# CS6170: Randomized Algorithms
# Problem Set #1

Name: Your name | Marks: 25

Roll No: Your roll number | Due: August 27, 23:59

## Problem 1 — 3 marks

Suppose that you want to generate a random permutation of the sequence of numbers 1 to $n$. You have at your disposal, a source of unbiased random bits. Give an efficient algorithm to generate a random permutation using as few random bits as possible from the source.

**Solution:** Type your solution here.

## Problem 2 — 4 marks

While discussing Frievald's algorithm for verifying matrix multiplication, the following algorithms were proposed in class.

1. **Algorithm 1**: Given $A$, $B$, $C$, choose a number $j$ uniformly at random from $\{1, 2, \ldots, n\}$ and multiply $A$ with the $j^{th}$ column of $B$ and check if it matches the $j^{th}$ column of $C$ entrywise.
2. **Algorithm 2**: Given $A$, $B$, $C$, choose two numbers $i$ and $j$ uniformly at random from $\{1, 2, \ldots, n\}$ and multiply the $i^{th}$ row of $A$ and the $j^{th}$ column of $B$ and check if the product is equal to the $(i, j)^{th}$ entry of $C$.

Analyze the two algorithms and explain which one is better. Are these algorithms better than Frievald's algorithm? What is the running time of this algorithm if I want to make the error probability $\epsilon$?

**Solution:** Type your solution here.

## Problem 3 — 5 marks

An $s$-$t$-cut in a graph is a set of edges such that their removal gives a new graph which does not contain a path from $s$ to $t$. Consider the following modification of Karger's algorithm to compute the smallest $s$-$t$-cut in the graph: Choose a random edge in the graph such that it not between supernodes containing $s$ and $t$, and contract it; keep continuing until the only two supernodes are the ones containing $s$ and $t$, and output this as the minimum $s$-$t$-cut.

Show that there are graphs such that the success probability of this algorithm finding the minimum $s$-$t$-cut is exponentially small.

**Solution:** Type your solution here.

## Problem 4 — 8 marks

Consider the following randomized algorithm.

**Algorithm 1:**

```
Set X ← 0
repeat n times
    Set X ← X + 1 with probability 1/2^X
Set Y ← 2^X − 1
```

(a) (5 marks) Compute $\mathbb{E}[Y]$.

**Solution:** Type your solution here.

(b) (3 marks) Give a tight bound on the number of bits required to represent $X$. Notice that the number of bits required to represent $X$ is a random variable.

**Solution:** Type your solution here.

## Problem 5 — 5 marks

A collection of $n$ bits $X_1, X_2, \ldots, X_n$ are said to be $k$-wise independent if for every subset $S$ of $k$ bits among the $n$, and for $b_1, b_2, \ldots, b_k \in \{0, 1\}$, we have

$$\Pr\left[\bigcap_{i \in S} X_i = b_i\right] = \prod_{i \in S} \Pr\left[X_i = b_i\right]$$

Consider the following construction: Let $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n \in \{0, 1\}^\ell$ be $n$ vectors such that every set of $k$ vectors are linearly independent over $\mathbb{F}_2$. Let $\mathbf{y} \in \{0, 1\}^\ell$ be chosen uniformly at random. Define $X_i$s as follows:

$$X_i = \left(\sum_{j=1}^{\ell} \mathbf{x}_{i,j} \mathbf{y}_j\right) \bmod 2.$$

Show that $X_i$s are $k$-wise independent.

**Solution:** Type your solution here.