Lehrstuhl für Informatik I
— Informationsstrukturen und
wissensbasierte Systeme —
Universität Würzburg

Prof. Dr. H. Noltemeier

Würzburg, 2. Juli 1998

Übungen zur Vorlesung
Praktische Informatik II (SS98)

6. Übungsblatt

Aufgabe 20: (Volle Persistenz)

Voll persistente Datenstrukturen werden z.B. im CIM-Bereich im Automobilbau benötigt, um auf die verschiedenen Ausstattungs-Versionen eines Fahrzeugtyps zuzugreifen und diese auch verändern zu können.

Ein Knoten der kurzlebigen Datenstruktur DS bestehe aus den Feldern

- B : Begriff
- A : Ausführungsoption
- P : Pointer

Ein Beispielknoten sei

- B = Sportgetriebe
- A = 5-Gang
- P = Pointer auf den nächsten Begriff

Die Knoten der kurzlebigen Datenstruktur bilden eine lineare Liste, beginnend mit dem Startknoten und endend mit dem (ersten) Knoten mit $P = nil$.

Bilden Sie mittels der „fat node"-Methode zu der folgenden Sequenz von Operationen eine Versionenliste VL und eine (voll) persistente Datenstruktur; hierbei ist die letzte Komponente jeweils der Zeitstempel der aufgerufenen Version; V_0 ist die „leere Startversion".

1. Generieren Sie einen Startknoten (Karosserie / grün / 0).
2. Führen Sie nacheinander folgende Operationen aus:
   (a) Insert(Sportgetriebe / 5-Gang, 1)
   (b) Insert(Klimaanlage / —, 2)
   (c) Insert(Sitzheizung / nur Fahrer, 3)
   (d) Insert(Fensterheber / mechanisch, 3)

(e) INSERT(Schiebedach / elektrisch, 1)
(f) UPDATE(Sitzheizung / beide Vordersitze, 4)
(g) UPDATE(Fensterheber / elektrisch, 6)
(h) INSERT(Alarmanlage / fernbedienbar, 7)
(i) DELETE(Sportgetriebe, 5)
(j) INSERT(Automatikgetriebe / 4-Gang, 10)
(k) ACCESS(Klimaanlage, 9)
(l) ACCESS(Sitzheizung, 7)
(m) DELETE(Klimaanlage, 5)

(**4 Punkte**)

Aufgabe 21: (Optimale Serialisierung)

Gegeben seien Listen A_i ($i = 1, \dots, L$), die bereits alle monoton wachsend sortiert sind und zu einer sortierten Gesamtliste sortiert werden sollen. Die Anzahlen der Listenelemente seien jeweils $b_1, \dots, b_L$. Das „Zusammenfassen" gehe jeweils paarweise vor, z.B. das Mischen von A_i und A_k zu einer sortierten Liste A_{ik} kann in $b_i + b_k$ elementaren Operationen erfolgen. Die Reihenfolge der Misch-Operationen kann folglich durch einen binären Wurzelbaum repräsentiert werden, dessen Blätter genau die Listen $A_1, \dots, A_L$ repräsentieren und dessen Nicht-Blätter jeweils zwei Söhne aufweisen.

Wir wollen nun das folgende Problem betrachten:

In welcher Reihenfolge sollen die Paare von Listen A_i, A_k gewählt werden, so daß die Gesamtzahl aller elementaren Misch-Operationen so klein wie möglich wird?

(a) Beweisen Sie: Ist $T_{L,2}$ ein binärer Wurzelbaum der obigen Art mit L Blättern und sind die Blätterhöhen h_i ($i = 1, \dots, L$), so benötigt man insgesamt $\sum_{i=1}^{L} h_i \cdot b_i$ elementare Mischoperationen. (**2 Punkte**)

(b) Ein optimaler „Misch-Plan", repräsentiert durch ein $T_{opt} \in \mathbb{T}_{L,2}$ (Menge aller binären Bäume mit L Blättern) erfüllt daher mit $b := (b_1, \dots, b_L)$

$$\tilde{L}_{(T_{opt};b)} := \sum_{i=1}^{L} \tilde{h}_i \cdot b_i = \min_{T \in \mathbb{T}_{L,2}} \sum_{i=1}^{L} h_i \cdot b_i$$

wobei $\tilde{h}_i$ die Höhe von A_i in T_{opt} ist; oder gleichwertig:

$$\tilde{L}_{(T_{opt};b)}/B = \min_{T \in \mathbb{T}_{L,2}} \sum_{i=1}^{L} h_i \cdot b_i/B$$

(=minimaler Erwartungswert der Blätterhöhe in $\mathbb{T}_{L,2}$ zur Wahrscheinlichkeitsverteilung $P := (b_1/B, \dots, b_L/B)$ auf den Blättern mit $B := \sum_{i=1}^{L} b_i$)

Bestimmen Sie zu $L = 12$ und $b = (5, 3, 7, 9, 8, 4, 6, 8, 9, 5, 3, 6)$ einen optimalen Misch-Plan. (**3 Punkte**)

Aufgabe 22: (Suchprozesse, Wurzelbäume, Codes)

(a) Sei eine Menge S von 15 Münzen gegeben, die von 1 bis 15 numeriert sind. Genau eine der Münzen ist defekt, d.h. schwerer als die anderen Münzen. Eine Wiegung entspricht der Wahl von 2 disjunkten Teilmengen A und B von $\{1, \ldots, 15\}$ mit $|A| = |B|$, wobei A und B die Menge der Münzen aus der linken und rechten Waagschale bezeichnen. Wieviele Wägungen benötigt man bis man feststellt, welche der Münzen die defekte Münze ist? **(2 Punkte)**

(b) Sei aus der Menge S von 15 Münzen wieder genau eine defekt, wobei defekt nun bedeutet, daß diese Münze schwerer oder leichter ist als die restlichen. Wieviele Wägungen benötigt man, um die defekte Münze zu ermitteln? **(2 Punkte)**

(c) Aus der Menge S von 15 Münzen sind nun 2 Münzen defekt (beide schwerer als die restlichen Münzen). Zeigen Sie, daß man mit 5 Wägungen die 2 defekten Münzen ermitteln kann. Formulieren Sie ihre Lösung als Suchprozess und geben Sie einen Entscheidungsbaum für Ihren Algorithmus an. **(3 Punkte)**

(d) Gibt es einen binären Suchbaum, dessen Nicht-Blätter (innere Ecken) jeweils 2 Söhne haben und dessen 13 Blätter die Höhen 2, 2, 3, 3, 4, 4, 5, 5, 6, 6, 6, 6, 6 haben? Beweis! **(2 Sonderpunkte)**

Aufgabe 23: (Public Key Cryptosystem)

In der Vorlesung wurde die RSA-Methode als Beispiel für Falltürfunktionen angegeben. Jeder Benutzer T_l eines Kommunikationssystems wählt 2 verschiedene Primzahlen p_l und q_l mit $n_l = p_l \cdot q_l$ und $p_l, q_l > m$ und dazu eine Zahl e_l mit $3 < e_l < \lambda(n_l) := kgV\{(p_l - 1), (q_l - 1)\}$ und $ggT\{e_l, \lambda(n_l)\} = 1$. ($m$ ist dabei die größte Dezimalzahl, die in dem System zu übertragen ist.) Sein privater Schlüssel ist das Tupel (n_l, d_l). Dabei sei d_l eindeutig gegeben durch $e_l \cdot d_l \equiv 1 \mod \lambda(n_l)$.

Teilnehmer T_l teilt dem Systemverwalter den öffentlichen Schlüssel (n_l, e_l) mit. Eine Nachricht M von T_i nach T_j (mit $0 \leq M \leq m$) wird von Teilnehmer T_i gemäß $C := E(M) := M^{e_j} \mod n_j$ chiffriert. T_j decodiert $C = E(M)$ mittels $D(C) = D(M^{e_j} \mod n_j) := (M^{e_j})^{d_j} \mod n_j$.

(a) Zeigen Sie, daß nachfolgender Algorithmus $C = M^{e_j} \mod n_j$ korrekt berechnet und höchstens $2 \cdot \lceil \log_2 e_j \rceil$ Multiplikationen und $2 \cdot \lceil \log_2 e_j \rceil$ Divisionen benötigt.

(2 Punkte)

Algorithmus 1

Es sei $e^j_k e^j_{k-1} \dots e^j_0$ die Binärrepräsentation von e_j.
$C := 1$
for $i := k, k-1, \dots, 0$ **do**
  $C := C^2 \mod n_j$
  if $e^j_i = 1$ **then**
    $C := C \cdot M \mod n_j$

(b) Seien für den Adressaten T_2 die Parameter $p_2 = 47$, $q_2 = 59$, $n_2 = p_2 \cdot q_2 = 47 \cdot 59 = 2773$ und $e_2 = 17$ gegeben. Codieren Sie die folgende Message von T_1 an T_2

James$\sqcup$Bond$\sqcup$ist$\sqcup$da

zeichenweise per RSA-Chiffre zu den gegebenen Parametern. (Die Rechnung soll ersichtlich sein!) Codieren Sie dazu die Message zunächst über dem Alphabet $\{00, 01, \dots, 26\}$ mit $\sqcup \to 00, A \to 01, \dots, Z \to 26$.

(3 Punkte)

Abgabetermin: Die Bearbeitungen zu diesem Übungsblatt sind bis Montag, den 13. Juli 1998, bis 10^{00} Uhr in den dafür vorgesehenen Kästen vor der Teilbibliothek Mathematik/Informatik abzugeben.

Hinweis: Maximal zwei Teilnehmer dürfen ein Übungsblatt bearbeiten.