TU Ilmenau, Fakultät IA
Institut für Theoretische Informatik
FG Komplexitätstheorie und Effiziente Algorithmen
Univ.-Prof. Dr. Martin Dietzfelbinger
http://www.tu-ilmenau.de/iti/lehre/lehre-ss-2018/akkta/

„Ausgewählte Kapitel der Algorithmik“
Übungsblatt 1, SS 2018

Besprechung am Donnerstag, 19.4.2018 (mit Möglichkeit zum Vorrechnen)

Aufgabe 1 (Unabhängigkeit bei Gruppenoperation, Tabellenhashing)

Es sei $(G, \oplus, 0)$ eine additiv geschriebene endliche abelsche (oder: kommutative) Gruppe. (Als konkrete Beispiele können Sie sich $\{0,1\}^n$ mit bitweiser XOR-Operation oder $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ mit Addition modulo m vorstellen.)
(a) Sei $a \in G$ fest. Wir wählen $b \in G$ rein zufällig (d. h. jedes Element von G mit der gleichen Wahrscheinlichkeit). Zeigen Sie: $a \oplus b$ ist in G rein zufällig.
(b) Wir wählen a und b in G rein zufällig. Zeigen Sie: Das Paar $(a, a \oplus b)$ ist in $G \times G$ rein zufällig (uniform) verteilt, d. h.: Für $u, v \in G$ gilt: $\mathbf{Pr}(a = u \wedge a \oplus b = v) = 1/|G|^2$.
(c) Betrachten Sie *Tabellenhashing*: Für Alphabet $\Sigma = \{1, \ldots, s\}$ ist $U = \Sigma^r$, die Menge aller Wörter über Σ der Länge r. Für eine Tabelle/Matrix $T \in G^{r \times s}$ und $x = (c_1, \ldots, c_r) \in U$ sei

$$h_T((c_1, \ldots, c_r)) = T[1, c_1] \oplus \cdots \oplus T[r, c_r].$$

Zeigen Sie: Die Klasse $\mathcal{H}^{\text{tab}}_{\Sigma,G,r}$ aller so definierten Funktionen ist 1-universell.
(d) Gibt es Probleme mit den hier gemachten Aussagen, wenn die Gruppe G nicht abelsch ist?
Literaturhinweis: Definitionen und Grundaussagen zu (abelschen) Gruppen finden sich z. B. im Buch „Diskrete Strukturen, Bd. 1, Kombinatorik, Graphentheorie, Algebra“ von A. Steger.

Aufgabe 2 (Eine 1-universelle Klasse)

Es sei $\mathbb{F} = \text{GF}(2^s)$ ein endlicher Körper. Wir können die Elemente von $\mathbb{F}$ als s-Bit-Strings auffassen, also als Elemente von $\mathbb{Z}_2^s$. Die Körperaddition ist dasselbe wie bitweises $\oplus$, also die Vektorraumaddition. Weiter sei $\pi\colon \mathbb{Z}_2^s \to \mathbb{Z}_2^\ell$ eine beliebige *surjektive* $\mathbb{Z}_2$-lineare Abbildung. Beweisen Sie, dass die Klasse

$$\mathcal{H}^{\text{mult}}_{\mathbb{F},2^\ell} = \{h_a \mid a \in \mathbb{F}\}$$

mit $h_a(x) = \pi(a \cdot x)$ für $x \in U = \mathbb{F}$ 1-universell ist.

Aufgabe 3 (Maximale Bucketgröße)

Sei $\mathcal{H} \subseteq [m]^U = \{h \mid h\colon U \to [m]\}$ eine c-universelle Klasse, $S \subseteq U$ sei Schlüsselmenge der Größe n. Für $0 \le i < m$ definieren wir die Zufallsmengen $B_i = \{x \in S \mid h(x) = i\}$, und dann:

$$b_{\max} = \max\{|B_i| \mid 0 \le i < m\}.$$

Schätzen Sie $\mathbf{E}(b_{\max})$ nach oben ab.
Hinweise: 1. Die Ungleichung $\mathbf{E}(X)^2 \le \mathbf{E}(X^2)$ gilt für beliebige Zufallsvariable.
2. $(\max\{|B_i| \mid 0 \le i < m\})^2 \le \sum_{0 \le i < m} |B_i|^2$.
3. $s^2 = 2\binom{s}{2} + s$, für $s \in \mathbb{N}$.

Aufgabe 4 (Platzbedarf bei FKS)

Nehmen Sie an, die Schlüssel im FKS-Algorithmus haben $s = 2 \log n$ Bits, und die Datensätze bestehen nur aus den Schlüsseln. Verwenden Sie 1-universelle Hashklassen wie etwa $\mathcal{H}^{\text{mult}}_{\mathbb{F},2^\ell}$, für $\mathbb{F} = \text{GF}(2^s)$ und $0 \leq \ell \leq s$, so dass die Darstellung einer Hashfunktion (Level-1 oder Level-2) ebenfalls $2 \log n$ Bits benötigt. Achtung: Die Haupttabelle und die Subtabellen müssen nun Zweierpotenzgröße haben.
Bestimmen Sie durch Variieren der Größe der Zwischentabelle T eine möglichst kleine Konstante c, so dass die FKS-Datenstruktur $(c + o(1))n \log n$ Bits Platz benötigt.