Gedächtnisprotokoll zur Diplomprüfung in Theoretischer Informatik

Fächer:	**Algorithmische Kryptographie** (nach Buch Delfs/Knebl), **Effiziente Algorithmen** (nach der 2. Auflage des Buches) und **Angewandte Automatentheorie** nach dem alten Skript vom Februar 2002
Prüfer:	Prof. Hromkovič
Datum:	14.05.2004
Dauer:	40 Minuten
Note:	1.0

Hromkovič: Möchten Sie die Fächer in einer bestimmten Reihenfolge geprüft haben?
Ich: Ja, und zwar bitte erst Kryptographie, dann Effiziente Algorithmen und schließlich Automatentheorie.

Hromkovič: Welche Public-Key Kryptosysteme kennen Sie?
Ich: RSA, El Gamal und Rabin.

Hromkovič: Dann erklären Sie mal Rabin
Ich: Habe Schlüsselerzeugung ($n = pq$, p, q prim), Verschlüsselung durch Quadrieren und Entschlüsselung erklärt und erwähnt, dass man das Wurzelziehen mit Hilfe des Chinesischen Restesatzes machen kann, weil man p und q kennt. Das sollte ich dann noch detailliert erklären. Also habe ich erklärt, dass man das Wurzelziehen in Z_n erledigen kann, wenn man die Quadratwurzeln der Reste $x_1 = x \bmod p$ und $x_2 = x \bmod q$ in Z_p bzw. Z_q bestimmt, was dann für $p \equiv 3 \pmod 4$ direkt und für $p \equiv 1 \pmod 4$ immerhin noch mit einem sehr effizienten probabilistischen Algorithmus (im Anhang des Buches) funktioniert. Schließlich kamen wir noch darauf zu sprechen, wie sicher Rabin (im Vergleich mit anderen Verfahren) ist, worauf ich erklärte, dass es beweisbar genauso schwer ist wie die Faktorisierung. Das sollte ich dann auch noch beweisen. Die eine Richtung hatte ich ihm ja schon erklärt, also habe ich nur noch gezeigt, wie man aus zwei Wurzeln $u \neq \pm v$ mit $\mathrm{ggT}(n, (u + v))$ einen Primfaktor von n bestimmen kann. Ist auch im Anhang erklärt.

Hromkovič: Können Sie dann mal El Gamal erklären?
Ich: Zu El Gamal habe ich dann wieder erstmal erklärt, wie öffentlicher und privater Schlüssel aussehen, wie man eine Nachricht verschlüsselt und wieder

entschlüsseln kann. Das hat dann auch schon gereicht.

Hromkovič: Kommen wir zu "Zero-Knowledge". Worum geht es da?
Ich: Habe ihm die Definiton erklärt, wann ein interaktives proof system (P,V) zero-knowledge ist. Als Beispiel habe ich ihm Simplified Shamir genannt.

Hromkovič: Dann erklären Sie das mal.
Ich: Habe angefangen beim Geheimnis $x = y^2$ des Provers alle Schritte des Protokolls erklärt und sollte zeigen, wie man als Verifier die Antworten mit $b^2 \stackrel{?}{=} ax^e$ verifizieren kann.

Das hat ihm dann zur Kryptographie gereicht und er hat gesagt, dass er das Thema wechselt und wir haben mit Effiziente Algorithmen weitergemacht.

Hromkovič: Erklären Sie mal das Konzept der Pseudo-Polynomial-Zeit Algorithmen
Ich: Habe zuerst erklärt, was ein Zahlwertproblem ist, und dann die Definition erklärt, wobei ich die Anforderung an die Zeitkomplexität $Time_A = O(p(|x|, MaxInt(x)))$ aufgeschrieben habe.

Hromkovič: Was für Beispiele kennen Sie?
Ich: DPKP (Rucksackproblem mit dynamischer Programmierung) und Ford-Fulkerson MaxFlow/MinCut

Hromkovič: Dann erklären Sie bitte mal Ford-Fulkerson und worum es dabei geht.
Ich: Dazu habe ich dann erst erklärt, was ein Netzwerk und ein Fluss in einem Netzwerk ist. Dann eine Definition von MaxFlow und MinCut. Dabei gab es dann erstmal ein kleines Missverständnis, weil ich mich wohl etwas unklar ausgedrückt hatte, so dass er dann nochmal sehr explizit nach einer exakten Definition des zu MaxFlow dualen Problems MinCut nachgehakt hat. Als das geklärt war, habe ich die Funktionsweise des Algorithmus erklärt und dabei die augmenting paths erwähnt. Zur Komplexität wollte er nichts wissen.

Hromkovič: (hier weiß ich nicht mehr, was er genau gefragt hat, jedenfalls ging es um stark NP-harte Probleme)
Ich: Dazu habe ich ihm erklärt, was $Value(p) - U$ ist und auf die Frage nach

einem Beispiel, habe ich darauf verwiesen, dass TSP stark NP-hart ist und man da eine Reduktion $HC \leq_p Lang_{value(p)-TSP}$ machen kann. Zu der Reduktion habe ich erst kurz erklärt, dass es sich bei der rechten Seite um eine Threshold-Sprache handelt und dann brauchte ich lediglich die Konstruktion der neuen Eingabe erklären.

Hromkovič: Wir hatten da auch noch einen randomisierten Algorithmus für SAT
Ich: Ja, und zwar gab es da von Schöning einen randomisierten multi-start local search Algorithmus der mit einer exponentiell sinkenden Fehlerwahrscheinlichkeit 3SAT in $O(|F|n^{3/2}(4/3)^n)$ löst. Dazu meinte er dann, dass er die genaue Zeitkomplexität nicht so wichtig sei und fragte, ob ich den Algorithmus grob erklären könne.

Also habe ich ihm erklärt, dass zufällig eine Belegung gewählt wird, von der aus dann lokale Suche startet. Dabei war ihm wichtig, welche Anforderungen an eine Nachbarschaftstrafo mittels Flip gestellt werden (es wird eine Klausel erfüllt, die vorher nicht erfüllt war) und wie die Wahrscheinlichkeiten sind, dass man der richtigen Belegung α^* näher kommt.

Wie die Wahrscheinlichkeit ist, dass man eine Belegung rät, die eine Distanz j zu α^* hat ($p_j = \binom{n}{j}/2^n$), konnte ich ihm noch erklären. Bei der Wahrscheinlichkeit, mit einem Random-Walk mit i Schritten in die falsche und $j+i$ Schritten in die richtige Richtung zu kommen, kannte ich den letzten Faktor von $q_j = \binom{2i+j}{i}(\frac{1}{3})^{j+i}(\frac{2}{3})^i \frac{j}{j+2i}$ nicht, was aber auch nicht so schlimm war. Hromkovič erzählte, dass er dafür letztens selber 3 Seiten gebraucht hat und das den Rahmen des Buches gesprengt hätte (von wegen "short combinatorial calculation"...).

Wichtig war ihm aber die in der Fußnote im Buch erwähnte Anmerkung, wodurch dieser Bruch zu Stande kommt. Und zwar wollte er hören, dass jeder Pfad-Suffix mehr Schritte in die richtige als in die falsche Richtung haben muss. Da bin ich aber erst nach einigen Hilfen wieder drauf gekommen.

Schließlich habe ich ihm noch erklärt, wie man aus der so errechenbaren kleinen Wahrscheinlichkeit $p \geq \sum_{j=0}^{n} p_j q_j$, die richtige Belegung zu finden, durch häufiges Wiederholen auf eine fast 100% Erfolgswahrscheinlichkeit kommt, aber das war ihm nicht so wichtig.

Hromkovič: Dann sagen Sie noch was zu Simulated Annealing
Ich: Habe ihm die Analogie zur Festkörperphysik erklärt und die Formel für die Wahrscheinlichkeit, eine Verschlechterung zu akzeptieren hingeschrieben: $p(q \to s) = e^{-\frac{\Delta cost}{kT}}$. Dazu hat er dann noch nachgefragt, wobei ich zunächst

nicht ganz verstanden hatte, worauf er hinaus wollte. Offensichtlich wollte er nur nochmal hören (wie man an der Formel ja eigentlich direkt ablesen kann), dass man große Verschlechterungen seltener akzeptiert und man bei kleinerer Temperatur ebenfalls seltener Verschlechterungen akzeptiert.

Das hat ihm dann zu den Effizienten Algorithmen gereicht und er kam zum letzten Teil.

Hromkovič: Erzählen Sie mal was zur Minimierung von DFAs
Ich: Habe angefangen bei der Nerode-Kongruenz und dann den Markierungsalgorithmus zur Trennung von nicht-äquivalenten Zuständen erklärt. Dazu wollte er wissen, warum der terminiert, was ich ihm dann unter Verweis auf die endliche Zahl von Zustandspaaren und das endliche Alphabet begründet habe.

Hromkovič: Wie sieht das mit der Minimierung bei NFAs aus?
Ich: Da ist das wohl PSPACE-schwer, was aber im Skript gar nicht gezeigt wird. Man kann statt Minimierung aber immerhin eine Reduktion mittels Bisimulations-Äquivalenz machen.

Hromkovič: Gut, kommen wir zu Petri-Netzen. Was ist das, wie kann man damit Sprachen erkennen?
Ich: Bei der Frage hätte ich fast Probleme bekommen, weil ich die letzten Kapitel des Skripts nur sehr rudimentär vorbereitet hatte, da in alten Protokollen noch nie Fragen zu Petri-Netzen, kommunizierenden Systemen o.ä. vorkamen. Ich habe ihm dann sehr grob erklärt, wie ein Petri-Netz aussieht (Stellen, Transitionen, Marken etc.) und wie man damit Wörter erkennen kann (Buchstaben an Transitionen). Dann kam noch irgendeine Nachfrage bezüglich der Sprachen, die man damit erkennen kann und ich erinnerte mich zum Glück daran, dass man nicht-reguläre Sachen wie $a^n b^n c^n$ erkennen kann. Für $a^n b^n$ sollte ich dann mal ein Netz aufmalen, was mir allerdings nicht ganz gelungen ist. Meine Version hätte etwas zu viel erkannt und ich hab dann auch nicht mehr gesehen, woran es lag. Er hat es dann erklärt und es war echt einfach. Ihm war es aber letztlich auch egal, dass ich nicht drauf gekommen bin.

An der Stelle war die Prüfung dann vorbei. Ich konnte sogar direkt drinnen bleiben, weil er meinte, die Note sei klar :-)

Wie man auch in anderen Protokollen schon lesen konnte, ist Prof. Hromkovič als Prüfer sehr zu empfehlen. Die Atmosphäre war sehr angenehm und

man sollte sich nicht zu sehr (Kommentar W. Unger auf dem Flur "Oh, ich rieche Angstschweiß") verrückt machen lassen, sondern einfach souverän auftreten. Ein bisschen kann man die Prüfung auch selber steuern. Die Frage nach dem Beweis, dass Faktorisierung so schwer ist wie das Wurzelziehen, habe ich beispielsweise etwas provoziert, weil ich wusste, dass ich den Beweis konnte und das hat dann auch einen guten Eindruck gemacht. Andersherum muss man bei der Beantwortung einer Frage ja keine verwandten Themen erwähnen, die man gerade nicht so gut kann.