Diplom-Vorprüfung Frühjahr 2003

Klausur im Prüfungsfach

EINFÜHRUNG IN DIE THEORETISCHE INFORMATIK

04.04.2003

Prüfer: Prof. Dr. Klaus Leeb, Prof. Dr. Horst Müller, Prof. Dr. Volker Strehl

GeTEXte Version des Originals

nach bestem Wissen und Gewissen vom Arnie
und völlig ohne Gewähr

Name, Vorname, Geburtsdatum:

.....

.....

Studienfach, Matrikelnummer:

.....

Gesamtzahl der gehefteten Blätter: 18

Gesamtzahl der abgegebenen Blätter:

Nicht von der geprüften Person auszufüllen!

Erreichbare Punktzahl:	90
Erreichte Punktzahl:	
Note:	

Organisatorische Hinweise

BITTE SORGFÄLTIG DURCHLESEN UND KENNTNISNAHME DURCH UNTERSCHRIFT (S.U.) BESTÄTIGEN!

1. Bitte legen Sie Studentenausweis, Lichtbildausweis und Zulassungsbescheid bereit.

2. Als Hilfsmittel sind nur Schreibmaterialien zugelassen.

3. Schmierpapier wird nicht abgegeben und nicht korrigiert.

4. Sie können bei der Aufsicht zusätzliche Bearbeitungsblätter anfordern. Diese müssen Ihrer Arbeit angeheftet und bei der Geasmtzahl der abgegebenen Blätter mitgezählt werden.

5. Unleserliches wird nicht bewertet.

ERKLÄRUNG

1. Im Falle einer während der Prüfung auftretenden Prüfungsunfähigkeit zeige ich dies sofort der Aufsicht an und befolge deren Anweisungen. Ich weiß, daß ich die volle Beweislast trage. Ich lasse mir das Formular des Prüfungsamtes, das für diese Fälle vorgesehen ist, aushändigen und verfahre nach den dort niedergelegten Richtlinien.

2. Ich weiß, daß im Falle des Täuschungsversuchs oder der Benutzung unerlaubter Hilfsmittel („Unterschleif") der Prüfungsausschuss die Entscheidung treffen kann, die betroffene Prüfungsleistung als mit „nicht ausreichend" bewertet gelten zu lassen.

3. Ich habe die obigen organisatorischen Hinweise zur Kenntnis genommen.

Erlangen, den 02.04.2003 .....
(Unterschrift)

EINWILLIGUNG

(nur bei Zustimmung zu Unterschreiben)

Ich bin damit einverstanden, daß mein vorläufiges Ergebnis anonymisiert, jedoch unter Angabe der Matrikelnummer, am schwarzen Brett des Lehrstuhl Informatik 1 veröffentlicht wird. Die Bekanntgabe des vorläufigen Ergebnisses begründet keinen Rechtsanspruch. Die Bekanntgabe des endgültigen Ergebnisses erfolgt ausschließlich durch das Prüfungsamt.

Erlangen, den 02.04.2003 .....
(Unterschrift)

Aufgabe I-1. **(2 Punkte)** Beweisen oder widerlegen Sie (für beliebige Sprachen L_1, L_2):

- $(L_1\ L_2)^* = (L_1^*)(L_2^*)$

Aufgabe I-2. **(4 Punkte)** Konstruieren Sie einen deterministischen erkennenden Automaten, der die Sprache L(a(ba)*b) akzeptiert.

Aufgabe I-3. **(7 Punkte)** Man beweise folgende Variante des Pump-Lemmas für reguläre Sprachen:

- Zu jeder regulären Sprache L über Σ gibt es eine Pumpzahl $p \in \mathbb{N}$ mit

  $\forall x \in \Sigma^* : \forall y \in \Sigma^* : \forall z \in \Sigma^*$
  $(xyz \in L \wedge |y| \geq p \rightarrow \exists u, v, w, \in \Sigma^* : (y = uvw \wedge |v| > 0 \wedge |uv| \leq p \wedge \forall i \in \mathbb{N}: xuv^iwz \in L))$

Aufgabe I-4. **(7 Punkte)** Skizzieren Sie eine Turing-Maschine, die die Vorgänger-Funktion (für Zahlen in Binärdarstellung) berechnet, d.h. aus einer Anfangskonfiguration " s bin(x) b " soll für x $>$ 0 eine Endkonfiguration der Form " b^i e bin(x - 1) b^j " erreicht werden (b: Blank-Sambol; s: Startzustand; e: Endzustand; i, j, x $\in \mathbb{N}$).

Wie verhält sich Ihre Maschine für x = 0 ?

Aufgabe I-5. **(10 Punkte)** Σ sei ein endlicher Zeichenvorrat. Ist die Sprache aller Doppelwörter ww mit $w \in \Sigma^*$ (Begründungen!)

a) mit einer Turingmaschine akzeptierbar?

b) kontextsensitiv ?

c) regulär?

II, Leeb (Wo Sie für Antworten und Figuren mehr Platz brauchen, benützen Sie bitte die linke Seite, Zutreffendes bitte unterstreichen, *Nichtzutreffendes bitte schräg durchstreichen*! Die Fragen sind im Text durch fettdruck hervorgehoben.)

Aufgabe II-1: Funktionale Vollständigkeit, 2-wertige Clones (4 Punkte)

Die linearen booleschen Funktionen sind aufgebaut aus Variablen, XOR und 1. Kommt die 1 (als Summand, nicht als Koeffizient) genau einmal vor, so spricht man von einer inhomogenen, auch echt affinen (Abkürzung A), Funktion. Homogene (Abkürzung H) lineare Funktionen sind reine XOR-Summen aus (lauter verschiedenen, denn yXORy = 0) Variablen.

Eine andere Unterteilung der linearen Funktionen ist die nach der Parität der Anzahl der Variablen. Schreiben wir E für even (=gerade) und O für odd (=ungerade).

Beschreiben Sie, wie sich die Klassen A, H, bzw. E, O kombinieren, wenn man eine lineare Funktion für eine Variable in einer anderen linearen Funktion substituiert! **Tragen Sie** die Werte in die bereits viel aussagende Tafel **ein**:

A.A = H.H = , A.H = H.A = ; E.E = O.O = , E.O = O.E =

Welche der Klassen A, H, bzw. E, O ist dann unter Substitution abgeschlossen (ein Clone)?

Wieso kann man NAND nicht aus XOR und NOT zusammenstöpseln?

Aufgabe II-2: Limites in Kategorien, Unifikation (5 Punkte)

Welches der Limeskonstrukte für Diagramme: Produkt, Summe, Differenzkern, Differenzcokern müssen Sie verwenden, um die Menge der Fixpunkte einer einstelligen Funktion zu beschreiben? **Zeichnen Sie** das Diagramm, dessen Limes (oberer **oder** unterer?) Sie hierzu bilden!

Nun beantworten Sie **dieselben** Fragen für "Menge der Zusammenhangskomponenten einer einstelligen Funktion"!

In welcher Ihnen bekannten gleichungsdefinierten Klasse von Gruppen ist garantiert jede Untergruppe auch schon Normalteiler?

Die Identität namens Assoziativität ist eine Gleichung zwischen zwei Termen (Bäumen) mit drei Variablen (Blättern). (Das Operationssymbol ist zweistellig.) Es gibt genau fünf Bäume, die sich durch einmalige Anwendung der Assoziativität ergeben. **Zeichnen Sie alle** Verbindungskanten zwischen diesen fünf Bäumen, die sich durch einmalige Anwendung der Assoziativität ergeben.

Welche Form hat dieser Verbindungsgraph (Stern, Pfad, Ring)?

f sei eine zweistellige Funktionskonstante, x und y Individuenvariablen, G eine zweistellige Funktionsvariable. **Welche Gestalt** der Lösungsbäume G wird durch die Unifikationsgleichung G(f(x,y), f(x,y)) = f(G(x,y), G(x,y)) erzwungen?

Aufgabe II-3: Erzeugung von Untergruppen, "Gittern" (5 Punkte)

Der Springer hat als zulässige Schritte alle acht Vektoren der Länge, des Radius, SQRT(5) im Gitter $(\mathbb{Z} \times \mathbb{Z}, +)$. **Geben Sie** drei Schritte an, die den Einheitsvektor (1,0) aufbauen. Finden Sie die Radiusquadrate für alle in zwei Schritten erreichbaren Punkte. Am schnellsten gewinnen Sie eine vollständige Übersicht, indem Sie den Kreis der acht (minus eins) zweiten Schritte ab dem Ziel (2,1) eines ersten Schritts verfolgen. Von (0,0) aus gemessen ergeben sich die Radiusquadrate (**Liste vervollständigen!**): 20, 18, , , , , 0.

Verallgemeinern wir nun den Springer, indem wir für seinen Schritt einen anderen Radius wählen. Hier ist eine Liste von Datensätzen bestehend aus je einem Vektor, davor dem zugehörigen Radiusquadrat und dahinter der zughörigen Gitterdeterminante (= Fläche der Gittermasche = Index der erzeugten Untergruppe von $\mathbb{Z} \times \mathbb{Z}$): 1(1,0)1, 2(1,1)2, 4(2,0)4, 5(2,1)1, 8(2,2)8, 9(3,0)9, 10(3,1)2, 13(3,2)1, 16(4,0)16, 17(4,1)1, 18(3,3)18, 20(4,2)4, 25(4,3)1. Da (3,4,5) das erste Pythagoräische Tripel ist, 9 + 16 = 25, gibt es hier das erstemal 12 ganzzahlige Punkte auf dem Kreis.

Beweisen Sie, daß für jedes k der ($2k$ + 1,1)-Springer so wie der (1,1)-Bischof des üblichen Schachspiels Gitterdeterminante 2 hat, d.h. so wie er in genau zwei Farben auftritt. **Beweisen Sie**, daß der ($2k$,1)-Springer überallhin gelangt; **in wieviel** Schritten zum Einheitsvektor? (Beachten Sie die achtfache Symmetrie durch Vorzeichenwechsel an jeder der beiden Komponenten und durch deren Vertauschen!)

Aufgabe II-4: Sortiernetzwerk (5 Punkte)

Wenn man als Generatoren der symmetrischen Gruppe auf n = {0, 1, 2, ... , n - 1} die Transpositionen (i, i+1) nimmt, so ist die teuerste Permutation, d.i. die, welche die meisten Faktoren erfordert, die Spiegelung (0, n - 1) · (1, n - 2) · (1, n - 3) · ... . Sie kostet genau nüber2 Faktoren. Diese kann man als eine Abfolge von immer kürzer werdenden Doppeltreppen um die Mitte herum anordnen. Für n = 5 ergeben sich die 10 Faktoren (01)(12)(23)(34)(23)(12)(01)(12)(23)(12).

Diese Folge von Transpositionen können Sie auch als Sortiernetzwerk betrachten. **Verfolgen Sie, wie** die Anordnung 41032 durch dieses Netzwerk rückgeordnet wird, **und welche** der Faktoren (durchnumeriert als 0, 1, 2, 3, ... , 9) dabei aktiv werden.

An welchem Charakteristikum der Anordnung 41032 hätten Sie die Zahl der erforderlichen Faktoren auch ablesen können?

Aufgabe II-5: Logik, Quantoren, Ordnungen (4 Punkte)

Aus der Mathematik kennen Sie das Konzept der Nullfolge, also einer gegen Null strebenden Folge.

In der Logik ist es manchmal sinnvoll, die Komplexität einer Formel an der Anzahl der abwechselnden $\exists$ und $\forall$-Blöcke zu messen. **Finden Sie** also die **Quantorenblockstruktur** des Konzepts Nullfolge!

Zählt man bei den Ehrenfeucht-Fraïssé-Spielen auch **nur** die alternierenden **Blöcke oder jeden einzelnen** Quantor in Schachtelung? Die Quantorenstruktur für dicht(e Ordnung) ist z.B. $\forall\forall\exists$. Zählt das als 2 **oder** als 3?

Logik erster Ordnung in der Sprache der Arithmetik ist nicht imstande, die Struktur der natürlichen Zahlen bis auf Isomorphie zu beschreiben. Für abzählbar unendliche Modelle waren wir aber imstande, zumindest die Ordnungsstruktur bis auf Isomorphie zu beschreiben. Dabei half und der Satz von Cantor, der die natürliche Ordnung der rationalen Zahlen bis auf Isomorphie zu charakterisieren gestattet:

Die positiven ganzen Zahlen sind unter Teilbarkeit wie geordnet: linear, partiell aber nicht linear, oder gar quasi aber nicht partiell? Noethersch? Wohl-partiell?

Sei d(n) die Anzahl der Teiler von n. Was ist im Sinne der Analysis (Zahlen ergänzt um -Unendlich und +Unendlich) liminf d(n), während n nach unendlich strebt. Sei omega(n) die Anzahl der verschiedenen Primfaktoren in n. Was ist limsup omega(n), während n nach Unendlich strebt?

Was ist - auch ohne jegliches Hintergrundwissen - gegen folgende Definition vorzubringen: "Zahlen deren Teiler eine teilbare Zahl ist"? (Kurioserweise übersetzt "teilbar" loc. cit. nicht "composite".)

Aufgabe II-6: Syntax, Semantik (2 Punkte)

Welche programmsyntaktisch definierte Klasse von einstelligen Funktionen sind genau die Schließlich-modular-stückweise-affinen-Funktionen-mit-rationalen-Koeffizienten-und-ganzen-Werten? (Hilft Ihnen der Name Tsichritzis bzw. Periodizität im Abhängigkeitsdigraphen der Variablen?)

Ist eine solche Funktion zufällig eine Permutation, gehört dann ihre Inverse (als Permutation) auch wieder zur Klasse SmsaFmrKugW? Rechnen Sie nicht, sondern betrachten Sie lieber den Graphen einer solchen Permutation und dessen modulare Stücke! Wenn man die an der Hauptdiagonale spiegelt, dann ...

Aufgabe II-7: Informationstheorie (3 Punkte)

Die Symmetriegruppe einer Permutation besteht aus allen Permutationen, die gleichgroße Zyklen vertauschen und jeden Zyklus beliebig verdrehen dürfen. So hat also die Symmetriegruppe einer Permutation vom Zykeltyp 887775555 (die Pluszeichen haben wir nicht geschrieben) auf X = 57(=siebenundfünfzig) die Größe 2!.8.8.3!.7.7.7.4!.5.5..5.5..

Finden Sie für allgemeines X eine informationsreichste (entspricht kleinster Symmetriegruppe) Permutation, also ihren Zykeltyp! Wenige große Faktoren tragen weniger zum Produkt bei als viele kleine mit der gleichen Summe. Allerdings trägt ein Faktor 1 zum Produkt überhaupt nichts bei.

Aufgabe II-8: Bistabiles Analogspeicherelement (2 Punkte)

Zwei gleichgroße kreisrunde ebene Löcher kommunizieren über ein Rohr, in welches durch eine dritte Öffnung Luft eingeblasen werden kann. Auf jedem der beiden Löcher sitzt eine Seifenblase. Bekanntlich ist der Druck der Krümmung proportional, also invers zum Radius. Beschreiben Sie alle Gleichgewichtslagen - mit Angabe, ob stabil oder labil - der beiden Seifenblasen! Als Codebuchstaben für die verschiedenen für die verschiedenen Bereiche verwenden Sie l für large, h für Halbkugel, und s für small (ll bezeichne somit zwei Blasen gleicher Krümmung, die größer als die Halbkugel sind; hl, hs, lh und sh sind gewiß keine Gleichgewichtslagen, weil h den höchsten Druck hat). Jenseits welchen Gesamtvolumens (gemessen außerhalb der Löcher) gibt es Bistabilität, ein Flipflop? Scherzfrage an Studenten einer technischen Fakultät: Mißt man Oberflächenspannung in Volt mal Quadratzentimeter oder in Newton pro Meter?

Aufgabe III-1[1]

Geben Sie das asymptotische Verhalten der beiden folgenden Funktionen (in Abhängigkeit von den Argumenten $n \in \mathbb{N}$) in Θ-Notation an.

1. Harmonische Zahlen $H_n = 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}$

$H_n \in \Theta($ $)$

2. Binomialkoeffizienten $\binom{n}{k}$ (für festes $k \in \boldsymbol{N}$).

$\binom{n}{k} \in \Theta($ $)$

(2 P.)

Aufgabe III-2[1]

Geben Sie die Komplexität der folgenden Algorithmen in Θ-Notation an.

1. Anzahl der Vergleichoperationen von `Quickselect` in Abhängigkeit von der Listenlänge n bei deterministischer Pivot-Wahl

im worst-case $\in \Theta($ $)$ im average-case $\in \Theta($ $)$

2. Anzahl der Vergleichsoperationen von `Heapsort` in Abhängigkeit von der Listenlänge n

im worst-case $\in \Theta($ $)$ im average-case $\in \Theta($ $)$

(4 P.)

Aufgabe III-3[1]

Bestimmen Sie die Menge der Lösungen in $\boldsymbol{Z}$ der folgenden Kongruenzsysteme.

1. $\begin{cases} x \equiv 5 \bmod 9 \\ x \equiv 11 \bmod 15 \end{cases}$ Lösungsmenge:

2. $\begin{cases} x \equiv 8 \bmod 9 \\ x \equiv 4 \bmod 15 \end{cases}$ Lösungsmenge:

(4 P.)

1. Jeweils nur die Antwort in den Kasten eintragen; keine Begründung erforderlich!

Aufgabe III-4[2]

Zur Berechnung eines Problems stehen zwei Algorithmen $\mathcal{A}$ und $\mathcal{B}$ zur Verfügung. Für deren jeweilige Komplexität (= Laufzeit auf Instanzen der Grösse n) gelte

$$t_{\mathcal{A}}(n) = \sqrt{n} \quad \text{bzw.} \quad t_{\mathcal{B}}(n) = 2^{\sqrt{\log_2 n}}$$

1. Welcher der beiden Algorithmen ist asymptotisch besser (= schneller)?

2. Wo liegt der break-even-point, d.h. von welchem Wert der Instanzengrösse n an ist der asymptotisch bessere Algorithmus immer im Vorteil?

(2 P.)

2. Geben Sie den Lösungsweg mit an.

Aufgabe III-5

Ein Feld $A[1...2n]$ der Länge $2n$ mit Elementen aus einer totalgeordneten Menge heisst *n-sortiert*, wenn $A[k] \leq A[n+k]$ für $1 \leq k \leq n$ gilt.

Durch paralleles Sortieren

$$A[1...n] \mapsto B[1...n] \quad \text{und} \quad A[n+1...2n] \mapsto B[n+1...2n]$$

der Teilfelder $A[1...n]$ bzw. $A[n+1...2n]$ der Länge entsteht das Feld $B[1...2n]$.

1. Geben Sie für $n = 4$ ein konkretes Beispiel eines 4-sortierten Feldes $A[1...8]$ an, dessen Elemente die Zahlen 1, 2, ..., 8 in einer geeigneten Umordnung sind, so dass das durch paralleles entstehende Feld $B[1...8]$ nicht vollständig ist.

2. Zeigen Sie allgemein (für beliebiges n also), dass das Feld $B[1...2n]$ immer noch n-sortiert ist, falls dies für das ursprüngliche Feld $A[1...2n]$ galt.

3. Wieviele Inversionen kann $B[1...2n]$ im ungünstigsten Fall noch haben?

(4 P.)

Aufgabe III-6[3]

Für einen Teilnehmer an einem public-key RSA-Kryptosystem werden die Symbole, aus denen die Nachrichten zusammengesetzt sind, mittels der Zahlen $x \in \mathbb{Z}_{377}$ dargestellt, mittels der Abbildung $x \mapsto x^e \bmod 377$ verschlüsselt und mittels der Abbildung $x \mapsto x^d \bmod 377$ entschlüsselt.

Der öffentliche Schlüssel sei $e = 59$

Welches ist der private Schlüssel d ?

(4 P.)

Aufgabe III-7

Für einen binären Baum t bezeichne $e(t)$ die Anzahl seiner Blätter und $\bar{h}(t)$ deren mittlere Höhe. Erläutern Sie dieses Konzept der "mittleren Höhe" von Blättern in Binärbäumen und dessen Bedeutung, wobei Sie die verwendeten Begriffe sorgfältig definieren und auf folgende Fragen eingehen sollten:

a) Wie verhält sich $\bar{\mathrm{h}}(\mathrm{t})$ im Bezug auf den rekursiven Aufbau von Binärbäumen?

b) In welcher Beziehung stehen die beiden Grössen $e(t)$ und $\bar{h}(t)$ zueinander? Wie beweist man dies?

c) Welche Konsequenzen hat die Aussage in b) für die average-case-Komplexität von vergleichsbasierten Sortieralgorithmen?

(10 P.)

3. Geben Sie den Lösungsweg mit an.