Homework for Computational Complexity — Created: 14/05/2020
Spring 2020, UPC Barcelona — Last modified: 14/05/2020
Instructor: Albert Atserias

Homework

Exercise: More on hash functions Let p be a prime number, let $\mathbb{Z}_p$ denote the field of arithmetic mod p. For each $a, b, c \in \mathbb{Z}_p$, let $P_{a,b,c} : \mathbb{Z}_p \to \mathbb{Z}_p$ be the quadratic polynomial defined by $P_{a,b,c}(x) = ax^2 + bx + c$ mod p. Show that the family of functions $\{P_{a,b,c} : a, b, c \in \mathbb{Z}_P\}$ satisfies the following 3-universal property: for every three *distinct* $x_1, x_2, x_3 \in \mathbb{Z}_p$ and every $y_1, y_2, y_3 \in \mathbb{Z}_p$ we have

$$\Pr_{a,b,c \in_r \mathbb{Z}_p}[P_{a,b,c}(x_i) = y_i \text{ for } i = 1, 2, 3] = \frac{1}{p^3}.$$

The notation "$a, b, c \in_r \mathbb{Z}_p$" under "Pr" means that a, b and c are chosen uniformly and independently at random in $\mathbb{Z}_p$.

Exercise: More on hashing for estimating sizes of sets Let m and k be positive integers and let $U = U_{m,k}$ be a 2-universal family of hash functions from m bits to k bits. For any fixed set $S \subseteq \{0,1\}^m$ and a randomly chosen $h \in U$, let $I(S, h)$ be the indicator random variable for the event that h has collisions on S: "there exist two distinct $x, y \in S$ with $h(x) = h(y)$". Prove the following:

1. If $|S| > 2^{2k}$, then $\Pr_{h \in_r U}[I(S, h) = 1] = 1$
2. If $|S| < 2^k$, then $\Pr_{h \in_r U}[I(S, h) = 1] \leq 1 - 2^{-k}$.

Recall that the notation "$h \in_r U$" under "Pr" means that h is chosen uniformly at random in U.

Exercise: Approximate counting up to a square Use the result of the previous exercise to show that for any #P function f there exists a *deterministic* polynomial time algorithm that, given an n-bit input x and access to an $\mathrm{NP}^{\mathrm{NP}}$-oracle, outputs a number t satisfying $t \leq f(x) \leq t^2$.