Pop Quiz 5

CSCI 4030 / CSCI 6220: Randomized Algorithms

Fall 2026

Rensselaer Polytechnic Institute

Universality and independence

Write the formal definition of each of the following, and prove that if a hash function family is full 2-wise independent, then it is universal.

1. **Full k-wise independence:** When is a hash function family $\mathcal{H}$ of functions $U \to \{0,1\}^\ell$ fully k-wise independent? (Write a precise quantified statement.)

2. **Universality:** When is a hash function family $\mathcal{H}$ universal? (Write a precise quantified statement.)

3. **Implication:** Prove that full 2-wise independence implies universality.