Assignment 2 Answers

log will refer to $\log_2$.

1. Show using Definition 27.2 that

   (a) $\epsilon(n) = n^{-\log\log n}$ is a negligible function. How large does n need to be before $\epsilon(n) \leq n^{-100}$?

   Answer: For a given c, if $n > 2^{2^c}$, then $\log\log n > c$, meaning $n^{-\log\log n} < n^{-c}$. This is if and only if, so in particular, n needs to exceed $2^{2^{100}}$ before $\epsilon(n) < n^{-100}$.

   (b) If $\epsilon(n)$ is a negligible function, and n^r is a polynomial, then $n^r\epsilon(n)$ is also a negligible function.

   Answer: Let $c > 0$. Then $c + r > 0$. Since $\epsilon(n)$ is negligible, there is an integer N such that when $n > N$, $epsilon(n) < n^{-(r+c)}$. Then $n^r\epsilon(n) < n^{-c}$.

   (c)
   $$f(n) = \begin{cases} 1/n^{99} & \text{if n is prime} \\ 2^{-n} & \text{otherwise} \end{cases}$$

   is not a negligible function.

   Answer: For any prime n, $f(n) = 1/n^{99} > 1/n^{100}$. Since there are infinitely many primes, $f(n) > 1/n^{100}$ infinitely often. Therefore it is not negligible.

2. Suppose that $f : \{0,1\}^* \to \{0,1\}^*$ is such that $|f(x)| < c\log(|x|)$ for every $x \in \{0,1\}^*$, where $c > 0$ is some fixed constant. (Here $|\cdot|$ denotes the length of a string.) Prove that f is not a strong one-way function.

   Answer: Let $x \leftarrow \{0,1\}^n$ be randomly chosen and let $y = f(x)$. The procedure $\mathcal{A}(1^n, y)$ simply does the following:

   - Sample $x' \leftarrow \{0,1\}^n$ uniformly at random.
   - Return x'.

   The idea is that since the length of $f(x)$ is so limited, there are not many possible outputs, and so the probability of being correct is non-negligible. Since $|f(x)| < c\log(|x|) = c\log(n)$, then the range of f is within $\{0,1\}^{\lfloor c\log(n)\rfloor}$. Thus the size of the range is at most $2^{\lfloor c\log(n)\rfloor} \leq 2^{c\log n} = n^c$. Let m denote this size. For each i from 1 to m, let $p_i = P[x \leftarrow \{0,1\}^n : f(x) = y_i]$. Since this covers the range of f, $\sum_{i=1}^m p_i = 1$. Then we can see that since the input y of A came as a result of a uniformly chosen x, and $\mathcal{A}$ independently chooses another uniformly random x', that the probability of $\mathcal{A}$ succeeding is

$$\begin{aligned}
P[f(\mathcal{A}(y)) = y] &= P[x \leftarrow \{0,1\}^n; x' \leftarrow \{0,1\}^n; f(x) = f(x')] \\
&= \sum_{i=1}^{m} P[x \leftarrow \{0,1\}^n; x' \leftarrow \{0,1\}^n; f(x) = y_i = f(x')] \\
&= \sum_{i=1}^{m} P[x \leftarrow \{0,1\}^n : f(x) = y_i] P[x' \leftarrow \{0,1\}^n : f(x) = y_i] \\
&= \sum_{i=1}^{m} p_i^2.
\end{aligned}$$

This exceeds $(\sum_{i=1}^{m} p_i)/m = 1/m$ by the Cauchy-Schwarz inequality (it is minimized when all probabilities are equal to $1/m$). So

$$P[f(\mathcal{A}(y)) = y] \geq 1/m \geq 1/n^c.$$

Thus it succeeds with probability greater than any negligible function, and therefore f isn't a strong one-way function.

3. Suppose we have an efficiently computable function $f : \{0,1\}^* \to \{0,1\}^*$ such that for any adversary $\mathcal{A}$ and all n,

$$P[x \leftarrow \Pi_n; y \leftarrow f(x) : f(\mathcal{A}(1^n, f(x))) = y] < e^{-n}.$$

Note that x is being sampled from the set of n-bit primes. Show that f is a weak one-way function.

Answer:

One approach using a contradiction argument: We will show that for any adversary $\mathcal{A}$,

$$P[x \leftarrow \{0,1\}^n; y \leftarrow f(x) : f(\mathcal{A}(1^n, f(x))) = y] < 1 - 1/4n.$$

Suppose this is not the case, so there exists an adversary $\mathcal{A}$ such that

$$P[x \leftarrow \{0,1\}^n; y \leftarrow f(x) : f(\mathcal{A}(1^n, f(x))) = y] \geq 1 - 1/4n$$

infinitely often. We will use this to create an adversary $\mathcal{A}'$ which contradicts the probability bound we were given. Let $\mathcal{A}'$ do the following for its input $y = f(p)$, where $p \leftarrow \Pi_n$:

- Sample $x \leftarrow \{0,1\}^n$
- Check if x is prime

- If x is prime, output $x' \leftarrow \mathcal{A}(1^n, y)$. Otherwise, output nothing.

Now, $\mathcal{A}'$ will fail when x is not prime (event E), or when $\mathcal{A}$ fails (event F). So we have

$$\begin{aligned}
P[\mathcal{A}' \text{ fails}] &= P[E \cup F] \\
&\leq P[E] + P[F] \\
&\leq (1 - 1/2n) + P[F] \quad \text{(using our lower bound on the number of primes)} \\
&\leq (1 - 1/2n) + 1/4n \quad \text{(using our assumption)} \\
&= 1 - 1/4n.
\end{aligned}$$

Therefore,

$$P[x \leftarrow \Pi_n; y \leftarrow f(x) : f(\mathcal{A}'(1^n, f(x))) = y] > 1/4n > e^{-n}$$

for large n, a contradiction. Therefore, we must have that for every adversary $\mathcal{A}$,

$$P[x \leftarrow \{0,1\}^n; y \leftarrow f(x) : f(\mathcal{A}(1^n, f(x))) = y] < 1 - 1/4n.$$

Second approach: We will show that for any adversary $\mathcal{A}$,

$$P[x \leftarrow \{0,1\}^n; y \leftarrow f(x) : f(\mathcal{A}(1^n, f(x))) = y] < 1 - 1/4n.$$

Let $\mathcal{A}$ be an adversary.

$$\begin{aligned}
P[\mathcal{A} \text{ succeeds on } x \leftarrow \{0,1\}^n] &= P[\mathcal{A} \text{ succeeds on } x \leftarrow \{0,1\}^n | x \in \Pi_n] P[x \in \Pi_n] \\
&\quad + P[\mathcal{A} \text{ succeeds on } x \leftarrow \{0,1\}^n | x \notin \Pi_n] P[x \notin \Pi_n] \\
&\leq e^{-n} P[x \in \Pi_n] + (1) P[x \notin \Pi_n] \\
&\leq e^{-n}(1) + (1)(1 - \frac{1}{2n}) \\
&< \frac{1}{4n} + (1 - \frac{1}{2n}) \\
&= 1 - \frac{1}{4n}
\end{aligned}$$

for large enough n.

4. Prove that if $f : \{0,1\}^n \to \{0,1\}^*$ is a strong one-way function, then the function $g : \{0,1\}^{2n} \to \{0,1\}^*$ defined by $g(x_1, x_2) = (x_1, f(x_2))$, is a strong one-way function.

   Answer: Suppose it is not a strong one-way function. Since f is efficiently computable, clearly g is as well. So there must be an adversary $\mathcal{A}$ and a polynomial $p(n)$ such that

   $$P[(x_1, x_2) \leftarrow \{0,1\}^{2n}; (y_1, y_2) \leftarrow g(x_1, x_2) : g(\mathcal{A}(1^{2n}, (y_1, y_2))) = (y_1, y_2)]$$

   infinitely often. We will use this to construct an adversary $\mathcal{A}'$ which inverts f. Let $\mathcal{A}'$ do the following on input $y = f(x)$, where $x \leftarrow \{0,1\}^n$:

- Sample $x_1 \leftarrow \{0,1\}^n$
- Find $(x_1', x_2') \leftarrow \mathcal{A}(x_1, y)$
- Output x_2'.

We can see that since y was computed from a uniformly selected x and x_1 is independently sampled uniformly, (x_1, y) is the result of $g(x_1, x)$ computed on a uniformly selected $(x_1, x) \leftarrow \{0,1\}^{2n}$. Thus $\mathcal{A}'$ succeeds with probability $1/p(n)$ infinitely often, contradicting f being a strong one-way function.

5. Explain why it is the case that when algorithm A' (Algorithm 33.6) uses A as a subroutine, A does indeed receive the product of two uniformly distributed n-bit integers, assuming that A' received the product of two uniformly random n-bit primes.

   Answer: We want to show that for any $a, b \in \{0,1\}^n$ (the bit-wise representation of integers in $[0, 2^n)$), $Pr[(a,b)$ were chosen and $z = ab$ was given to $\mathcal{A}] = (1/2^n)(1/2^n)$.

   Case 1: a, b are not both prime. Then this pair will be given to the subroutine $\mathcal{A}$ if and only if they are generated at the beginning of procedure $\mathcal{A}'$. So

   $$Pr[(a,b) \text{ were chosen and } z = ab \text{ was given to } \mathcal{A}] =$$

   $$Pr[(x,y) = (a,b) \text{ generated at the beginning of procedure } \mathcal{A}'] = (1/2^n)(1/2^n)$$

   Case 2: a, b are both prime. Then for (a,b) to be chosen and the product given to $\mathcal{A}'$ in the procedure, two things need to occur: One is that (a,b) be the initial pair that was given to $\mathcal{A}'$, which were each chosen uniformly in Π_n. The next thing that needs to happen is that $\mathcal{A}'$ generates two random primes x, y at the beginning of the procedure. These two processes are independent. So

   $$\begin{aligned}
   &Pr[(a,b) \text{ were chosen and } z = ab \text{ was given to } \mathcal{A}] \\
   &= Pr[(a,b) \text{ generated and } ab \text{ given to } \mathcal{A}']Pr[(x,y) \text{ at the beginning of } \mathcal{A} \text{ both prime}] \\
   &= \left(\frac{1}{|\Pi_n|}\right)^2 \left(\frac{|\Pi_n|}{2^n}\right)^2 \\
   &= (1/2^n)(1/2^n)
   \end{aligned}$$

6. (Based on the discussion on page 34) Justify the comment that this modified algorithm A'' succeeds in factoring with at least the same if not greater probability than A'.

Answer: So we can make these changes to Algorithm 33.6 to describe A'': in line 2 it doesn't actually check, in line 5 "$z' \leftarrow z$" (so a pointless if/else), and in line 8 "Return w"

Let E be the event that the two integers A'' samples x and y are prime. Then we split into two cases based on whether E occurs, and we compare the success probability of A'' vs A'.

$$
\begin{aligned}
P[\mathcal{A}'' \text{ succeeds}] &= P[\mathcal{A}'' \text{ succeeds} \cap E] + P[\mathcal{A}'' \text{ succeeds} \cap \overline{E}] && (1)\\
&= P[\mathcal{A}' \text{ succeeds} \cap E] + P[\mathcal{A}'' \text{ succeeds} \cap \overline{E}] && (2)\\
&\geq P[\mathcal{A}' \text{ succeeds} \cap E] + 0 && (3)\\
&= P[\mathcal{A}' \text{ succeeds} \cap E] + P[\mathcal{A}' \text{ succeeds} \cap \overline{E}] && (4)\\
&= P[\mathcal{A}' \text{ succeeds}] && (5)
\end{aligned}
$$

Line (1) is partitioning the probability according to E (the two integers are prime). Line (2) is noting that in the case where both integers are prime, $\mathcal{A}''$ is doing the same thing that $\mathcal{A}'$ would do, so it succeeds with the same probability. The inequality in line (3) should be clear (probabilities are nonnegative). Line (4) follows from the fact that $\mathcal{A}'$ always fails in the case where x and y are not both prime (it does not return anything).

7. Suppose we repeatedly and independently pick a random n-bit integer until we find one that is prime. Let X be the number of times we have to sample before successfully finding a prime (assume we do prime-checking in a deterministic way).

   (a) What kind of random variable is X?

   Answer: Geometric.

   (b) Find an upper bound on $E[X]$.

   Answer: Let p be the probability of success. We know that $p \geq 1/(2n)$. Therefore, $E[X] = 1/p \leq 2n$.

   (c) Find an upper bound on $P[X > m]$. Find a function $m(n)$ that makes this upper bound a negligible function of n.

   Answer:

$$
\begin{aligned}
P[X > m] &= P[\text{The first } m \text{ integers we selected were all not prime}]\\
&= (1-p)^m\\
&\leq (1 - 1/(2n))^m\\
&\leq e^{-m/(2n)}
\end{aligned}
$$

So we can choose for instance $m = 2n^2$ to make this probability at most e^{-n}, which is negligible.