Diplomprüfung

Gedächtnisprotokoll
Theoretische Informatik

Prüfer: Prof. Juraj Hromkovic
Fächer: Effiziente Algorithmen,
Kryptographie
Compilerbau
Datum: 03.11.2005
Name: Laszlo Bardos
Note: 1.0

Effiziente Algorithmen:

Hro: Was ist parametrisierte Komplexität?

Ich: Definition aufgesagt.

Hro: Wie groß kann die Funktion f sein? (bei p(|x|)*f(Par(x))

Ich: Hab zuerst polynomiell gesagt, dann gemerkt dass das nicht so stimmen kann und als Beispiel die Komplexität vom ersten Par VC Algorithmus hingeschrieben und gesagt, dass das n ja nur polynomiell sein darf. Und er frage nach dem k und da ist bei mir der Groschen gefallen, dass ja Par(x) sich auf das k^2k bezieht und f deswegen beliebig sein darf.

Hro: Wir haben zwei Beispiele zu Par Algorithmen gehabt.

Ich: Hab die zwei Beobachtungen erklärt (runterbeten reichte hier nicht, ich sollte erklären warum die erste Beobachtung so ist .. konnte ich zum Glück). Zum Algorithmus wollte er nicht mehr viel wissen. Habe nur gesagt, dass man die Knoten mit Grad größer k entfernt und checkt, ob |V| nicht zu groß ist und man dann mit Backtracking weitermacht. Den zweiten VC Algorithmus hab ich auch erklärt und er wollte dann nur noch wissen warum das O(2^k*n) Laufzeit hat. Hab erklärt dass man immer zwei Teilprobleme erhält und das k mal und dass der triviale Fall O(n) ist. Er sagte, dass man eigentlich O(n) wegen der Konstruktion von G' aus G erhält. Ich hab zugegeben, dass ich nicht sicher war, weil im Buch an zwei Stellen O(n) erwähnt wurden.

Hro: Was sind Diamanten?

Ich: Diamanten hingemalt und erklärt.

Hro: Für was werden Diamanten gebraucht?

Ich: Reduktion HC auf RHC erklärt.

Kryptographie:

Hro: Wie Funktioniert RSA?

Ich: Schlüsselerzeugung, Ver- und Entschlüsselung erklärt.

Hro: Können Sie die Eindeutigkeit von RSA zeigen?

Ich: Fall eins und zwei wie im Unger Skript hingeschrieben (viel verständlicher als das was im Buch steht). Und gesagt dass der dritte Fall (p und q teilen n) nicht in der Praxis vorkommt weil wir m < n wählen.

Hro: Warum gilt das hier und zeigt auf erste Zeile vom ersten Fall?

Ich: Wegen dem Satz von Euler. (w^(phi(n) kongruent 1 mod n)

Hro: Warum gilt das hier und zeigt auf letzte Zeile vom zweiten Fall?
Ich: Wegen dem chinesischen Restsatz.

Hro: Was ist Zero Knowledge?

Ich: Definition aufgesagt.

Hro: Kennen Sie ein Beispiel?

Ich: Simplified Fiat Shamir aufgeschrieben. Kurz vertan an der stelle y^2 = x. Hatte x^2 = y geschrieben, aber hab mich korrigiert bevor er was sagen musste/konnte. Hab dann noch gezeigt warum das Zero Knowledge ist.

Compilerbau:

Hro: Was sind LR(k) Grammatiken?

Ich: Definition zusammen mit $first_k$ aufgeschrieben.

Hro: Wie können Sie prüfen, ob eine Grammatik LL(k) ist?

Ich: Äääähh .. Hab irgendwas Nebulöses von first-Mengen erzählt und daraufhin hat er mir dann die Antwort quasi gegeben.

Wichtige Anmerkung!
Ich will jetzt keine Panikmache betreiben, aber der Kollege der mit mir am gleichen Tag die Prüfung bei Prof. Hromkovic gemacht hat und eigentlich auf einem ähnlich guten Wissenstand war wie ich, hat eine 4.0 bekommen. Er hatte eigentlich nach der Prüfung mit einer 1,7 oder 2,0 gerechnet und war ziemlich überrascht über die Note. Was vorgefallen war: Die allererste Frage war, was NP Vollständigkeit ist. Mein Kollege hat in der Definition einen Fehler gemacht und behauptet „ … wenn man für alle U aus stark NP schwer U $<_p$ L … “. Das hat dazu geführt, dass Prof. Hromkovic überzeugt war, dass er von EA keine Ahnung hat, da die Antwort Grundwissen wäre. Weiterhin hat er dann bei den anderen Fragen in der Prüfung immer wieder tiefer nachgehakt. Obwohl 80% der Fragen richtig beantwortet wurden (u.a. Christofides) sagte Prof. Hromkovic, dass jemand der die einfachen Fragen nicht kann eigentlich durchfallen würde.
Deswegen würde ich jedem Empfehlen sich gerade in EA (was Prof. Hromkovics Hauptgebiet ist) gut vorzubereiten und nicht nur Definitionen auswendig zu lernen. Das kann klappen, muss aber nicht.