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

„Ausgewählte Kapitel der Komplexitätstheorie/Algorithmik“ Übungsblatt 2, SS 2018 (Korrigiert 09.05.2018)

Besprechung am 17.05.2018 (09:00 Uhr, mit Möglichkeit zum Vorrechnen)

Aufgabe 1 (Projektion bei Δ-universellen Klassen führt zu 1-universellen Klassen)

Es sei $(R, \oplus)$ eine beliebige endliche kommutative Gruppe. (Konkretes Beispiel: $\{0,1\}^\ell$ mit bitweisem XOR als Operation.) Das Inverse von a bezeichnen wir mit $-a$, das Element $a \oplus (-b)$ mit $a - b$. Eine Hashklasse $\mathcal{H} \subseteq R^U$ heißt Δ-universell, wenn für alle $\{x, y\} \in \binom{U}{2}$ und alle $b \in R$ gilt:

$$\mathbf{Pr}_{h\in\mathcal{H}}(h(x) - h(y) = b) = \frac{1}{|R|}.$$

(Das „Δ“ soll an „Differenz“ erinnern.)

(a) **Zeigen Sie**, dass für $U = R = \mathbb{F}$, wobei $\mathbb{F}$ ein endlicher Körper ist, die Klasse $\{h_a \mid a \in \mathbb{F}\}$, $h_a(x) = a \cdot x$, Δ-universell ist. Dabei ist $(R, \oplus)$ die additive Gruppe in $\mathbb{F}$.

(b) Finden Sie mit Hilfe der 2-fach unabhängigen Klassen der Vorlesung andere Δ-universelle Klassen. (Hinweis: „Inhomogenität“ weglassen.)

(c) Sei g ein surjektiver Gruppenhomomorphismus von $(R, \oplus_R)$ nach $(R', \oplus')$. **Zeigen Sie:** Wenn $\mathcal{H} \subseteq R^U$ Δ-universell ist, dann ist auch $\mathcal{H}' = \{g \circ h \mid h \in \mathcal{H}\}$ Δ-universell (also auch 1-universell). *Hinweis*: „Homomorphiesatz“ der Gruppentheorie.

Aufgabe 2 (Komponentenweises Zusammensetzen in der Schlüsselmenge)

Ziel dieser Aufgabe ist es, Hashfunktionen für größere Universen aus solchen für kleinere Universen zu gewinnen. (Dies funktioniert bis hin zur 2-fachen Unabhängigkeit.=
Sei $\mathcal{H} \subseteq R^U$ eine Hashklasse, wobei $(R, \oplus)$ eine kommutative Gruppe ist. Wir definieren eine neue Klasse $\mathcal{H}_{U^k,R} \subseteq R^{U^k}$

$$\mathcal{H}_{U^k,R} = \{(h_1, \ldots, h_k) \mid h_1, \ldots, h_k \in \mathcal{H}\}, \text{ mit } (h_1, \ldots, h_k)((x_1, \ldots, x_k)) = h_1(x_1) \oplus \cdots \oplus h_k(x_k) \in R.$$

Zeigen Sie: Wenn $\mathcal{H} \subseteq R^U$ Δ-universell ist, dann ist $\mathcal{H}_{U^k,R}$ ebenfalls Δ-universell. (Analog für 2-fache Unabhängigkeit.) *Hinweis*: Man betrachte ein i mit $x_i \neq y_i$, wie üblich. O.B.d.A. $i = 1$.

Aufgabe 3 (Komponentenweises Zusammensetzen im Bild)

Ziel dieser Aufgabe ist es, Hashfunktionen für größere Wertebereiche aus solchen für kleinere Wertebereiche zu gewinnen.
Sei $\mathcal{H} \subseteq R^U$ eine Hashklasse, wobei $(R, \oplus)$ eine kommutative Gruppe ist.

(a) Wir definieren eine neue Klasse $\mathcal{H}_{U,R^\ell} \subseteq (R^\ell)^U$ wie folgt:

$$\mathcal{H}_{U,R^\ell} = \{(h_1, \ldots, h_\ell) \mid h_1, \ldots, h_\ell \in \mathcal{H}\}, \text{ mit } (h_1, \ldots, h_\ell)(x) = (h_1(x), \ldots, h_\ell(x)) \in R^\ell.$$

Zeigen Sie: Wenn $\mathcal{H} \subseteq R^U$ Δ-universell (2-fach unabhängig) ist, dann ist $\mathcal{H}_{U,R^\ell}$ ebenfalls Δ-universell (2-fach unabhängig). (Das gleiche gilt z. B. für 1-Universalität. Was passiert, wenn $\mathcal{H}$ nur c-universell ist?)

(b) Wenn man gleichzeitig Definitionsbereich und Wertebereich vergrößern will, bietet sich folgender Ansatz an (Woelfel 1999), der der *Konvolution* nachempfunden ist. Eine Hashklasse $\mathcal{H}_{U^k,R^\ell}$ wird realisiert, indem man $k+\ell-1$ Hashfunktionen aus $\mathcal{H}$ zufällig wählt und

$$h((x_1,\ldots,x_k)) = (u_1,\ldots,u_\ell)$$

definiert, wobei $u_i = h_i(x_1) \oplus \cdots \oplus h_{i+k-1}(x_k) \in R$ ist, für $1 \le i \le \ell$. Zeigen Sie: Wenn $\mathcal{H} \subseteq R^U$ Δ-universell ist, dann ist die Klasse $\mathcal{H}_{U^k,R^\ell}$ ebenfalls Δ-universell.

Aufgabe 4 (Kollabieren des Universums mit fixem Körper)

$\mathbb{F} = \mathrm{GF}(q)$ sei ein endlicher Körper, $U = \mathbb{F}^k$. Gegeben sei weiter $S \subseteq U$ mit $|S| = n$.
Wir suchen eine „Kollapsfunktion“ $h\colon U \to \mathbb{F}$, die (mit möglichst großer Wahrscheinlichkeit) auf S injektiv ist.
Dazu definieren wir für $x = (x_0, x_1, \ldots, x_{k-1}) \in U$ und $a \in \mathbb{F}$:

$$h_a(x) = x_0 + x_1 \cdot a + x_2 \cdot a^2 + \cdots + x_{k-1} \cdot a^{k-1},$$

und $\mathcal{H}_{\mathrm{coll}} = \{h_a \mid a \in \mathbb{F}\}$.

(a) Zeigen Sie: Wenn h aus $\mathcal{H}_{\mathrm{coll}}$ zufällig gewählt wird, gilt

$$\mathbf{Pr}(h \text{ ist auf } S \text{ nicht injektiv}) \le \frac{n^2 \cdot (k-1)}{2q}.$$

Hinweis: Ein Polynom über einem Körper $\mathbb{F}$ vom Grad $k-1$ hat maximal $k-1$ Nullstellen, wenn es sich nicht um das Nullpolynom handelt.

(b) Wenn $U = [u]$ keine sichtbare Struktur hat, die etwas mit einem Körper zu tun hat, kann man folgendermaßen vorgehen: Eine „passende“ Primzahl p wird gewählt. Die Binärdarstellung von $x \in U$ wird in $k \le \lceil \log u \rceil / \lfloor \log p \rfloor + 1$ Stücke der Länge $\lfloor \log p \rfloor$ zerlegt, die man als Zahlen $x_0, \ldots, x_{k-1} \in [p]$ interpretiert. Dann wählt man $a \in [p]$ zufällig und rechnet im Körper $\mathbb{F} = \mathbb{Z}_p$.
Finden Sie zu gegebenem u und n einen möglichst kleinen Wert p, so dass $\mathbf{Pr}(h \text{ ist auf } S \text{ nicht injektiv}) \le \frac{1}{n}$ gilt. (Lassen Sie in den Rechnungen die $\lfloor\cdot\rfloor$- und $\lceil\cdot\rceil$-Operatoren weg.)