# Exercises for Unit 10

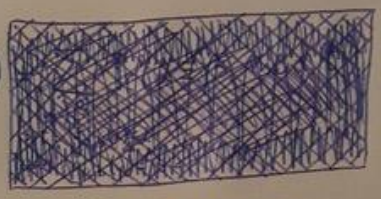
① $h_{a,b}(x) = (a \cdot x + b \bmod p) \bmod t$

$\mathcal{H} = \{h_{a,b} \mid 0 < a < p,\ 0 \le b < p\}$

$Pr(h_{a,b}(x) = h_{a,b}(y)) = Pr((ax+b) \bmod p \equiv (ay+b) \bmod p \bmod t) = (*)$

$g_{a,b}(x) := (ax+b) \bmod p$

$(*) = Pr(g_{a,b}(x) \equiv g_{a,b}(y) \bmod t)$



$= \sum_{\substack{\alpha,\beta \\ \text{s.t.} \\ \alpha \equiv \beta \bmod t}} Pr(g_{a,b}(x) = \alpha \wedge g_{a,b}(y) = \beta) = (\star)$

Claim: $Pr(g_{a,b}(x) = \alpha \wedge g_{a,b}(y) = \beta) = \begin{cases} 0, & \alpha = \beta \\ \frac{1}{p(p-1)}, & \text{otherwise} \end{cases}$

(1) $ax + b = \alpha$ (2) $ay + b = \beta$

$ax + \beta - ay = \alpha \longleftarrow b = \beta - a \cdot y$

$\boxed{a = (\alpha - \beta)(x-y)^{-1}}$ $\boxed{b = \beta - (\alpha - \beta)(x-y)^{-1} \cdot y}$

⇒ when we take some $\alpha, \beta$ and want $g_{a,b}(x) = \alpha$ and $g_{a,b}(y) = \beta$, this happens for only one choice of $a, b$ — namely $a, b$ that we can calculate from the formulas above

- for $\alpha = \beta$, $a = 0$ and by assumption $a > 0$ ⇝ we cannot have $g_{a,b}(x) = \alpha$ and $g_{a,b}(y) = \beta = \alpha$
- when $\alpha \neq \beta$, only one $g_{a,b}$ is "good" - meaning (1) and (2) are satisfied, and there are $p \cdot (p-1)$ functions in total ($p$ choices for $b$ and $p-1$ for $a$)

∎

$$(\star) = \sum_{\substack{\alpha,\beta \\ \alpha \neq \beta \text{ s.t.} \\ \alpha \equiv \beta \bmod t}} \frac{1}{p(p-1)} = \left|\{(\alpha,\beta) : \alpha \neq \beta \wedge \alpha = \beta \bmod t\}\right| \cdot \frac{1}{p(p-1)}$$

$$= p \cdot \overbrace{\left(\left\lceil \frac{p}{t} \right\rceil - 1\right)}^{\beta \text{ has to come from the same class as } \alpha \text{ but } \beta \neq \alpha} \cdot \frac{1}{p(p-1)} \leq p \cdot \frac{p-1}{t} \cdot \frac{1}{p(p-1)} = \frac{1}{t}$$

- $p$: choices for $\alpha$
- $\left\lceil \frac{p}{t} \right\rceil - 1$: max. size of class mod $t$ for numbers $\{0, 1, \dots, p-1\}$

# Algorithms and Data Structures (WS15/16)

Example Solutions for Unit 10


## Question 2

We show a slight generalization of the problem:
Let $f : U \to T \in \mathcal{H}$, with $\mathcal{H} \subseteq U \to T$ universal, $g : U \to T' \in \mathcal{H}'$, with $\mathcal{H}' \subseteq U \to T'$ universal and $(f, g) : U \to T \times T'$ with $(f, g)(x) := (f(x), g(x))$.
Then: $\mathcal{H} \star \mathcal{H}' = \{(f, g) | f \in \mathcal{H}, g \in \mathcal{H}'\}$ is a universal family of functions $U \to T \times T'$.

**Proof:** Assume $\mathcal{H} \subseteq U \to T$, $\mathcal{H}' \subseteq U \to T'$ universal und $|T| = t$, $|T'| = t' \Rightarrow P(h(x) = h(y) | h \in \mathcal{H}) \leq \frac{1}{t} \wedge P(h(x) = h(y) | h \in \mathcal{H}') \leq \frac{1}{t'}$

Then the probability of a collision in $\mathcal{H} \star \mathcal{H}'$ is:

$$\begin{aligned} P\Big(h(x) = h(y) \Big| h \in \mathcal{H} \star \mathcal{H}'\Big) &= P\Big((f,g)(x) = (f,g)(y) \Big| f \in \mathcal{H}, g \in \mathcal{H}'\Big) \\ \text{with } f, g \text{ independent} &= P\Big(f(x) = f(y) \Big| f \in \mathcal{H}\Big) \cdot P\Big(g(x) = g(y) \Big| g \in \mathcal{H}'\Big) \\ &\leq \frac{1}{t} \cdot \frac{1}{t'} \\ &\leq \frac{1}{|T \times T'|} \end{aligned}$$

□