Info IV Tutorium

Letztes Tutorium

Thomas Pajor

ITEC Dillmann
ITEC Beyerer

24. Juli 2006

Wiederholung: Lower Bound Theorem (Satz A)

Betrachte das RAM–Modell:

- Operiert auf *reellen* Zahlen
- Arithmetische Grundoperationen: $+$, $-$, $\cdot$, $/$
- Zeiger / Indexoperationen
- Vergleiche: Test auf „$x > 0$?“

$\Rightarrow$ Darstellung eines Algorithmus durch *rationale* Funktionen!

$\rightsquigarrow$ Entscheidungsbaum

Wiederholung: Lower Bound Theorem (Satz A)

Theorem (Satz A)

Sei $f : W \to \mathbb{R}^n$ mit $W \subseteq \mathbb{R}^n$ eine Funktion und $A(X)$ ein Algorithmus, der f im RAM–Modell berechnet. Außerdem:

- $\varepsilon > 0$
- *q paarweise verschiedene Punkte $X_1, \ldots, X_q \in W$*
- *q paarweise verschiedene rationale Funktionen $Q_1, \ldots, Q_q$ mit $Q_i(X) = f(X)$ für alle $X \in U(X_i, \varepsilon) \subseteq W$*

Dann gilt, dass im schlechtesten Fall die Zahl R der Vergleiche zur Berechnung von $A(X)$ der Ungleichung

$$R \geq \log_2 q$$

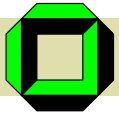
genügt.

Wiederholung: Aufgabe 1.

- Eve hört eine RSA–verschlüsselte Nachricht ab, die sie entschlüsseln möchte

Wiederholung: Aufgabe 1.

- Eve hört eine RSA–verschlüsselte Nachricht ab, die sie entschlüsseln möchte
- Dazu muss sie eine große Zahl N faktorisieren



Wiederholung: Aufgabe 1.

- Eve hört eine RSA–verschlüsselte Nachricht ab, die sie entschlüsseln möchte
- Dazu muss sie eine große Zahl N faktorisieren
- Sie weiß: $N = p \cdot q$ für zwei Primzahlen p und q zwischen 2 und 2^{1024}

Wiederholung: Aufgabe 1.

- Eve hört eine RSA–verschlüsselte Nachricht ab, die sie entschlüsseln möchte
- Dazu muss sie eine große Zahl N faktorisieren
- Sie weiß: $N = p \cdot q$ für zwei Primzahlen p und q zwischen 2 und 2^{1024}
- Eve entwirft einen Algorithmus der eine reelle Zahl $2 \leq N \leq 2^{2048}$ als Eingabe hat, und den kleinsten Primteiler von $\lfloor N \rfloor$ ausgibt.

Wiederholung: Aufgabe 1.

Aufgabe 1.

Bestimmen Sie eine (möglichst gute) untere Schranke für Eve's Algorithmus im worst–case.

Hinweis: Für jedes $n \in \mathbb{N}$ gilt, dass es $\Theta(\frac{n}{\ln(n)})$ Primzahlen p mit $p \leq n$ gibt.

Wiederholung: Hashing

- Ist G die Grundmenge aller Eingaben, so möchten wir G auf eine kleinere Menge I abbilden (i.d.R. $I := \{0, \ldots, n-1\}$)

Wiederholung: Hashing

- Ist G die Grundmenge aller Eingaben, so möchten wir G auf eine kleinere Menge I abbilden (i.d.R. $I := \{0, \ldots, n-1\}$)
- Abbildung $h : G \to I$ mit $I \ll G$ heißt *Hashfunktion* (i.A. nicht injektiv!)

Wiederholung: Hashing

- Ist G die Grundmenge aller Eingaben, so möchten wir G auf eine kleinere Menge I abbilden (i.d.R. $I := \{0, \ldots, n-1\}$)
- Abbildung $h : G \to I$ mit $I \ll G$ heißt *Hashfunktion* (i.A. nicht injektiv!)
- $x, y \in G$, $x \neq y$ mit $h(x) = h(y)$ heißt *Kollision* ($\rightsquigarrow$ Methoden zur Kollisionsauflösung)

Wiederholung: Hashing

- Ist G die Grundmenge aller Eingaben, so möchten wir G auf eine kleinere Menge I abbilden (i.d.R. $I := \{0, \ldots, n-1\}$)
- Abbildung $h : G \to I$ mit $I \ll G$ heißt *Hashfunktion* (i.A. nicht injektiv!)
- $x, y \in G$, $x \neq y$ mit $h(x) = h(y)$ heißt *Kollision* ($\rightsquigarrow$ Methoden zur Kollisionsauflösung)
- Eigenschaften guter Hashfunktionen
  - Surjektivität (keine großen „Lücken“)
  - Gute Gleichverteilung
  - Betrachte nach Möglichkeit die komplette Eingabe
  - Regelmäßige Muster in der Eingabe sollen trotzdem zu guter Streuung führen

Wiederholung: Aufgabe 2.

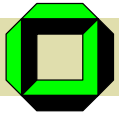
Aufgabe 2.

Gegeben sei ein Zellraster mit n Zellen sowie natürliche Zahlen k, n mit $n > 3$ und $k < n$.

(a) Wie viele Möglichkeiten gibt es für k Schlüssel, durch Hashing in die n Zellen einsortiert zu werden?

(b) Wie viele Möglichkeiten gibt es noch, wenn man nur kollisionsfreie Hashfunktionen betrachtet?

(c) Wie hoch ist die Wahrscheinlichkeit, dass beim gleichverteilten Hashing von $k = n$ Schlüsseln in die n Zellen die dritte Zelle leer bleibt?



Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt.

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0.

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus.

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus. ✓

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus. ✓
- Ein Quader ist in jedem Raum eine rationale Dünnmenge.

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus. ✓
- Ein Quader ist in jedem Raum eine rationale Dünnmenge. X

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus. ✓
- Ein Quader ist in jedem Raum eine rationale Dünnmenge. X
- Bei einem symmetrischen Kanal ist das Eingabealphabet stets gleich dem Ausgabealphabet.

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus. ✓
- Ein Quader ist in jedem Raum eine rationale Dünnmenge. X
- Bei einem symmetrischen Kanal ist das Eingabealphabet stets gleich dem Ausgabealphabet. X

Wiederholung: Wahr / Falsch?

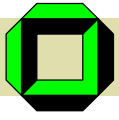
- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus. ✓
- Ein Quader ist in jedem Raum eine rationale Dünnmenge. X
- Bei einem symmetrischen Kanal ist das Eingabealphabet stets gleich dem Ausgabealphabet. X
- Bei der Übertragung von LZW kodierten Daten braucht das Wörterbuch oft den meisten Platz.

Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus. ✓
- Ein Quader ist in jedem Raum eine rationale Dünnmenge. X
- Bei einem symmetrischen Kanal ist das Eingabealphabet stets gleich dem Ausgabealphabet. X
- Bei der Übertragung von LZW kodierten Daten braucht das Wörterbuch oft den meisten Platz. X

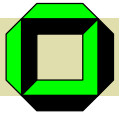
Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus. ✓
- Ein Quader ist in jedem Raum eine rationale Dünnmenge. X
- Bei einem symmetrischen Kanal ist das Eingabealphabet stets gleich dem Ausgabealphabet. X
- Bei der Übertragung von LZW kodierten Daten braucht das Wörterbuch oft den meisten Platz. X
- Sei $\Omega(f(n))$ eine bekannte, bewiesene untere Schranke für ein Problem A. Kann man ein Problem B mit vernachlässigbarem Aufwand auf das Problem A reduzieren, so hat man bewiesen, dass $\Omega(f(n))$ auch eine untere Schranke für das Problem B ist.



Wiederholung: Wahr / Falsch?

- Ein Huffmancode zu einer bestimmten WV ist immer eindeutig bestimmt. X
- Bei einem B–Baum beträgt der Höhenunterschied zwischen zwei Blättern immer 0. ✓
- Für die Berechnung der booleschen Funktion $f(x, y) = x \Leftrightarrow y$ durch ein neuronales Netz reicht ein Neuron nicht aus. ✓
- Ein Quader ist in jedem Raum eine rationale Dünnmenge. X
- Bei einem symmetrischen Kanal ist das Eingabealphabet stets gleich dem Ausgabealphabet. X
- Bei der Übertragung von LZW kodierten Daten braucht das Wörterbuch oft den meisten Platz. X
- Sei $\Omega(f(n))$ eine bekannte, bewiesene untere Schranke für ein Problem A. Kann man ein Problem B mit vernachlässigbarem Aufwand auf das Problem A reduzieren, so hat man bewiesen, dass $\Omega(f(n))$ auch eine untere Schranke für das Problem B ist. X



Das war's

Alles Gute für die Klausur!