CS3230 Semester 1 2024/2025

Design and Analysis of Algorithms

Tutorial 05
Randomized Algorithms
For Week 06

Document is last modified on: September 11, 2024

1 Lecture Review: Randomized Algorithms

Techniques: Linearity of expectations, indicator random variables, Markov inequality, union bound, principle of deferred decision, amplification of success probability.

Algorithms: Freivalds' algorithm (Monte Carlo), (Randomized) Quick Sort (Las Vegas).

Balls and bins: coupon collector (probability of no empty bin), chain hashing (expected bin size).

2 Tutorial 05 Questions

Q1). In the class, we show that Freivalds' algorithm succeeds with a probability of at least $1/2$. Show that the bound $1/2$ in the analysis is actually the best possible by constructing an input (A, B, C) on which the success probability of Freivalds' algorithm is precisely $1/2$.

For Q2). and Q3). Consider the equality testing problem, where Alice holds an n-bit string $S_A \in \{0,1\}^n$, Bob holds an n-bit string $S_B \in \{0,1\}^n$, and they want to decide whether $S_A = S_B$. Consider the following communication protocol, where an n-bit string is seen as a number expressed in base-2.

1. Let S be the set of n^2 smallest prime numbers.

2. Alice samples a number p from S uniformly at random.

3. Alice sends p and $S_A \bmod p$ to Bob (thus, only $O(\log p) \subseteq O(\log n)$ bits are sent, see Q3).).

4. After receiving Alice's message, Bob calculates $S_B \bmod p$.

5. If $S_A \bmod p = S_B \bmod p$, Bob decides that $S_A = S_B$, otherwise Bob decides that $S_A \neq S_B$.

Q2). Show that this (randomized) communication protocol is correct with a probability of at least (the target probability for this question is redacted, try to self-analyse as much as possible first).

Remark: By the prime number theorem, $p \in O(n^2 \log n)$, so this communication protocol only requires communicating $O(\log p) \subseteq O(\log n)$ bits. This demonstrates an <u>exponential separation</u> between randomized and deterministic algorithms, as any deterministic algorithm solving the equality testing problem requires communicating $\Omega(n)$ bits in the worst case.

Q3). Show that any deterministic algorithm solving the equality testing problem requires communicating $\Omega(n)$ bits in the worst case.

For Q4). and Q5). You are given a graph $G = (V, E)$ (without self-loops) and your task is to partition its vertex set into two parts $V = V_1 \cup V_2$ randomly as follows.

- Each vertex $v \in V$ flips an unbiased coin independently.

    - If the outcome is head, which happens with probability $1/2$, v joins V_1.
    - If the outcome is tail, which happens with probability $1/2$, v joins V_2.

Q4). Show that the expected number of edges crossing V_1 and V_2 is exactly $|E|/2$.

Remark: As a corollary, we obtain the following result in graph theory.

- Any graph $G = (V, E)$ admits a cut of size of at least $|E|/2$.

Here a cut is a partition of the vertex set into two parts, and the size of a cut is the number of edges crossing the two parts.

There is a last Q5). that is redacted for now.