1 Negligible Functions

We will prove that $f(n) = 2^{-n}$ is a negligible function. Let's start by using a definition of negligible functions given in Katz & Lindell, section 3.1.

Definition 1.1 (Negligible Function)**.** *Let f be a function mapping the natural numbers to the non-negative real numbers. f is **negligible** if for every constant c, there exists an $N \in \mathbb{N}$ such that for all $n > N$, it holds that*

$$f(n) < n^{-c}$$

Theorem 1.2. *$f(n) = 2^{-n}$ is negligible.*

Proof.

1. Let us be given an arbitrary $c > 0$. Then the following conditions are equivalent:

$$2^{-n} < n^{-c} \tag{1}$$
$$-n \cdot \log_2(2) < -c \cdot \log_2(n) \tag{2}$$
$$0 < n - c \cdot \log_2(n) \tag{3}$$

   Let $g(n) = n - c \cdot \log_2(n)$. We just need to show that there exists an $N \in \mathbb{N}$ such that for all $n > N$, it holds that $g(n) > 0$.

2. First, we'll show that $g(n)$ is an increasing function when $n \geq 2c$.

   Lemma 1.3. *For any N, n, if $2c \leq N < n$, then $g(N) < g(n)$.*

   Proof.

   (a) For now, treat $g(n)$ as a function whose domain is the positive real numbers, so that we can take the derivative.

$$g'(n) = 1 - \frac{c}{\ln(2) \cdot n}$$

   (b) When $n \geq 2c$,

$$\begin{aligned} g'(n) &\geq 1 - \frac{c}{\ln(2) \cdot 2c} = 1 - \frac{1}{2\ln(2)} \\ &> .27 > 0 \end{aligned}$$

   (c) Pick N, n such that $2c \leq N < n$. Then by the mean value theorem:

$$\frac{g(n) - g(N)}{n - N} > 0$$

   Therefore, $g(N) < g(n)$.

   □

3.

Lemma 1.4. *There exists an $N \geq 2c+1$ such that $g(N) > 0$.*

Proof.

(a) First we'll show that for all $n \geq c+1$, $g(2n) \geq g(n)+1$.

$$\begin{aligned} g(2n) &= 2n - c \cdot \log_2(2n) = n + n - c \cdot \log_2(n) - c \cdot \log_2(2) \\ &= n - c \cdot \log_2(n) + n - c \\ &\geq g(n) + 1 \end{aligned}$$

(b) For any $n \geq c+1$ and any $d \in \mathbb{N}$, we can use induction to prove that $g(n \cdot 2^d) \geq g(n) + d$.

(c) Next, choose $N = (2c+1) \cdot 2^{\lceil |g(2c+1)| \rceil + 1}$. Note that $\lceil |g(2c+1)| \rceil + 1 \in \mathbb{N}$, and $\lceil |g(2c+1)| \rceil + 1 > |g(2c+1)|$.

(d) Putting everything together, we can show that:

$$g(N) \geq g(2c+1) + \lceil |g(2c+1)| \rceil + 1 > 0$$

□

4. Combining lemma 1.3 and lemma 1.4, we can show that there exists an $N \in \mathbb{N}$ such that for all $n > N$, $g(n) > 0$. This is sufficient to prove that for all $n > N$, $2^{-n} < n^{-c}$.

□