

---

## Homework 1 – Due ~~Thursday, January 29 in class~~ Sunday, February 1 at midnight.

**Reminders:** Collaboration is permitted on homeworks, but you must (a) list your collaborators on the problem set and (b) **understand and write your solutions yourself**.

Clarity is an important component of the grade on your problem sets. Poorly explained solutions will not receive full marks, even if they are correct.

1. (**P and NP**) The 3-COLOR decision problem is to determine whether or not a graph given as input is 3-colorable (A graph is 3-colorable if you can color each of the vertices red, green, or blue, so that every edge has two different colors.) The  $k$ -COLOR problem is defined similarly, but you can use  $k$  colors.

(a) Prove that  $k$ -COLOR is in NP, for any constant  $k$ .

(b) 3-COLOR is known to be NP-complete.

Prove that 4-COLOR is NP-complete by giving a reduction from 3-COLOR to 4-COLOR. (Make sure you get the direction of the reduction right.)

(c) Prove that if  $P = NP$ , then pseudorandom generators do not exist. (*Hint:* Use the fact that circuit satisfiability can be solved in polynomial-time if  $P = NP$ .)

### 2. (Probability)

(a) Beatrice has  $n$  children, where  $n$  is even. (As above, each child is equally likely to be a boy or a girl, and that the gender of each child is independent of the genders of other children.) Consider the probability  $p_n$  that she has exactly  $n/3$  boys. One can write  $p_n = 2^{-cn \pm o(n)}$  for some constant  $c$ . What is  $c$ ? *Hint:* Use Stirling's approximation.

(b) You are given a hash function  $h$  which maps 200-bit inputs to 160 bit outputs, i.e.  $h : \{0, 1\}^{200} \rightarrow \{0, 1\}^{160}$ . Assume that the hash function is *balanced*, i.e. every output has the same number of pre-images.

Suppose that you sample  $k$  inputs  $x_1, \dots, x_k$  uniformly at random, without replacement, from  $\{0, 1\}^{200}$  and compute  $h(x_1), \dots, h(x_k)$ . The number of collisions among these sampled inputs is the number of pairs  $i, j$ ,  $i \neq j$  such that  $h(x_i) = h(x_j)$ . If  $k = 2^{80}$ , what is the expected number of collisions?

*Hint:* Define an indicator random variable  $I_{i,j}$  which is 1 if inputs  $i$  and  $j$  collide, and 0 otherwise. Compute the expectation of  $I_{i,j}$ , and use linearity of expectation to compute the expected number of collisions.

(see over.)

### 3. (Perfect Secrecy)

- (a) Katz-Lindell (KL), Exercise 2.5.
- (b) In class, we saw the following alternative definition of perfect secrecy: An encryption scheme  $(\text{Gen}, \text{Enc}, \text{Dec})$  *perfectly hides all functions of the message* if for every probability distribution over  $\mathcal{M}$ , for every function  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ , and for every algorithm  $\mathcal{A}$ , there exists an algorithm  $\mathcal{A}'$  such that

$$\Pr(\mathcal{A}(\text{Enc}(M)) = f(M)) = \Pr(\mathcal{A}'() = f(M)).$$

Prove that this definition is implied by perfect secrecy (KL, Definition 2.1).

*Hint:* The algorithm  $\mathcal{A}'$  may depend on the message distribution and  $\mathcal{A}$ .

- 4. **Extra credit:** Consider a symmetric encryption scheme with  $\mathcal{M} = \{0, 1\}^n$  and  $\mathcal{K} = \{0, 1\}^{n-1}$ . Show that if  $P = NP$ , then there is a polynomial-time adversary that can win the “message indistinguishability” game (Definition 2.4 in the KL book) with probability at least  $3/4$ .