CSC265 Fall 2020 Homework Assignment 4

due Tuesday, October 13, 2020

Consider the probability space $\mathcal{B}_n$ consisting of all n-bit vectors, each equally likely.

1. Let $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \{0,1\}^n$ be *distinct* n-bit vectors.
   Prove that
   $$\operatorname*{Prob}_{X \in \mathcal{B}_n} [aX = bX] = \frac{1}{2},$$
   where $aX = \left(\sum_{i=1}^{n} a_i X_i\right) \bmod 2$ denotes the inner product of a and $X = (X_1, \ldots, X_n) \bmod 2$.

2. Let C, D be *distinct* $n \times n$ Boolean matrices.
   Prove that
   $$\operatorname*{Prob}_{X \in \mathcal{B}_n} [CX = DX] \leq \frac{1}{2},$$
   where CX denotes the product of the matrix C and the vector X mod 2.
   Note that, if $Y = (Y_1, \ldots, Y_n)$ is a vector of natural numbers, then $Y \bmod 2$ is the vector $(Y_1 \bmod 2, \ldots, Y_n \bmod 2)$.

3. Give a randomized algorithm that takes as input three $n \times n$ Boolean matrices, P, Q, and R, and, in $O(kn^2)$ time, tries to check whether $PQ = R$, where PQ denotes the product of the matrices P and Q mod 2.
   Note that if S is a matrix of natural numbers, then $S \bmod 2$ is the matrix obtained from it by taking each entry mod 2.
   If $PQ = R$, your algorithm must answer true.
   If $PQ \neq R$, your algorithm must answer false with probability at least $1 - 2^{-k}$.

   Explain why your algorithm is correct and runs in time $O(kn^2)$.