Karlsruher Institut für Technologie
Institut für Theoretische Informatik

Prof. Dr. Dennis Hofheinz
Lukas Barth, Lisa Kohl

4. Übungsblatt zu Algorithmen I im SoSe 2016

https://crypto.iti.kit.edu/index.php?id=algo-sose16
{lisa.kohl,lukas.barth}@kit.edu

Aufgabe 1 (*Doktor Meta und Wahrscheinlichkeiten,* 5 *Punkte*)

Der ebenso geniale wie einfallsreiche Wissenschaftler und Superbösewicht Doktor Meta ist geschäftig. Da er sich auf seine menschlichen Gehilfen nicht verlassen kann, hat er beschlossen, einen willenlosen Automaten in Form eines mechanischen Arbeiters herzustellen. Dazu hat er sich den Bausatz røbøt gekauft und macht sich sogleich an die Arbeit. Bevor er mit der eigentlichen Montage beginnt, möchte er die n Komponenten aus dem Bausatz strukturieren. Dazu hat er zusätzlich b verschiedene Boxen gekauft.

a) Zunächst geht Doktor Meta davon aus, dass die n Komponenten alle unterschiedlich sind und überlegt, sie in beliebiger Weise in die b Boxen zu verteilen - wieviele Möglichkeiten gibt es dafür?

b) Die Bauteile sind mit einer zufälligen 10-stelligen Seriennummer versehen. Nehmen Sie für diesen Aufgabenteil an, Doktor Meta hat $b = n$ Boxen gekauft. Wie kann Doktor Meta vorgehen, um später die benötigten Teile in erwartet konstanter Zeit zu finden?

c) Doktor Meta beginnt trotz der vorherigen Überlegungen, die Bauteile einfach zufällig über die Boxen zu verteilen, wobei jede Zuordnung unabhängig von den vorherigen ist und jede Box gleich wahrscheinlich gewählt wird. Wieviele Teile wird Dr. Meta abhängig von b erwartet in Boxen verteilen, bevor zwei Komponenten in derselben Box landen?

d) Als die ersten zwei Komponenten in derselben Box landen, vergleicht Doktor Meta sie und bemerkt, dass sie bis auf die Seriennummer exakt identisch sind. Mehr noch, bei genauerem Hinsehen stellt Doktor Meta mit großem Ärger fest, dass bei der Produktion etwas schief gegangen sein muss: alle gelieferten Bauteile sehen gleich aus. In der Wut entfernt er die Seriennummer von allen Bauteilen und hat jetzt wirklich n ununterscheidbare Komponenten vor sich. Wieviele Möglichkeiten gibt es davon ausgehend, die n Komponenten über b Boxen zu verteilen?

e) Damit keine Box überflüssig ist, möchte Doktor Meta die Bauteile auch wirklich über alle Boxen verteilen - wieviele Möglichkeiten gibt es, n ununterscheidbare Komponenten so über b Boxen zu verteilen, dass keine Box leer bleibt?

Begründen Sie Ihre Antworten.

Aufgabe 2 (*Hashing,* $3 + 1 + 2 + 1$ *Punkte*)

Gegeben sei eine Hashtabelle mit 14 Einträgen. Dabei sei die Hashfunktion h definiert über $h(x) = x \bmod 14$.

a) Verwenden Sie einerseits Hashing mit verketteten Listen, andererseits Hashing mit linearer Suche (zyklisches Array), um folgende Operationen durchzuführen:

Einfügen von 75, 44, 46, 53, 14, 2, 40, 61, 87, 86, 13, 28 Geben Sie jeweils die Tabellen nach dem Einfügen von 2 und nach dem Einfügen von 28 an.

b) Geben Sie die Anzahl der beim Einfügen betrachteten Hashtabellenplätze für beide Verfahren an!

c) Nehmen Sie an, dass nach jedem Datum wird mit gleicher Wahrscheinlichkeit gesucht wird. Welche Kosten sind für das jeweilige Verfahren für eine erfolgreiche Suche zu erwarten?

d) Wie groß ist der Speicherverbrauch, wenn sowohl Zeiger als auch Element ein Maschinenwort benötigen, und mit einem Nullzeiger, das Ende einer Liste markiert werden kann?

Aufgabe 3 (*Algorithmenentwurf,* $3 + 2$ *Punkte*)

Herzlichen Glückwunsch, Sie wurden zum Übungsleiter (oder zur Übungsleiterin) befördert! Jetzt stehen Sie vor folgender Aufgabe: Die Klausur wurde gerade geschrieben, und Sie haben eine Liste mit Tupeln der Form *(Matrikelnummer, Klausur-ID, Punkte)*. Des weiteren haben Ihre Studenten zum größten Teil fleißig die Übungsblätter bearbeitet (wie Studenten eben so sind!), und daher haben Sie eine weitere Liste mit Tupeln der Form *(Matrikelnummer, Klausur-ID, Bonuspunkte)*.
Sie stehen nun vor der Aufgabe, für alle Studenten die finale Punktzahl ausrechnen zu müssen. Leider sind einige Studenten vor der Klausur so aufgeregt, dass sie Ihre Matrikelnummer und ihre Klausur-ID beim Eintragen vertauscht haben - die Klausur-Liste enthält also Dreher in den *(Matrikelnummer, Klausur-ID)*-Paaren.
Die Klausur-IDs haben Sie wie folgt generiert: Für jeden Studenten haben Sie eine Zufallszahl gewürfelt, und von dieser die Matrikelnummer abgezogen. Hierbei werden Zufallszahlen verworfen, die bereits vorgekommen sind. Die Differenz ist die Klausur-ID des betreffenden Studenten. Außerdem sind alle Klausur-IDs (genauso wie alle Matrikelnummern) 7-stellig.

a) Entwerfen Sie einen Algorithmus basierend auf Hashing, der mit erwartet linearem Zeitaufwand (linear in der Anzahl der Studenten) die finale Punktzahl für alle Studenten berechnet.

b) Sei n die Anzahl der Studenten. Verbessern Sie Ihren Algorithmus so, dass Ihre Hashfunktion nur maximal $2n$ mal aufgerufen werden muss.

Aufgabe 4 (*Universelle Hashfunktionen,* $2 + 2 + 2$ *Punkte* $+ 1$ *Zusatzpunkt*)

Es sei $m \in \mathbb{N}$, $[m] \coloneqq \{0, 1, \ldots, m-1\}$ und $\mathcal{H} \subseteq \{h \colon U \to [m]\}$ eine Familie von Hashfunktionen. Dann heißt $\mathcal{H}$ 2-universell, wenn für jedes Schlüsseltupel $(k_1, k_2) \in U \times U$ and für jede zufällig aus der Familie $\mathcal{H}$ gezogene Funktion h gilt, dass die Folge $(h(k_1), h(k_2))$ zufällig gleichverteilt auf $[m] \times [m]$ ist, d.h. dass $(h(k_1), h(k_2))$ mit gleicher Wahrscheinlichkeit jedes der m^2 möglichen Tupel ist.

a) Zeigen Sie, dass jede 2-universelle Famile von Hashfunktionen $\mathcal{H}$ auch universell ist.

b) Es sei nun $p \in \mathbb{N}$ eine Primzahl, $l \in \mathbb{N}$ und $U \coloneqq [p]^l$ (mit $[p] \coloneqq \{0, 1, \ldots, p-1\}$). Wir definieren für jedes $\mathbf{a} \coloneqq (a_i)_{i \in [l]} \in [p]^l$ die Funktion

$$h_{\mathbf{a}} \colon (x_i)_{i \in [l]} \mapsto \sum_{i=0}^{l-1} a_i x_i \mod p.$$

Nach der Vorlesung ist $\mathcal{H} \coloneqq \{h_{\mathbf{a}} \colon U \to [p] \mid \mathbf{a} \in [p]^l\}$ universell. Zeigen Sie, dass $\mathcal{H}$ nicht 2-universell ist.
Zusatzpunkt: Wie kann man die Familie $\mathcal{H}$ so modifizieren, dass man eine 2-universelle Familie $\mathcal{H}'$ von Hashfunktionen erhält?

c) Erinnern Sie sich an Aufgabe 1. Doktor Meta möchte nun einem Gehilfen über die Fortschritte der Konstruktion seines willenlosen Arbeiters berichten. Dieser Gehilfe hat sich auf der Suche nach neuen Techniken und Materialien auf eine Weltreise gemacht. Bevor er losgefahren ist, hat er sich im Geheimen mit Doktor Meta auf eine Hashfunktion h aus einer 2-universellen Familie von Hashfunktionen $\mathcal{H} \subseteq \{h \colon U \to [m]\}$ geeinigt. Außerdem haben Sie im Voraus ausgemacht, was die verschiedene Schlüsselwerte $k \in U$ bedeuten. Doktor Meta schickt nun je nach Ausgang $(k, h(k))$ an seinen Gehilfen. Dieser überzeugt sich von der Authentizität einer Nachricht (k, σ), indem er überprüft, ob $\sigma = h(k)$ gilt. Begründen Sie, warum ein Angreifer, der die Nachricht von Doktor Meta abfängt, abändert und weiterleitet, selbst unter Kenntnis der universellen Familie $\mathcal{H}$ (aber nicht der geheimen Hashfunktion h) den Gehilfen nur mit Wahrscheinlichkeit $1/m$ von einer Nachricht $k' \neq k$ überzeugen kann.

Ausgabe: Mittwoch, 11.05.2016
Abgabe: Freitag, 20.05.2016, 12:45 im Briefkasten im Untergeschoss von Gebäude 50.34

Deckblatt Übungsblatt 4
Algorithmen I

A1	**A2**	**A3**	**A4**	$\sum$

Tutoriumsnummer:

Name	**Matrikelnummer**	**Unterschrift**

Mit unseren Unterschriften bestätigen wir, dass die Aufgaben von den Unterzeichnern eigenständig gelöst worden sind.

Hinweis: Das Übungsblatt darf in Gruppen von bis zu zwei Personen bearbeitet werden. Beide Personen müssen demselben Tutorium zugeteilt sein. Möchte jemand seine Abgaben-Gruppe innerhalb des Semesters wechseln, so ist dies im Voraus mit dem Tutor abzusprechen. **Bitte tragt in das obere Quadrat *groß* die Nummer eures Tutoriums ein.** Die Lösung des Übungsblattes ist in jedem Fall mit diesem Deckblatt abzugeben.