Prüfungsprotokoll
Algebraic Methods in Combinatorics

X. M. Zheng

27. Februar 2023

- Studiengang: M.Sc. Mathematics
- Prüfungsdauer: 30 Minuten[1]
- Prüfer: Dr. Christian Reiher
- Beisitzer: Prof. Mathias Schacht
- Vertiefung: Diskrete Mathematik
- Belegt im: WS 2022 - 2023
- Umfang: 6 ECTS
- Prüfungssprache: Deutsch
- Note: 1.0
- War diese Note angemessen? Ja.

Prüfungsstil

Die Prüfung war sehr angenehm. Reiher stellt faire Fragen[2] und es kommt auch nicht auf jede Rechnung an, sondern, dass man kapiert hat, was die Ideen bzw. Schritte der Beweise sind. Es gab eine Transferfrage, die aber nicht wirklich schwer war. Sowohl zugunsten des Prüflings als auch Reiher / Schacht selbst hat man mehrere Blätter und verschiedenfarbige Stifte zur Verfügung. Schacht hat paar Fragen gestellt, die – gegeben das er an der Vorlesung nicht wirklich mitgewirkt hat – etwas ausholend waren. Jedoch schien da Reiher auch sehr fair, wenn man in dem Fall einen Fehler macht. Insgesamt eine sehr entspannte Atmosphäre also.

Hat sich der Besuch / Nichtbesuch der Veranstaltung für dich gelohnt?

Der Besuch der Vorlesung hat sich schon gelohnt. Dadurch, dass Reiher die Vorlesungsnotizen sehr spät herausgebracht hat, ist es im Grunde notwendig, in Präsenz zur Vorlesung zu erscheinen, um auf dem aktuellen Stand zu sein. Aber auch didaktisch gesehen macht es Reiher gut, auch wenn er vergleichsweise schnell im Tempo ist. Langweilig wird es also nicht, insbesondere wenn Reiher in einer Vorlesung kurz mal eine neulich gelöste Vermutung behandelt oder Anekdoten über Leute wie Aubrey de Grey

[1] Die Prüfung hat theoretisch 45 Minuten gedauert, mehr im Prüfungsverlauf.
[2] Fragen zu Sätzen, Beweisen, was man halt so erwartet.

macht. Da es auch keine Musterlösung zu den Übungsblättern gibt, war der Besuch der Übung im Grunde Pflicht. Aber die gestaltet sich meist kurz und schmerzlos.

Wie lange und wie hast du dich alleine oder mit anderen auf die Prüfung vorbereitet?

Ich habe effektiv alleine 10 Tage lang intensiv gelernt. Dabei bin ich mehr oder weniger mehrfach durch meinen inoffiziellen Mitschrieb von der Vorlesung durchgegangen und habe bei Klärungsbedarf auch Reihers hochgeladene Vorlesungsnotizen ausgenutzt.

Ich habe dabei insbesondere wert darauf gelegt, die Absicht, warum man dort jetzt das Lemma braucht etc., und allgemein die Zusammenhänge zwischen den verschiedenen Sätzen herauszuarbeiten. Im Lernen habe ich insbesondere die hinteren Kapitel öfter wiederholt, da diese trotz ihrer Kürze vergleichsweise anspruchsvoller sind.

Die Übungsaufgaben waren für mich weniger wichtig, jedoch bin ich sie gut genug durchgegangen, dass ich zumindest die grobe Idee zu jeder Aufgabe im Kopf hatte.

Akt 0: Struwwelpeter

Ich weiß nicht mehr warum, aber irgendwie hat Reiher im Smalltalk darüber geredet, wie man in der Grundschule aufgefordert wurde, nicht während des Unterrichts auf dem Stuhl zu wippen. Das artete so aus, das Reiher von seiner Verschwörungstheorie hinter einer der Geschichten (*„Die Geschichte vom Daumenlutscher“*) vom Struwwelpeter erzählte. Er habe nämlich immer vermutet, dass die Mutter der Schneider ist, wie sonst würde der Schneider wissen, wann das Kind seinen Daumen lutscht. Es müsse sich um eine Art Crossdressing / um einen Transvestiten handeln. Es war bemerkenswert, wie gut Reiher teils im Wortlaut Textausschnitte vom Struwwelpeter aufsagen konnte. Irgendwann kamen dann Schacht und Reiher in die Diskussion, ob Struwwelpeter ein geeignetes Buch für Kinder sei. Schließlich habe das Buch keine positiven Kindheitsvorbilder und alle Kinder würden in den Geschichten „verrecken“. Kurz ging es dann darum, ob ein Kind, dessen Daumen abgeschnitten wurde, zur Zeit des Struwwelpeters überleben würde mit dem Fazit „Nein, aber anderen ging es nicht viel besser.“. In der Diskussion ist wohl Schacht auch zum ersten Mal aufgefallen, dass es „Struwwelpeter“ und nicht „Struppelpeter“ oder „Strubelpeter“ heißt.[3] Nach 15 Minuten brach das Schacht schließlich ab, und die Prüfung begann.

[3] „Das ist doch sicher was Nordbayerisches.“ – Prof. Mathias Schacht

Akt 1: Der kombinatorische Nullstellensatz

Reiher startete die Prüfung und fragte, was ich als erstes Thema mir wünsche. Ich habe natürlich vollkommen verpeilt, dass man sich das erste Thema aussuchen darf, und wählte halbwegs bedacht den kombinatorischen Nullstellensatz. Diesen musste ich dann aufsagen, wobei ich etwas wegen dem Satz von Chevalley-Warning anfangs etwas durcheinander kam. Dass ich den Beweis von dem Satz konnte, glaubte Reiher mir, stattdessen fragte er mich nach Anwendungen. Ich wählte das Komjáth Problem:

Was ist die kleinste Anzahl an Hyperebenen, um alle bis auf eine Ecke des Einheitswürfels zu überdecken?

Ich habe also eine optimale Überdeckung durch n (= Dimension von unserem Raum) Hyperebenen angegeben, die alles bis auf die Null überdeckt. Dann habe ich die Optimalität von n mittels dem kombinatorischen Nullstellensatz nachgewiesen. Reiher war zufrieden, zückte aber direkt eine Transferaufgabe:

Was ist die kleinste Anzahl an (affinen) Geraden in $\mathbb{F}_p^2$, um alle Elemente von $\mathbb{F}_p^2$ bis auf die Null zu überdecken?

Ich brauchte etwas, um die Aufgabe zu verstehen, machte mich aber dann schnell nach einer (wahrscheinlich) optimalen Überdeckung auf der Suche: Zuerst wählte ich die Geraden gegeben durch $\{y = (x - c)\}$ für $c \in \mathbb{F}_p \setminus \{0\}$. Um dann noch die – wie Reiher schön sagte und später in der Formulierung einen Rückzieher machte – „Winkelhalbierende“ (bis auf die Null) zu überdecken, habe ich dann noch die senkrechten Geraden $\{x = c\}$ für $c \in \mathbb{F}_p \setminus \{0\}$ genommen. Dadurch kommt man dann (wenn man sich nicht wie ich verzählt und dann netterweise von Reiher korrigiert wird) auf $2(p - 1)$ Geraden.

Rückblickend wäre die Wahl $\{x = c\}, \{y = c\}$ für $c \in \mathbb{F}_p \setminus \{0\}$ natürlicher gewesen, aber naja. . .

Ich sagte dann nervös, dass ich erstmal annehme (bzw. bete), dass das optimal ist, und Reiher ließ es durchgehen, schien also richtig zu sein. Ich machte mich also auf die Suche nach einem Widerspruchsbeweis: Angenommen $g_1, \dots, g_m$ seien affine Geraden, die alle Punkte in $\mathbb{F}_p^2$ bis auf die Null überdecken, wobei $m < 2(p - 1)$. Die erste Frage war dann für mich, ob man sie algebraisch über die „Normalenform“ oder die „Parameterform“ kodieren sollte. Reiher wies darauf hin, dass hier wahrscheinlich die „Normalenform“ besser ist. Es sei also für alle $i \in [m]$ g_i gerade die Menge an Lösungen $(x, y) \in \mathbb{F}_p^2$, sodass $\langle a_i, x\rangle = b_i$, wobei $a_i \in \mathbb{F}_p^2$ und $b_i \in \mathbb{F}_p$. Dabei gilt stets $b_i \neq 0$, da $0 \notin g_i$ ist. Reiher fragte, ob man auch o.B.d.A. $b_i = 1$ verlangen darf und ja, darf man, da b_i sonst invertierbar ist und wir die Gleichung mit b_i^{-1} durchmultiplizieren können. Es sei also o.B.d.A. $b_1 = \cdots = b_m = 1$.

Angelehnt an das Komjáth Problem, habe ich als Ansatz das Polynom

$$P(x) = \prod_{i=1}^{m}(1 - \langle a_i, x\rangle) - \prod_{j=1}^{2}(1 - x_j)$$

definiert. Reiher wies darauf hin, dass der Grad so (für einen Widerspruchsbeweis über den Nullstellensatz) nicht stimmen kann. Und ich erkannte, das der hintere Term noch mit dem kleinen Satz von Fermat korrigiert werden muss:

$$P(x) = \prod_{i=1}^{m}(1 - \langle a_i, x\rangle) - \prod_{j=1}^{2}\left(1 - x_j^{p-1}\right).$$

Reiher schmunzelt und war zufrieden. Tatsächlich tut es dieses Polynom auch: Wegen $m < 2(p-1)$ ist ein Monom maximalen Grades in P gegeben durch $x_1^{p-1}x_2^{p-1}$, also muss nach dem kombinatorischen Nullstellensatz es $x \in \mathbb{F}_p^2$ geben, sodass $p(x) \neq 0$. Das kann aber nicht sein, da dieses Polynom wegen der Voraussetzungen für alle $x \in \mathbb{F}_p^2$ Null sein muss. Damit war dann der Abschnitt zu dem kombinatrischen Nullstellensatz gemeistert.

Akt 2: Borsuks Vermutung

Reiher wollte als nächstes wissen, was Borsuks Vermutung ist:

„*Wenn* $A \subseteq \mathbb{R}^n$ *endlichen Durchmesser hat (also beschränkt ist), dann gibt es eine Partition* $A = A_1 \mathbin{\dot\cup} \ldots \mathbin{\dot\cup} A_{n+1}$ *mit* $\operatorname{diam}(A_i) < \operatorname{diam}(A)$ *für* $i = 1, \ldots, n+1$. “

Ich sagte also die Vermutung auf und das die Vermutung falsch ist, wie Kahn oder Kalai – ich hatte es nicht mehr im Kopf – beweisen würden.[4] Das sollte ich also jetzt zeigen. Hierfür nannte und bewies ich zuerst die folgende Folgerung:

Satz. Es seien p eine Primzahl und

$$\mathcal{A} \subseteq [4p-1]^{(2p-1)}$$

ein Mengensystem mit $|A \cap B| \neq p-1$ für alle $A, B \in \mathcal{A}$. Dann ist

$$|\mathcal{A}| \leqslant \binom{4p-1}{p-1}.$$

Hierfür habe ich zuerst auch den Satz von Alon-Babai-Suzuki aufgesagt und gezeigt, wie man mit diesem den obigen Satz folgern kann.

[4]Sie haben es tatsächlich gemeinsam gezeigt.

Reiher interessierte noch, was die obige Konsequenz zum Satz von Alon-Babai-Suzuki so interessant macht bzw. was denn das Wachstum circa sei von $\mathcal{A}$ im Vergleich zu $[4p-1]^{(2p-1)}$. Ihm reichte es, wenn man sagt, dass asymptotisch $\binom{4p-1}{2p-1}/\binom{4p-1}{p-1}$ exponentiell (in p) wächst.

Es ging jetzt also darum, wie Kahn und Kalai für Primzahlen $p \geqslant 13$ Borsuks Vermutung in Dimension $\binom{4p-1}{2p-1}$ widerlegten. Ich habe also den Beweis wiedergegeben, wobei ich mich wegen der Bedeutung von „n" als einerseits bei Mengensystemen die Größe der Grundmenge, und andererseits als Dimension des Raums etwas verhapselte, was aber schnell korrigiert war. Glücklicherweise war auch Reiher nur wichtig, dass man nicht jede Rechnung ausführen muss, sondern was effektiv dann der Fall war.

En Détail, wenn wir den Durchmesser der Menge

$$\mathcal{A} = \left\{ \Phi(A) \,\middle|\, A \in [4p-1]^{[2p-1]} \right\} \subseteq \mathbb{R}^{[4p-1]^{(2)}}$$

untersuchen, wobei

$$\Phi(A) \coloneqq \left\{ \{x, y\} \in [4p-1]^{(2)} \,\middle|\, x \in A, y \notin A \right\},$$

so realisiert ein Paar $(\Phi(A), \Phi(B)) \in \mathcal{A}^2$ den Durchmesser von $\mathcal{A}$, wenn $|A \cap B| = p-1$ ist. Ist also $\mathcal{A} = \mathcal{A}_1 \uplus \ldots \uplus \mathcal{A}_m$ eine Partition mit $\operatorname{diam}(\mathcal{A}_i) < \operatorname{diam}(\mathcal{A})$ für $i = 1, \ldots, m$, so muss dann für alle $A, B \in [4p-1]^{(2p-1)}$ mit $\Phi(A), \Phi(B) \in \mathcal{A}_i$ $|A \cap B| \neq p-1$ gelten.

Nach dem obigen Satz ist also $|\mathcal{A}_i| \leqslant \binom{4p-1}{p-1}$ für alle $i \in [m]$. Somit gilt

$$m \geqslant \frac{\binom{4p-1}{2p-1}}{\binom{4p-1}{p-1}} > \binom{4p-1}{2} + 1 = n + 1$$

für $p \geqslant 13$. Damit ist Borsuks Vermutung für Dimension $\binom{4p-1}{2p-1}$ falsch. Insbesondere sieht man, dass die kleinste Zahl $f(n)$, sodass man jede Menge $A \subseteq \mathbb{R}^n$ in $f(n)$ Mengen mit kleinerem Durchmesser partitionieren kann, exponentiell in der Wurzel von n wächst.

Akt 3: Der Satz von Alon-Babai-Suzuki

Es waren noch 8 Minuten übrig und Schacht meint, ich solle doch den Satz von Alon-Babai-Suzuki zeigen, jetzt wo ich ihn angewendet habe. Wissend, dass der Beweis in der Vorlesung lang war, wahrscheinlich zu lang für 8 Minuten, wurden sowohl ich als auch Reiher etwas nervös. Währenddessen meinte Schacht, welcher an eine *einfachere Version* vom Satz von Alon-Babai-Suzuki dachte, das den Beweis so lang zu zerren doch das Krasse wäre.

Satz (Alon-Babai-Suzuki)**.** Es seien p eine Primzahl, $L \subset \mathbb{F}_p$, $|L| = s$ und k eine natürliche Zahl mit $k \notin L$.[5] Ferner seien $n \geqslant k + s$ und $\mathcal{A} \subseteq 2^{[n]}$ ein Mengensystem mit:

- Für alle $A \in \mathcal{A}$ ist $|A| \equiv k \pmod p$.
- Für alle verschiedenen $A, B \in \mathcal{A}$ ist $|A \cap B| \in L$.

Dann gilt $|\mathcal{A}| \leqslant \binom{n}{s}$.

Ich begann also: Folgendes Lemma durfte ich ohne Beweis voraussetzen.

Lemma. Seien $k, s \in \mathbb{N}_0, n \geqslant k + s$ und F ein Körper. Ferner sei $\alpha\colon 2^{[n]} \to F$ eine Funktion mit

(a) $\alpha(U) = 0$ für $|U| \geqslant s$,
(b) $\sum_{T \subseteq X} \alpha(T) = 0$ falls $k < |X| \leqslant k + s$.

Dann gilt $\alpha = 0$.

Mit diesem kann man zeigen, dass folgendes Lemma gilt:

Lemma. Es seien p eine Primzahl und $k, s, n \in \mathbb{N}_0$ mit $p > k, s \geqslant 0$ und $n \geqslant k + s$. Setze $\Omega = \{0, 1\}^n$. Definiere $f\colon \Omega \to \mathbb{F}_p$ durch $f(x_1, \dots, x_n) = \sum_{i=1}^{k} x_i - k$. Für $B \subseteq [n]$ setze $x_B = \prod_{i \in B} x_i$. Dann ist

$$\{x_B \cdot f \mid B \subseteq [n] \text{ und } |B| < s\}$$

linear unabhängig in $\mathbb{F}_p^{\Omega}$.

Effektiv geht der Beweis so vor, dass man einen Widerspruchsbeweis führt, also annimmt, dass es Skalare, nicht alle Null, gibt, die mit den $x_B \cdot f$ eine nicht-triviale Linearkombination der Null bilden. Diese Skalare nehmen dann die Rolle von $\alpha\colon 2^{[n]} \to F$ aus dem zuvorigen Lemma an. (a) ist trivialerweise erfüllt und (b) weise man für $k < |X| \leqslant k + s$ nach, indem man es in die Linearkombination einsetzt.

Mit dem Lemma ist der Beweis dann relativ unkompliziert, und läuft darauf hinaus, dass man zu $\mathcal{A} = \{A_1, \dots, A_m\}$ die Polynome

$$P_i(x) = \prod_{\lambda \in L} (\langle x, A_i \rangle - \lambda) \in \mathbb{F}_p^{\Omega} \qquad (i \in [m])$$

definiert und dann nachweist, dass

$$\{P_i \mid i \in [m]\} \cup \{x_B \cdot f \mid B \subseteq [n] \text{ und } |B| < s\}$$

linear unabhängig sind. Da diese aber Elemente des Untervektorraums

$$V = \langle \{x_B \mid B \subseteq [n] \text{ und } |B| \leqslant s\} \rangle$$

[5] Natürlich in dem Sinne, dass k's Restklasse nicht in L ist.

sind, folgt also

$$m + \binom{n}{s-1} + \cdots + \binom{n}{0} \leqslant \binom{n}{s} + \cdots + \binom{n}{0}.$$

Damit wäre $|\mathcal{A}| = m \leqslant \binom{n}{s}$ gezeigt.

Die Prüfung wäre damit zu Ende, aber natürlich, als Schüler von Rödl, fragte Schacht noch, ob eine Version des ersten Satzes existiert, der nicht nur für Primzahlen gilt. Nach etwas Raten, ob er auf den Satz von Frankl-Wilson oder dem Satz von Ray-Chaudhuri-Wilson hinaus will, kam nur noch der – **in der Vorlesung nicht bewiesene** – Satz von Frankl-Rödl in Frage:

Satz (Frankl-Rödl)**.** Für alle $0 < \alpha < \beta < 1$ existiert ein $\varepsilon \in (0,1)$ derart, dass jedes Mengensystem $\mathcal{A} \subseteq [n]^{\lfloor \beta n \rfloor}$ mit $|A \cap B| \neq \lfloor \alpha n \rfloor$ für alle $A, B \in \mathcal{A}$ höchstens die Größe

$$|\mathcal{A}| \leqslant (1-\varepsilon)^n \binom{n}{\lfloor \beta n \rfloor}$$

hat.

Dann aber sich beschweren, wenn man den Satz aufsagen kann und darauf hinweist, dass Reiher im Tafelanschrieb des Satzes (wahrscheinlich) einen Typo hatte.[6] Reiher hat mich aber verteidigt, weil ich das inoffizielle Skript schreibe und es deswegen dürfe, lol.

Damit war auch dieser Teil zu Ende.

Fazit

Nachdem sie mich nach der Besprechung reinholten hieß es 1.0, was wohl nach der Transferaufgabe für sie bereits klar war (sofern ich nicht einen sehr groben Fehler noch mache).

Reiher fragte, was ich die restlichen Ferien noch vor habe und ich meinte, dass ich noch Modelltheorie schreiben werde. Natürlich hatte Reiher auch darin Ahnung, überfragte mich über Modelltheorie, und nannte Anekdoten zu Paul Cohen[7], wie er die ganze Modelltheorie für trivial hielt.

[6] „Immer diese Überschlauen. . . “ – Prof. Mathias Schacht

[7] Mathematiker, der mit der von ihm entwickelten Forcing-Methode zeigte, dass die Kontinuumshypothese nicht mit ZFC beweisbar ist.