + |B| - 4$ an. □

2 Anwendungen in der Zahlentheorie

Im folgenden Abschnitt über Anwendungen in der Zahlentheorie wenden wir uns verschiedenen Ansätzen zu, die Kardinalität von eingeschränkten Mengenadditionen nach unten abzuschätzen. Nach dem Chouchy-Davenport Theorem und dem kurzen Korollar aus dem letzten Abschnitt über die Minkowskisumme geht es hier um die mittlerweile bewiesene Erdős-Heilbronn Vermutung, Fortschritte bei einer Vermutung von Lev und zuletzt eine Vermutung von Snevily.

2.1 Erdős-Heilbronn Vermutung

Theorem 2.1. *Für $A \subset \mathbb{F}_p$ mit p Primzahl ist*

$$|\{a + a' : a, a' \in A, a \neq a'\}| \geq min\{p, 2|A| - 3\}.$$

Diese Aussage wurde 1964 von Erdős und Heilbronn [25] vermutet. Nach unterschiedlichen Teilerfolgen gelang es zum ersten Mal da Silva und Hamidoune 1994 [21] die allgemeinere Form $|\{a_1 + \cdots + a_n : a_i \in A, a_i \neq a_j \forall i \neq j\}| \geq min\{p, n|A| - n^2 + 1\}$ zu beweisen.

Für arithmetische Folgen A sind die Ungleichungen scharf. Gleiches gilt für das Cauchy Davenport Theorem 1.5. Vosper [61] und Károlyi [30] gelang es sogar zu zeigen, dass dies die einzigen extremalen Fälle sind.

Bei dem Beweis der allgemeineren Variante von Dias da Silva wurden Hilfsmittel der linearen Algebra und Darstellungstheorie symmetrischer Gruppen benutzt. Alon, Nathanson und Rusza [9] formulierten dafür einen Beweis mit Hilfe der Polynommethode, Theorem 1.7. Wir geben mit Hilfe des Nullstellensatzes für Theorem 2.1 einen kürzeren Beweis, ähnlich dem vom Cauchy Davenport Theorem 1.5. Dabei folgen wir der Idee von Alon, Nathanson und Rusza [8], die diesen zwar noch nicht zur Verfügung hatten, aber wie bereits erläutert, lassen sich entscheidende Parallelen feststellen. Zunächst zeigen wir eine allgemeinere Version, die dann das Erdős-Heilbronn Theorem impliziert.

Theorem 2.2. *Für $A \neq B \subset \mathbb{F}_p$ mit p Primzahl, $A\hat{+}B := \{a+b : a \in A, b \in B, a \neq b\}$ und $|A| \neq |B|$ gilt*

$$|A\hat{+}B| \geq min\{p, |A| + |B| - 2\}.$$

Beweis. Ohne Beschränkung der Allgemeinheit sei $|A| > |B|$. Falls $|A|+|B|-2 > p$, dann wählen wir eine Menge $B' \subset B$ der größe $|B'| = p - |A| + 2$. Es gilt $2 \leq |B'| < |B| < |A|$ und $|A| + |B'| - 2 = p$. Wenn die Aussage für A und B' gilt, dann ist

$$|A\hat{+}B| \geq |A\hat{+}B'| \geq |A| + |B'| - 2 = p = min(p, |A| + |B| - 2).$$

Wir können also $|A| + |B| - 2 \leq p$ annehmen.

Sei $C = A\hat{+}B$. Angenommen $|C| \leq |A| + |B| - 3$. Wir definieren das Polynom

$$f(x, y) = (x - y) \prod_{c \in C} (x + y - c)$$

in $\mathbb{F}[x, y]$. Das Polynom hat Grad $\deg(f) \leq |A|+|B|-2$ und für $t_1 = |A|-1$, $t_2 = |B|-1$ ist der Koeffizient vor $x^{t_1}y^{t_2}$ in f

$$\binom{|A| + |B| - 3}{|A| - 2} - \binom{|A| + |B| - 3}{|A| - 1} = \frac{(|A| - |B|)(|A| + |B| - 3)!}{(|A| - 1)!(|B| - 1)!} \not\equiv 0 \pmod{p},$$

da $|A| \neq |B|$ und $|A| + |B| - 3 < p$. Für $n = 2$, $S_1 = A$ und $S_2 = B$ greift jetzt Theorem 1.3, es existieren also $a \in A$ und $b \in B$ mit $f(a, b) \neq 0$.

Andererseits verschwindet das Polynom f für jedes Paar $(a, b) \in A \times B$, denn für $a = b$ wird die linke Seite Null und sonst ist $a + b \in C$. Zusammen haben wir einen Widerspruch und die Annahme war falsch. □

Károlyi [31] erweiterte im Jahr 2009 das Theorem 2.2 auch für den Fall $|A| = |B|$, für den in unserem Polynom der Koeffizient vor dem entscheidenden Monom Null wäre. Falls $|A| = |B| \geq 2$, dann gilt mit $B' := B \setminus \{b\}$ direkt

$$|A\hat{+}B| \geq |A\hat{+}B'| \geq |A| + |B'| - 2 = |A| + |B| - 3.$$

Für den Beweis genügt es also zu zeigen, dass aus $|A| = |B|$ und $|A\hat{+}B| = 2|A|-3$, sofort $A = B$ folgt. Er verwendete das selbe Polynom f und ebenfalls den kombinatorischen Nullstellensatz, aber diesmal direkt Theorem 1.1.

Beweis von Theorem 2.1. $|A| = 1$ ist trivial und für $|A| \geq 2$ wählen wir ein $a \in A$ und definieren $B := A \setminus \{a\}$. Dann ist $|B| = |A| - 1$ und mit Theorem 2.1 folgt

$$|A\hat{+}A| \geq |A\hat{+}B| \geq min\{p, |A| + |B| - 2\} \geq min\{p, 2|A| - 3\}.$$

□

Eine Erweiterung der allgemeinen Variante von Dias da Silva mit Hilfe des kombinatorischen Nullstellensatzes kam 2009 von Pan und Sun [47].

2.2 Levs Vermutung

Das Kempermann-Scherk Theorem [33, 53] besagt für Teilmengen $A, B \subseteq \mathbb{F}_p$, dass $|A+B| \geq |A| + |B| - \min\limits_{c \in A+B} v_{A,B}(c)$, wobei $v_{A,B}(c) = |\{(a,b) \in A \times B : a+b = c\}|$. Motiviert durch dieses Theorem und die Erdős-Heilbronn Vermutung formulierte Lev [38] folgende Vermutung:

Vermutung 2.3. *Seien A, B Teilmengen einer abelschen Gruppe G, dann gilt*

$$|A \hat{+} B| \geq |A| + |B| - 2 - \min_{c \in A+B} v_{A,B}(c).$$

Die Ungleichung ist scharf, wie man für $G = (\mathbb{Z}, +)$ und $A = B = \{0, 5, 10\}$ leicht sieht $|A \hat{+} B| = 3 = 3+3-2-1$, wobei $\min\limits_{c \in A+B} v_{A,B}(c) = v_{A,B}(0) = 1$. Mit Hilfe des kombinatorischen Nullstellensatzes konnten Pan und Sun [46] deutliche Fortschritte verzeichnen. Für einige Spezialfälle gelang es ihnen allgemeinere Resultate zu zeigen.

Theorem 2.4. *Seien A, B endliche Teilmengen eines Körpers $\mathbb{F}$. Sei $f \in \mathbb{F}[x,y]$ und $C = \{a+b : a \in A, b \in B, f(a,b) \neq 0\}$. Falls $C \neq \emptyset$ dann gilt*

$$|C| \geq |A| + |B| - deg(f) - \min_{c \in C} v_{A,B}(c).$$

Mit $f(x,y) = x - y$, also $\deg(f) = 1$ und wegen $\min\limits_{c \in C} v_{A,B}(c) \geq \min\limits_{c \in A+B} v_{A,B}(c)$ erhalten wir eine stärkere Aussage als Vermutung 2.3 für Körper $\mathbb{F}$.

Theorem 2.5. *Seien A, B Teilmengen einer abelschen Gruppe G, deren Torsionsgruppe*

$$Tor(G) = \{g \in G : ord(g) \text{ endlich}\}$$

zyklisch ist. Für $i = 1, \ldots, l$ seien m_i und n_i nicht negative ganze Zahlen und $d_i \in G$. Angenommen

$$C = \{a+b : a \in A, b \in B, m_i a - n_i b \neq d_i \forall i = 1, \ldots, l\} \neq \emptyset,$$

dann gilt

$$|C| \geq |A| + |B| - \sum_{i=1}^{l} (m_i + n_i) - \min_{c \in C} v_{A,B}(c).$$

Sind in diesem Fall $l = 1$, $m_1 = 1$, $n_1 = 1$ und $d_1 = 0$, dann impliziert dies Vermutung 2.3 für G mit zyklischer Torsionsgruppe. Beide Aussagen können wir zusammenfassen um folgendes Resultat zu erhalten.

Theorem 2.6. *Seien A, B, S endliche nichtleere Teilmengen einer abelschen Gruppe G mit*

$$C = \{a+b : a \in A, b \in B, a - b \notin S\} \neq \emptyset.$$

(i) Wenn G torisionsfrei ($Tor(G) = \{1\}$) oder elementar abelsch (alle Elemente bis auf die 1 haben Ordnung p für eine Primzahl), dann

$$|C| \geq |A| + |B| - |S| - \min_{c \in C} v_{A,B}(c).$$

(ii) Wenn $Tor(G)$ zyklisch ist, dann

$$|C| \geq |A| + |B| - 2|S| - \min_{c \in C} v_{A,B}(c).$$

Zum Beweis der Theoreme benötigen wir folgendes technisches Lemma, welches den Kern der Beweise ausmacht.

Lemma 2.7. *Seien A und B endliche nichtleere Teilmengen von $\mathbb{F}$ und*

$$v_i = |\{(a,b) \in A \times B : a + \lambda_i b = \mu_i\}|$$

für $i = 1, \ldots, k$, wobei $\lambda_i \in \mathbb{F} \setminus \{0\}$ und $\mu_i \in \mathbb{F}$. Sei $h(x,y) \in \mathbb{F}[x,y]$. Angenommen für alle $i = 1, \ldots, k$ gibt es $a \in A$ und $b \in B$ mit $h(a,b) \neq 0$ und $a + \lambda_i b = \mu_i$ und für jedes $(a,b) \in A \times B$ mit $h(a,b) \neq 0$ gibt es genau ein $i \in \{1, \ldots, k\}$ mit $a + \lambda_i b = \mu_i$. Dann haben wir

$$k + min\{v_1, \ldots, v_k\} \geq |A| + |B| - \deg(h).$$

Beweis. Nach Voraussetzung verschwindet

$$f(x,y) := h(x,y) \prod_{j=1}^{k} (x + \lambda_j y - \mu_j)$$

über $A \times B$, denn falls $h(a,b) \neq 0$, dann gibt es ein $i \in \{1, \ldots, k\}$ mit $a + \lambda_i b = \mu_i$. Setze $g_A(x) = \prod_{a \in A}(x - a)$ und $g_B(x) = \prod_{b \in B}(x - b)$. Wegen Theorem 1.1 gibt es $h_A(x,y), h_B(x,y) \in \mathbb{F}[x,y]$, so dass

$$f(x,y) = g_A(x)h_A(x,y) + g_B(y)h_B(x,y) \tag{5}$$

wobei

$$max\{\deg(g_A) + \deg(h_A), \deg(g_B) + \deg(h_B)\} \leq \deg(f).$$

Fixieren wir ein $i \in \{1, \ldots, k\}$ und schreiben $h_B(x,y) = \sum_{s,t \geq 0} c_{st} x^s y^t$, mit $c_{st} \in \mathbb{F}$. Dann ist

$$h_B(x,y) = \sum_{s,t \geq 0} c_{st}((x + \lambda_i y - \mu_i) + \mu_i - \lambda_i y)^s y^t = (x + \lambda_i y - \mu_i)q(x,y) + r(y), \tag{6}$$

wobei $q(x,y) \in \mathbb{F}[x,y]$ und $r(y) = h_B(\mu_i - \lambda_i y, y)$ ist vom Grad höchstens $\deg(h_B)$.

Nehmen wir nun an, dass $k + v_i < |A| + |B| - \deg(h)$. Daraus leiten wir einen Widerspruch her. Setze

$$A_0 = \{a \in A : (\mu_i - a)/\lambda_i \notin B\},$$

dann ist $|A_0| = |A| - v_i$. Für $a \in A_0$ gilt

$$g_B(\frac{\mu_i - a}{\lambda_i})h_B(a, \frac{\mu_i - a}{\lambda_i}) \overset{(5)}{=} f(a, \frac{\mu_i - a}{\lambda_i}) - g_A(a)h_A(a, \frac{\mu_i - a}{\lambda_i}) = 0,$$

da $f(a, \frac{\mu_i - a}{\lambda_i}) = 0$, $g_A(a) = 0$ und wegen $g_B((\mu_i - a)/\lambda_i) \neq 0$ gilt

$$h_B(a, \frac{\mu_i - a}{\lambda_i}) = 0 \text{ und mit (6) folgt } r(\frac{\mu_i - a}{\lambda_i}) = 0.$$

Es gilt nach Annahme $\deg(f) = \deg(h) + k < |A| + |B| - v_i$ und daraus folgt $\deg(r) \leq \deg(f) - \deg(g_B) < |A| - v_i = |A_0|$. Mit Lemma 1.4 haben wir $r(y) \equiv 0$, oder anders formuliert: $h_B(x, y)$ ist teilbar durch $x + \lambda_i y - \mu_i$. Nach Voraussetzung gibt es für das fixierte i ein $a_0 \in A$ und $b_0 \in B$ mit $h(a_0, b_0) \neq 0$ und $a_0 + \lambda_i b_0 = \mu_i$. Also ist $h_B(a_0, b_0) = 0$ und das Polynom $h(a_0, y) \prod_{j=1}^{k}(a_0 + \lambda_j y - \mu_j) = f(a_0, y) = g_B(y)h_B(a_0, y)$ ist teilbar durch $(y - b_0)^2$, da $y - b_0 | g_B(y)$ und $y - b_0 | h_B(a_0, y)$. Weiter ist der hintere Teil $\prod_{j=1}^{k}(a_0 + \lambda_j y - \mu_j)$ nicht durch $(y - b_0)^2$ teilbar, da $a_0 + \lambda_j b_0 \neq \mu_j$ für jedes $j \neq i$, und es folgt $y - b_0 | h(a_0, y)$ im Widerspruch zu $h(a_0, b_0) \neq 0$. Also war die Annahme falsch uns es gilt $k + v_i \geq |A| + |B| - \deg(h)$, insbesondere auch für das Minimum der v_i. □

Beweise von Theorem 2.4. Seien $\mu_1, \ldots, \mu_k$ alle verschiedene Elemente aus C. Wenden wir Lemma 2.7 mit $\lambda_1 = \cdots = \lambda_k = 1$ an, so erhalten wir

$$|C| + \min_{c \in C} v_{A,B}(c) \geq |A| + |B| - \deg(h),$$

wie behauptet. □

Beweis von Theorem 2.5. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass G endlich erzeugt ist. Sei $c_0, c_1, \ldots, c_r$ eine minimale Basis von G, wobei c_0 ein Torsionselement der Ordnung h ist. Dann bilden wir c_0 auf $e^{2\pi i/h}$ und $c_1, \ldots, c_r$ auf beliebige algebraisch unabhängige Elemente des überabzählbaren Einheitskreises $\{e^{2\pi i\theta} : 0 \leq \theta < 1\}$ ab. Diese Abbildung lässt sich auf natürliche Weise zu einer Einbettung φ von G in die multiplikative Gruppe $\mathbb{C}^*$ erweitern. Wir rechnen ab jetzt mit der Multiplikation in $\mathbb{C}$ und den Bilder von A, B und den d_i mittels φ. Also ist

$$C = \{ab : a \in A, b \in B \text{ und } a^{m_i} b^{-n_i} \neq d_i \text{ für alle } i = 1, \ldots, l\}.$$

Seien $-\lambda_1, \ldots, -\lambda_k$ alle verschiedenen Elemente von C und definiere

$$h(x, y) = \prod_{i=1}^{l}(x^{m_i} y^{n_i} - d_i).$$

Dann gibt es für jedes $j \in \{1, \dots, k\}$ ein $a \in A$ und $b \in B$, so dass $a + \lambda_j b^{-1} = 0$ und $h(a, b^{-1}) \neq 0$. Wenn $a \in A$, $b \in B$ und $h(a, b^{-1}) \neq 0$, dann gibt es genau ein $j \in \{1, \dots, k\}$, so dass $\lambda_j = -ab$ (oder anders $a + \lambda_j b^{-1} = 0$). Wenden wir Lemma 2.7 auf die Mengen A und B^{-1} mit $\mu_1 = \dots = \mu_k = 0$ an, so erhalten wir

$$k + \min_{1 \leq j \leq k} |\{(a, b) \in A \times B : a + \lambda_j b^{-1} = 0\}| \geq |A| + |B^{-1}| - \deg(h).$$

Also

$$|C| \geq |A| + |B| - \sum_{i=1}^{l} (m_i + n_i) - \min_{c \in C} |\{(a, b) \in A \times B : ab = c\}|$$

wie gewünscht. □

Beweise von Theorem 2.6. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass G durch die Menge $A \cup B$ endlich erzeugt wird.

Wenn $G \cong \mathbb{Z}^n$, dann können wir G einfach als den Ring der algebraischen Zahlen in dem algebraischen Körper K mit $[K : \mathbb{Q}] = n$ betrachten. Wenn $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ mit p Primzahl, dann ist G isomorph zur additiven Gruppe des endlichen Körpers über p^n Elemente. Also folgt Teil (i) mit $f(x, y) = \prod_{s \in S}(x - y - s)$ direkt aus Theorem 2.4.

Seien $d_1, \dots, d_l$ alle verschiedenen Elemente von S, dann erhalten wir mit Theorem 2.5 und $m_i = n_i = 1$ für alle $i = 1, \dots, l$ direkt Teil (ii). □

Die immer noch offene Vermutung 2.3 wurde 2005 noch verallgemeinert:

Vermutung 2.8 ([39])**.** *Für beliebige endliche nichtleere Teilmengen A und B einer abelschen Gruppe gilt*

$$|A \hat{+} B| \geq min\{|A + B|, |A| + |B| - 1\} - 2.$$

2.3 Snevilys Vermutung

Im Folgenden wird eine Vermutung von Snevilys betrachtet, die von Alon im Jahr 2000 teilweise bestätigt wurde:

Vermutung 2.9. *Sei G eine additive geschriebene abelsche Gruppe, wobei $|G|$ ungerade ist. Seien A und B Teilmengen von G mit $|A| = |B| = n > 0$. Dann gibt es eine Nummerierung $(a_i)_{i=1}^n$ der Elemente von A und $(b_i)_{i=1}^n$ der Elemente von B, so dass $a_i + b_i$ paarweise verschieden sind.*

Alon [2] bewies für $G = \mathbb{F}_p$ eine stärkere Version, in der es multiple Elemente in A gibt.

Theorem 2.10. *Sei p eine Primzahl, angenommen $n < p$, $(a_i)_{i=1}^n$ eine Folge von Elementen aus dem Körper $\mathbb{F}_p$ und $B \subseteq \mathbb{F}_p$ mit $|B| = n$. Dann existiert eine Nummerierung $\{b_i\}_{i=1}^n$ der Elemente von B, so dass $a_i + b_i$ paarweise verschieden sind in $\mathbb{F}_p$.*

Im Fall $n = p$ setzen wir einfach $a_i = b_i$. Das Theorem selbst gilt in diesem Fall nicht, wie $a_1 = a_2 = \cdots = a_{p-1} = 0$, $a_p = 1$ und $B = \{0, 1, \ldots, p-1\}$ zeigen. Ebenso ist für das Theorem die Voraussetzung notwendig, dass wir in einem Primzahlkörper sind, wie das Beispiel $a_1 = a_2 = \cdots = a_{k-1} = 0$, $a_k = s$ und $B = \{0, s, 2s, \ldots, (k-1)s\}$ zeigt, falls $p = ks$.

Beweis. Wir betrachten das folgende Polynom in n Variablen über $\mathbb{F}_p$

$$f(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j) \prod_{1 \le i < j \le n} (a_i + x_i - a_j - x_j).$$

Das Monom $\prod_{i=1}^{n} x_i^{n-1}$ hat Grad $\deg(f)$ in f und daher genügt es Monome von diesem Grad zu betrachten um den Koeffizienten in f zu bestimmen.

$$\prod_{1 \le i < j \le n} (x_i - x_j) \prod_{1 \le i < j \le n} (x_i - x_j) = \prod_{1 \le i < j \le n} (x_i - x_j)^2$$

Dieser Koeffizient ist $\pm n!$, wie man anhand der Dyson Vermutung, Theorem 3.2, sieht, oder direkt aus der Determinante der Vandermonde-Matrix ableiten kann:

$$\prod_{1 \le i < j \le n} (x_i - x_j) = \det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{pmatrix} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} x_i^{\pi(i)-1}.$$

Das Produkt $\prod_{1 \le i < j \le n} (x_i - x_j)$ hat exakt $n!$ Summanden der Form $\prod_{i=1}^{n} x_{\pi(i)}^{n-i}$ repräsentiert durch die Permutation π, von denen sich jeder auf exakt eine Weise zu $\prod_{i=1}^{n} x_i^{n-1}$ ergänzen lässt, nämlich durch den Summanden von $\pi'(i) := n + 1 - \pi(i)$. Um mit Hilfe von Transpositionen π in π' umzuwandeln genügt es k mit $n + 1 - k$ zu vertauscht für $k = 1, \ldots, \lfloor \frac{n}{2} \rfloor$. Also ist $\operatorname{sgn}(\pi) = (-1)^{\lfloor \frac{n}{2} \rfloor} \operatorname{sgn}(\pi')$ und somit ist der gesuchte Koeffizient $\pm n!$.

Da $n < p$ ist dieser Koeffizient ungleich null modulo p und damit folgt aus Theorem 1.3 die Existenz von $b_i \in B$ mit

$$f(b_1, \ldots, b_n) = \prod_{1 \le i < j \le n} (b_i - b_j) \prod_{1 \le i < j \le n} (a_i + b_i - a_j - b_j) \neq 0.$$

Also sind für $i \in \{1, \ldots, n\}$ sowohl die Elemente b_i paarweise verschieden, wie auch die Summen $a_i + b_i$. □

Neben Erweiterungen von Alon gelang es 2001 Dasgupta, Károlyi, Serra und Szegedy [22] die Vermutung für zyklische Gruppen ungerader Ordnung zu beweisen. Weitere Fortschritte konnte Sun 2006 [58] wiederum mit dem kombinatorischen Nullstellensatz verzeichnen.

3 Anwendungen in der Kombinatorik

In diesem Abschnitt stellen wir zwei vor kurzem publizierte Resultate aus dem Gebiet der Kombinatorik vor.

3.1 Ein Platzproblem zu Tisch

Ein König lädt n Paare an seine Tafel mit $2n+1$ Plätzen ein. Für jedes Paar schreibt der König einen Abstand d_i zwischen 1 und n vor, den die Partner einhalten müssen, wobei bei Abstand 1 die Partner nebeneinander sitzen müssen. Natürlich bleibt ein Platz für den König frei.

Theorem 3.1. *Es gibt für beliebige Abstände d_i eine Lösung für das Sitzproblem genau dann, wenn $2n+1$ eine Primzahl ist.*

Kohen und Sadofschi [34] fanden mit Hilfe von Theorem 1.3 einen neuen Beweis für dieses Problem, welches erstmals von Mischler und Preissmann [49] bewiesen wurde. Diesen und auch einen topologischen Beweis publizierten kurz darauf Karasev und Petrov [29], die das Theorem allerdings zahlentheoretisch formulierten. In jedem Fall brauchen wir zum Anwenden des kombinatorischen Nullstellensatz noch eine Vermutung von Dyson [23], die unabhängig 1962 von Wilson [62] und Gunson [27] bewiesen wurde.

Theorem 3.2. *Der Koeffizient vor $\prod_{i=1}^{n} x_i^{a-a_i}$ im Polynom*

$$\prod_{1\le i<j\le n} (-1)^{a_j}(x_i-x_j)^{a_i+a_j} \text{ entspricht } \frac{(a_1+\cdots+a_n)!}{a_1!\cdots a_n!}$$

mit $a=\sum_{i=1}^{n} a_i$.

Für einen kombinatorischen Beweis verweisen wir ausnahmsweise auf [63]. Mit Hilfe einer Abwandlung vom kombinatorischen Nullstellensatz gelang auch Karasev und Petrov [29] ein Beweis dieses Theorems.

Beweis von Theorem 3.1. Wenn $2n+1$ keine Primzahl ist, dann gibt es einen Teiler k mit $1<k<2n+1$. Setzen wir nun alle Abstände $d_i=k$, nummerieren die Sitze im Uhrzeigersinn von 1 bis $2n+1$ und legen die Bahnen von j als alle Sitze mit Nummer kongruent zu $j \pmod k$ fest. Jede Bahn hat die $\frac{2n+1}{k}$ Sitze, da $k|2n+1$, und natürlich sind zwei Sitze mit Abstand k in der selben Bahn. Die Anzahl der Sitze in jeder Bahn ist ungerade, also gibt es jeweils einen leeren Platz, aber nur einen König und damit keine Lösung für das Sitzproblem, da $k>1$.

Sei nun $p=2n+1$ eine Primzahl und seien $d_1,\dots,d_n$ die n Abstände, dann ist $(x_1,\dots,x_n)$ genau dann eine Lösung für das Sitzproblem, wenn die $2n$ Zahlen $x_1,\dots,x_n$, $x_1+d_1,\dots,x_n+d_n$ paarweise verschieden Modulo $p=2n+1$ sind. Dazu betrachten wir folgendes Polynom in $\mathbb{F}_p[x_1,\dots,x_n]$

$$f(x_1,\dots,x_n)=\prod_{1\le i<j\le n}(x_i-x_j)(x_i+d_i-x_j)(x_i-x_j-d_j)(x_i+d_i-x_j-d_j).$$

Das ist das Produkt aller paarweisen Differenzen von $x_1, \ldots, x_n, x_1 + d_1, \ldots, x_n + d_n$ und damit ist genau dann $f(x_1, \ldots, x_n) \neq 0$, wenn $(x_1, \ldots, x_n)$ eine Lösung des Sitzproblems ist.

Wir haben $\deg(f) = 4\binom{n}{2} = n(2n-2)$, also ist $x_1^{2n-2} \cdots x_n^{2n-2}$ ein Monom von Grad $deg(f)$. Um den Koeffizienten dieses Monoms in f zu finden genügt es Monome maximalen Grades in f zu betrachten.

$$\prod_{1 \leq i < j \leq n} (x_i - x_j)^4$$

Nach Theorem 3.2 ist der Koeffizient vor $\prod_{i=1}^n x_i^{2n-2}$ in diesem Polynom $\pm\frac{(2n)!}{2^n}$. Nach Wilsons Theorem ist n genau dann eine Primzahl, wenn $(n-1)! \equiv -1 \pmod{n}$ ist, also ist der Zähler $(2n)! = (p-1)! \equiv -1 \pmod{p}$. Im Nenner wenden wir das kleine fermatsche Theorem an, wonach für p eine Primzahl $a^p \equiv a \pmod{p}$ ist und für $p \nmid a$ weiter $a^{p-1} \equiv 1 \pmod{p}$. Daraus folgt $p | 2^{p-1} - 1 = 2^{2n} - 1 = (2^n + 1)(2^n - 1)$, also $2^n \equiv \pm 1 \pmod{p}$.

Deshalb ist der Koeffizient vor dem betrachteten Monom $\frac{(2n)!}{2^n} \equiv \pm 1 \pmod{p}$ und mit Theorem 1.3 folgt die Existenz der Lösung. □

Eine stärkere Vermutung, die besagt, dass es immer genau dann eine Lösung gibt, wenn die Abstände d_i invertierbar Modulo $2n+1$ sind, ist noch offen. Für den kombinatorischen Nullstellensatz ist erforderlich, dass $\mathbb{Z}/(2n+1)\mathbb{Z}$ ein Körper ist. Auch die Erweiterung des Nullstellensatzes auf Ringe, die wir in Abschnitt 8 vorstellen lässt sich wegen der zusätzlichen Voraussetzung nicht anwenden.

3.2 Damen in Reih und Glied

Martin Gardner führte 1976 das *minimum no-3-in-a-line problem* ein. Dies beinhaltet die Frage nach der minimalen Anzahl an Figuren, die man auf einem $n \times n$ Schachbrett so platzieren kann, dass jede zusäztliche Figur eine Reihe mit 3 Figuren erzeugt. Wir betrachten die Variante mit Damen, also nur orthogonale und diagonale Linien. Ein einfaches Beispiel auf dem klassischen Schachbrett mit 9 Damen sieht man in Abbildung 1, das Hinzufügen einer weiteren Dame erzeugt drei in einer Linie. Es lässt sich nachprüfen, dass 8 Steine nicht ausreichen.

Wir schauen uns erstmal eine schwache untere Schranke für das Problem an. Von q Damen deckt jeder höchstens $4n-4$ Felder ab und jedes der n^2 Felder benötigt entweder zwei Damen, die es abdecken, oder eine die darauf steht. Damit erhalten wir für die benötigte Anzahl der Damen $q + \frac{1}{2}(4n-4)q \geq n^2$ und schließlich $q > \frac{n}{2}$.

Im Jahr 2012 präsentierten Cooper, Pikhurko, Schmitt und Warrington [18] ihre Lösung:

Theorem 3.3. *Für $n \geq 1$ ist die Antwort auf das Damenproblem mindestens n.*

Mit Hilfe eines *brute-force* Algorithmus untersuchten sie das Problem bis $n = 11$ und stellten unter anderem fest, dass es mit 11 Damen nicht möglich ist das 11×11 Brett so

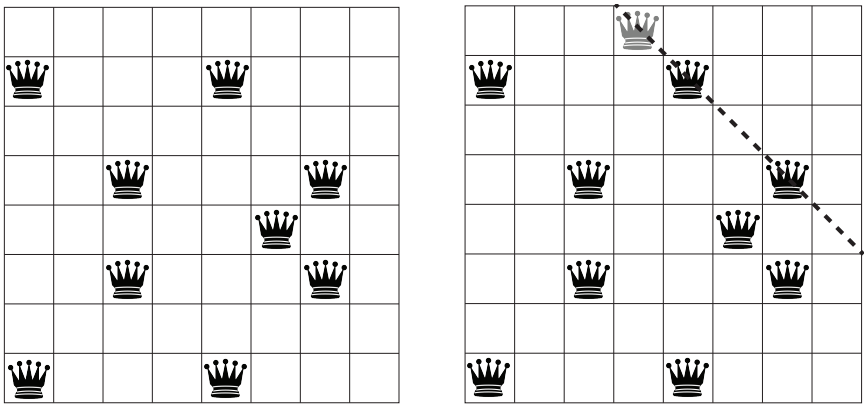

Abbildung 1: Maximale 8×8 Platzierung aus [18]

auszulegen, dass jede weitere Dame eine Dreierreihe erzeugt. Theorem 3.3 ist also nicht für alle n scharf. Weitere Zahlen, Hintergünde und Beispiele finde sich bei Cooper et al. [18].

Neben einem elementaren Beweis für ungerade n geben sie einen Beweis für alle n mit Hilfe des kombinatorischen Nullstellensatzes an, der durch den Beweis von Theorem 1.6 inspiriert wurde.

Beweis von Theorem 3.3. Wir betrachten das Gitter $\mathbb{Z}^2$ und die endliche Teilmenge $B_n = [1, n] \times [1, n]$ als Brett. Linien sind Geraden mit Steigung $0, +1, -1$ oder ∞ und eine Teilmenge S beschreibt die Platzierung von Damen. Jede Platzierung definiert eine Menge von Linien durch alle Damen, die in derselben Spalte oder Zeile liegen. Eine Platzierung ist gut, wenn keine 3 Damen in einer Reihe liegen, jeder weitere aber einer Dreierreihe erzeugt.

Wir unterscheiden vier Fälle nach der Restklasse von $n \pmod 4$. Sei also $n = 4k + 1$, wobei $k \in \{1, 2, \dots\}$. Angenommen es gibt eine gute Platzierung S auf B_n der Größe $s = |S| \leq 4k$. Wir wollen nun ein Polynom $f(x, y)$ von Grad $8k$ konstruieren, dass auf jedem Feld $(x, y) \in B_n$ verschwindet. Mit Hilfe des kombinatorischen Nullstellensatzes soll sich daraus ein Widerspruch ergeben. Die anderen Fälle behandeln wir im Anschluß nach dem selben Prinzip.

Das Polynom f wird aus Linearfaktoren verschiedener Art zusammengesetzt. Als erstes alle durch zwei Damen aus S definierten Linien. Da S eine gute Platzierung ist, liegt jedes unbesetzte Feld auf mindestens einer Linie.

Allerdings kann es Damen geben, die auf keiner schon definierten Linien liegen. Sei $S' = \{S_1, \dots, S_{s'}\}$ die möglicherweise leere Teilmenge der Damen, die nicht auf einer Linie mit einer anderen liegt, und $s' = |S'|$ deren Anzahl. Für jedes $S_i \in S'$ definieren wir eine neue Linie durch das von S_i besetzte Feld. Wir können die Steigung der Linie frei wählen, da alle freien Felder bereits durch Linien abgedeckt werden. Die i-te Linie bekommt die j-te Steigung aus $\{0, +1, -1, \infty\}$, wobei $j \equiv i \pmod 4$. Nun liegt auch jedes besetzte Feld auf einer Linie der beiden Sorten.

Da S eine gute Platzierung ist liegen maximal zwei Damen in einer Reihe. Linien gleicher Steigung liegen also parallel und werden durch zwei Damen definiert. Für jede der möglichen Steigungen gibt es damit höchstens $\lfloor \frac{4k-s'}{2} \rfloor$ Linien der ersten und höchstens $\lceil \frac{s'}{4} \rceil$ der zweiten Sorte. Zusammen ergibt das für jede Steigung höchstens $2k$ Linien. Um später den Nullstellensatz anwenden zu können fügen wir nun beliebige weitere Linien hinzu bis wir jeweils $2k$ haben.

Sei $L = \{L_1, \dots, L_{8k}\}$ die Menge aller $8k$ Linien und $l_i = 0$ die Gleichung in Variablen x und y, die L_i beschreibt. Wir definieren

$$f(x,y) = \prod_{i=1}^{8k} l_i \in \mathbb{R}[x,y].$$

Wie gewünscht gilt $f(x,y) = 0$ für $(x,y) \in B_n$. Nach Konstruktion hat f Grad $8k$. Sortiert nach der Steigung können wir f umschreiben zu

$$f(x,y) = \prod_{j=1}^{2k} (x-\alpha_j)(y-\beta_j)(x-y-\gamma_j)(x+y-\delta_j)$$

mit geeigneten Konstanten $\alpha_j, \beta_j, \gamma_j, \delta_j$. Den Koeffizienten vor $x^{4k}y^{4k}$ in f finden wir, indem wir nur Monome maximalen Grades betrachten. Wir erhalten ein neues Polynom $\prod_{j=1}^{2k} xy(x-y)(x+y) = x^{2k}y^{2k}(x^2-y^2)^{2k}$ und mit dem Binomischen Lehrsatz ist der Koeffizient vor $x^{2k}y^{2k}$ in $(x^2-y^2)^{2k}$ exakt $\pm\binom{2k}{k} \neq 0$, also auch der vor $x^{4k}y^{4k}$ in f. Nun wenden wir Theorem 1.3 an und erhalten mit $f(x,y) \neq 0$ für ein $(x,y) \in B_n$ den gesuchten Widerspruch.

Sei nun $n = 4k$ für $k \in \{1, 2, \dots\}$. Ähnlich wie oben betrachten wir wieder eine gute Platzierung S auf B_n, diesmal der Größe $s \leq 4k-1$ gesucht. Weiter sei $s' = 4r + s$ die Größe von S' mit $r, s \in \{0, 1, \dots\}$ und $0 \leq s \leq 3$. Wie zuvor definieren wir die ersten beiden Sorten von Linien und erhalten als maximale Anzahl für jede Steigung abhängig von r und s

$$g(r,s) = \left\lfloor \frac{4k-1-4r-s}{2} \right\rfloor + \left\lceil \frac{4r+s}{4} \right\rceil,$$

wobei der erste Summand wieder die Linien der ersten Sorte und der zweite Summand die der zweiten Sorte beschreibt.

Für $s \neq 1$ haben wir $g(r,s) \leq 2k-1$, genauso für $s = 1$ und $r > 0$. In diesen Fällen verfahren wir wie oben und fügen Linien hinzu, bis wir von jeder Steigung $2k-1$ haben. Wir konstruieren ein Polynom von Grad $8k-4$ mit Koeffizienten vor $x^{4k-2}y^{4k-2}$ ungleich Null und kommen wieder mit Theorem 1.3 zum Widerspruch.

Es bleibt der Fall $s = 1$ und $r = 0$, also $q' = 1$. Wir haben $g(1,0) = 2k$ und bekommen daher möglichweise schon $2k-1$ Linien der ersten Sorte. Wir fügen eine Linie für die Dame in S' mit Steigung ∞ hinzu und danach so lange weitere Linien bis wir $2k$ mit Steigung ∞ haben und $2k-1$ für die anderen. Unser Polynom hat nun Grad $8k-3$ und wir betrachten das folgenden führende Monom mit Koeffizienten ungleich

Null $\binom{2k-1}{k} x^{2k} y^{2k-1} (x^2)^{k-1} (-y^2)^k = (-1)^k \binom{2k-1}{k} x^{4k-2} y^{4k-1}$. Wie zuvor erhalten wir mit Theorem 1.3 einen Widerspruch.

Der Fall $n = 4k+2$ geht analog wie der eben beschriebene, nur haben wir jeweils eine Linie mehr und die Grade der Polynome sind um 4 größer. Bei $n = 4k+3$ verfahren wir wieder wie im ersten Fall. Es entstehen maximal $2k+1$ Linien jeder Steigung und wir konstruieren ein Polynom von Grad $8k+4$ mit Koeffizienten ungleich Null vor $x^{4k+2} y^{4k+2}$. In allen Fällen gelangen wir mit dem kombinatorischen Nullstellensatz zum Widerspruch. Die Annahme, dass es eine gute Platzierung der Größe $n-1$ gibt, ist also jeweils falsch. □

Analog zu dem hier behandelten Problem führte Gardner das *maximum no-3-in-a-line* Problem ein, welches nach dem Maximum an Damen sucht, die sich auf dem Brett platzieren lassen, ohne dass 3 auf einer Linie stehen. Aus dem Taubenschlagprinzip erhalten wir $2n$ als obere Schranke, da in jeder Spalte höchstens 2 Damen platziert werden können. Guy und Kelly [28] stellten die Vermutung auf, dass für große n sind keine $2n$ Damen platzieren lassen, und untermauerten diese Vermutung mit Wahrscheinlichkeitstheoretischen Berechnungen.

4 Anwendungen in der Graphentheorie

Die Graphentheorie ist ein wichtiges Teilgebiet der diskreten Mathematik, in der viele interessante Konzepte entwickelt wurden.

Ein Graph $G = (V, E)$ besteht aus einer Menge von Knoten $V(G) = V$ und Kanten $E(G) = E$ auf V. Wir unterscheiden zwischen gerichteten $E \subseteq V \times V$ und ungerichteten $E \subseteq \{\{v, w\} : v, w \in V\}$ Graphen. Eine Orientierung eines ungerichteten Graphen $G = (V, E)$ ist ein gerichteter Graph D, so dass für alle $\{v, w\} \in E$ gilt entweder $(v, w) \in E(D)$ oder $(w, v) \in E(D)$.

Wenn wir auch Mehrfachkanten zulassen wollen, dann ist E eine Multimenge. Als Schleife bezeichnen wir eine Kante (v, v) bzw. $\{v\}$. Wir nennen einen ungerichteten Graphen ohne Mehrfachkanten und Schleifen einfach. Der Grad eines Knoten bezeichnet die Anzahl der adjazenten Kanten. Wir definieren $d(v) = |\{w \in V : \{v, w\} \in E\}|$ als den Grad in ungerichtete Graphen. In gerichteten Graphen unterscheiden wir Eingrad $d^-(v) = |\{w \in V : (w, v) \in E\}|$ bzw. Ausgrad $d^+(v) = |\{w \in V : (v, w) \in E\}|$ für jeden Knoten $v \in V$. Wenn nicht deutlich wird, in welchem Graphen wir den Grad suchen, führen wir diesen als Index mit.

4.1 Untergraphen

Nach einer 1982 von Taśkinow [59] bewiesenen Vermutung von Berge und Sauer enthält jeder einfache 4-reguläre Graph einen 3-regulären Untergraphen. Für Graphen mit Mehrfachkanten ist dies falsch, wie Abbildung 2 zeigt. Dieser Umstand lässt sich aber durch eine beliebige zusätzliche Kante beheben, wovon man sich an dem Graphen überzeugen kann und durch den Fall $p = 3$ des folgenden Theorems bewiesen wird.

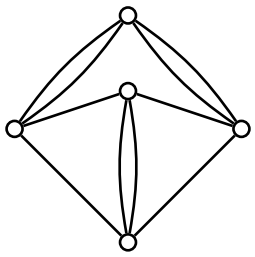

Abbildung 2: 4-regulärer Graph ohne 3-regulären Untergraphen

Theorem 4.1 ([4])**.** *Für eine Primzahl p enthält ein schleifenloser Graph $G = (V, E)$ mit durchschnittlichem Grad größer als $2p - 2$ und maximalem Grad höchstens $2p - 1$ einen p-regulären Untergraphen.*

Beweis. Sei $(a_{v,e})_{v \in V, e \in E}$ die Inzidenzmatrix von G, definiert durch $a_{v,e} = 1$, falls $v \in e$, und $a_{v,e} = 0$ sonst. Wir weisen jeder Kante $e \in E$ eine Variable x_e zu und betrachten das Polynom

$$f = \prod_{v \in V} \left[1 - \left(\sum_{e \in E} a_{v,e} x_e \right)^{p-1} \right] - \prod_{e \in E} (1 - x_e)$$

über $\mathbb{F}_p$. Der Grad von f ist $|E|$, denn der Grad des zweiten Produktes ist genau $|E|$ und der des ersten ist höchstens $(p-1)|V|$, also nach der Voraussetzung über den durchschnittlichen Grad $\frac{1}{2}(2p-2)|V| < |E|$. Des Weiteren ist der Koeffizient vor $\prod_{e \in E} x_e$ in f genau $(-1)^{|E|+1} \neq 0$.

Also existieren mit Theorem 1.3 Werte $x_e \in \{0, 1\}$, so dass $f(x_e : e \in E) \neq 0$. Nach Definition von f ist $(x_e : e \in E)$ nicht der Nullvektor, denn $f(\mathbf{0}) = 0$. Außerdem ist für diesen Vektor $\sum_{e \in E} a_{v,e} x_e \equiv 0 \pmod{p}$ für alle $v \in V$, da sonst $\left(\sum_{e \in E} a_{v,e} x_e\right)^{p-1} = 1$ und damit $f = 0$ an dieser Stelle wäre. Also sind in dem Untergraphen von G, der durch alle Kanten $e \in E$ induziert wird für die $x_e = 1$ ist, alle Grade teilbar durch p. Da aber der maximale Grad kleiner als $2p$ ist, sind alle positiven Grade exakt p. Durch Weglassen aller überflüssigen Kanten und Knoten mit Grad 0 erhalten wir den gesuchten p-regulären Graphen. □

Die Aussage wird von Alon et al. [4] auch für Primzahlpotenzen bewiesen, der allgemeine Fall bleibt allerdings offen. Mit Hilfe dieses Theorems zeigte Pyber [50], dass jeder Graph mit mindestens $200n \log(n)$ Kanten einen 3-regulären Untergraphen besitzt und beschränkte damit die maximale Anzahl an Kanten, die ein Graph ohne 3-regulären Untergraphen haben kann.

Folgende Anwendung, die sich ebenfalls auf Primzahlpotenzen p erweitern lässt, ist nicht sehr naheliegend, zeigt aber die Vielseitigkeit der Methode:

Proposition 4.2. *Sei p eine Primzahl und $G = (V, E)$ ein Graph auf $|V| > d(p-1)$ Knoten. Dann gibt es eine nichtleere Teilmenge U der Knoten von G, so dass die Anzahl der K_d in G die U schneiden 0 modulo p ist.*

Beweis. Für jede Teilmenge I von Knoten von G, sei $K(I)$ die Anzahl der Kopien von K_d in G, die I enthalten. Wir weisen jedem Knoten $v \in V$ eine Variable x_v zu und betrachten das Polynom

$$f = \prod_{v \in V} (1 - x_v) - 1 + g,$$

über $\mathbb{F}_p$, wobei

$$g = \left(\sum_{\emptyset \neq I \subset V} (-1)^{|I|+1} K(I) \prod_{i \in I} x_i \right)^{p-1}.$$

$K(I)$ ist Null für alle I der Kardinalität größer als d und der Grad von g ist höchstens $d(p-1) < |V|$. Also ist der Grad von f $|V|$. Des Weiteren ist der Koeffizient vor $\prod_{v \in V} x_v$ in f genau $(-1)^{|V|} \neq 0$. Also gibt es mit Theorem 1.3 $x_v \in \{0, 1\}$, so dass $f(x_v : v \in V) \neq 0$. Da f auf dem Nullvektor Null wird sind nicht alle x_v Null und damit $g(x_v : v \in V) \neq 1$. Mit Fermats kleinem Theorem folgt

$$\sum_{\emptyset \neq I \subset V} (-1)^{|I|+1} K(I) \prod_{i \in I} x_i \equiv 0 \pmod{p}.$$

Jedenfalls ist die linke Seite der Kongruenz nach der Inklusions-Enklusions-Formel exakt die Anzahl der Kopien von K_d, die die Menge $U = \{v : x_v = 1\}$ schneiden. Da U nicht leer ist folgt die Behauptung. □

4.2 Graphenfärbung

Dieser Abschnitt behandelt die korrekte Färbung eines Graphen $G = (V, E)$. Der klassische Ansatz der Knotenfärbung sucht nach einer Funktion $h : V \to \{1, 2, \ldots, k\}$, die benachbarte Knoten unterschiedlich färbt, also $h(v) \neq h(w)$ für alle $\{v, w\} \in E$, und bezeichnet G dann als k-färbbar. Wir werden in diesem Abschnitt zwei weiterführende Konzepte miteinander verbinden.

Beim *list colouring*, initiiert unter anderem von Erdös, Rubin und Taylor [26], wird die Auswahl der Farben für jeden Knoten eingeschränkt. Ist L eine Farblistenzuweisung, weist also jedem Knoten eine Menge von Farben zu, so ist der Graph L-färbbar, wenn es eine korrekte Knotenfärbung h gibt mit $h(v) \in L(v)$ für alle $v \in V$.

Für $p \geq q \in \mathbb{Z}$ sind $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ unsere Farben und der Abstand zwischen zwei Farben $i, j \in \mathbb{Z}_p$ ist definiert als $|i - j|_p = min\{|i - j|, p - |i - j|\}$. Dies ist als p Punkte auf einem Kreis vorstellbar, wobei der Abstand der kürzeste Weg auf diesem Kreis von i nach j ist. Eine (p, q)-Färbung eines Graphen $G = (V, E)$ ist nun eine Abbildung $h : V \to \mathbb{Z}_p$, so dass die Farben benachbarter Knoten einen Abstand von mindestens q haben, für jede Kante $\{u, v\} \in E$ gilt $|h(u) - h(v)|_p \geq q$. Dieses *circular colouring* wurde erstmals von Vince [60] eingeführt.

Als motivierendes Beispiel von Lin et al. [41] stellen wir uns V als Menge von Aufgaben vor, die mit Periode p immer wieder erfüllt werden müssen, beispielsweise bei einem

Wartungsprozess. Ein Zeitplan ist jetzt eine Abbildung $h : V \to \mathbb{Z}_p$, wobei $h(v)$ das Starten von Aufgabe v repräsentiert. Eine Kante zwischen zwei Aufgaben bedeutet, dass diese nicht parallel ausgeführt werden dürfen. Wenn jede Aufgabe also eine feste Zeit q benötigt, dann muss der Abstand des Startzeitpunktes für Aufgaben $v, w \in V$ mit $\{v, w\} \in E$ größer als q auf dem Kreis sein, also $|h(v) - h(w)|_p \geq q$. Ein solcher periodische Zeitplan ist dann eine (p, q)-Färbung des Graphen $G = (V, E)$. Nun können natürlich noch weitere Bedingungen, wie eine Einschränkung der möglichen Starzeiten von v auf $L(v) \subseteq \mathbb{Z}_p$, hinzukommen, weil bestimmte Aufgaben vor anderen begonnen werden müssen.

Wir verbinden also beide Konzepte und erhalten das *list circular colouring*. Ein Graph G ist L-(p, q)-färbbar für eine p-Farblistenzuweisung L, also $L(v) \subseteq \mathbb{Z}_p$, wenn es eine (p, q)-Färbung h von G gibt mit $h(v) \in L(v)$ für alle $v \in V$.

Sei D eine Orientierung eines Graphen. Ein Untergraph D' ist genau dann eulersch, wenn $d^+(v) = d^-(v)$ für alle $v \in V$. Wir bezeichnen mit $EE(D)$ die Anzahl der eulerschen Untergraphen von D mit einer geraden Anzahl an Kanten und $EO(D)$ die mit einer ungeraden Anzahl. Folgendes Theorem von Alon und Tarsi [11] enthält im Beweis die Grundzüge des kombinatorischen Nullstellensatzes.

Theorem 4.3. *Angenommen G hat eine Orientierung D für die $EE(D) \neq EO(D)$. Wenn L eine Farblistenzuweisung ist und $|L(v)| = d_D^+(v) + 1$ für alle $v \in V$, dann ist G L-färbbar.*

Eine Übersicht über Anwendungen und Folgerungen dieses Theorems wurde von Alon [1] zusammengestellt. Wir schauen uns eine Verallgemeinerung von Norine, Wong und Zhu [45] auf (p, q)-Färbungen an. Ein eulerscher Untergraph D' von D entspricht einer Abbildung $\phi : E(D) \to \{0, 1\}$ mit $\sum_{e \in E_D^+(v)} \phi(e) = \sum_{e \in E_D^-(v)} \phi(e)$. Dabei definieren wir $E_D^+(v) = \{(w, v) \in E(D)\}$ bzw. $E_D^-(v) = \{(v, w) \in E(D)\}$. Für jedes $q \in \mathbb{N}$ nennen wir die Abbildung $\phi : E(D) \to \{0, 1, 2, \ldots, 2q - 1\}$ eulersch (bezüglich q), falls $\sum_{e \in E_D^+(v)} \phi(e) = \sum_{e \in E_D^-(v)} \phi(e)$ für alle $v \in V$. Ein eulersche Abbildung ϕ ist gerade bzw. ungerade, wenn $\sum_{e \in E(D)} \phi(e)$ gerade bzw. ungerade ist.

Angenommen ϕ ist eine eulersche Abbildung (bezüglich zu q) und $p \geq q$, dann weisen wir ϕ das Gewicht

$$w_{p,q}(\phi) = \prod_{e \in E(D)} a_{\phi(e)}$$

zu, wobei

$$a_{\phi(e)} = \sum_{K \subseteq \{-q+1, \ldots, q+1\}, |K| = \phi(e)} \prod_{k \in K} \alpha^k.$$

Dabei ist α eine primitive p-te Einheitswurzel, also $\alpha^p = 1$, aber $\alpha^k \neq 1$ für $1 \leq k < p$. $a_{\phi(e)}(p, q)$ ist reell, denn es stimmt mit seinem komplex konjugierten überein

$$\overline{a_{\phi(e)}} = \sum_{K \subseteq \{-q+1, \ldots, q-1\}, |K| = \phi(e)} \prod_{k \in K} \alpha^{-k} = a_{\phi(e)}.$$

Theorem 4.4. *Angenommen $G = (V, E)$ hat eine Orientierung D für die*

$$\sum_{\phi \text{ gerade eulersch}} w_{p,q}(\phi) \neq \sum_{\phi \text{ ungerade eulersch}} w_{p,q}(\phi). \tag{7}$$

Wenn L eine p-Farblistenzuweisung ist mit $|L(v)| = d_D^+(v)(2q-1)+1$, dann ist G L-(p,q)-färbbar.

Für $q = 1$ ist $w_{p,1} = 1$ und damit ist Gleichung (7) äquivalent zu $EE(D) \neq EO(D)$. Das Theorem von Alon und Tarsi ist also ein Spezialfall. Offen bleibt hier die Frage, nach der Umkehrung: Genügt es wenn ein Graph eine Orientierung besitzt, für die $EE(D) \neq EO(D)$ gilt, damit er auch eine besitzt, die Gleichung (7) für alle p,q erfüllt?

Beweis. Für $V = \{v_1, \ldots, v_n\}$ betrachten wir das Polynom $f(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ definiert durch

$$f(x_1, \ldots, x_n) = \prod_{(v_i,v_j)\in E(D)} \prod_{t=-q+1}^{q-1} (x_i - \alpha^t x_j).$$

Die Abbildung $\gamma : \mathbb{Z}_p \to \mathbb{C}$ definiert durch $\gamma(k) = \alpha^k$ für $k \in \mathbb{Z}_p$ ist wohldefiniert, da $\alpha^p = 1$. Für eine Kante $(v_i, v_j) \in E(D)$ und eine Färbung $h : V \to \mathbb{Z}_p$ betrachten wir nun $\gamma(h(v_i))$ und $\gamma(h(v_j))$. Das α erzeugt die Gruppe der p-ten Einheitswurzeln und definiert eine zyklische Anordnung. Für die verschiedenen t durchläuft $\alpha^t\gamma(h(v_j))$ also die Werte aller Nachbarn von v_j mit Abstand kleiner q in dieser Anordnung. Es existiert damit genau dann ein $t \in \{-q+1, \ldots, q-1\}$ mit $\gamma(h(v_i)) - \alpha^t\gamma(h(v_j)) = 0$, wenn $|h(v_i) - h(v_j)|_p < q$. Also ist h eine korrekte (p,q)-Färbung genau dann, wenn

$$f(\gamma(h(v_1)), \gamma(h(v_2)), \ldots, \gamma(h(v_n))) \neq 0.$$

Es folgt direkt, dass Graph L-(p,q)-färbbar ist für $S_i = \{\gamma(a) : a \in L(v_i)\}$ genau dann, wenn es $s_i \in S_i$ gibt, so dass $f(s_1, \ldots, s_n) \neq 0$.

Sei $t_i = d_D^+(v_i)(2q-1) = |S_i|$ für $i = 1, \ldots, n$. Dann ist $\deg(f) = |E|(2q-1) = \sum_{i=1}^n t_i$. Um den Beweis mit Theorem 1.3 zu beenden genügt es also zu zeigen, dass der Koeffizient vor $\prod_{i=1}^n x_i^{t_i}$ in f nicht Null ist.

Ist eine Abbildung $\phi : E(D) \to \{0, 1, \ldots, 2q-1\}$ eulersch (bezüglich q), so erhalten wir

$$\prod_{e=(v_i,v_j)\in E(D)} x_i^{2q-1-\phi(e)} x_j^{\phi(e)} = \prod_{i=1}^n \left(\prod_{e\in E_D^+(v_i)} x_i^{2q-1-\phi(e)} \right) \left(\prod_{e\in E_D^-(v_i)} x_i^{\phi(e)} \right) = \prod_{i=1}^n x_i^{d_D^+(v_i)(2q-1)}.$$

Man sieht, ϕ leistet einen Beitrag zu dem Koeffizienten vor $\prod_{i=1}^n x_i^{t_i}$ in f genau dann, wenn ϕ eulersch ist.

Für eine einzelne Kante (v_i, v_j) in $E(D)$ und $0 \leq l \leq 2q-1$ ist der Koeffizient vor $x_i^{2q-1-l} x_j^l$ in $\prod_{t=-q+1}^{q-1}(x_i - \alpha^t x_j)$ exakt

$$\sum_{K\subseteq\{-q+1,\ldots,q-1\},|K|=l} \prod_{k\in K} -\alpha^k = (-1)^l a_l.$$

Also entspricht der Koeffizient vor $\prod_{i=1}^{n} x_i^{t_i}$ in f genau

$$\sum_{\phi \text{ ist eulersch}} \prod_{e \in E(D)} (-1)^{\phi(e)} a_{\phi(e)} = \sum_{\phi \text{ ist gerade eulersch}} w_{p,q}(\phi) - \sum_{\phi \text{ ist ungerade eulersch}} w_{p,q}(\phi).$$

Nach Voraussetzung ist dies nicht Null und damit G ist L-(p,q)-färbbar. □

Von Norine et al. [45] wird zusätzlich gezeigt, dass für einen Graphen G mit Orientierung D ohne ungeraden gerichteten Kreis auch Gleichung (7) gilt und damit wie in Theorem 4.4 G auch L-(p,q)-färbbar ist. Zusätzlich wurde eine stärkere Aussage für bipartite Graphen bewiesen. Außerdem wurden Folgerungen für die verschiedenen chromatischen Zahlen genannt, welche eine Einordnung und Bewertung der Ergebnisse ermöglichen.

4.3 Eigenschaften von Graphen durch Polynomideale

Die folgenden Theoreme liefern uns allesamt Aussagen über bekannte Eigenschaften von Graphen genau dann, wenn bestimmte Polynome in vorgegebenen Idealen liegen. Es handelt sich also um eine Verknüpfung zwischen Graphentheorie und Algebra. Da unser Polynomring kommutativ ist und eine Eins besitzt ist für eine Menge $A \subseteq R[x_1, \ldots, x_n]$ das von ihr erzeugte Ideal definiert als

$$(A) = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R[x_1, \ldots, x_n], a_i \in A\}.$$

Unter den Voraussetzungen von Theorem 1.1 liegt das f aus $\mathbb{F}[x_1, \ldots, x_n]$ also im von den g_i erzeugten Ideal $f \in (\{g_i(x_i) : 1 \leq i \leq n\})$.

Das Graphpolynom $f_G = f_G(x_1, \ldots, x_n)$ eines Graphen $G = (V, E)$ auf einer Menge $V = \{v_1, \ldots, v_n\}$ von n-Kanten ist definiert durch

$$f_G(x_1, \ldots, x_n) = \prod_{\substack{i<j \\ \{v_i, v_j\} \in E}} (x_i - x_j)$$

Theorem 4.5 (Alon, Tarsi [11]). *Ein Graph G auf n Knoten $\{1, 2, \ldots, n\}$ ist nicht k-färbbar genau dann, wenn das Graphpolynom f_G in dem Ideal liegt, welches von den Polynomen $\{x_i^k - 1 : 1 \leq i \leq n\}$ erzeugt wird.*

Insbesondere ist also G genau dann bipartit, wenn f_G nicht in dem von den Polynomen $x_i^2 - 1$ erzeugten Ideal liegt. Wir betrachten als Knotenfärbung einen Vektor $\mathbf{s} \in \mathbb{F}^n$, der jedem Knoten seine Farbe zuweist. G ist k-färbbar, wenn es eine Knotenfärbung gibt, die mit k Farben auskommt.

Beweis. Wenn f_G im von den Polynomen $x_i^k - 1$ erzeugten Ideal liegt, dann wird es Null, sofern $\mathbf{s}$ nur aus k-ten Einheitswurzeln besteht. Das bedeutet, dass es in jeder Knotenfärbung $\mathbf{s}$ von G aus k-ten Einheitswurzeln ein paar adjazenter Knoten mit der selben Farbe gibt, da sonst $f_G(\mathbf{s})$ nicht Null wäre. G ist also nicht k-färbbar.

Nehmen wir andersherum an, dass G nicht k-färbbar ist. Dann ist $f_G(\mathbf{s}) = 0$, wenn $\mathbf{s}$ nur k verschiedene Einträge hat, also insbesondere für k-te Einheitswurzeln. Das sind genau die Nullstellen der Polynome $g_i(x_i) = x_i^k - 1$ und mit Theorem 1.1 gilt $f_G = \sum_{i=1}^{n} h_i g_i$ für Polynome $h_i \in R[x_1, \ldots, x_n]$. f_G liegt also im von $\{x_i^k - 1 : 1 \leq i \leq n\}$ erzeugten Ideal. □

Der entscheidende Punkt, der uns die Anwendung des kombinatorischen Nullstellensatzes ermöglicht ist, dass wir die Polynome, die das Ideal erzeugen für Mengen $S_i \subseteq \mathbb{F}$ als $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$ schreiben können. Es gibt noch vergleichbare Theoreme mit einer Bedingung an das Graphenpolynom z.B. von Li und Li [40] oder Kleitmann und Lovász [42, 43], bei denen das Ideal aber selbst von Graphenpolynomen erzeugt wird. Diese Polynome hängen von mehreren Variablen ab und lassen sich daher nicht durch Mengen S_i beschreiben. Deshalb ist nur der Hilbertsche Nullstellensatz anwendbar, wodurch aber weitere Probleme entstehen.

In diesem Zusammenhang stellen wir jetzt drei weitere Beispiele vor, von denen das erste eigenständig entwickelt wurde und die hinteren beiden von Alon [1] stammen.

Theorem 4.6. *Sei α eine primititve n-te Einheitswurzel ($\forall 1 \leq k < n : \alpha^k \neq 1$).Ein Graph G besitzt keinen Hamiltonkreis genau dann, wenn das Polynom*

$$P_G(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \prod_{v \in V} \prod_{(v,w) \notin E} (\alpha x_v - x_w)$$

im von den Polynomen $\{x_i^n - 1 : 1 \leq i \leq n\}$ erzeugten Ideal liegt.

Wenn $\mathbf{s} = (s_1, \ldots, s_n)$ aus n Verschiedenen n-ten Einheitswurzeln besteht, dann definiert $\mathbf{s}$ eine zyklische Anordnung, wobei αs_i der Nachfolger von s_i ist. Dies kann dadurch verdeulicht werden, dass α eine primitve n-te Einheitswurzel ist, damit $\alpha^k s_i$ ebenfalls und $\alpha^k s_i \neq s_i$ für alle $1 \leq i \leq n$ und $1 < k < n$.

Beweis. Falls P_G in dem Ideal liegt, ist $P_G(\mathbf{s}) = 0$ wenn $\mathbf{s}$ nur aus n-ten Einheitswurzeln besteht. Insbesondere auch dann, wenn alle s_i verschieden sind und das erste Produkt nicht Null werden kann. Dann muss es ein $(v, w) \notin E$ mit $\alpha s_v - s_w = 0$ geben damit das zweite Produkt Null wird. Die Kante von v nach w fehlt also in G und $\mathbf{s}$ definiert keinen Hamiltonkreis. Da $\mathbf{s}$ uns jede beliebige Permutation der Kanten liefert kann es keinen Hamiltonkreis geben.

Angenommen G hat keinen Hamiltonkreis. Wir betrachten $P_G(\mathbf{s})$ für $\mathbf{s}$ aus n-ten Einheitswurzeln. Gibt es $i \neq j$ mit $s_i = s_j$, so wird das erste Produkt Null. Andernfalls sind alle s_i verschieden. $\mathbf{s}$ kann aber keinen Hamiltonkreis darstellen, es muss also eine Kante fehlen. Damit existiert $(u, w) \notin E$ mit $\alpha s_v - s_w = 0$ und das zweite Produkt wird Null. Zusammen wird das Polynom P_G Null für Werte aus $S_i = \{s : s^n = 1\}$. Wegen Theorem 1.1 liegt das Polynom wie gewünscht in dem von den Polynomen $g_i(x_i) = x_i^n - 1$ erzeugtem Ideal. □

Das Theorem lässt sich auch auf Kreise beliebiger Länge $k \leq n$ erweitern. Dabei wird allerdings der vordere Teil des Polynoms P_G sehr komplex, da er sicherstellen muss, dass jede k-te Einheitswurzel vorkommt.

Eine weitere eingehend untersuchte Eigenschaft von Graphen ist die Bandbreite, welche auch für Bäume schwierig zu bestimmen ist. Für einen Graphen $G = (V, E)$ auf n Knoten ist die Bandbreite die kleinste Zahl k, so dass eine Bijektion $f : V \to \{1, 2, \ldots, n\}$ existiert mit $|f(u) - f(v)| \leq k$ für alle $\{u, v\} \in E$. Es geht also darum, die Knoten so auf einer Linie anzuordnen, dass ein möglichst geringer Abstand zwischen benachbarten Knoten liegt. Abbildung 3 zeigt zwei einfache Beispiele. Eine gute Übersicht über die Thematik findet sich bei Chung [17].

Die Motivation die Bandbreite von Graphen zu studieren entstand in der numerischen Analysis. In einer $n \times n$ Matrix (a_{ij}) mit Nullen auf der Diagonale sollen alle weiteren Nullen möglichst dicht um die Diagonale verteilt sein, damit Algorithmen wie der Gauß- oder Invertierungs-Algorithmus effizienter arbeiten. Die Bandbreite des Graphens auf n Knoten mit Kantenmenge $E = \{\{i, j\} : a_{ij} = 0\}$ gibt uns das schmalst mögliche Band um die Diagonale in der wir alle Nullen platzieren können.

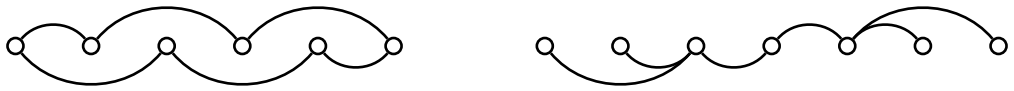

Abbildung 3: C_6 und $T_{2,3}$ haben Bandbreite 2.

Theorem 4.7. *Die Bandbreite eines Graphen $G = (V, E)$ auf n Knoten ist mindestens $k + 1$ genau dann, wenn das Polynom*

$$Q_{G,k}(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \prod_{ij \in E, i<j} \prod_{k<l<n} (x_i - x_j - l)$$

in dem Ideal liegt, welches von den Polynomen

$$\{g_i(x_i) = \prod_{j=1}^{n} (x_i - j) : 1 \leq i \leq n\}$$

erzeugt wird.

Offensichtlich hat ein Graph mit maximalem Grad größer als k eine Bandbreite von mindestens $k + 1$.

Beweis. Wenn $Q_{G,k}$ in dem oben beschriebenen Ideal liegt, wird es Null, falls wir Werte s_i aus $\{1, 2, \ldots, n\}$ für die x_i einsetzen. Insbesondere auch dann, wenn wir verschiedene Werte für diese Variablen einsetzten und das erste Produkt nicht Null werden kann. Es gibt also eine Kante $(i, j) \in E$ mit $|s_i - s_j| = l > k$, die Bandbreite ist also größer als k.

Nehmen wir andersherum an, dass die Bandbreite von G größer als k ist. Wir betrachten $Q_{G,k}(s_1, \ldots, s_n)$ für s_i aus $\{1, 2, \ldots, n\}$. Falls es $i \neq j$ gibt mit $s_i = s_j$, dann wird das erste Produkt Null. Andererseits bilden die s_i eine Permutation von $\{1, 2, \ldots, n\}$ und wegen der Voraussetzung an die Bandbreite gibt es für diese Permutation eine Kante

$(i,j) \in E$ mit $|s_i - s_j| > k$. Also wird in diesem Fall der hintere Teil des Polynoms Null. Zusammen wird das Polynom $G_{G,k}$ Null für Werte aus $S_i = \{1, 2, \ldots, n\}$ und wegen Theorem 1.1 liegt das Polynom wie gewünscht im von den $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$ erzeugten Ideal. □

Ein Hypergraph $H = (V, E)$ besteht aus endlich vielen Knoten V und einer Kantenmenge $E \subseteq \mathcal{P}(V)$ bestehend aus Teilmengen von V. Er ist k-uniform, falls jede Kante Kardinalität k besitzt. Also wäre ein 2-uniformer Hypergraph einfach ein üblicher ungerichteter Graph. H ist 2-färbbar, wenn es eine Knotenfärbung von H mit zwei Farben gibt, so dass keine Kante einfarbig ist.

Theorem 4.8. *Der 3-uniforme Hypergraph $H = (V, E)$ ist nicht 2-färbbar genau dann, wenn das Polynom*

$$\prod_{e \in E}[(\sum_{v \in e} x_v)^2 - 9]$$

in dem Ideal liegt, welches von den Polynomen $\{x_v^2 - 1 : v \in V\}$ erzeugt wird.

Beweis. Wenn das Polynom in dem von $\{x_v^2 - 1 : v \in V\}$ erzeugten Ideal liegt, wird es Null für Werte von x_v aus $\{-1, 1\}$. Wir finden also in jeder Knotenfärbung mit $\{-1, 1\}$ eine monochromatische Kante e_0 mit $(\sum_{v \in e_0} x_v)^2 = (\pm 3)^2 = 9$. Der Graph H kann also nicht 2-färbbar sein.

Angenommen H ist nicht 2-färbbar, dann ist in jeder Knotenfärbung mit Farben $\{-1, 1\}$ eine monochromatische Kante enthalten. Das Polynom verschwindet also für diese Werte und liegt mit Theorem 1.1 im gesuchten Ideal. □

Auf diese Weise lassen sich noch viele andere Eigenschaften von Graphen an Idealen fest machen. Es wäre schön aus einer dieser Aussagen interessante kombinatorische Folgerungen ziehen zu können.

5 Anwendungen in der Algebra

Im letzten Abschnitt haben wir bereits einige algebraische Bedingungen gesehen. Nun betrachten wir eine unmittelbare Folgerung für die Permanente einer Matrix aus Theorem 1.3 mit einigen Anwendungen und ein Resultat über die Lösungsmenge von Polynomgleichungen.

5.1 Permanenten-Lemma

Die Permanente einer $n \times n$ Matrix $A = (a_{ij})$ ist definiert als

$$Per(A) = \sum_{\tau \in S_n} a_{1,\tau(1)} \ldots a_{n,\tau(n)}.$$

Bis auf das Vorzeichen ist diese also ähnlich der Determinante der Matrix, woraus sich auch einige Gemeinsamkeiten ergeben. Die Permanente ist linear in Zeilen und Spalten und für Dreiecksmatrizen genügt es das Produkt der Diagonalen zu bilden. Die Berechnungsformeln der Determinante lassen sich ebenfalls übernehmen, wobei die negativen Vorzeichen wegzulassen sind. Der Hauptunterschied liegt darin, dass die Permanente von nicht regulären Matrizen nicht zwangsläufig Null ist, wie man sofort an einer Matrix nur aus Einsen sehen kann.

In der bereits eingangs erwähnten Arbeit von Alon und Tarsi [10] taucht folgendes Lemma in etwas schwächerer Form auf. Es lässt sich direkt aus Theorem 1.3 ableiten und besitzt einige interessante Anwendungen.

Lemma 5.1. *Sei $A = (a_{ij})$ eine $n \times n$ Matrix über dem Körper $\mathbb{F}$ und angenommen die Permanente $Per(A)$ ist ungleich Null (über $\mathbb{F}$). Dann gibt es für einen beliebigen Vektor $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}^n$ und eine Familie von Mengen $S_1, \ldots, S_n \subset \mathbb{F}$ mit $|S_i| = 2$ einen Vektor $\mathbf{s} \in S_1 \times \cdots \times S_n$, so dass sich für jedes i die i-te Koordinate von $A\mathbf{s}$ von b_i unterscheidet.*

Beweis. Das Polynom

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{n} (\sum_{j=1}^{n} a_{ij} x_j - b_j)$$

hat Grad n und der Koeffizient vor $\prod_{i=1}^{n} x_i$ ist $Per(A) \neq 0$. Aus Theorem 1.3 folgt also direkt die Existenz eines $\mathbf{s} \in S_1 \times \cdots \times S_n$ mit $f(\mathbf{s}) \neq 0$ und damit das gewünschte Resultat. □

Für $S_i = \{0, 1\}$ zeigt uns das Lemma für jedes $\mathbf{b}$ die Existenz einer Auswahl von Spalten der Matrix, deren Summe sich in jeder Koordinate von $\mathbf{b}$ unterscheidet.

Die folgende Anwendung des Permanenten-Lemmas zeigt dessen Bedeutung. Dazu definieren wir $f(n, d)$ als die kleinste Zahl f, so dass jede Folge von f Elementen der abelschen Gruppe $\mathbb{Z}_n^d = (\mathbb{Z}/n\mathbb{Z})^d$ eine Teilfolge von n Elementen besitzt, deren Summe Null ist (in $\mathbb{Z}_n^d$). 1961 zeigten Erdős, Ginzeburg und Ziv [24] lange vor dieser Definition, dass $f(n, 1) \leq 2n - 1$ für alle n hält. Die Größte Herausforderung dabei steckt in den Fällen für Primzahlen $n = p$. Danach lässt sich der allgemeine Fall mit Induktion zeigen. Es sei an dieser Stelle schon mal festgestellt, dass $f(n, 1) > 2n - 2$, da $(n - 1)$-Mal die 0 und $(n - 1)$-Mal die 1 in der Summe niemals n ergeben.

Proposition 5.2. *Für jede Primzahl p enthält jede Folge von $2p - 1$ Elementen von $\mathbb{Z}_p$ eine Teilfolge der Länge p, deren Summe 0 ist (in $\mathbb{Z}_p$).*

Beweis. Seien $2p - 1$ Elemente aus $\mathbb{Z}_p$ gegeben und wir sortieren $a_1, \ldots, a_{2p-1}$ mit $0 \leq a_1 \leq \cdots \leq a_{2p-1}$. Falls es ein $i \leq p - 1$ gibt mit $a_i = a_{i+p-1}$, dann ist der Beweis abgeschlossen, denn $a_i + \cdots + a_{i+p-1} \equiv 0 \pmod{p}$.

Andernfalls ist $a_i \neq a_{i+p-1}$ und wir setzten $S_i = \{a_i, a_{i+p-1}\}$ mit $|S_i| = 2$ für alle $i = 1, \ldots, p-1$. Sei weiter A eine $(p-1) \times (p-1)$ Matrix aus Einsen und $b_1, \ldots, b_{p-1}$ die Menge aller Elemente von $\mathbb{Z}_p$ bis auf $-a_{2p-1}$. Da $Per(A) = (p-1)! \not\equiv 0 \pmod{p}$ erhalten

wir mit Lemma 5.1 die $s_i \in S_i$, so dass sich die Summe $\sum_{j=1}^{p-1} s_i$ von b_j unterscheidet, also gleich $-a_{2p-1}$ ist. Auch in diesem Fall ist die Aussage gezeigt, denn

$$a_{2p-1} + \sum_{i=1}^{p-1} s_i \equiv 0 \pmod{p}.$$

□

Wir haben also bewiesen, dass $f(p,1) = 2p-1$ für Primzahlen p. Wenn nun aus $f(p,1) \leq 2p-1$ und $f(q,1) \leq 2q-1$ folgt, dass $f(pq,1) \leq 2pq-1$, dann sind wir fertig da sich jede Zahl n als Produkt von Primzahlen darstellen lässt. In $2pq-1$ Elementen $a_1, \ldots, a_{2pq-1}$ finden wir mit Proposition 5.2 auf jeden Fall p Elemente deren Summe ein Vielfaches von p ist. Diesen Vorgang wiederholen wir $(2q-2)$-Mal und uns bleiben $2pq-1-(2q-2)p = 2p-1$ Elemente. Noch ein weiteres Mal und wir haben $2q-1$ verschiedene Folgen $a_1^{(i)}, \ldots, a_p^{(i)}$ mit $\sum_{j=1}^{p} a_j^{(i)} = c_i \cdot p \equiv 0 \pmod{p}$ für $1 \leq i \leq 2q-1$.

Da unsere Proposition auch für q gilt finden wir q Elemente $c_{i_1}, \ldots, c_{i_q}$, so dass $\sum_{k=1}^{q} c_{i_r} \equiv 0 \pmod{q}$. Es folgt direkt

$$\sum_{k=1}^{q} \sum_{j=1}^{p} a_j^{(i_k)} = p \sum_{k=1}^{q} c_{i_k} \equiv 0 \pmod{pq},$$

womit wir folgendes bewiesen haben:

Theorem 5.3. *Für alle n gilt $f(n,1) = 2n-1$.*

Eine Vermutung von Kemnitz [32], welche $f(n,2) = 4n-3$ besagt, wurde von Reiher [51] bewiesen.

Eine Anwendung von Lemma 5.1 über additive Basen im Vektorraum findet sich in der Arbeit von Alon, Linial und Meshulan [7]. Zum Abschluß des Abschnitts über das Permanenten-Lemma folgt ein einfaches Beispiel über gerichtete Graphen. Dabei hat ein 1-regulärer Untergraph eines gerichteten Graphen Ein- und Aus-Grad exakt 1 in jedem Knoten, anders formuliert handelt es sich dabei um einen aufspannenden Untergraphen bestehend aus gerichteten Kreisen.

Theorem 5.4. *Sei $D = (V, E)$ ein gerichteter Graph der einen 1-regulären Untergraphen enthält. Dann gibt es für jede Zuweisung einer Menge S_v von zwei reelen Zahlen zu jedem Knoten $v \in V$ eine Wahl $s_v \in S_v$, so dass für $u \in V$ die Summe $\sum_{v:(u,v)\in E} s_v \neq 0$ ist.*

Beweis. Sei $A = (a_{uv})$ die Adjazenmatrix von D definiert durch $a_{uv} = 1$ genau dann, wenn $(u,v) \in E$ und $a_{uv} = 0$ sonst. Die Permanente einer Adjazenzmatrix ist niemals negativ und wegen des 1-regulären Untergraphen nicht Null, also ist $Per(A) > 0$. Mit Lemma 5.1 folgt die Existenz von $\mathbf{s} \in S_1 \times \cdots \times S_{|V|}$ mit $\sum_{v:(u,v)\in E} s_v \neq b_u = 0$ für alle $u \in V$ und $b_u = 0$. □

5.2 Chevalleys und Warnings Theorem

Theorem 5.5 (Chevalleys Theorem 1935)**.** *Sei $\mathbb{F}$ ein endlicher Körper und Polynome $f_1, \ldots, f_r \in \mathbb{F}[x_1, \ldots, x_n]$. Wenn $n > \sum_{i=1}^{r} \deg(f_i)$ und die Polynome f_i die triviale Nullstelle gemeinsam haben (oder äquivalent keine konstanten Terme besitzen), dann haben sie eine nichttriviale gemeinsame Nullstelle $(a_1, \ldots, a_n) \in \mathbb{F}_p^n$.*

Einen Beweis mit Theorem 1.3 hat schon Alon [1] beschrieben. Die folgende Erweiterung von Brink [14], dessen Beweis ebenfalls auf dem kombinatorischen Nullstellensatz basiert, kommt ohne direkte Voraussetzung an die Anzahl der Variablen aus.

Theorem 5.6 (2008)**.** *Für eine Primzahlpotenz q seien $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_n]$ und $A_1, \ldots, A_n \subset \mathbb{F}_q$, so dass*

$$\sum_{i=1}^{n} (|A_i| - 1) > \sum_{j=1}^{r} \deg(f_j)(q-1). \tag{8}$$

Dann ist die Lösungsmenge

$$V = \{a \in A_1 \times \cdots \times A_n : f_i(a) = 0 \text{ für alle } i\}$$

nicht einelementig.

Wir bemerken, dass für $A_i = \mathbb{F}_q$ die Gleichung (8) wieder zu $n > \sum_{i=1}^{r} \deg(f_i)$ wird und es nicht nur die triviale Lösung geben kann. In diesem Fall sehen wir auch, dass die Voraussetzung scharf ist, denn die Polynome $f_i = x_i$ für $i = 1, \ldots, r = n$ haben nur die triviale Nullstelle gemeinsam und im Widerspruch zu (8) gilt für $A_i = \mathbb{F}_q$ eben $\sum_{i=1}^{n} (|A_i| - 1) = n(q-1)$.

Beweis. Angenommen $V = \{\mathbf{a}\} = \{(a_1, \ldots, a_n)\}$, dann gilt für $p(x) = \prod_{j=1}^{r} (1 - f_j(x)^{q-1})$

$$p(x) = \begin{cases} 1 & \text{für } x = a \\ 0 & \text{für } x \in A_1 \times \cdots \times A_n \setminus \{a\} \end{cases}$$

und für $q(x) = \prod_{i=1}^{n} \prod_{b \in A_i \setminus \{a_i\}} (x_i - b)$

$$q(x) = \begin{cases} \delta & \text{für } x = a \\ 0 & \text{für } x \in A_1 \times \cdots \times A_n \setminus \{a\} \end{cases}$$

für ein $\delta \in \mathbb{F}_q$ ungleich Null. Das Polynom $f(x) := q(x) - \delta \cdot p(x)$ verschwindet also auf $A_1 \times \cdots \times A_n$ und $x_1^{|A_1|-1} \cdots x_n^{|A_n|-1}$ hat nach Gleichung (8) maximalen Grad in f. Der gesuchte Widerspruch ergibt sich mit Theorem 1.3, es existiert ein $a' \in A_1 \times \cdots \times A_n$ mit $f(a') \neq 0$. □

Im Originalbeweis von Chevalley [15] kommt bereits ein Spezialfall ($\mathbb{F}$ endlich und $S_i = \mathbb{F}$) des kombinatorischen Nullstellensatzes vor.

Warning [16] bewies, dass die Anzahl der Lösungen $|\{a \in \mathbb{F}_q^n : f_j(a) = 0 \text{ für alle } j\}|$ durch die Charakteristik von $\mathbb{F}_q$ teilbar ist, falls $n > \sum_{i=1}^{r} \deg(f_i)$. Diese Erweiterung lässt sich durch leichte Modifikationen ebenfalls beweisen.

6 Die Komplexität und ein Algorithmus

Der Beweis des zweiten Teils des Nullstellensatzes ist nicht konstruktiv. In diesem Abschnitt beschäftigen wir uns mit der Frage, wie wir diese Nicht-Nullstelle effizient finden können. Wir untersuchen also die Komplexitätsklasse des algorithmischen Problems zum kombinatorischen Nullstellensatz. Durch einen effizienten Algorithmus würden wir auch eine effiziente Lösung für zahlreiche Anwendungen erhalten, für die bisher nur Existenzbeweise bekannt sind.

Zum Beispiel ist beim Sitzproblem aus Abschnitt 3.1 auch der Originalbeweis nicht konstruktiv. Ein effizienter Algorithmus würde uns jeweils direkt die richtige Sitzordnung liefern. Ebenso bekämen wir bei dem Theorem zur Snevilys Vermutung aus Abschnitt 2.3 direkt die Nummerierung geliefert und in Theorem 4.1 den p-regulären Untergraphen. Bei Widerspruchsbeweisen, wie der Erweiterung von Chevalleys Theorem 5.6, bringt uns die reine Kenntnis der Nicht-Nullstelle natürlich nicht weiter.

6.1 Die Komplexität

Bevor wir uns der Suche nach einem Algorithmus widmen, möchten wir ohne formelle Definitionen den theoretischen Hintergrund beschreiben. Effizient heißt für uns in polynomieller Zeit, gemessen in der Eingabegröße. Die Komplexitätsklasse **P** enthält alle Entscheidungsprobleme, die in polynomieller Zeit gelöst werden können, wohingegen in **NP** nur eine Verfizierung der Lösung in polynomieller Zeit gefordert wird ($\mathbf{P} \subseteq \mathbf{NP}$). Analog sind **FP** und **FNP** die Klassen der Suchprobleme, die entweder in polynomieller Zeit ein Lösung finden oder verifizieren. Ein Problem ist **NP**-vollständig, wenn es in **NP** liegt und zugleich härter als alle Probleme in **NP** ist. Das bedeutet wir können mit einer Lösung jedes Problem in **NP** lösen und damit gilt falls $\mathbf{P} \cap \mathbf{NP}\text{-vollständig} \neq \emptyset$, dass $\mathbf{P} = \mathbf{NP}$. Analog gilt das für **FNP**.

Dazwischen liegt **TFNP**, die Menge aller Suchprobleme für die eine Lösung garantiert ist und diese in polynomieller Zeit überprüft werden kann ($\mathbf{FP} \subseteq \mathbf{TFNP} \subseteq \mathbf{FNP}$). Mit dieser Klasse und weiteren Unterklassen hat sich Papadimitriou [48] intensiv beschäftigt. Wenn bekannt ist, dass es immer eine Lösung gibt, ist es dann auch einfach diese zu finden? Offensichtlich ist der kombinatorische Nullstellensatz in **TFNP**, denn Theorem 1.3 verspricht die Existens einer Lösung und wir können eine Lösung in polynomieller Zeit überprüfen. Alle direkt mit dem kombinatorischen Nullstellensatz bewiesenen Probleme, wie die oben genannten, liegen damit automatisch auch in **TFNP**.

Alon [1] hält es für wahrscheinlich, dass es einen Algorithmus gibt, der in polynomieller Zeit eine Lösung findet. Hier setzt auch die offene Problemstellung über die Komplexität des kombinatorischen Nullstellensatzes aus *REGS in combinatorics* [54] der Universität von Illinois an.

6.2 Ein Algorithmus

Gegeben ist ein Polynom $f \in \mathbb{F}[\mathbf{x}]$ vom Grad $\sum_{i=1}^{n} t_i$ für $t_i \in \mathbb{N}$ und $S_i \subseteq \mathbb{F}$ mit $|S_i| \geq t_i + 1$ alles für $i = 1, \ldots, n$. Wir suchen ein $\mathbf{s} \in S_1 \times \cdots \times S_n$ mit $f(\mathbf{s}) \neq 0$ in Zeit

polynomiell in $|f|$. Das bedeutet, wir messen die Laufzeit in der Eingabegröße $|f|$.

Wir können annehmen, dass $|S_i| = t_i + 1$. Der erste Ansatz alle Möglichkeiten durchzuprobieren scheitert am dafür erforderlichen exponentiellen Aufwand. Wenn wir die t_i oder die Elemente von S_i einschränken ändert sich daran nichts. Erst eine weitere Voraussetzung an den Grad des Polynoms in den einzelnen Variablen bringt uns weiter. Wie schon in Lemma 1.4 verallgemeinert hat ein Polynom $f \not\equiv 0$ n-ten Grades höchstens n Nullstellen. Ist der Grad von f nun in jeder Variablen durch t_i beschränkt, also $\deg_i(f) \leq t_i$, dann ist f als Polynom in einer Variablen nicht auf ganz S_i Null.

Aus dieser Idee lässt sich Algorithmus 6 entwickeln, der zum Beispiel auch in [52] in ähnlichem Kontext vorgestellt wird. Es werden schlicht alle Variablen durchgegangen und aus jedem S_i ein Element gesucht, welches das Polynom im entsprechenden Schritt nicht Null werden lässt. Wir lassen für f nur die Eingabeform als Summe von Monomen zu, damit wir das Polynom an einzelnen Stellen in lineare Zeit auswerten können. Offensichtlich garantiert uns der kombinatorische Nullstellensatz die Existenz der Lösung.

Input : Polynom $f \in \mathbb{F}[x_1, \ldots, x_n]$ mit $\deg(f) = \sum_{i=1}^{n} t_i$ und $\deg_{x_i}(f) \leq t_i$ für $t_i \in \{0, 1, \ldots\}$ und $S_i \subseteq \mathbb{F}$ mit $|S_i| = t_i + 1$ für $i = 1, \ldots, n$
Output : $\mathbf{s} \in S_1 \times \cdots \times S_n$ mit $f(s) \neq 0$

```
1  begin
2      for i = 1 to n do
3          repeat
4              Wähle s_i aus S_i;
5              S_i := S_i \ {s_i};
6          until f|_{x_i=s_i} ≢ 0;
7          f := f|_{x_i=s_i};
8      end
9      return s = (s_1, ..., s_n);
10 end
```

Algorithmus 1: Finden einer Nicht-Nullstelle

Theorem 6.1. *Algorithmus 1 terminiert in polynomieller Zeit gemessen in der Eingabegröße $|f|$.*

Beweis. Der Algorithmus terminiert, da wir in jedem Schritt f als Polynom in einer Variablen auffassen können. Ein solches Polynom $f \not\equiv 0$ mit $\deg_i(x_i) \leq t_i$ kann auf einer Menge S_i mit $|S_i| = t_i + 1$ nicht komplett Null sein. Für Zeile 6 des Algorithmus findet sich also immer mindestens ein $s_i \in S_i$, welches $f|_{x_i=s_i} \not\equiv 0$ erfüllt. Die Voraussetzungen für den kombinatorische Nullstellensatz sind nach dem Ersetzten $f := f|_{x_i=s_i}$ immer noch erfüllt, also ist der gefundene Wert Teil einer Lösung $\mathbf{s}$.

Die Auswertung in Zeile 6 benötigt lineare Zeit und mit den beiden verschachtelten Schleifen kommen wir auf eine kubische Laufzeit. □

Der Algorithmus kann mit leichten Veränderungen auch weitere Nicht-Nullstellen finden, die uns zum Beispiel Theorem 5.6 verspricht. Folgender Korollar folgt direkt.

Korollar 6.2. *Unter den eingangs beschriebenen Voraussetzungen und insbesondere* $\deg_i(f) \leq t_i$ *findet man* $s \in S_1 \times \cdots \times S_n$ *mit* $f(s) \neq 0$ *in Zeit polynomiell in* $|f|$.

Damit ist die Frage für einige Polynome bereits beantwortet. In Hinblick auf den Beweis von Theorem 1.1 lässt sich dieser noch etwas erweitern.

Korollar 6.3. *Sei* $f \in \mathbb{F}[x_1, \ldots, x_n]$ *in monomialer Darstellung. Angenommen der Grad von* f *ist* $\sum_{i=1}^{n} t_i$ *mit* $t_i \in \mathbb{N}$ *und der Koeffizient vor* $\prod_{i=1}^{n} x_i^{t_i}$ *nicht Null. Wenn für Teilmengen* $S_1, \ldots, S_n$ *von* $\mathbb{F}$ *mit* $|S_i| = t_i + 1$ *das Polynom* $g_i(x_i) = \prod_{s_i \in S_i}(x_i - s_i)$ *jeweils aus höchstens zwei Monomen besteht, dann findet man* $s \in S_1 \times \cdots \times S_n$ *mit* $f(s) \neq 0$ *in Zeit polynomiell in* $|f|$.

Beweis. Wir können $g_i(x_i)$ schreiben als $g_i(x_i) = x_i^{t_i+1} - a x_i^b$ für $a \in \mathbb{F}$ und $b \in \{0, \ldots, t_i\}$. Damit erhalten wir $x_i^{t_i+1} = a x_i^b$ für $x_i \in S_i$ und können wie im Beweis von Theorem 1.1 Potenzen von x_i, die höher sind als t_i, sukzessive ersetzen. Dieser Prozess läuft auf polynomiellem Platz und in polynomieller Zeit ab da keine zusätzlichen Monome entstehen. Wir erhalten ein Polynom $\tilde{f}$ mit folgenden Eigenschaften:

(i) $\deg(\tilde{f}) = \deg(f)$,
(ii) $\tilde{f}(s) = f(s)$ für alle $s \in S_1 \times \cdots \times sS_n$,
(iii) der Koeffizient vor $\prod_{i=1}^{n} x_i^{t_i}$ hat sich nicht verändert und
(iv) $\deg_i(\tilde{f}) \leq t_i$.

Damit können wir nun Korollar 6.2 anwenden und erhalten in polynomieller Zeit das gesuchte $s \in S_1, \ldots, S_n$ mit $\tilde{f}(s) = f(s) = 0$. □

Vernachlässigen wir die Bedingung an g_i so könnte das Polynom $\tilde{f}$, welches aus f entsteht exponentiell mehr Monome besitzen und damit exponentiell viel Platz und auch Zeit beanspruchen. Ein Beispiel für dieses Ergebnis sind boolschen Mengen, also $t_i = 1$ und $S_i = \{0, 1\}$ für $i = 1, \ldots, n$. Dann gilt $x_i^2 = x_i$ für $x_i \in S_i$ und wir können in polynomieller Zeit für ein Polynom von Grad n mit Koeffizientem ungleich Null vor $\prod_{i=1}^{n} x_i$ eine Nicht-Nullstelle finden. Ähnlich funktioniert das auch, wenn die S_i eine Gruppe, beispielsweise die der Einheitszwurzeln, oder sogar einen Körper bilden.

Dies können wir leider nicht auf Theorem 4.1 anwenden, welches uns einen p-regulären Untergraphen garantiert, falls der durchschnittliche Grad größer als $2p - 2$ und der maximale kleiner als $2p - 1$ ist. Wir suchen zwar eine Nicht-Nullstelle des Polynoms aus $\{0, 1\}^{|E|}$ stellvertretend für den Untergraphen, aber das im Beweis beschriebene Polynom

$$f = \prod_{v \in V} \left[1 - \left(\sum_{e \in E} a_{v,e} x_e \right)^{p-1} \right] - \prod_{e \in E} (1 - x_e)$$

besitzt exponentiell viele Monome in $|V|$, und daher hilft uns die Lösung in Zeit polynomiell in $|f|$ nicht weiter. Auch das Fixieren von p bringt keinen Vorteil, da das vordere Produkt zum Anwenden der Multilinearisierung ausgerechnet werden muss und somit ebenfalls exponentiell viele Monom in $|V|$ entstehen. Das Problem liegt darin, dass die einzelnen Faktoren nur lokale Informationen enthalten, aus denen sich nicht schließen lässt ob ein Knoten für den Zielgraphen relevant ist oder nicht. Zuletzt scheitert auch

der Versuch die Multilinearisierung zu umgehen, da wir in diesem Fall zum Auswerten des Polynoms eine Monomialdarstellung benötigen, welche erneut exponentiell viele Monome enthalten würde.

Die Schwierigkeiten kommen nicht überraschend, denn selbst für das Finden eines 3-regulären Untergraphen in einem schlichten 4-regulären Graphen wurden bisher nur in einigen Spezialfälle direktere polynomielle Algorithmen gefunden. Bei den von Sridharan [56] vorgestellten Algorithmen wird sofern vorhanden ein perfektes Matching aus dem Graphen gelöscht und übrig bleibt ein 3-regulärer Graph. Das allgemeine Problem, ob für ein festes $k \geq 3$ ein beliebiger Graph einen k-regulären Untergraphen besitzt, ist **NP**-vollständig [57] und das entsprechende Suchprobleme dann **FNP**-vollständig.

Die Lösung des Problems scheitert also nicht unbedingt am Algorithmus, sondern bereits am zu komplexen Polynom. Selbst das Wissen um die Existenz der Lösung, macht in diesem Fall noch nicht den entscheidenden Unterschied aus. Die Stärke von Algorithmus 1 liegt darin, dass wir in jedem Schritt keinen Fehler machen können. Dies scheint auch der wichtigste Ansatz für eine effiziente Lösung zu sein.

7 Erweiterungen des Konzeptes

Im Laufe der Zeit stieß der kombinatorische Nullstellensatz immer wieder an Grenzen. Manchmal erschienen die Probleme für eine Lösung mit dem kombinatorischen Nullstellensatz gut geeignet, aber die Voraussetzungen wurden nicht ganz erfüllt. Daraus entstanden neue Varianten in verschiedene Richtungen, die das Anwendungsspektrum erweiterten. Ball und Serra [13] verzichteten in einer punktierten Version auf eine gemeinsame Nullstelle der g_i mit f und erweiterten das Theorem auf Nullstellen von f höherer Vielfachheit. Danach schwächte Lasoń [37] die Vorraussetzung an das nichtverschwindende Monom ab und zuletzt formulierten Kós, Mészáros und Rónyai [36, 35] Varianten für Multimengen und Ringe. Daraus ergaben sich neue Möglichkeiten für Anwendungen, bei denen der klassische kombinatorische Nullstellensatz nicht ausreichte. Wir wollen im folgenden einige dieser Erweiterungen zusammen mit charakteristischen Anwendungen vorstellen, die weiter die Vielseitigkeit des kombinatorischen Nullstellensatzes und die Vorteile der neuen Erweiterungen deutlich machen.

7.1 Vorraussetzung an das Monom

Wir beginnen zunächst mit einer einfachen Verallgemeinerung von Lasoń [37], bei der wir die Voraussetzung an das Monom mit Koeffzienten ungleich Null abschwächen. Das Monom muss nicht mehr den größten Grad haben, sondern es genügt eine Maximalitätseigentschaft. Sei $\mathbb{F}$ ein Körper und $f \in \mathbb{F}[x_1, \ldots, x_n]$ ein Polynom. Wir definieren $\mathrm{Supp}(f) := \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n : \text{der Koeffizient vor } \prod_{i=1}^n x_i^{\alpha_i} \text{ in } f \text{ ist nicht Null}\}$. Auf der Menge $\mathbb{N}^n$ und damit auch auf $\mathrm{Supp}(f)$ haben wir eine natürliche partielle Ordnung durch $(\alpha_1, \ldots, \alpha_n) \geq (\beta_1, \ldots, \beta_n)$ genau dann, wenn $\alpha_i \geq \beta_i$ für alle i.

Theorem 7.1. *Sei $\mathbb{F}$ ein beliebiger Körper und $f \in \mathbb{F}[x_1, \ldots, x_n]$. Angenommen das n-Tupel $(\alpha_1, \ldots, \alpha_n)$ ist maximal in Supp(f), dann gibt es für Teilmengen $A_1, \ldots, A_n$ von $\mathbb{F}$ mit $|A_i| \geq \alpha_i + 1$ ein $\mathbf{a} \in A_1 \times \cdots \times A_n$, so dass $f(\mathbf{a}) \neq 0$.*

Der Grad des Monoms mit Koeffizienten ungleich Null muss also nicht mehr dem Grad von f entsprechen, sondern es genügt, wenn dieses Monom kein anderes Monom höheren Grades mit Koeffizienten ungleich Null teilt. Der Beweis folgt einer Idee von Michalek [44], die auch schon für den klassischen kombinatorischen Nullstellensatz einen kürzeren Beweis per Induktion lieferte.

Beweis. Wir führen Induktion nach $\alpha_1 + \cdots + \alpha_n$ durch. Für $\alpha_1 + \cdots + \alpha_n = 0$ ist $f \equiv c \neq 0$ und damit ist die Aussage wahr. Wenn $\alpha_1 + \cdots + \alpha_n > 0$, dann können wir ohne Beschränkung der Allgemeinheit annehmen, dass $\alpha_1 > 0$. Fixieren wir ein $a \in A_1$ und teilen f durch $(x_1 - a)$, so erhalten wir

$$f = g \cdot (x_1 - a) + h,$$

wobei der Grad von h in x_1 Null ist. Das Polynom h hängt also nur von den Variablen $x_2, \ldots, x_n$ ab. Wenn es $a_2 \in A_2, \ldots, a_n \in A_n$ gibt mit $h(a_2, \ldots, a_n) \neq 0$, dann gilt auch $f(a_1, a_2, \ldots, a_n) \neq 0$, was die Aussage beweist. Andernfalls ist $h|_{A_2 \times \cdots \times A_n} \equiv 0$. Nach dem Divisionsalgorithmus haben wir dann

$$\text{Supp}(g) \subseteq \{(\beta_1 - r, \beta_2, \ldots, \beta_n) : (\beta_1, \beta_2, \ldots, \beta_n) \in \text{Supp}(f), 1 \leq r \leq \beta_1\}$$

und $(\alpha_1 - 1, \alpha_2, \ldots, \alpha_n) \in \text{Supp}(g)$. Also ist das Tupel $(\alpha_1 - 1, \alpha_2, \ldots, \alpha_n)$ maximal in Supp(g). Nach Induktionsvoraussetzung existieren $a_1 \in A \setminus \{a\}, a_2 \in A, \ldots, a_n \in A_n$, so dass $g(a_1, a_2, \ldots, a_n) \neq 0$ und damit

$$f(a_1, a_2, \ldots, a_n) = (a_1 - a) \cdot g(a_1, a_2, \ldots, a_n) \neq 0,$$

was die Aussage beweist. □

Wir gehen jetzt auf eine Anwendung über *lucky labelings* von Graphen ein, bei der der klassische kombinatorische Nullstellensatz nicht zu funktionieren scheint. Hierbei wird eine Idee von Czerweiński, Grytczuk und Żelazny [20] verallgemeinert. Für einen einfachen Graphen $G = (V, E)$ und eine Funktion $c : V \to C \subseteq \mathbb{N}$ sei $S(u) = \sum_{v \in N(u)} c(v)$. Die Funktion c wird *lucky labeling* von G genannt, wenn $S(u) \neq S(w)$ für beliebige adjazente Knoten u und w. $S(v)$ beschreibt also das Gewicht der Nachbarschaft von v, welches nach Möglichkeit für alle adjazenten Knoten verschieden sein soll. Es wird vermutet, dass jeder k-färbbare Graph ein *lucky labelings* für $C = \{1, 2, \ldots, k\}$ besitzt und immerhin bewiesen, dass schon die Menge $\{1, 2, 3\}$ für jeden planaren bipartiten Graphen ausreicht. Wir schauen uns folgende Variante von Lasoń an.

Theorem 7.2. *Sei G ein bipartiter Graph, der eine Orientierung mit durch k beschränktem Ausgrad hat. Angenommen jeder Knoten v ist ausgestattet mit einem nicht konstanten Polynom $f_v \in \mathbb{R}[x]$ von Grad höchstens l und positivem führenden Koeffizienten.*

Dann gibt es eine Färbung $c : V(G) \to C = \{1, 2, \ldots, kl + 1\}$, so dass für beliebige zwei adjazente Knoten u und w

$$c(u) - \sum_{v \in N(u)} f_v(c(v)) \neq c(w) - \sum_{v \in N(w)} f_v(c(v)) \tag{9}$$

gilt.

Beweis. Wir weisen jedem Knoten v eine Variable x_v zu, fixieren eine Orientierung G' mit maximalem Ausgrad k und betrachten das Polynom

$$h(x_1, \ldots, x_n) = \prod_{(u,w) \in E(G')} \left(x_u - \sum_{v \in N(u)} f_v(x_v) - x_w + \sum_{v \in N(w)} f_v(x_v) \right).$$

Wir wollen zeigen, dass es Werte $a_v \in \{1, \ldots, kl + 1\}$ für x_v gibt, so dass h ungleich Null ist. Dies würde uns die gesuchte Färbung c mit $c(v) = a_v$ liefern, da für beliebige adjazente Knoten Gleichung (9) gilt.

Für jede Kante $(u, v) \in E(G')$, die $u \to v$ orientiert ist, wählen wir das führende Monom von $f_u(x_u)$ aus dem Faktor in h aus, der zu dieser Kante gehört. Das Produkt all dieser Monome über alle Kanten in G ist ein Monom m von h mit $\deg_u(m) = d^+(u) \cdot \deg(f_u) \leq kl$, da das führende Monom aus $f_u(x_u)$ höchstens $d^+(u)$-mal multipliziert wird. Wir zeigen, dass der Koeffizient vor m in h nicht Null sein kann. Dafür behaupten wir, dass jedes Mal, wenn wir m als Produkt von Monomen der Faktoren aus h bilden, das Vorzeichen positiv ist, denn dann kann deren Summe in $\mathbb{R}$ nicht Null werden.

Auf der einen Seite hat das Monom m selber ein positives Vorzeichen da alle f_u positive führende Koeffizienten besitzen, nur in der hinteren Summe auftreten können und somit sich das einzelne x_u auch nur positiv auswirken kann.

Auf der anderen Seite kann aber m auch durch Kombination mit Summanden aus der vorderen Summe, die negative Vorzeichen besitzen, zustande kommen. Damit der Grad von m erreicht wird muss es sich aber um führenden Koeffizienten der selben f_v handeln. Das Austauschen der Faktoren ist also jeweils ein zyklischer Prozess. Nun ist G allerdings bipartit, es gibt somit keine ungeraden Kreise und wir können durch die gerade Anzahl an Vertauschungen auf das positive Vorzeichen schließen.

Die Maximalität von m in $\mathrm{Supp}(h)$ können wir einfach sehen, indem wir den Grad jeder Variable x_u mit $1/\deg(f_u)$ gewichten, denn dann hat m Grad $d^+(u)$ in x_u. Jedes andere Monom m', welches in $\mathrm{Supp}(h)$ größer gleich als m sein soll, muss also mindestens aus der selben Anzahl an Summanden in jeder Variablen bestehen und hat wegen $\sum_{u \in V(G)} d^+(u) = |E(G)|$ den selben Grad. Die Aussage folgt nun direkt aus Theorem 7.1 mit $A_i = \{1, 2, \ldots, kl + 1\}$. □

Das Problem des klassischen kombinatorischen Nullstellensatzes bei dieser Anwedung ist offensichtlich, dass das Monom m nicht zwangsläufig maximalen Grad haben muss. Es scheint also nicht zu funktionieren, zumindest nicht mit diesem Polynom. Einen weiteren Vorteil dieser Variante des Nullstellensatzes gegenüber dem klassischen zeigt uns folgender Korollar.

Korollar 7.3. *Sei $\mathbb{F}$ ein beliebiger Körper und $f \in \mathbb{F}[x_1, \ldots, x_n]$ ein Polynom. Angenommen $(\alpha_1, \ldots, \alpha_n)$ ist maximal in Supp(f) und $f(x_1, \ldots, x_n) = g(h(x_1), x_2, \ldots, x_n)$ mit $\deg(h) = k$. Seien $A_1, A_2, \ldots, A_n$ Teilmengen mit $|A_1| \leq \alpha_1/k + 1$, $|A_i| \leq \alpha_i + 1$ für $i = 2, \ldots, n$ und $h(a) \neq h(b)$ für alle Elemente $a \neq b \in A_1$. Dann verschwindet f nicht auf $A_1 \times \cdots \times A_n$.*

Im Vergleich zum klassischen kombinatorischen Nullstellensatz mit der zusätzlichen Voraussetzung $\deg(f) = \prod_{i=1}^{n} x_i^{\alpha_i}$ also eine fast k-mal kleinere Menge. Der Beweis ist eine direkte Folgerung aus der Subsitution $\tilde{x}_1 := h(x_1)$ und dem Theorem 7.1 angewandt auf $\tilde{f}(\tilde{x}_1, x_2, \ldots, x_n) = f(x_1, \ldots, x_n)$. Der klassische Nullstellensatz scheitert hier abermals, da nach der Substitution der Grad von dem betrachteten Monom nicht mehr maximal sein muss. Ein entsprechendes Korollar lässt sich auch leicht für weitere Variablen, die identisch zu einem Polynom sind, formulieren.

7.2 Punktierte Version und Multiplikativität

Bei der punktierten Variante des kombinatorischen Nullstellensatzes verzichten wir auf eine gemeinsame Nullstelle der g_i mit f. Sei $\mathbb{F}$ ein Körper und $f \in \mathbb{F}[x_1, \ldots, x_n]$. Für $i = 1, \ldots, n$ seien D_i und S_i endliche nichtleere Teilmengen von $\mathbb{F}$, wobei $D_i \subset S_i$ und definiere

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s) \text{ und } l_i(x_i) = \prod_{d \in D_i} (x_i - d)$$

Theorem 7.4. *Das Polynom f verschwinde über allen gemeinsamen Nullstellens von $g_1, \ldots, g_n$ bis auf mindestens ein Element von $D_1 \times \cdots \times D_n$. Es gibt also $\mathbf{d} \in D_1 \times \cdots \times D_n$ mit $f(\mathbf{d}) \neq 0$ und für alle $\mathbf{s} \in S_1 \times \cdots \times S_n \setminus \{D_1 \times \cdots \times D_n\}$ gilt $f(\mathbf{s}) = 0$. Dann gibt es Polynome $h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$ mit $\deg(h_i) \leq \deg(f) - \deg(g_i)$ und einem Polynom $w \not\equiv 0$, mit $\deg_i(w) \leq |S_i| = \deg_i(g_i)$ für alle i und $\deg(w) \leq \deg(f)$ mit der Eigenschaft, dass*

$$f = \sum_{i=1}^{n} h_i g_i + w$$

und

$$w = u \prod_{i=1}^{n} \frac{g_i}{l_i} = u \prod_{i=1}^{n} \prod_{s \in S_i \setminus D_i}$$

für ein Polynom $u \not\equiv 0$. Insbesondere gilt $\deg(f) \geq \sum_{i=1}^{n} (|S_i| - |D_i|)$.

Beweis. Wir können

$$f = \sum_{i=1}^{n} g_i h_i + w$$

schreiben für Polynome h_i mit $\deg(h_i) \leq \deg(f) - \deg(g_i)$ und ein Polynom w mit $\deg_i(w) < \deg_i(g_i)$ und $\deg(w) \leq \deg(f)$. Nach Voraussetzung ist das Polynom fl_i für jedes i an den gemeinsamen Nullstellen von $g_1, \ldots, g_n$ Null und damit gilt das Gleiche auch für wl_i. Mit Theorem 1.1 gibt es Polynome v_i, so dass

$$wl_i = \sum_{i=1}^{n} v_i g_i.$$

Weiter ist $\deg_j(wl_i) < \deg_j(g_j)$ für $j \neq i$, also in diesen Fällen $v_i \equiv 0$ und damit $wl_i = g_i v_i$. Also ist wl_i teilbar durch g_i. Da g_i von l_i geteilt wird folgt, dass w durch g_i/l_i teilbar ist und somit gilt

$$w = u \prod_{i=1}^{n} \frac{g_i}{l_i}$$

für ein Polynom $u \not\equiv 0$, da $0 \neq f(\mathbf{d}) = w(\mathbf{d})$ für ein $\mathbf{d} \in D_1 \times \cdots \times D_n$.

Da $w \not\equiv 0$ und $\deg(f) \geq \deg(w)$ erhalten wir aus den beschriebenen Teilbarkeiten $\deg(f) \geq \sum_{i=1}^{n}(|S_i| - |D_i|)$. □

Eine einfache Anwendung dieser Erweiterung führt zu folgendem Resultat, welches eine andere Richtung von Theorem 5.6 betrachtet.

Theorem 7.5. *Sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen und $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$. Sei weiter $d = |D_1| + \cdots + |D_n|$, wobei D_i die Menge von Elementen $a \in \mathbb{F}$ ist, die i-te Koordinate einer gemeinsamen Nullstelle von $f_1, \ldots, f_n$ sind. Wenn $d \neq 0$, oder anders gesagt, wenn die Polynome $f_1, \ldots, f_n$ eine gemeinsame Nullstellen haben, dann*

$$\sum_{i=1}^{m} \deg(f_i) \geq \frac{nq - d}{q - 1}.$$

Beweis. Wir betrachten

$$f(x_1, \ldots, x_n) = \prod_{i=1}^{m}(1 - f_i(x_1, \ldots, x_n)^{q-1})$$

und halten fest, dass f für die gemeinsamen Nullstellen der f_i nicht Null wird. Mit $S_i = \mathbb{F}_q$ folgt aus Theorem 7.4

$$(q-1)\sum_{i=1}^{m} \deg(f_i) \geq nq - \sum_{i=1}^{n} |D_i|$$

und damit das gewünschte Resultat. □

Als nächstes betrachten wir Nullstellen im Polynom f höherer Vielfachheit. Ein $\mathbf{a} \in \mathbb{F}^n$ ist eine Nullstelle mit Multiplikativität t eines Polynoms $f \in \mathbb{F}[x_1, \ldots, x_n]$, wenn t die maximale nicht negative ganze Zahl ist, so dass für jeden Term $x_1^{t_1} \cdots x_n^{t_n}$, welcher in $f(x_1 + a_1, \ldots, x_n + a_n)$ vorkommt, $t_1 + \cdots + t_n \geq t$ gilt.

Sei $T_{n,t}$ die Menge aller nicht fallenden Folgen der Länge t auf der Menge $\{1, 2, \ldots, n\}$. Für jedes $\tau \in T_{n,t}$ bezeichnet $\tau(i)$ das i-te Element in der Folge von τ.

Theorem 7.6. *Sei $\mathbb{F}$ ein Körper und $f \in \mathbb{F}[x_1, \ldots, x_n]$. Angenommen $S_1, \ldots, S_n$ sind beliebige nichtleere endliche Teilmengen von $\mathbb{F}$ und*

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s).$$

Wenn f eine Nullstelle der Multiplikativität t in allen gemeinsamen Nullstellen von $g_1, \ldots, g_n$ hat, dann gibt es $h_\tau \in \mathbb{F}[x_1, \ldots, x_n]$, mit $\deg(h_\tau) \leq \deg(f) - \sum_{i=1}^n \deg(g_{\tau(i)})$, so dass

$$f = \sum_{\tau \in T_{n,t}} g_{\tau(1)} \cdots g_{\tau(t)} h_\tau.$$

Beweis. Wir wenden doppelte Induktion nach n und t an. Falls $n = 1$, dann hat f eine Nullstelle der Multiplikativität t für alle $s_1 \in S_1$, also gilt $f = g(x_1)^t h(x_1)$. Für $t = 1$ ist das Theorem der normale kombinatorische Nullstellensatz von Alon (Theorem 1.1). Angenommen dies Aussage ist wahr für $m < n$ und $u \leq t$ oder wenn $m \leq n$ und $u < t$.

Sei $\alpha \in S_n$ und schreibe $f = (x_n - \alpha)A_\alpha + B_\alpha$, wobei $A_\alpha \in \mathbb{F}_q[x_1, \ldots, x_n]$ und $B_\alpha \in \mathbb{F}_q[x_1, \ldots, x_{n-1}]$. Das Polynom B_α hat eine Nullstelle der Multiplikativität t an allen Elementen von $S_1 \times \cdots \times S_{n-1}$. Also gilt nach Induktion

$$B_\alpha = \sum_{\tau \in T_{n-1,t}} g_{\tau(1)} \cdots g_{\tau(t)} k_\tau,$$

wobei $\deg(k_\tau) \leq \deg(f) - \sum_{i=1}^n \deg(g_{\tau(i)})$ für $\tau \in T_{n-1,t}$.

Sei $\beta \in S_n$ mit $\beta \neq \alpha$ und schreibe $A_\alpha = (x_n - \beta)A_\beta + B_\beta$, wobei $A_\beta \in \mathbb{F}_q[x_1, \ldots, x_n]$ und $B_\beta \in \mathbb{F}_q[x_1, \ldots, x_{n-1}]$. Erneut folgt nach Induktionsvoraussetzung

$$B_\beta = \sum_{\tau \in T_{n-1,t}} g_{\tau(1)} \cdots g_{\tau(t)} l_\tau,$$

für Polynome l_τ, wobei $\deg(l_\tau) \leq \deg(B_\beta) - \sum_{i=1}^n \deg(g_{\tau(i)}) \leq \deg(f) - 1 - \sum_{i=1}^n \deg(g_{\tau(i)})$ für $\tau \in T_{n-1,t}$.

Also können wir zusammen $f = (x_n - \alpha)(x_n - \beta)A_\beta + U_{\alpha\beta}$ schreiben für ein

$$U_{\alpha\beta} = \sum_{\tau \in T_{n-1,t}} g_{\tau(1)} \cdots g_{\tau(t)} m_\tau,$$

wobei $\deg(m_\tau) \leq \deg(f) - \sum_{i=1}^n \deg(g_{\tau(i)})$ für $\tau \in T_{n-1,t}$.

Wiederholen wir diesen Prozess, so erhalten wir am Ende $f = g_n(x_n)A + B$, wobei $\deg(A) \leq \deg(f) - \deg(g_n)$ und

$$B = \sum_{\tau \in T_{n-1,t}} g_{\tau(1)} \cdots g_{\tau(t)} o_\tau,$$

wobei $\deg(o_\tau) \leq \deg(f) - \sum_{i=1}^n \deg(g_{\tau(i)})$ für $\tau \in T_{n-1,t}$.

Das Polynom $g_n(x_n)A$ hat eine Null der Multiplikativität t in allen Punkten von $S_1 \times \cdots \times S_n$ und damit hat A ein Null der Multiplikativität $t-1$ in diesen Punkten. Nach Induktionsvoraussetzung gilt

$$A = \sum_{\tau \in T_{n,t-1}} g_{\tau(1)} \dots g_{\tau(t-1)} p_\tau,$$

wobei $\deg(p_\tau) \leq \deg(A) - \sum_{i=1}^{n} \deg(g_{\tau(i)})$ für $\tau \in T_{n,t-1}$.

Diese Form von A ergänzen wir nun mit $g_n(x_n)$ und zusammen mit B erhalten wir die ge"wunschte Form für f mit $h_\tau = o_\tau + p_\tau$, wobei alle noch nicht definierten o_τ und p_τ konstant Null sind. □

Diese beiden Theoreme möchten wir nun miteinander verbinden. Seien also g_i und l_i definiert wie zuvor.

Theorem 7.7. *Das Polynom f habe eine Nullstelle der Multiplikativität t in allen gemeinsamen Nullstellen von $g_1, \dots, g_n$, bis auf einen Punkt aus $D_1 \times \cdots \times D_n$, wo es eine Nullstelle der Multiplikativität echt kleiner t besitzt. Dann gibt es Polynome $h_\tau \in \mathbb{F}[x_1, \dots, x_n]$, mit $\deg(h_\tau) \leq \deg(f) - \sum_{i=1}^{n} \deg(g_{\tau(i)})$ und ein Polynom $u \not\equiv 0$ mit $\deg(u) \leq \deg(f) - \sum_{i=1}^{n} (\deg(g_i) - \deg(l_i))$, so dass*

$$f = \sum_{\tau \in T_{n,t}} g_{\tau(1)} \dots g_{\tau(t)} h_\tau + u \prod_{i=1}^{n} \frac{g_i}{l_i}.$$

Gibt es sogar einen Punkt in $D_1 \times \cdots \times D_n$, wo f nicht Null ist, dann gilt für jedes j

$$\deg(f) \geq (t-1)(|S_j| - |D_j|) + \sum_{i=1}^{n} (|S_i| - |D_i|).$$

Beweis. Wir führen einen ähnlichen Beweis wie bei Theorem 7.4 durch, nur mit einer anderen Ausgangssituation und Theorem 7.6 anstatt des klassischen kombinatorischen Nullstellensatzes. Wir können

$$f = \sum_{\tau \in T_{n,t}} g_{\tau(1)} \dots g_{\tau(t)} h_\tau + w$$

schreiben, wobei w kein Monom der Form $x_1^{r_1} \dots x_n^{r_n}$ besitzt, für das es ein $\tau \in T_{n,t}$ gibt mit $r_j \geq \sum_{j=1}^{n} |S_{\tau(j)}|$ für alle j.

Nach Voraussetzung hat $f l_i^t$ für alle i Nullenstellen der Multiplikativität t an allen gemeinsamen Nullstellen von $g_1, \dots, g_n$ und damit auch $w l_i^t$. Nach Theorem 7.6 gibt es Polynome v_τ mit der Eigenschaft, dass

$$w l_i^t = \sum_{\tau \in T_{n,t}} g_{\tau(1)} \dots g_{\tau(t)} v_\tau \tag{10}$$

Jedenfalls hat wl_i^t kein Monom $x_1^{r_1} \dots x_n^{r_n}$ für das es ein $\tau \in T$ gibt mit $r_j \geq \sum_{j=1}^{n} |S_{\tau(j)}|$ für alle j, außer wenn $\tau(j) = i$ für ein j. Daher ist

$$wl_i^t = g_i(x_i) \cdot \sum_{\tau \in T_{n,t-1}} g_{\tau(1)} \dots g_{\tau(t-1)} o_\tau,$$

für Polynome o_τ, woraus folgt, dass w durch g_i/l_i teilbar ist für jedes i. Also gilt weiter

$$f = \sum_{\tau \in T_{n,t}} g_{\tau(1)} \dots g_{\tau(t)} h_\tau + u \prod_{i=1}^{n} \frac{g_i}{l_i},$$

für ein Polynom $u \not\equiv 0$, da $f \notin (\{g_{\tau(1)}, \dots, g_{\tau(t)} | \tau \in T_{n,t}\})$.

Um eine untere Schranke für $\deg(f)$ zu finden, beweisen wir eine untere Schranke für $\deg(u)$. Sei $(d_1, \dots, d_n) \in D_1 \times \dots \times D_n$ mit $f(d_1, \dots, d_n) \neq 0$. Aus Gleichung (10) mit $i = 1$ (oder einem beliebigen anderen) bekommen wir

$$u(x_1, d_2, \dots, d_n) l_1^t \frac{g_1}{l_1} = g_1^t v_1,$$

für ein Polynom v_1 und damit ist $u(x_1, d_2, \dots, d_n)$ teilbar durch $(g_1/l_1)^{t-1}$.

Es bleibt nur noch zu zeigen, dass $u(x_1, d_2, \dots, d_n)$ nicht Null ist. Dies folgt aber direkt daraus, dass $f(x_1, d_2, \dots, d_n)$ für $x_1 = d_1$ Null ist und somit auch $u(x_1, d_2, \dots, d_n) g_1/l_1$ nicht. Also gilt für beliebiges j

$$\deg(f) \geq \deg(w) \geq \deg(u) + \sum_{i=1}^{n} \deg(\frac{g_i}{l_i}) \geq (t-1)(|S_j| - |D_j|) + \sum_{i=1}^{n} (|S_i| - |D_i|)$$

□

7.3 Anwendungen in der Geometrie

Für diese punktierte Erweiterung mit Multiplikativität betrachten wir eine Anwendung aus der Geometrie. Die n-dimensionale affine Geometrie über einem Körper $\mathbb{F}$ bezeichnen wir mit $AG(n, \mathbb{F})$. Im Unterschied zur euklidischen Geometrie verschwinden die Begriffe Abstand und Winkel, da diese unter affinen Transformationen keine Invarianten mehr sind. Für detaillierte Informationen vergleiche Coxeter [19].

Theorem 7.8. *Sei $\mathcal{A}$ eine Menge von Hyperebenen von $AG(n, \mathbb{F})$ und D_i echte nichtleere Teilmengen von endlichen Mengen $S_i \subseteq \mathbb{F}$. Wenn jeder Punkt $(s_1, \dots, s_n) \in S_1 \times \dots \times S_n$ in mindestens t Hyperebenen von $\mathcal{A}$ liegt, ausgenommen mindestens einem Punkt aus $D_1 \times \dots \times D_n$, der auf keiner der Hyperebenen von $\mathcal{A}$ liegt, dann gilt für alle j*

$$|A| \geq (t-1)(|S_j| - |D_j|) + \sum_{i=1}^{n} (|S_i| - |D_i|).$$

Bei Ball und Serra [13] wird noch eine Variante dieses Theorems für projektive Geometrie $PG(n, \mathbb{F})$, sowie ein ähnliches Theorem mit Translation der Hyperebenen und verschiedene Korollare vorgestellt.

Beweis. Definiere

$$f(x_1, \ldots, x_n) = \prod \left(\left(\sum_{i=1}^{n} a_i x_i \right) - a_{n+1} \right),$$

wobei jeder Faktor zu einer Hyperebene aus $\mathcal{A}$ gehört definiert durch die Funktion $\sum_{i=1}^{n} a_i x_i = a_{n+1}$. Nach Voraussetzung hat das Polynom f eine Nullstelle der Multiplikativität t an allen Punkten aus $S_1 \times \cdots \times S_n$ mit Ausnahme eines aus $D_1 \times \cdots \times D_n$, wo es nicht Null ist. Aus Theorem 7.7 folgt die Aussage. □

Folgende Theoreme von Alon und Füredi [5] stammen aus der selben Arbeit, wie das bereits mit dem klassischen Nullstellensatz bewiesene Theorem 1.6 und folgen direkt aus dem Fall $t = 1$ von Theorem 7.8.

Theorem 7.9. *Seien $h_1, h_2, \ldots, h_n \in \mathbb{N}$ und $G \subseteq \mathbb{R}^n$ die Menge der Gitterpunkte $(y_1, \ldots, y_n)$ mit $0 \leq y_i \leq h_i$ und $y_i \in \mathbb{N}$. Eine Menge von Hyperebenen im $\mathbb{R}^n$, die alle Punkte bis auf einen von G abdeckt hat Kardinalität mindestens $h_1 + h_2 + \cdots + h_n$.*

Theorem 7.10. *Sei $\mathcal{A}$ eine Menge von Hyperebenen in $AG(n, \mathbb{F})$. Wenn die Menge $S_1 \times \cdots \times S_n \subseteq \mathbb{F}^n$ nicht vollständig von $\mathcal{A}$ abgedeckt wird, dann liegen mindestens $min(\{d_1 \cdot d_2 \ldots d_n : |\mathcal{A}| \leq \sum_{i=1}^{n} (|S_i| - d_i), d_i < |S_i|\})$ Punkte aus $S_1 \times \cdots \times S_n$ nicht auf einer Hyperebene aus $\mathcal{A}$.*

8 Bemerkungen und Ausblick

Wir betrachten noch eine Erweiterung von Kós, Mészáros und Rónyai [36, 35]. Dort wird Theorem 1.3 ganz kanonisch auf Ringe und g_i über Multimengen, also mit Nullstellen höherer Vielfachhheit, erweitert. Damit lassen sich auch einfach einige Anwendungen auf Multimengen verallgemeinern, zum Beispiel die Theoreme 1.5 und 1.6.

Bei der Arbeit mit dem kombinatorischen Nullstellensatz stellt sich die natürliche Frage, auf welche Art von Problemen dieser angewendet werden kann und woran man dies erkennt. In dieser Arbeit wurden Anwendungen aus verschiedenen Gebieten vorgestellt, die natürlich eine gute Grundlage für weitere Anwendungen bieten. Die Annahme liegt allerdings fern, dass es nicht noch viele andere Anwendungsmöglichkeiten gibt, nicht zuletzt wegen der in jüngerer Zeit publizierten Erweiterungen [13, 36, 35]. Auf jeden Fall müssen die Probleme als Null- oder Nicht-Nullstelle eines Polynoms formuliert werden können. Untypisch sind asymptotische Probleme und solche, die algebraisch nicht greifbar sind, wie zum Beispiel die Planarität eines Graphen.

Als Spezialfall des kombinatorischen Nullstellensatz lässt sich ein Lemma von Schwartz und Zippel [55, 64] betrachten, welches wichtige Anwendungen in der theoretischen Informatik besitzt. Die gebräuchlichste Form besagt, dass ein Polynom $f \in \mathbb{F}[x_1, \ldots, x_n]$ höchstens $\deg(f)|\mathbb{F}|^{n-1}$ Nullstellen hat.

Neben der hier vorgestellten Variante einer polynomiellen Methode, die sich Nicht-Nullstellen von Polynomen zu nutze macht, gibt es auch noch viele andere, darunter besonders populär ein Dimensionsargument. Dabei wird verschiedenen Strukturen ein Polynom zugewiesen um anschließend deren Anzahl über die Dimension des entstehenden Polynomraumes einzugrenzen. Mehrere Anwendungen finden sich beispielsweise bei Babai und Frankl [12] und ein Resultat über die Turán-Zahl von bipartiten Graphen bei Alon, Krivelevich und Sudakov [6].

Literatur

[1] Alon, N.: *Combinatorial Nullstellensatz.* Combinatorics, Probability and Computing, 8(1-2):7–29, 1999.

[2] Alon, N.: *Additive latin transversals.* Israel Journal of Mathematics, 117:125–130, 2000.

[3] Alon, N., E. E. Bergmann, D. Coppersmith und A. M. Odlyzko: *Balancing sets of vectors.* IEEE Trans. Inf. Theor., 34(1):128–130, Januar 1988.

[4] Alon, N., S. Friedland und G. Kalai: *Regular subgraphs of almost regular graphs.* Journal of Combinatorial Theory, Series B, 37(1):79 – 91, 1984.

[5] Alon, N. und Z. Füredi: *Covering the Cube by Affine Hyperplanes.* European Journal of Combinatorics, 14(2):79 – 83, 1993.

[6] Alon, N., M. Krivelevich und B. Sudakov: *Turán Numbers of Bipartite Graphs and Related Ramsey-Type Questions.* Combinatorics, Probability and Compuing., 12(6):477–494, November 2003.

[7] Alon, N., N. Linial und R. Meshulam: *Additive bases of vector spaces over prime fields.* Journal of Combinatorial Theory, Series A, 57(2):203 – 210, 1991.

[8] Alon, N., M. B. Nathanson und I. Z. Ruzsa: *Adding distinct congruence classes modulo a prime.* American Mathematical Monthly, 102:250–255, 1995.

[9] Alon, N., M. B. Nathanson und I. Z. Ruzsa: *The Polynomial Method and Restricted Sums of Congruence Classes.* Journal of Number Theory, 56:404–417, 1996.

[10] Alon, N. und M. Tarsi: *A nowhere-zero point in linear mappings.* Combinatorica, 9(4):393–395, 1989.

[11] Alon, N. und M. Tarsi: *Colorings and orientations of graphs.* Combinatorica, 12:125–134, 1992.

[12] Babai, L. und P. Frankl: *Linear Algebra Methods in Combinatorics.*

[13] Ball, S. und O. Serra: *Punctured combinatorial Nullstellensätze.* Combinatorica, 29:511–522, 2009.

[14] Brink, D.: *Chevalleys theorem with restricted variables.* Combinatorica, 31:127–130, 2011.

[15] Chevalley, C.: *Dmonstration dune hypothse de M. Artin.* Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 11:73–75, 1935.

[16] Chevalley, H. und E. Warning: *Bemerkung zur vorstehenden Arbeit.* Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 11:76–83, 1935.

[17] Chung, F. R. K.: *Choosability in graphs.* Selected Topics in Graph Theory, 3:151–168, 1988.

[18] Cooper, A. S., O. Pikhurko, J. R. Schmitt und Gregory S. Warrington: *Martin Gardner's minimum no-3-in-a-line problem.* 2012.

[19] Coxeter, H. S. M.: *Introduction to geometry.* John Wiley, New York, 1969.

[20] Czerweiński, S., J. Grytczuk und W. Żelazny: *Lucky labelings of graphs.* Information Processing Letters, 109(18):1078 – 1081, 2009.

[21] Da Silva, J. A. D. und Y. O. Hamidoune: *Cyclic Spaces for Grassmann Derivatives and Additive Theory.* Bulletin of the London Mathematical Society, 26(2):140–146, 1994.

[22] Dasgupta, S., G. Károlyi und B. Szegedy O. Serra: *Transversals of additive Latin squares.* Israel Journal of Mathematics, 126:17–28, 2001.

[23] Dyson, F. J.: *Statistical Theory of the Energy Levels of Complex Systems. I.* Journal of Mathematical Physics, 3(1):140–156, 1962.

[24] Erdős, P., A. Ginzburg und A. Ziv: *Theorem in the additive number theory.* Bulletin Research Council Israel, 10F:41–43, 1961.

[25] Erdős, P. und H. Heilbronn: *On the Addition of Residue Classes mod p.* Acta Artihmetica, 9:149–159, 1964.

[26] Erdős, P., A. L. Rubin und H. Taylor: *Choosability in graphs.* Combinatorics, graph theory and computing, Seiten 125–157, 1979.

[27] Gunson, J.: *Proof of a Conjecture by Dyson in the Statistical Theory of Energy Levels.* Journal of Mathematical Physics, 3(4):752–753, 1962.

[28] Guy, R. und P. Kelly: *The no-three-in-line Problem.* Canadian Mathematical Bulletin, 11:527–531, 1968.

[29] Karasev, R.N. und F.V. Petrov: *Partitions of nonzero elements of a finite field into pairs.* Israel Journal of Mathematics, Seiten 1–14, 2012.

[30] Karolyi, G.: *An inverse theorem for the restricted set addition in Abelian groups.* Journal of Algebra, 290(2):557 – 593, 2005.

[31] Karolyi, G.: *Restricted set addition: The exceptional case of the Erdős Heilbronn conjecture.* Journal of Combinatorial Theory, Series A, 116(3):741 – 746, 2009.

[32] Kemnitz, A.: *On a lattics point problem.* Ars Combinatorica, 16b:151–160, 1983.

[33] Kemperman, J.H.B.: *On small sumsets in an abelian group.* Acta Mathematica, 103:63–88, 1960.

[34] Kohen, D. und I. Sadofschi: *A New Approach on the Seating Couples Problem.* ArXiv e-prints, Juni 2010.

[35] Kós, G. und L. Rónyai: *Alon's Nullstellensatz for multisets.* ArXiv e-prints, August 2010.

[36] Kós, G., T. Mészáros und L. Rónyai: *Some extensions of Alon's Nullstellensatz.* ArXiv e-prints, März 2011.

[37] Lasoń, M.: *A generalization of Combinatorial Nullstellensatz.* The electronic Journal of Combinatorics, 17(32), 2010.

[38] Lev, V. F.: *Restricted Set Addition in Groups I: The Classical Setting.* Journal of the London Mathematical Society, 62(1):27–40, 2000.

[39] Lev, V. F.: *Restricted set addition in abelian groups : results and conjectures.* Journal de théorie des nombres de Bordeaux, 17(1):181–193, 2005.

[40] Li, S.-Y. R. und W.-C. W. Li: *Independence numbers of graphs and generators of ideals.* Combinatorica, 1:55–61, 1981.

[41] Lin, W., D. Yang, C.-Y. Yang und X. Zhu: *Circular consecutive choosability of graphs.* Taiwanese Journal of Mathematics, 12(4):951–968, jul 2008.

[42] Lovasz, L.: *Bounding the Independence Number of a Graph.* Band 66 der Reihe *North-Holland Mathematics Studies*, Seiten 213 – 223. North-Holland, 1982.

[43] Lovasz, L.: *Stable sets and polynomials.* Discrete Mathematics, 124(13):137 – 153, 1994.

[44] Michalek, M.: *A Short Proof of Combinatorial Nullstellensatz.* American Mathematical Monthly, 117(9):821–823, 2010.

[45] Norine, S., T.-L. Wong und X. Zhu: *Circular choosability via combinatorial Nullstellensatz.* Journal of Graph Theory, 59(3):190–204, 2008.

[46] Pan, H. und Z.-W. Sun: *Restricted sumsets and a conjecture of Lev.* Israel Journal of Mathematics, 154:21–28, 2006.

[47] Pan, H. und Z.-W. Sun: *A new extension of the Erdős Heilbronn conjecture.* Journal of Combinatorial Theory, Series A, 116(8):1374 – 1381, 2009.

[48] Papadimitriou, C. H.: *On the complexity of the parity argument and other inefficient proofs of existence.* Journal of Computer and System Sciences, 48(3):498 – 532, 1994.

[49] Preissmann, E. und M. Mischler: *Seating Couples Around the King's Table and a New Characterization of Prime Numbers*. American Mathematical Monthly, 116(3):268–272, 2009.

[50] Pyber, L.: *Regular subgraphs of dense graphs*. Combinatorica, 5:347–349, 1985.

[51] Reiher, Christian: *On Kemnitz conjecture concerning lattice-points in the plane*. The Ramanujan Journal, 13:333–337, 2007.

[52] Schauz, U.: *Algebraically Solvable Problems*. Doktorarbeit, Eberhard-Karls Universität Tübingen, 2007.

[53] Scherk, P.: *Distinct elements in a set of sum*. American Mathematics Monthy, 62:46–47, 1935.

[54] Schreiber, Dan: *Complexity of the Combinatorial Nullstellensatz (2002)*. http://www.math.uiuc.edu/~west/regs/combnull.html, 2009. [Online; accessed 19-December-2012].

[55] Schwartz, J. T.: *Fast Probabilistic Algorithms for Verification of Polynomial Identities*. Journal of the ACM, 27(4):701–717, Oktober 1980.

[56] Sridharan, S.: *Polynomial time algorithms for two classes of subgraph problem*. RAIRO - Operations Research, 42(03):291–298, 2008.

[57] Stewart, I. A.: *Finding regular subgraphs in both arbitrary and planar graphs*. Discrete Applied Mathematics, 68(3):223 – 235, 1996.

[58] Sun, Z.-W.: *On Snevily's conjecture and restricted sumsets*. Journal of Combinatorial Theory, Series A, 103(2):291 – 304, 2003.

[59] Taskinov, V. A.: *Regular subgraphs pf regular graphs*. Soviet Mathematics Doklady, 26:37 – 38, 1982.

[60] Vince, A.: *Star chromatic number*. Journal of Graph Theory, 12(4):551–559, 1988.

[61] Vosper, A. G.: *The Critical Pairs of Subsets of a Group of Prime Order*. Journal of the London Mathematical Society, s1-31(2):200–205, 1956.

[62] Wilson, K. G.: *Proof of a Conjecture by Dyson*. Journal of Mathematical Physics, 3(5):1040–1043, 1962.

[63] Zeilberger, D.: *A combinatorial proof of Dyson's conjecture*. Discrete Mathematics, 41(3):317 – 321, 1982.

[64] Zippel, R.: *Probabilistic algorithms for sparse polynomials*. In: Edward, W. (Herausgeber): *Symbolic and Algebraic Computation*, Band 72 der Reihe *Lecture Notes in Computer Science*, Seiten 216–226. Springer Berlin Heidelberg, 1979.

Eidesstattliche Erklärung zur Bachelorarbeit

Ich versichere, die Bachelorarbeit selbstständig und lediglich unter Benutzung der angegebenen Quellen und Hilfsmittel verfasst zu haben.
Ich erkläre weiterhin, dass die vorliegende Arbeit noch nicht im Rahmen eines anderen Prüfungsverfahrens eingereicht wurde.

Berlin, den 18. Dezember 2012