CS 6222, Homework 2

Instructor: Wei-Kai Lin

Total points: 30. Points are noted after each problem.

Problem 1 (6pts)**.** This problem will prove the Chebyshev's bound on $\pi(n)$, that is, for all $n > 1$,

$$\pi(n) \geq \frac{n}{2\log n}, \tag{1}$$

where log is base 2.

(a) For any $n > 1, n \in \mathbb{N}$, let $N := \binom{2n}{n}$. Show that $N > 2^n$.

(b) For any $m \in \mathbb{N}$, consider the prime factorization of the factorial $m!$, which can be written as

$$m! = \prod_{p \text{ prime}} p^{\nu_p(m!)},$$

where $\nu_p(x) \in \mathbb{N}$ denotes the maximal power of p such that $p^{\nu_p(x)}$ divides x. Show that for any p, it holds that $\nu_p(m!) = \sum_{j=1,2,\ldots} \lfloor m/p^j \rfloor$.

(c) Take log on both sides of (a), and then show that

$$\sum_{p \text{ prime}} (\nu_p((2n)!) - 2\nu_p(n!)) \cdot \log p = \sum_{\text{prime } p<2n} (\nu_p((2n)!) - 2\nu_p(n!)) \cdot \log p > n \tag{2}$$

(d) Show that for any prime p, any $n > 1$,

$$\nu_p((2n)!) - 2\nu_p(n!) \leq \log_p(2n) = \frac{\log(2n)}{\log p}.$$

(e) Plug (d) into equation (2) and then show that $\pi(2n) \cdot \log(2n) > n$, and thus Equation (1) holds for all even n.

(f) Show Equation (1) holds for all odd $n > 1$.

Problem 2 (3pts)**.** Let G be a finite group with the binary operator $\otimes$. Let $H \subseteq G$ be a subset of G. Suppose that

- Identity: $1 \in H$ (where 1 is the identity of G), and
- Closure: for all $a, b \in H$, it holds that $a \otimes b \in H$.

Prove that H is a subgroup of G (by proving associativity and inverse for $\otimes$).

Problem 3 (2pts)**.** We say $N \in \mathbb{N}$ is a perfect power if $N = m^k$ for some $m, k \in \mathbb{N}, m > 1$. Consider any input $N < 2^n$ that is represented by an n-bit string. Show that perfect power can be decided in time polynomial in n through following steps. Notice that, we can only perform constant-bit computation in unit time, and thus the addition, multiplication, or exponentiation of n-bit integers take time $O(n), O(n^2), O(n^3)$ respectively.

(a) Show that if $N = m^k$, then $k < n$.

(b) Since there are only $O(n)$ possible k's, it suffices to decide if there exists integer m such that $m^k = N$. Write an algorithm to do that in time $O(n^4)$. **Hint:** binary search or Newton's method.

Problem 4 (5pts)**.** Recall that assuming factoring is hard, then the following function $f_{\text{mul}} : \mathbb{N}^2 \to \mathbb{N}$

$$f_{\text{mul}}(x, y) = \begin{cases} 1 & \text{if } x = 1 \text{ or } y = 1 \\ x \cdot y & \text{o.w.} \end{cases}$$

is a weak OWF. Show that efficient prime testing is *not needed* in the proof. Specifically, assume for contradiction, f_{mul} is not a weak OWF; that is, for any polynomial $q(n)$, there exists an NUPPT adversary A such that for infinitely many $n \in \mathbb{N}$,

$$\Pr[x, y \leftarrow \{0,1\}^n, z \leftarrow x \cdot y : f_{\text{mul}}(A(1^n, z)) = z] > 1 - \frac{1}{q(n)}.$$

Then, show the following NUPPT B takes as input a product z of two primes and then outputs a prime factor with non-negligible probability.

Algorithm $B(1^n, z)$:

1. Run $(x', y') \leftarrow A(1^n, z)$.
2. If $x' \neq 1$ and $y' \neq 1$ and $x' \cdot y' = z$, output (x', y'); otherwise, output $\perp$.

Hint: imagine the input z is sampled from the product of natural numbers $< 2^n$ (not necessarily primes), and then calculate the conditional probability when z happens to be a product of two primes.

Problem 5 (4pts)**.** Suppose that $f : \{\{0,1\}^n \to \{0,1\}^{l(n)}\}_{n \in \mathbb{N}}$ is a OWF. This problem will step-by-step prove that $g : \{\{0,1\}^n \to \{0,1\}^{2l(n)}\}_{n \in \mathbb{N}}$ constructed below is also a OWF. The construction of g is:

$$g(x) := f(x) \| f(x),$$

where $\|$ the concatenation of strings.

(a) Argue that g is an easy-to-compute function.

(b) Write the statement of "assume for contradiction, g is easy to invert" that is formally quantified by probability; in this statement, denote A as the adversarial algorithm.

(c) Write an algorithm $B(1^n, z)$ such that (i) B takes as input z sampled by $x \leftarrow \{0,1\}^n, z \leftarrow f(x)$, and then (ii) B runs A as a subroutine. Moreover, argue that B is NUPPT.

(d) Argue that B from the previous step inverts f with non-negligible probability, that is, there exists a polynomial $q(n)$ such that for infinitely many $n \in \mathbb{N}$,

$$\Pr[x \leftarrow \{0,1\}^n, z \leftarrow f(x) : f(B(1^n, z)) = z] \geq 1/q(n),$$

which contradicts that f is a OWF and completes this reduction.

Problem 6 (2pts)**.** Suppose that $g : \{\{0,1\}^n \to \{0,1\}^{l(n)}\}_{n \in \mathbb{N}}$ is a OWF. This problem will step-by-step disprove that $h : \{\{0,1\}^n \to \{0,1\}^{\lfloor l(n)/2 \rfloor}\}_{n \in \mathbb{N}}$ constructed below is a OWF. The construction of h is:

$$h(x) := g(x)[1, ..., \lfloor l/2 \rfloor] \oplus g(x)[\lfloor l/2 \rfloor + 1, ..., 2\lfloor l/2 \rfloor],$$

where $\oplus$ denotes bitwise XOR, $s[i, ..., j]$ denotes the substring $(s_i, s_{i+1}, ..., s_j)$ of string s, and $l := l(|x|)$, where $|x|$ denotes the bit-length of x.

It suffices to find a OWF g such that h is easy to invert when the above construction uses g.

(a) Find g so that g is a OWF but $h(x) = 0^{\lfloor l(|x|)/2 \rfloor}$ for such g.

(b) Write an NUPPT adversary A such that $A(1^n, z)$ inverts $z \leftarrow h(x), x \leftarrow \{0,1\}^n$ with probability 1.

Problem 7 (8pts)**.** Let $f_1, f_2 : \{\{0,1\}^n \to \{0,1\}^n\}_{n \in \mathbb{N}}$ be one-way functions. Prove or disprove each of the following function g is a OWF (there are 4 subproblems).

(a) $g(x) := f_1(x) \oplus (000 \| 1^{|x|-3})$

(b) $g(x) := f_1(x) \oplus f_2(x)$

(c) $g(x) := f_1(x)[1, ..., \lfloor |x|/2 \rfloor]$

(d) $g(x) := f_1(f_2(x))$