Prüfungsprotokoll Theoretische Informatik - WS08/09

- **Datum:** 19. März 2009
- **Prüfer:** Prof. Thomas, Prof. Mathar
- **Vorlesungen:**
  - Angewandte Automatentheorie (SS08)
  - Unendliche Spiele (WS08/09)
  - Automaten auf unendlichen Wörtern (WS08/09)
  - Cryptography I + II (WS07/08, SS08)
- **Dauer:** ca. 45 Min.
- **Note:** 1.7

1 AAT

- Welche Logik gibt es die äquivalent zu NEA ist? → MSO, bisschen was erklärt was man mit Mengenvariablen macht
- Wie stellt man den erfolgreichen Lauf eines NEA mit einer MSO-Formel da? → Grobe Skizze der Formel, Partition, Transitionen
- Wieviele Mengenvariable braucht man? → Naiv: Soviele wie Zustände. Man kann aber auch Zustände binär kodieren.
- Geht es auch mit nur einer Mengenvariable? → Ja! (kam wohl in einer Übung vor)
- Komplexität bei Übersetzung von MSO → NEA, insb. welche Operationen dabei schwer sind.
- Was für Baumautomaten haben wir kennengelernt? → Unterschied zwischen NTA und DTA und Top-Down und Bottom-Up erklärt, insb. welche äquiv. sind
- Geben sie mal ein Beispiel für eine Baumsprache die nicht von einem det. Top-Down-Baumautomat erkannt wird, nicht-deterministisch aber schon → Standardbeispiel aus Skript
- Kann man die Baumsprache der Bäume, so dass alle Pfade grade Länge besitzen, durch det. Top-Down-BA erkennen? → Hab ich mich ein wenig verhaspelt, geht nicht
- Was für unendliche Systeme haben wir kennengelernt → Hab auf PDS/PDA verwiesen
- Erreichbarkeitsproblem für diese Systeme? → Entscheidbar für PDS/PDA, Saturierungsalgo
- Und bei mehr als einem Stack? → Unentscheidbarkeit (durch Simulation von TM auf leerem Band). Erklärt wie man das Band der TM in Kellern darstellt.
- Wie ist das wenn wir einen Automat mit einer Queue haben? → Erst auf CFSM verwiesen und dann erklärt dass ein Queue-System äquiv. dazu ist
- Wie simuliert man TM mit Queue-System? → Letzten 3 Buchstaben auf dem Band durch Zustände merken, etc.

2 US/AauW

- Was sind Muller-Automaten? Wie sind die definiert? (also Akzeptanzverhalten)
- In welchem Zusammenhang stehen det. Muller-Automaten und nichtdet. Büchi-Automaten?
- Wenn sie eine Richtung der äquiv. beweisen müssten, welche würde sie wählen? → Da hab ich natürlich Muller → BA genommen und die Konstruktion erklärt (und Komplexität)
- Wie zeigt man die andere Richtung? → Da hab ich nur auf Safra-Bäume bzw. Muller-Schupp aus der Vorlesung verwiesen
- Was für Zustände hat man bei der anderen Richtung? → Safra-Bäume als Makrozustände (das hat ihm schon gereicht)
- Komplexität Safra-Konstruktion? → $2^{O(nlogn)}$
- Geht das besser? → Hinweis auf Beweis dass es nicht geht, Rabin-Automaten
- Spiele: Wie ist das Lösen eines Spiels definiert? → Gewinnbereichberechnung, Gewinnstrategien (wobei pos. gewünscht ist)
- Wie ist das bei Paritätsspielen? → Spiel determiniert, beide Spieler haben pos. Gewinnstrategien
- Wie kompliziert ist das? → Der Hinweis darauf dass die Gewinnbereichsberechnung in NP ∩ co-NP liegt.
- Ist das schlimm dass das in NP ∩ co-NP liegt? → Ähhhh

- Ordnen sie mal NP ∩ co-NP im Vergleich zu den anderen Komplexitätsklassen ein → Da hat er mich kalt erwischt und ich hab zuerst Mist gebaut, war aber auch nicht soo wichtig.
- Wie ist das mit Baumautomaten und Büchi/Muller? → Hinweis auf Nichtäquivalenz mit dem Baum der im Skript konstruiert wurde
- Muller-Spiele und Paritätsspiele, wie ist da der Zusammenhang → Reduktion von Muller auf Paritätsspiel, dadurch also Automatenstrategie
- Bauen sie mal ein einfaches Spiel wo man sieht dass für Muller-Spiele pos. Gewinnstrategie nicht reicht → Da hab ich das DJW-Spiel aufgemalt, er meinte das wäre schon das komplizierteste
- Also, einfaches Beispiel für Muller-Spiel genommen an dem man direkt sehen konnte dass pos. Gewinnstrategie nicht reicht.

3 Crypto I+II

(der Automaten-Teil war bis hierhin ganz gut gelaufen fand ich, und bei Crypto gings dann mächtig daneben da ich genau die Sachen nicht gut drauf hatte die Prof. Mathar abgefragt hat)

- Was ist perfekte Sicherheit (perfect secrecy)? Wie ist sie im Zusammenhang mit der Entropy definiert?
- Wie ist die Entropie genau definiert? Was sagt die aus?
- Wie hängt die Entropie mit stoch. Unabhängigkeit zusammen?
- Was heisst es also wenn ein System perfect secrecy besitzt?

(zu dem ganzen Abschnitt kam von mir nur relativ unzusammenhänger Kram, so dass Prof. Mathar zurecht sehr genervt wirkte)

- Was ist der diskrete Logarithmus? → Kurz erklärt, ist eigentlich klar
- Wie kann man den diskreten Logarithmus mit dem Diffie-Hellman-Key-Exchange benutzen? → Auch kurz erklärt, erklärt was Primitivwurzel ist
- Was ist das Diffie-Hellman-Problem? Liefert Lösung für DHP automatisch Lösung für disk. Log.?
- Gibt es immer Primitivwurzel zu einer Zahl? → Nein, nur für $n \in \{1, 2, 4, p^k, 2p^k\}$ mit p prim
- Wie findet man Primzahlen um sie z.B. bei Diffie-Hellman zu benutzen? → Kurzer Hinweis auf FPT und MRPT und dass das effektiv (probabilistisch) geht
- Wie findet man Primitivwurzeln zu einer Zahl?

(der Teil war ganz gut, waren auch noch paar andere kleinere Zahlenspiele drin, danach gings dann wieder abwärts leider)

- Was ist die Idee bei Elliptic Curve Cryptography?
- Was für Cryptoverfahren kann man damit benutzen? → Diskreter Log.
- Was für Operationen über Elliptischen Kurven gibt es?
- Wie berechnet man $n * P$? Geht das effizient → Hinweis auf Square-and-multiply

4 Fazit

Die Prüfung war angenehm, wer Prof. Thomas kennt kann sich auch die Atmosphäre vorstellen. Ich hab (zum Glück) mit dem Automatenteil angefangen, so dass ich erstmal relativ viel richtig hatte und ohne Stocken gut durchkam. Der Crypto-Teil danach war, wie schon angedeutet, ziemlich schlecht, so dass der Teil sicherlich eine bessere Note verhindert hat. Man sollte Fragen natürlich ruhig zuhören und dann auch genauso ruhig und strukturiert beantworten. Bei manchen Fragen hab ich mich überschlagen und musste dann nochmal ganz in Ruhe mit den Basics anfangen, sowas muss nicht sein. Wenn es Sinn macht sollte man die Fragen nicht nur so knapp beantworten wie möglich sondern ruhig auch ein bisschen ausschweifen warum man das macht oder obs da noch interessante Eigenschaften gibt. Gelernt habe ich über einen Zeitraum von 6 Wochen, hauptsächlich mit den Skripten und ein bisschen mit Folien bei AAT und AauW. Crypto kann man perfekt aus dem Skript lernen. Im Endeffekt hätte ich mit mehr Aufwand den Stoff vielleicht auch in 4 Wochen lernen können.

Dieses Protokoll ist zwar nur wenige Stunden nach der Prüfung entstanden, aber da fehlen auf jeden Fall noch ein paar kleinere Fragen, es kann also in 45 Minuten doch einiges abgefragt werden ;)