Przemysław Uznański February 27, 2017

# Advanced Data Structures

Spring Semester 2017

Exercise Set 2

**Exercise 1:**
Show that a family of hash functions $h(x) = (ax) \bmod m$, where $0 \leq a < m$, *is not* universal.

**Exercise 2:** $(\star)$
Assume that $u = 2^k$ and $m = 2^l$. Show that a family of hash functions $h(x) = \lfloor((ax) \bmod 2^k)/2^{k-l}\rfloor$, for *odd* $0 < a < 2^k$ is universal.
***Hint***:
(i) $A = \{a|0 < a < 2^k \text{ and } a \text{ is odd}\}$ forms multiplicative group modulo $2^k$.
(ii) Consider $x$ and $y$ such that $h(x) = h(y)$. What is the set $I$ of all the possible values of $a \cdot (x - y) \bmod 2^k$ (for any such $x$ and $y$)?
(iii) Show that number of such $a$'s that $a \cdot (x - y) \bmod 2^k \in I$ is equal to the number of such $a$'s that $a \cdot 2^s \bmod 2^k \in I$, where $2^s$ is the largest power-of-two divisor of $x - y$.

**Exercise 3:**
Let $h(x) = [(\sum_{i=0}^{k-1} a_i x^i) \bmod p] \bmod m$, where $0 \leq a_i < p$, $0 < a_{k-1} < p$ and $p$ is a prime number which is greater than $u$. Show that $h(x)$ is k-wise independent.
***Hint***:
Polynomial of degree $k - 1$ in $\mathbb{Z}_p$ is uniquely defined by its value on $k$ distinct points.

**Exercise 4:**
Let $u = 2^{c\ell}$. For every key $0 \leq x < u$, and $c \geq 2$. Let $h(x) = T_1(x_1) \oplus T_2(x_2) ... \oplus T_c(x_c)$, where $x_1, \ldots, x_c$ are digits of $x$ in $2^\ell$ basis, and each $T_i$ is totally random hash function $2^\ell \to 2^{\ell'}$, for some $\ell' \leq \ell$.
Show that family of $h(x)$ is 3-wise independent, but not 4-wise independent.

***Hint***:
4-wise independence: it is enough to point a single quadruple of distinct keys $A, B, C, D$ for which $h(A), h(B), h(C), h(D)$ are correlated.

3-wise independence:
Consider any triplet of keys $A, B, C$. Show that there is coordinate $i$, such that if we fix in place all hash functions except $T_i$, iterating over all possible values of $T_i$ gives us identical probability for all possible values of $(h(A), h(B), h(C))$.
Useful fact: for any fixed $0 \leq y < 2^\ell$, $x \to x \oplus y$ is a bijection.

**Exercise 5:**
Show that the longest chain in the FKS hashing scheme has length $\mathcal{O}(\frac{\lg n}{\lg \lg n})$, with high probability (that is, with probability at least $1 - 1/\text{poly}(n)$).

***Hint***:
Use Chernoff bound (where $\mu$ denotes $E[X]$):

$$\Pr(X > c\mu) < \left(\frac{e^{(c-1)}}{c^c}\right)^{\mu}.$$