General rules for solving exercises

- This is a theory course, which means: if an exercise does not explicitly say “you do not need to prove your answer” or “justify intuitively”, then a formal proof is always required.
- All exercises and their solutions, no matter whether they are graded or regular/optional ones, are part of the material relevant for the two exams.
- The tasks marked with the symbol $\star$ are more difficult than usual exercises, either because they require a non-standard idea or involve some non-trivial calculation. This is merely a help for you to decide which exercises you would like to spend how much of your time on. Note that all exercises and their solutions count as part of the material relevant for the two exams.

Exercise 1 - Average Case Performance

Prove: Let $W$ be a winner and $G$ a game. For $g$ a fixed instance of $G$ with $P^G(g) > 0$, let $p(g)$ denote the probability that at least one out of $k$ independent repetitions of $Wg$ outputs a winning bit 1. Then,

$$\Gamma^W(G) \leq \mathbb{E}[p(G)] \leq 1 - (1 - \Gamma^W(G))^k.$$ 

Exercise 2 - Distinguishers and Statistical Distance

(a) Prove Lemma 6.1 from the lecture notes.

(b) Let $X$ be a random variable taking values from a finite set $\mathcal{X}$ and let $U$ be a random variable distributed uniformly on $\mathcal{X}$. Define the distance of $X$ from uniform as $d(X) := \delta(X, U)$.

Furthermore, a quasi-group operation $\star$ on a set $\mathcal{X}$ is a function $\mathcal{X}^2 \to \mathcal{X}$ : $(a, b) \mapsto c = a \star b$ such that given any two of $a, b$ and $c$, the third value is uniquely determined.

Let $X$ and $Y$ be random variables over a finite set $\mathcal{X}$ and $\star$ a quasi-group operation on $\mathcal{X}$. Prove that

$$d(X \star Y) \leq 2d(X)d(Y).$$

(c) Show that in the setting of (b), if $|\mathcal{X}| = 2$, then equality holds, i.e.

$$d(X \star Y) = 2d(X)d(Y).$$

(d) Let $X_1, X_2, \ldots, X_n$ be independent binary random variables taking values from $\{0, 1\}$ (not necessarily identically distributed). Let, for any binary random variable taking values from $\{0, 1\}$,

$$b(X) := 2 \left( \Pr[X = 0] - \frac{1}{2} \right).$$

Use (b) and (c) to prove that

$$b(X_1 \oplus X_2 \oplus \ldots \oplus X_n) = \prod_{i=1}^{n} b(X_i).$$
Exercise 3 - One Way Functions

Let $\alpha, \beta, \epsilon, \epsilon' \in (0, 1)$ be fixed constants with $\epsilon > \epsilon'$. In this exercise, we presuppose that one-way functions exist and in particular that there exist one-way functions $f : \{0,1\}^n \rightarrow \{0,1\}^n$ (for all sufficiently large $n$) which are $\alpha$-weak (or $\beta$-weak) but not $\alpha-\epsilon'$-weak (or $\beta-\epsilon'$-weak). We also suppose that there exist one-way functions that satisfy these properties and are moreover bijective.

Under such assumptions, for each of the following three cases, give an example of an $\alpha$-weak one way function$^1$ $f : \{0,1\}^n \rightarrow \{0,1\}^n$ and a $\beta$-weak one way function $g : \{0,1\}^n \rightarrow \{0,1\}^n$ such that $h : \{0,1\}^n \rightarrow \{0,1\}^n$ is not a max{$\alpha, \beta$} $- \epsilon'$-weak one way function, where

(a) $h(x) := g(f(x))$,

(b) $h(x) := f(x) \oplus g(x)$, or

(c) $h(x_1||x_2) = f(x_1) \oplus g(x_2)$.

---

$^1$for the purpose of this exercise, in the definition of $\alpha$-weak one way function (Definition 6.3), let the term efficient be interpreted as polynomial time and the term negligible quantity as any quantity decreasing more quickly than the inverse of any polynomial.