

## Homework 3

Instructor: Anna Lysyanskaya

Due: Feb 14, 2007

**Problem 1: Statistical Indistinguishability**

In class we discussed statistical indistinguishability between two sets of faces M and F of equal size, where all faces were equally likely to be chosen.

Now consider a more general case. We have two possibly overlapping sets,  $S_{0,k}, S_{1,k} \subseteq \{0, 1\}^k$ . Let  $D_{0,k}$  be the distribution created by choosing each element  $\hat{x} \in S_{0,k}$  with probability  $P_{0,k}(\hat{x})$ . Let  $D_{1,k}$  be the distribution created by choosing each element  $\hat{x} \in S_{1,k}$  with probability  $P_{1,k}(\hat{x})$ .

Recall our definition of statistical indistinguishability: We first define the advantage of an algorithm Test:

$$\text{Adv}(\text{Test}) = |\Pr[x \leftarrow D_{k,0}; b \leftarrow \text{Test}(x) : b = 0] - \Pr[x \leftarrow D_{k,1}; b \leftarrow \text{Test}(x) : b = 0]|.$$

Two distributions  $D_{k,0}, D_{k,1}$  are statistically indistinguishable if for all algorithms Test, there exists negligible function  $\nu$  such that  $\text{Adv}(\text{Test}) = \nu(k)$ .

Intuitively, think of Test as an algorithm that gets an element  $x$  and tries to determine whether it was chosen from  $D_{0,k}$ , or  $D_{1,k}$ . If it thinks it came from  $D_{0,k}$ , it will output 0, and if it thinks it came from  $D_{1,k}$ , it will output 1. If it is just as likely (or within a negligible amount) to output 0 given an element chosen from the first distribution as it is given an element chosen from the second distribution, then that means it truly cannot tell the two distributions apart.

- Suppose we have a distinguisher Dave who knows everything about both distributions. In particular, he knows the probability of every element of each distribution. What is Dave's optimal strategy for distinguishing elements from these two sets (what is the best Test algorithm?).
- Let

$$\begin{aligned} \text{Adv}'(\text{Test}) = 1/2 & (|\Pr[x \leftarrow D_{0,k}; b \leftarrow \text{Test}(x) : b = 0] - \Pr[x \leftarrow D_{1,k}; b \leftarrow \text{Test}(x) : b = 0]| \\ & + |\Pr[x \leftarrow D_{0,k}; b \leftarrow \text{Test}(x) : b = 1] - \Pr[x \leftarrow D_{1,k}; b \leftarrow \text{Test}(x) : b = 1]|). \end{aligned}$$

Show that  $\text{Adv}(\text{Test})$  and  $\text{Adv}'(\text{Test})$  are equivalent.

- Now consider the following: We define the statistical distance between 2 sets as

$$\Delta(D_{0,k}, D_{1,k}) = 1/2 \sum_{\hat{x} \in (S_{1,k} \cup S_{0,k})} |\Pr[x \leftarrow D_{1,k} : x = \hat{x}] - \Pr[x \leftarrow D_{0,k} : x = \hat{x}]|$$

**Claim.**  $\Delta(D_{0,k}, D_{1,k}) = \nu(k)$  for  $\nu$  negligible  $\Leftrightarrow D_{1,k}$  and  $D_{0,k}$  are statistically indistinguishable.

Prove this claim (Hint: use the fact that in part a we found the best possible Test algorithm, and evaluate  $\text{Adv}'$  of that algorithm.)

## Problem 2: Notation Practice

For details on the experiment notation, see Handout 2 (posted on the class website).

- Recall the Shannon one-time pad cryptosystem: to encrypt length  $k$  message  $m$ , we choose a random secret key  $r \leftarrow \{0, 1\}^k$ , and produce the ciphertext  $c = m \oplus r$ . Let  $E(\hat{c})$  be the probability that when a random message is encrypted with a random key, the result is ciphertext  $\hat{c}$ . Represent  $E(\hat{c})$  using the experiment notation.
- Note that the following two probabilities are equivalent:

$$\Pr[\text{coin} \leftarrow \{\text{male}, \text{female}\}; \text{ if } \text{coin} = \text{male}, \text{face} \leftarrow M \\ \text{otherwise, face} \leftarrow F; \quad b \leftarrow \text{Test}(\text{face}) : b = 0 \mid \text{coin} = \text{male}]$$

and

$$\Pr[\text{face} \leftarrow M; b \leftarrow \text{Test}(\text{face}) : b = 0] \tag{1}$$

This shows how we can often remove a condition by changing our notation.

Recall HW1 problem b: we are given a machine which successfully distinguishes male and female faces with probability .7. We wish to build an algorithm for identifying the gender of CS concentrators, 80% of whom are male. We determined that the best algorithm is to run the machine on the given face, use its output if it succeeds, and output male if it fails. Represent the event that this algorithm succeeds using the experiment notation. Analyze the probability of this event, using the above technique whenever possible to simplify the notation.

## Problem 3: 2/3-Indistinguishability

For  $q \geq 1/2$ , let  $B_q$  denote the binary space where

$$\Pr[b \leftarrow B_q : b = 0] = q$$

(I.e.  $B_q$  outputs 0 with probability  $q$ , and 1 with probability  $1 - q$ .)

**Definition 1.** For  $q \geq 1/2$ , two families of sets of faces,  $M_k, F_k$  are  $q$ -indistinguishable if for all probabilistic poly-time tests  $\text{Test}$  there exists a negligible  $\nu(k)$  such that

$$\Pr[\text{coin} \leftarrow B_q; \text{ if } \text{coin} = 0, \text{face} \leftarrow M_k \\ \text{otherwise, face} \leftarrow F_k; \quad b \leftarrow \text{Test}(\text{face}) : b = \text{coin}] \leq q + \nu(k)$$

As mentioned in class, It turns out that for  $q > 1/2$ ,  $q$ -indistinguishability does not imply  $(1/2)$  indistinguishability. Here we prove this for  $q = 2/3$ .

We will construct a contrived pair of sets that is  $2/3$ -indistinguishable, but is not  $1/2$ -indistinguishable.

- Suppose we have 2 sets of faces, one of baby girls ( $F_k$ ), and one of baby boys ( $M_k$ ). Of course, given a picture of a baby's face, it is very hard to tell whether it is male or female. In fact, let's suppose that no algorithm  $\text{Test}$  can distinguish male and female baby faces with probability better than negligible  $\nu(k)$ . However, each face is also stored with an extra bit of information. Let  $g = 0$  for a male face and  $g = 1$  for a female face. When a face is added to the set, a random bit  $x \leftarrow B_{\frac{1}{2} + \frac{1}{k}}$  is chosen, and  $y = g \oplus x$  is computed. The face is now stored together with this bit  $y$ , so we have  $\text{face}' = (\text{face}, y)$ , and we now have two databases,  $M'_k$  and  $F'_k$  which include these pairs instead of just faces.

Prove that  $M'_k$  and  $F'_k$  are not  $1/2$ -indistinguishable. (I.e. describe an algorithm that takes a (face, bit) pair that is equally likely to have come from  $M'_k$  and from  $F'_k$ , and correctly guesses which set it came from with probability  $1/2 + \epsilon(k)$  for nonnegligible  $\epsilon$ .)

- b. Now we want to show that  $M'_k, F'_k$  constructed above are  $2/3$ -indistinguishable. Let  $\text{Test}$  be a distinguishing algorithm. Let  $p_T$  be its success probability. I.e.,

$$p_T = \Pr[\text{coin} \leftarrow B_{\frac{2}{3}}; \text{if } \text{coin} = 0, \text{face}' \leftarrow M'_k \\ \text{otherwise, face}' \leftarrow F'_k; b \leftarrow \text{Test}(\text{face}') : b = \text{coin}]$$

We wish to show that  $p_T \leq 2/3 + \nu(k)$  for some negligible  $\nu(k)$ .

Let us introduce further notation:

$$p_T^{(M, \hat{y})} = \Pr[(\text{face}, y) \leftarrow M'_k; b \leftarrow \text{Test}(\text{face}, y) : b = 0 \mid y = \hat{y}] \\ p_T^{(F, \hat{y})} = \Pr[(\text{face}, y) \leftarrow F'_k; b \leftarrow \text{Test}(\text{face}, y) : b = 1 \mid y = \hat{y}]$$

I.e.,  $p_T^{(M, \hat{y})}$  is the probability that  $\text{Test}$  produces the correct answer when the face is male and the appended bit is  $\hat{y}$ .

Assuming that the original sets  $F_k$  and  $M_k$  are  $1/2$ -indistinguishable, prove that for all probabilistic poly-time algorithms  $\text{Test}$ , for  $y \in \{0, 1\}$ , there exists a negligible  $\nu_y(k)$  such that  $|p_T^{(M, y)} - (1 - p_T^{(F, y)})| = \nu_y(k)$ .

(Hint: Recall the definition of indistinguishability that was presented in class:

**Definition 2.** Two distributions  $D_{k,0}, D_{k,1}$  are computationally indistinguishable if for all probabilistic polynomial algorithms  $\text{Test}$ , there exists negligible function  $\nu$  such that  $\text{Adv}(\text{Test}) = \nu(k)$ . (Where  $\text{Adv}$  is as defined in Problem 1).

Now try rewriting the advantage of  $T$  in terms of  $p_T^{(M, y)}$ , and  $p_T^{(F, y)}$ .)

- c. For a moment, imagine that  $\nu_0(k) = \nu_1(k) = 0$  (where  $\nu_0$  and  $\nu_1$  are as defined in part (b) relative to adversary  $\text{Test}$ ). So, substituting this into the equations we derived in part b, we get  $p_T^{(M, y)} = 1 - p_T^{(F, y)} = a_y$ . Show that in this case

$$p_T = \frac{1}{3} + \frac{a_0 + a_1}{6} + \frac{a_0 - a_1}{k}$$

(Hint: express  $p_T$  in terms of  $p_T^{(M,0)}, p_T^{(M,1)}, p_T^{(F,0)}, p_T^{(F,1)}$ .)

- d. Use the result of part c to prove that if  $\nu_0(k) = \nu_1(k) = 0$  and  $k \geq 6$ , then  $p_T \leq 2/3$ .
- e. Recompute parts c and d for the case when we allow  $\nu_0(k), \nu_1(k) \neq 0$  (but still require  $k \geq 6$ ), and find an upper bound for  $p_T$ . (Hint: now let  $a_y = p_T^{(M, y)} \leq 1 - p_T^{(F, y)} + \nu_y(k)$ .) Conclude that  $M'_k$  and  $F'_k$  are  $2/3$ -indistinguishable.