1 Asymptotical Notations

Among the following functions in n, please select all that are polynomial or negligible functions in n.

Definition (Negligible Function) A function $\epsilon(n)$ is negligible if for every c, there exists some n_0 such that for all $n > n_0$,

$$\epsilon(n) \leq \frac{1}{n^c}.$$

Definition (Polynomial Function). A function $p(n)$ is polynomial if there exists c, n_0 such that for all $n > n_0$,

$$p(n) \leq n^c.$$

1. n^{100}
2. $2^{\log n}$
3. 2^n
4. $n^{\log \log n}$
5. $\frac{1}{2^{n^2}}$
6. $\frac{1}{2^n}$
7. $\frac{1}{n^{\log \log n}}$
8. $n^{-\log \log \log n}$
9. n^{-3}

Sol.

1. $\frac{1}{2^n}$ is negligible.

   To show $\frac{1}{2^n}$ is negligible in n, it suffices to derive that for any constant c, there exists constant n_0 such that for all $n > n_0$, $\frac{1}{2^n} \leq \frac{1}{n^c}$. Rearranging and taking $\lg(\cdot)$ on both sides of the inequality, we want $c \lg n \leq n$. Therefore, choosing $n_0 = \max(c^2, 16)$, we consider two cases: $c \geq 4$ or $c < 4$.

   Case 1: $c \geq 4$ and thus $n_0 = c^2 \geq 16$, then for all $n > c^2 \geq 16$,

   $$c \leq \frac{c^2}{2 \lg c} < \frac{n}{\lg n},$$

   where both inequality hold by that fact that $x/\lg x$ is monotonically increasing for any $x \geq 4$.

   Case 2: $c < 4$, and $n_0 = 16$. It holds that $c < 4 = \frac{16}{\lg 16} < \frac{n}{\lg n}$ for all $n > n_0$ (also by $x/\lg x$ is monotonically increasing for any $x \geq 4$).

   Note that to show $x/\lg x$ is increasing, we need to take its derivative and find its minimum for those large enough x. In fact, we could have $n_0 = \max(c^2, 4)$ in the above with more involved minimum calculation.

2. $\frac{1}{2^{\log n}}$ is not negligible.

   To show $1/2^{\log n}$ is not negligible, it suffices to show that there exists constant c such that for infinitely many n, $1/2^{\log n} > 1/n^c$. Rearranging it, we want some c such that $n^c > 2^{\log n} = n$ holds. Choosing $c = 2$, we have $n^2 > n$ for all $n > 1$. As desired, there are infinitely many such n as there are infinitely many natural numbers.

2 Closure Under Operations

Suppose that $f_1(n), f_2(n)$ are negligible functions in n, and $g(n)$ some fixed polynomial in n. Which of the following must be negligible functions in n?

1. $f_1(n) + f_2(n)$
2. $f_1(n)f_2(n)$
3. $f_1(n)g(n)$
4. $g(n)$
5. $f_1(n)^{g(n)}$
6. $\sqrt{f_1(n)}$

Let $g_1(n), g_2(n)$ denote two fixed polynomials in n. Which of the following must be polynomial in n:

1. $g_1(n) + g_2(n)$
2. $g_1(n)g_2(n)$
3. $g_1(n)^{g_2(n)}$
4. $g_1(n) + 203942$
5. $g_1(n) + 2^n$
6. $2^{g_1(n)}$
7. $g_1(n)^{100}$

Sol. $f_1(n) + f_2(n)$ is negligible.

To show $f(n) = f_1(n) + f_2(n)$ is negligible in n, it suffices to derive that for any constant c, there exists constant n_0 such that for all $n > n_0$, $f(n) \leq \frac{1}{n^c}$.

With fixed c, given that f_1, f_2 are both negligible, we have that (a) there exists constant n_1 such that for all $n > n_1$, $f_1(n) \leq 1/n^{c+1}$, and (b) there exists constant n_2 such that for all $n > n_2$, $f_2(n) \leq 1/n^{c+1}$. Therefore, for all c, choosing constant $n_0 = \max(n_1, n_2, 2)$, we have, for all $n > n_0$,

$$f(n) = f_1(n) + f_2(n) \leq \frac{1}{n^{c+1}} + \frac{1}{n^{c+1}} = \frac{2}{n \cdot n^c} \leq \frac{1}{n^c},$$

as desired. Note that $f_1(n) \leq 1/n^{c+1}$ holds for large enough n because $c + 1$ is a constant and f_1 is negligible (and that of f_2 similarly).

3 Union Bound

Let $A_1, A_2, \ldots, A_n$ be events. Then,

$$\Pr[A_1 \cup A_2 \cup \ldots, \cup A_n] \leq \Pr[A_1] + \Pr[A_2] + \cdots + \Pr[A_n].$$

Proof. We claim that for any events A, B, $\Pr[A \cup B] \leq \Pr[A] + \Pr[B]$, and then the union bound of n events holds by induction. To show it, by inclusion-exclusion principle, we have $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B] \leq \Pr[A] + \Pr[B]$, where the second step holds because $\Pr[A \cap B] \geq 0$. □

Example. $G(n, p)$ is the graph G on n nodes, where for every pair of vertices an edge is included with probability p. Show that the probability that there is an isolated vertex is upper bounded by $n(1 - p)^{n-1}$.

Proof.

$$\Pr[\text{vertex 1 is isolated}] = (1 - p)^{n-1}$$

By the union bound,

$$\Pr[\text{exists isolated vertex }] = n(1 - p)^{n-1}$$

□

Note that the event that vertex 1 is isolated and the event that vertex 2 is isolated are *not independent*. The union bound is used everywhere in cryptography, especially because you do not need independence to apply the union bound.

4 Perfectly Secret Encryption

Example 1. A perfectly secret encryption can *leak* information about secret key.

Sol. The encryption scheme is described as follows: Message space $M = \{0, 1\}^{10}$, key space $K = \{0, 1\}^{11}$, and

- Gen: output $k \leftarrow K$.
- $\mathsf{Enc}(k, m)$: use the first 10 bits of k to XOR m, and leaks the 11-th bit of k. That is, output $c := k_{1\to 10} \oplus m||k_{11}$, where $||$ denotes concatenation.
- $\mathsf{Dec}(k, c)$: use first 10 bits of k to recover m.

This scheme is perfectly secure by the same proof of the One-time pad, but it clearly leaks information, the 11-th bit, about secret key k.

Example 2. Leaking nothing about secret key doesn't imply perfect secrecy.

Sol. We can propose an encryption algorithm $\mathsf{Enc}(k, m)$ that outputs plaintext m directly, which leaks no information about secret key k but not secure.

5 Identical Distributions

Let $D : \{0, 1\}^3 \to \{0, 1\}^3$ be an randomized algorithm such that $D(x) := r \leftarrow \{0, 1\}^3$, output $x \oplus r$. Let $a = 110, b = 001$. Sample random variables $X_1 \leftarrow D(a), X_2 \leftarrow D(b), X_3 \leftarrow \{0, 1\}^3$. Prove of disprove the if the pairs of the following distributions are identical

1. Distributions of X_1, X_2.
2. Distributions of X_2, X_3.

Sol. X_1, X_2, X_3 are identical distribution.

To show that, fix any t and consider $\Pr[X_1 = t]$ and $\Pr[X_2 = t]$. If $t \notin \{0, 1\}^3$, then $\Pr[X_1 = t] = 0 \Pr[X_2 = t]$. If not, $t \in \{0, 1\}^3$, and $\Pr[X_1 = t] = \Pr[r \leftarrow \{0, 1\}^3 : r \oplus t = a]$ by definition of X_1, RHS equals to $\Pr[r \leftarrow \{0, 1\}^3 : r = a \oplus t]$ by XOR, and finally it equals to $1/8$ as $a \oplus t$ is a fixed value. Similarly, $\Pr[X_2 = t] = 1/8$, and we conclude that $\Pr[X_1 = t] = \Pr[X_2 = t]$ for all t. We can also show that $X_2 = X_3$ in the same way.

6 Perfect Secrecy

Consider the following encryption schemes. Prove or disprove if the schemes are perfectly secret. In the schemes below, the key generation function simply outputs one of the keys at uniformly random.

(Recall that to show that a scheme is not perfectly secret you just have to give a counter example with two messages and a ciphertext and compute the probabilities)

6.1 Scheme 1

$M = \{00, 01, 10, 11\}$, $K = \{0, 1\}$,

- `Enc` is described using the following table

k	m	$Enc(k, m)$
0	00	01
0	01	10
0	10	11
0	11	00
1	00	10
1	01	01
1	10	00
1	11	11

- `Dec` can be read from the same table by swapping the second and third columns and renaming them c and $Dec(k, c)$ respectively.

Sol. Consider the definition of perfect secrecy:

$$\forall m_1, m_2 \in M, \forall c \in C, \quad \Pr[k \leftarrow \texttt{Gen}(1^n) : \texttt{Enc}_k(m_1) = c] = \Pr[k \leftarrow \texttt{Gen}(1^n) : \texttt{Enc}_k(m_2) = c]$$

Let $m_1 = 00$, $m_2 = 11$, $c = 11$, then

$$\Pr[k \leftarrow \texttt{Gen}(1^n) : \texttt{Enc}_k(m_1) = c] = 0$$

$$\Pr[k \leftarrow \texttt{Gen}(1^n) : \texttt{Enc}_k(m_2) = c] = \Pr[k \leftarrow \texttt{Gen} : k = 1] = \frac{1}{2}$$

$\therefore$This scheme is **not** perfectly secure.

6.2 Scheme 2: Variant of Caesar-cipher

$M = \{0, 1, ..., 7\}$, $K = \{0, 1, ..., 7\}$,

- $\texttt{Enc}(k, m) = (m + k) \mod 8$. (+ denotes addition and not the XOR operation)
- $\texttt{Dec}(k, c) = (c - k) \mod 8$

where $(a \mod 8)$ is the remainder obtained when a is divided by 8.

Sol. $\forall m_1, m_2 \in M, \forall c \in C$,

$$\Pr[k \leftarrow \texttt{Gen}(1^n) : \texttt{Enc}_k(m_1) = c] = \Pr[k \leftarrow \texttt{Gen} : k = (c - m_1) \mod 8] = \frac{1}{8}$$

$$\Pr[k \leftarrow \texttt{Gen}(1^n) : \texttt{Enc}_k(m_2) = c] = \Pr[k \leftarrow \texttt{Gen} : k = (c - m_2) \mod 8] = \frac{1}{8}$$

$\therefore$This scheme is perfectly secure.

6.3 Scheme 3: Revisit Scheme 2

$M' = M \times M$, $K = \{0, 1, ..., 7\}$, M is defined in Scheme 2.

- $\texttt{Enc}(k, (m_1, m_2)) = ((m_1 + k) \mod 8, (m_2 + k) \mod 8)$. (+ denotes addition and not the XOR operation)
- $\texttt{Dec}(k, (c_1, c_2)) = ((c_1 - k) \mod 8, (c_2 - k) \mod 8)$

where $(a \mod 8)$ is the remainder obtained when a is divided by 8.

Sol. Let $m_1 = (1, 1)$, $m_2 = (1, 2)$, $c = (1, 1)$, then

$$\Pr[k \leftarrow \texttt{Gen}(1^n) : \texttt{Enc}_k(m_1) = c] = \Pr[k \leftarrow \texttt{Gen} : k = 0] = \frac{1}{8}$$
$$\Pr[k \leftarrow \texttt{Gen}(1^n) : \texttt{Enc}_k(m_2) = c] = 0$$

$\therefore$This scheme is **not** perfectly secure.