

## 1 Negligible functions

*Exercise 1.* Show that  $\alpha(n) = n^{\log n}$ , and  $\beta(n) = 2\sqrt{(n)}$  are negligible.

**Definition 1.** A function  $\gamma : \mathbf{N} \rightarrow [0, \infty)$  is noticeable if

$$\exists c, n_0 \forall n > n_0 \gamma(n) > \frac{1}{p(n)}.$$

*Exercise 2.* Are there functions  $\gamma : \mathbf{N} \rightarrow [0, \infty)$  that are not negligible and not noticeable?

## 2 One-way functions

A *one-way function* is a function that is easy to compute but “hard to invert”. Formally:

**Definition 2.** A function  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$  is one-way if it can be computed in polynomial-time, and for every probabilistic polynomial-time algorithm  $\mathcal{A}$  we have

$$P(f(x') = f(x) : x \leftarrow \{0, 1\}^n; x' \leftarrow \mathcal{A}(1^n, f(x)))$$

is negligible in  $n$ .

Note that we just require that it is hard to compute such  $x'$ , but we do not require that the entire  $x'$  is secret (whatever it could mean). An example of a “candidate for a one-way function” is:

$$f(p, q) = p \cdot q,$$

where  $p$  and  $q$  are primes of equal length (of course, this function is not defined on  $\{0, 1\}^*$ , but on pairs of primes, but let’s forget about this for now).

*Exercise 3.* Prove that if one-way functions exist then  $P \neq NP$  (and hence there is little hope for an unconditional proof that they exist).

*Exercise 4.* Let  $f$  be one-way. Which of the following functions are *always* one-way?

1.  $f_1(x) :=$  “the first half of  $f(x)$ ”,
2.  $f_2(x_1, x_2) := (f(x_1), x_2)$ , where  $|x_1| = |x_2|$ ,
3.  $f_3(x) := f(f(x))$ ,
4.  $f_5(x) := f(x) \oplus x$  (assume that  $|f(x)| = |x|$ , i.e. it is *length-preserving*).