Homework 1

1. ((4+1) + (4+1) points) Use Jensen's Inequality to prove the following inequalities.
   - Let A, B and C be the three angles of a triangle. Prove that $\sin A + \sin B + \sin C \leqslant \frac{3\sqrt{3}}{2}$. Find the exact criterion for equality.
   - Let $\mathbb{X}$ be a random variable over a finite sample space Ω. We define the entropy of the random variable $\mathbb{X}$ as $\mathrm{H}(\mathbb{X}) := -\sum_{x\in\Omega} \mathbb{P}[\mathbb{X}=x] \lg \mathbb{P}[\mathbb{X}=x]$. Prove that $\mathrm{H}(\mathbb{X}) \leqslant \lg|\Omega|$. Find the exact criterion for equality.

2. (10 points) Let M be a $n\times m$ matrix such that each of its entries is 0 or 1. Let $B = \{(i,j) : i \in [n], j \in [m], M(i,j) = 1\}$. Suppose $|B| \geqslant \varepsilon \cdot (nm)$, i.e., the set B covers at least an ε fraction of the entries of the matrix. Let R be the set of rows i such that $\sum_{j=1}^{m} M(i,j) \geqslant (\varepsilon/2)\cdot m$. Intuitively, R is the set of rows in the matrix where at least $\varepsilon/2$ fraction of the entries at in the set B. Prove that $|R| \geqslant (\varepsilon/2)n$.

3. (10 points) Let $\pi(x)$ represent the number of prime numbers that are less than x. For example, $\pi(16) = \big|\{2,3,5,7,11,13\}\big| = 6$. The celebrated "Prime Number Theorem" shows that $\pi(x)$ roughly behaves like $x/\lg x$, for large enough x. In this question assume that $\pi(x) = x/\lg x$.

   Let $r(x)$ represent the number of bits that are needed to represent the number x in binary. For example, $r(9) = 4$.

   Let $\Omega_n = \{p : p \text{ is a prime, and } r(p) \leqslant n\}$. Let $\mathbb{X}_n$ be uniform distribution over Ω_n. What is $\mathbb{E}\big[r(\mathbb{X}_n)\big]$?

4. (10 points) Let $f(x)$ be a convex upward function for $x \geqslant 1$. Prove that

$$\sum_{i=1}^{n} f(i) \leqslant \frac{f(1)+f(n)}{2} + \int_{1}^{n} f(x)\,\mathrm{d}x$$

5. (3 + 3 + 2 + 5 + 2 points) The "Stirling Approximation" states that $x!$ is roughly $\sqrt{2\pi x}\left(\frac{x}{e}\right)^x$, for large enough x. So, this approximation cannot be applied to small values of x.

   Let $p \in (0, 1/2)$ be a constant. Let $B(n,p)$ be the number of n-bit binary strings that have at most pn 1s. Note that we have:

$$B(n,p) = \sum_{0\leqslant i\leqslant pn} \binom{n}{i}$$

   We will upper bound this number.

   (a) Prove that, for $1 \leqslant i \leqslant pn$, we have:

$$\binom{n}{i-1} \leqslant \frac{p}{1-p}\binom{n}{i}$$

(b) Prove that, for $0 \leqslant k \leqslant pn$, we have:

$$\binom{n}{pn-k} \leqslant \left(\frac{p}{1-p}\right)^k \binom{n}{pn}$$

(c) Prove that

$$B(n,p) \leqslant \left(\frac{1-p}{1-2p}\right) \binom{n}{pn}$$

(d) Let $h\colon [0,1] \to [0,1]$ be the binary entropy function defined as follows:

$$h(x) = -x \lg x - (1-x) \lg(1-x)$$

Use Stirling Approximation to show that

$$\binom{n}{pn} \text{ is roughly } \frac{2^{h(p)n}}{\sqrt{2p(1-p)\pi n}}$$

(e) Prove that, for large enough n, $B(n,p) \leqslant 2^{h(p)n}$.

6. (Extra Credit) Suppose we are given a black-box B. If we ping this black-box, it outputs a uniformly random real number in the range $[0,1]$.

Let S_n denote the set of all permutations of size n (A size n permutation is a bijection from $[n] \to [n]$). We are interested in constructing an algorithm that uses this black-box to output a permutation that is drawn uniformly at random from S_n. Consider the following conjectured approach:

```
function Uniform_Permutation_Generator(n)
    for i = 1 to n do
        Ping B to obtain to obtain a sample x_i
    end for
    Let (x_{i_1}, ..., x_{i_n}) be the sorting of the sequence (x_1, ..., x_n) in an increasing order. (If there
are collisions, i.e. there are i < j such that x_i = x_j, then the sorted sequence has x_i before x_j)
    Let π be the permutation such that, for k ∈ [n], we have π(k) = i_k.
    Output π
end function
```

Let $\mathbb{X}_n$ be the random variable corresponding to the output of the algorithm described above. Prove or disprove that, for any $\pi \in S_n$, we have

$$\mathbb{P}\left[\mathbb{X}_n = \pi\right] = \frac{1}{n!}$$