Klausur

Theoretische Informatik

14.09.2004

Prüfer: Prof. Dr. Horst Müller, Prof. Dr. Herbert Stoyan, Prof. Dr. Volker Strehl

Punktevergabe:

I-1: 6 Punkte
I-2: 5 Punkte
I-3: 4 Punkte
I-4: 6 Punkte
I-5: 9 Punkte
II-1: 8 Punkte
II-2: 8 Punkte
II-3: 5 Punkte
II-4: 3 Punkte
II-5: 6 Punkte
III-1: 5 Punkte
III-2: 8 Punkte
III-3: 10 Punkte
III-4: 7 Punkte

I-1 (6 Punkte) Teilbarkeit in $\mathbb{Z}$

Gegeben sei die Folge der Dezimalzahlen $z_k = 10^k + 4 * 10^{k-1} + 4$

1. Zeigen Sie mittels Induktion, dass jedes z_k für $k \geq 2$ durch 36 teilbar ist.
2. Zeigen Sie die Teilbarkeit aus 1. durch Anwendung von Teilbarkeitsregeln. Formulieren Sie jeder der von ihnen benutzten Regel.

I-2 (5 Punkte) Matrix-Potenzen

Gegeben sei die Matrix $A := \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

Zeigen Sie: Notwendig und hinreichen für $A^n = E$ ist die Bedingung 4 | n. Dabei ist $E := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ die Einheitsmatrix. (Hinweis: Zum Nachweis der Notwendigkeit der Bedingung teilen Sie n durch 4 mit Rest: n = 4 * q + r)

I-3 (4 Punkte) Partielle Ordnung

1. Definieren Sie den Begriff der partiellen Ordnung.
2. Zeigen Sie: Die Menge $\mathbb{N}$ der natürlichen Zahlen ist bzgl. Teilbarkeit partiell geordnet.
3. T(n) bezeichne die Menge der Teiler der natürlichen Zahl **n**, mit der Teilbarkeit als partielle Ordnung. Geben Sie eine Teilmenge U von T(24) an, die kein kleinstes Element hat. Geben Sie die minimalen Elemente der von Ihnen gewählten Menge U an.

I-4 (6 Punkte) Markov-Algorithmus

1. Entwerfen Sie einen Markov-Algorithmus, dessen Wirkung f darin besteht, von einem nicht-leeren Wort $w \in \{0,1\}^*$ das letzte (am rechten Ende stehende) Zeichen zu entfernen, also z.B. $w = 01001 \rightarrow f(w) = 0100$

2. Modifizieren Sie den Algorithmusaus 1. so, dass auch noch gilt: $f(\varepsilon) = \varepsilon$

I-5 (9 Punkte) Logik

1. Eine Funktion kann spezifiziert werden, indem man ihre Input-/Output- Beziehung beschreibt. Das kann geschehen, wenn man ein Paar „(Formel1, Formel2)“ von zwei (prädikaten) logischen Formeln notiert, von denen die erste die Bedingung für die Argumentwerte und die zweite die Werte der Funktion beschreibt. Spezifizieren Sie die Quadratwurzel **sqrt**!
2. Prüfen Sie die Widerlegbarkeit der Formel $(((a \vee b) \rightarrow \neg a) \wedge ((c \vee d) \rightarrow c))$!
3. Modelle einer Formel(-menge) können geordnet werden, wenn man zunächst die Universen (Grundmengen) und dann die Funktionen(-mengen) und Relationen(-mengen) miteinander vergleicht. Ist die Relation eine Halbordnung oder eine Totalordnung? (Warum?) Definieren Sie zwei Modelle für die Formel $\forall x \exists y.(P(x, y, a) \rightarrow P(x, b, a))$, wobei das erste das zweite umfassen soll!

II-1 (8 Punkte)

Es sei $\Sigma=\{a,b\}$. Ein Wort **u** heißt bekanntlich Faktor eines Wortes **w**, wenn **w=xuy** gilt für gewisse Wörter $x,y\in\Sigma^*$.

Geben sie einen minimal vollständigen, deterministischen Automaten **U** an, der die Menge aller derjenigen Wörter Σ^* erkennt, in denen der Faktor **aba** vorkommt.

Konstruieren Sie einen Automaten **B**, der die Menge aller derjenigen Wörter in Σ^* erkennt, in denen der Faktor **aba** nicht vorkommt und geben sie dann einen regulären Ausdruck für die Sprache **L(B)** an.

II-2 (8 Punkte)

Gegeben sei die Grammatik G durch $S \to \varepsilon \mid aSbS$

Zeigen Sie:

a) Für jedes $n \in \mathbb{N}$ gilt $a^n b^n \in L(G)$

b) Für alle $n, m \in \mathbb{N}$ mit $n \neq m$ gilt $a^n b^m \notin L(G)$

c) Wenn $u, v \in L(G)$ sind, dann ist auch $uv \in L(G)$

d) L(G) ist nicht regulär

II-3 (5 Punkte)

Abgeschlossen (+) oder nicht (-)?
$(\cap$ *Durchschnitt* $, \cup$ *Vereinigung* $, \setminus$ *Mengendifferenz* $, \cdot$ *Mengenprodukt* $, * -$ *Operator*$)$

Typen	***Operationen***				
	$\cap$	$\cup$	$\setminus$	$\cdot$	$*$
Typ 3					
Typ 2					
Typ 1					
Typ 0					

II-4 (3 Punkte)

Es sei $F: \mathbb{N} x \mathbb{N} \to \mathbb{N}$ die partielle Funktion

$$F:(x,y) \to \left\{ \begin{matrix} 1 \; falls \; x \le y \\ undef. \; sonst \end{matrix} \right\}$$

und $G(x,y) := F(x,y) - 1$. Geben Sie die Funktion μG an (Minimalisierung nach der letzten Komponente. Es ist nicht nach der Definition gefragt!)

II-5 (6 Punkte)

Es sei f eine einstellige primitiv rekursive Funktion. Geben Sie zwei primitiv rekursive Funktionen g und h an, so dass die Funktion $F(x,y): f^y(x)$ (y-fache Anwendung von f auf x) durch primitive Rekursion aus g und h hervorgeht.

III-1 (1+2+2 = 5 Punkte)

Die Funktion $merge_{m,n}$ erhält als Eingabe zwei sortierte Listen $a=[a_1, a_2, \ldots, a_m]$ und $b=[b_1, b_2, \ldots, b_m]$ der Längen m und n von Elementen aus einer totalgeordneten Menge und liefert als Resultat die sortierte Liste der in a und b vorkommenden Elemente. (Der Einfachheit halber sollen diese m+n Elemente paarweise verschieden sein).

a) Wieviele Blätter muss jeder Entscheidungsbaum mindestens haben, der einen Algorithmus für $merge_{m,n}$ auf der Basis von paarweisen Vergleichsoperationen realisiert?

b) Betracten Sie speziell den Fall m=n: wie verhält sich diese Anzahl der Blätter aus a) in Abhängigkeit von der Listenlänge n asymptotisch für $n \to \infty$?

c) Welche Folgerungen ergeben sich aus der asymptotischen Anzahlaussage in b) für die Vergleichs-Komplexität von merge-Algorithmen?

III-2 (1+5+2 = 8 Punkte)

Es bezeichne B^n die Menge der Bitstrings der Länge n. Für p mit $0 \le p \le 1$ bezeichne $bin_p^{(n)}$ die Binomialverteilung zum Parameter p auf B^n, d.h jeder Bitstring $w \in B^n$ erhält die Wahrscheinlichkeit $bin_p^{(n)}(w) = p^{\|w\|}(1-p)^{n-\|w\|}$, wobei $\|w\| = \#_1(w)$ das HAMMING-Gewicht von w bezeichnet. Diese Daten definieren die Quellen $Q_p^{(n)} = (B^n, bin_p^{(n)})$.

$H(x, 1-x) = -x \cdot \log_2(x) - (1-x) \cdot \log_2(1-x)$ bezeichne die bekannte Entropiefunktion.

a) Wie drückt sich die Entropie $H_p^{(n)}$ der Quelle $Q_p^{(n)}$ mittels der Entropiefunktion $H(x, 1-x)$ aus?

b) Berechnen Sie für die Quelle $Q_{1/8}^{(3)}$ deren Entropie, sowie einen optimalen binären Präfixcode und bestimmen Sie dessen mittlere (erwartete) Wortlänge. (Hinweis: Verwenden sie $\log_2(7) = 2{,}8073...$, bei der Berechnung des Codes ist es bequemer, mit Häufigkeiten statt mit Wahrscheinlichkeiten zu rechnen)

c) Sei $\mu_p^{(n)}$ die mittlere (erwartete) Wortlänge eines optimalen Präfixcodes für die Quelle $Q_p^{(n)}$.

Zeigen Sie: $\lim_{n \to \infty} \frac{\mu_p^{(n)}}{n} = H(p, 1-p)$

III-3 (3+3+2+2 = 10 Punkte)

Die Zahl N = 1105 hat 1105 = 5 * 13 *17 als Primfaktorisierung. Gemäß dem chinesischen Restesatz ist daher der Ring $\mathbb{Z}_{1105}$ isomorph zu dem Ring $\mathbb{Z}_5 x \mathbb{Z}_{13} x \mathbb{Z}_{17}$, was man beim Verfahren der modularen Arithmetik ausnutzt.

a) Die Gleichung $X^2 = 1$ hat in $\mathbb{Z}_{1105}$ genau acht verschiedene Lösungen, nämlich alle diejenigen Elemente, deren Darstellung in $\mathbb{Z}_5 x\ \mathbb{Z}_{13} x\ \mathbb{Z}_1$ von der Form $(\pm 1, \pm 1, \pm 1)$ ist. Dabei gelten nach chinesischem Restesatz die Entsprechungen

$$\mathbb{Z}_{1105} \ni 1 \Leftrightarrow (+1,+1,+1) \in \mathbb{Z}_5 x \mathbb{Z}_{13} x \mathbb{Z}_{17}$$

$$\mathbb{Z}_{1105} \ni -1 = 1104 \Leftrightarrow (-1,-1,-1) = (4,12,16) \in \mathbb{Z}_5 x \mathbb{Z}_{13} x \mathbb{Z}_{17}$$

Welchem Element von $\mathbb{Z}_{1105}$ entspricht $(+1,+1,-1) \in \mathbb{Z}_5 x \mathbb{Z}_{13} x \mathbb{Z}_{17}$?

b) Berechnen Sie die Ordnungen des Elements a=2 in $\mathbb{Z}_5^*$, in $\mathbb{Z}_{13}^*$ und in $\mathbb{Z}_{17}^*$

c) Verwenden Sie die Resultate von b), um das dem Element $2^{69} \, mod \, 1105$ von $\mathbb{Z}_{1105}$ entsprechende Element von $\mathbb{Z}_5 x \mathbb{Z}_{13} x \mathbb{Z}_{17}$ zu berechnen!

d) Zeigen Sie, dass a=2 ein MILLER-RABIN-Zeuge dafür ist, dass N=1105 keine Primzahl ist (Hinweis: es ist N-1 = 1104 = 14*69)

III-4 (7 Punkte)

Stellen Sie KARATSUBAs Idee zur schnelleren (als der „klassischen“) Multiplikation von natürlichen Zahlen bzw. Polynomen dar. Zeigen Sie, wie man eine Aufwandsabschätzung für die Anzahl der Ziffern bzw. Koeffizientenoperationen in Form einer Rekursionsgleichung erhält und geben Sie die asymptotische Form der Lösung an. (Hinweis: es genügt, wenn sie eine der beiden Versionen darstellen, also die Multiplikation oder die Multiplikation von Polynomen)