Przemysław Uznański
Giorgi Nadiradze

February 21, 2017

Advanced Data Structures

Spring Semester 2017

Exercise Set 1

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

Exercise 2:
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) $A = \{a | 0 < a < 2^k$ and a 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 Z_p is uniquely defined by its value on k distinct points.