Prüfungs-Abschrift "Einführung in die theoretische Informatik" vom 16.09.2003

P.S.: der Mozilla stellts richtig dar, der IE kennt einige mathematische Symbole ("element von", "abrundung") ned - is aber ned mein Problem *g*; Fehler, Flames, Ergänzugen nehm ich gern entgegen!

I-1 (8 Pkte)

Konstruieren Sie einen vollständigen determinsistischen erkennenden Automaten, der die Sprache L aller Wörter über {a,b}, die aab als Teilwort enthalten, akzeptiert.

I-2 (8 Pkte)

Ist die Sprache L aller Wörter der Form a^n w w^{rev} mit natürlicher Zahl n und w $\in$ $\{a,b\}^*$ (w^{rev} ist das Spiegelwort von w; Begründung!)

1. mit einer Turing-Maschine akzeptierbar?
2. kontextsensitiv?
3. kontextfrei?
4. regulär?

I-3 (3 Pkte)

Beweisen Sie: Ist eine Sprache L kontextfrei, so ist auch L^* kontextfrei.

I-4 (3 Pkte)

Sei f die Funktion <m,n --> if m = 0 then n else 0 fi>. Zeigen Sie, dass f primitiv-rekursiv ist.

I-5 (8 Pkte)

Konstruieren Sie eine Turing-Maschine, die die Kleiner-Relation auf der Menge der natürlichen Zahlen entscheidet, wobei unäre Zahlen-Darstellung verwendet wird.

II-1 (2 Pkte) (Zusammensetzung von Funktoren)

Funktoren sind wie Transformatoren (Übertrager mit galavanischer Trennung). Funktoren gibt es in zwei Varianten: covariant (Symbol +) und contravariant (Symbol -). Füllen Sie die Tafel, in der die Varianz der Zusammensetzung zweier Funktoren der angegebenen Varianz als Ergebnis stehen soll, aus:

+.+= , +.-= , -.+= , -.-= .

Was macht ein contravarianter Funktor mit Quelle und Ziel?

II-2 (4 Pkte)

In welchen Gruppen reicht es zur Erzeugung einer Untergruppe allein die Multiplikation, nicht aber die Inversion einzusetzen?

Betrachten Sie einige Operationen: null, eins, addition, subtraktion, multiplikation, summe der geometrischen Reihe 1 / (1 - x) (dort wo sie konvergiert). Kann man einen uniform für alle Argumente funktionierenden Term bilden "aus dem Zeug", der die Operation der multiplikativen Inversion darstellt? Wenn nein: In welchem Bereich der reellen Zahlen klappt dies mit einer Anwendung der geometrischen Reihe? Jetzt steht zusätzlich das Quadratwurzelziehen zur Verfügung. Gibt es nun etwas, um für jede Zahl einen Term zu bauen, der ihr Inverses ausdrückt? Gibt es einen festen Term für alle Zahlen?

In einem Ring mit nilpotenten Elementen x ($\exists$ n: $x^n = 0$) kann man bei der Darstellung von 1/y die unendliche Reihe durch eine endliche Summe ersetzen, wenn man weiß, dass $(1 - y)^n = 0$ ist? Formel!

Das allgemeinste Element in einem Ring R, das dem einer endlichen Menge G erzeugte Linksideal I angehört, hat die Form Summe aller r(g).g, wobei r eine Funktion von G --> R ist. Dies beruht auf dem Distributiv-Gesetz. Nehmen wir nun ein von G erzeugtes zweiseitiges Ideal J eines nicht kommutativen Rings. Kann man nun das allgemeinste Element von J wieder in der Form einer Summe der Länge von G schreiben? Glauben Sie, dass die Algebra-Lehrer der Zukunft bald ein Distributiv-Gesetz kennen, das a.m.b + c.m.d zu vereinfachen gestattet?

II-3 (freie Algebren, 4 Pkte)

Wie bildet man Elemente der freien Gruppe auf einem endlichen Alphabet > 1?

Wie invertiert man sie?

Wie multipliziert man sie?

Welche geometrische Form hat die freie Gruppe auf A (eigentlich ihr Caley-Graph: Kante - Multiplikation von rechts mit einem weiteren Symbol)?

Welche geometrische Form hat eine freie kommutative Gruppe auf A?

Welche Form ein freier kommutativer Monoid auf A?

Entfernt man auf der reellen Zahlengeraden unbeschränkt wachsende Teile, wie viele zusammenhängende Stücke bleiben im Limes übrig?

Entfernt man auf der euklidischen Ebene unbeschränkt wachsende Teile, wie viele zusammenhängende Stücke bleiben im Limes übrig?

[...] da kämen noch ein paar Fragen, ausgelassen wegen... naja kein Bock mehr *g*

II-5 (4 Pkte)

Wie sollte eine Transposition t auf einem vollen Zyklus z liegen damit beider gemeinsames Erzeugnis die gesamte Symmetrische Gruppe ist? Beweisen Sie, dass die diagonale Transposition (02) auf einem Viererzyklus (0123) für diesen Zweck nicht geeignet ist. Denn alles Erzeugte ist unter Konjugation mit ... invariant, Eigenschaft, die nicht allen Permutationen auf 4 zukommt [Frage: war des echt ne 4 oder hab ich mein t schlampig geschrieben? Hat des jemand auch abgeschrieben und kanns verifizieren/falsifizieren?]. Wie sieht man aber leicht, dass (02) auf (01234) günstig liegt?

(Hinweis: behalten Sie t, aber ersetzen Sie z!)

II-6 Unifikation höherer Ordnung (5 Pkte)

[Ned abgeschrieben da keinen Bock mehr]

II-7 Quantoren sparen, Isomorphie, elementare Äquivalenz, wechselseitige Einbettung bei Logik 1. Ordnung mit Gleichheit (5 Pkte)

[siehe II-6]

II-8 Informationstheorie (3 Pkte)

Ein Kaktus ist eine zusammenhängende einstellige Funktion, bei der die in den Zyklus mündenden Bäume höchstens Gebüsche der Höhe 1 sind, also Bouquets von Stacheln. Auf einer endlichen Menge X, wie lang muss der Zyklus mindestens sein, damit der Kaktus moch starr, d.h. seine Symmetriegruppe die 1, werden kann?

III-1

Wie viele Vergleiche auf Bitebene benötigt man beim Vergleich von Bitvektoren der Länge n in der lexikographischen Ordnung

1. im worst case (über alle Paare von Bitvektoren der Länge n)? (1 Pkt)
2. im Mittel (Gleichverteilung über alle Paare von Bitvektoren der Länge n)? (2 Pkte)

III-2 (3 Pkte)

Wie verhalten sich die Lösungen, angegeben in der Landau-Θ-Notation, für folgende divide and conquer-Rekursionen (wobei unterstellt werden kann, dass die Argumente Potenzen von 2 sind, die Rekursionsgleichung für n > 1 gilt und Anfangswert T(1) > 0 ist; c > 0 ist eine Konstante).

1. $T(n) = T(n/2) + c \log_2 n$
2. $T(n) = 2\ T(n/2) + c\ n$
3. $T(n) = 7\ T(n/2) + c\ n^2$

III-3

1. Welche Bedingungen müssen die ganzen Zahlen a und b erfüllen, damit das System von zwei Kongruenzen
   (*) $x \equiv a \bmod 24$, $x \equiv b \bmod 18$
   ganzzahlig lösbar ist? (1 Pkt)
2. Berechnen Sie für a=11 und b=5 die größte negative Zahl $x \in Z$, die Lösung von (*) ist. (3 Pkte)

III-4

Nachrichten, die mittels Zahlen $m \in N_{2003}$ numerisch kodiert wurden, können mittels

$x \dashrightarrow x^{17} \bmod 2003$

verschlüsselt werden. (NB: 2003 ist Primzahl)

1. Welches ist der Exponent d für die zugehörige Entschlüsselungsabbildung
   $x \dashrightarrow x^d \bmod 2003$ (2 Pkte)
2. wie viele Multiplikationen in Z_{2003} benötigt man für eine solche Entschlüsselung? (2 Pkte)

Für beide Lösungen muss ein Rechenweg bzw. eine Begründung angegeben werden.

III-5

1. Eine Quelle mit Alphabet A = {a,b,c,d,e,f,g,h} erzeugt Symbole mit den Wahrscheinlichkeiten:

p_a	p_b	p_c	p_d	p_e	p_f	p_g	p_h
0,5	0,2	0,1	0,05	0,05	0,05	0,03	0,02

   Konstruieren Sie einen optimalen binären Präfix-Code für die Quelle und berechnen Sie die mittlere Codewortlänge. Es genügt, die Codierung ohne Herleitung in geeigneter Form (z.B. Liste, Binärbaum) anzugeben (3 Pkte)
2. Sei A = {a,b,c,d} das Alphabet einer Quelle und seien die Wahrschienlichkeiten der Symbole gegeben durch

p_a	p_b	p_c	p_d
p^2	$p\,(1 - p)$	$p\,(1 - p)$	$(1 - p)^2$

   mit $1/2 \leq p < 1$. In welchem Bereich für p führt die optimale binäre Huffman-Codierung auf eine Codierung mit Wortlängen (1,2,3,3)? (3 Pkte)

III-6

heapsort macht Gebrauch vom Algorithmus createheap, der ein Feld A[1 ... n] der Länge n von ganzen Zahlen in einen heap B[1 ... n] transformiert, der die gleichen Zahlen enthält.

1. Welcher Eigenschaft müssen die Elemente eines Feldes A[1 ... n] genügen, damit dieses Feld einen heap repräsentiert? (2 Pkte)
2. Führen Sie createheap an folgenden Beispiel durch:
   A =

3	1	5	4	7	2	6	8	9

   B =

   (Es ist nur das Resultat anzugeben) (2 Pkte)
3. Eine Analyse von createheap zeigt, dass die Anzahl $V_{create}(n)$ der Vergleichsoperationen für diese Transformation bei Feldlänge n durch

   $(\tau)\ V_{create}(n) \leq 2 \sum^{n}_{i=1} (\lfloor \log_2 n \rfloor - \lfloor \log_2 i \rfloor)$

   beschränkt ist. Geben Sie eine Beschreibung von createheap ab (pseudocode oder hinreichend präzise verbalisiert) und leiten Sie daraus die Beschränkung (τ) ab (4 Pkte)
4. Zeigen Sie, wie aus (τ) die Komplexitätsaussage $V_{create}(n) \in O(n)$ folgt. (2 Pkte)

Marcus Schmid
Last modified: Thu Sep 18 00:23:13 CEST 2003