Ling Li, ling@cs.caltech.edu
January 26, 2001

10.1 Neither negligible nor nonnegligible?

A function $\nu : \mathcal{N} \to \mathcal{R}_{\geq 0}$ is negligible if $\forall c \in \mathcal{R}$, $\limsup \nu(n)/n^c = 0$. Thus, ν is not negligible if $\exists c \in \mathcal{R}$, there are infinity number of n such that $\nu(n)/n^c \geq 1$.

A function $\nu : \mathcal{N} \to \mathcal{R}_{\geq 0}$ is nonnegligible if $\exists c \in \mathcal{R}$, $\liminf \nu(n)/n^c > 0$. Thus, ν is not nonnegligible if $\forall c \in \mathcal{R}$, there are infinity number of n such that $\nu(n)/n^c < 1$. (I should say: ν is not nonnegligible if $\forall c \in \mathcal{R}$ and $\forall r > 0$, there are infinity number of n such that $\nu(n)/n^c < r$. However, if for $r < 1$ and $(c + \ln r)$, there are infinity number of n such that $\nu(n)/n^{c+\ln r} < 1$, we have for such $n \geq 3$,

$$\nu(n)/n^c < n^{\ln r} < e^{\ln r} = r,$$

i.e., there are infinity number of n such that $\nu(n)/n^c < r$. So, since we consider '$\forall c$', we can just consider this simpler situation that there are infinity number of n such that $\nu(n)/n^c < 1$.)

Define $\lceil \cdot \rceil_f : \mathcal{R} \to \mathcal{N}$ as the ceiling of factorial:

$$\lceil x \rceil_f = k!, \text{ if } (k-1)! < x \leq k!.$$

For example, $\lceil 6 \rceil_f = 6$ since $6 = 3!$; $\lceil 6.1 \rceil_f = 24$ since $3! < 6.1 \leq 4! = 24$. Easy to see that $\lceil \cdot \rceil_f$ is monotonic non-decreasing.

Consider $\nu(n) = 2^{-\lceil \log_2(n+1) \rceil_f}$. For $n = 2^{k!} - 1$ and $k \geq 2$, $\nu(n) = 2^{-k!}$. Thus for $c = -2$, $\nu(n)/n^c = 2^{-k!}(2^{k!} - 1)^2 > 2^{k!} - 2 > 1$. So, there are infinity number of n ($= 2^{k!} - 1$ for $k \geq 2$) such that $\nu(n)/n^c \geq 1$. So $\nu(n)$ is not negligible.

For any $c \in \mathcal{R}$, let $k_0 = \max\{\lceil -c \rceil, 1\}$. For any integer $k \geq k_0$ and $n = 2^{k!}$, $\lceil \log_2(n+1) \rceil_f = (k+1)!$, thus $\nu(n) = 2^{-(k+1)!} = n^{-k-1}$. So from $k \geq k_0 \geq -c$ and $n = 2^{k!} \geq 2$, we know

$$\nu(n)/n^c \leq n^{-k-1} \cdot n^k = n^{-1} < 1.$$

Thus $\nu(n)$ is not nonnegligible.

$\nu(n)$ is monotonic non-increasing, since $\log(\cdot)$ and $\lceil \cdot \rceil_f$ are both monotonic non-decreasing, and 2^{-x} is monotonic decreasing of x. So $\nu(n) = 2^{-\lceil \log_2(n+1) \rceil_f}$ is a monotonic non-increasing function that is neither negligible nor nonnegligible.

10.2 Alternate definition of SOF

For any $f : \{0,1\}^* \to \{0,1\}^*$ in SOF′, there exist positive constants c_1 and c_2 such that $|x|^{c_1} \le |f(x)| \le |x|^{c_2}$. Thus $|f(x)|^{1/c_2} \le |x| \le |f(x)|^{1/c_1}$. For any PPT A, we can design:

PPT Algorithm A': For input $f(x)$, compute $k_{\min} = \left\lceil |f(x)|^{1/c_2} \right\rceil$ and $k_{\max} = \left\lfloor |f(x)|^{1/c_1} \right\rfloor$. For integer $k' \in_U [k_{\min}, k_{\max}]$ (that is, k' is randomly selected from within $[k_{\min}, k_{\max}]$ with uniform probability), return $A(1^{k'}, f(x))$.

Since $f \in$ SOF′, there is a negligible function ν such that

$$P(f(A'(f(x))) = f(x) : x \in_U \{0,1\}^k) \le \nu(k).$$

Since $k_{\min} \ge |f(x)|^{1/c_2} \ge |x|^{c_1/c_2}$, and $k_{\max} \le |f(x)|^{1/c_1} \le |x|^{c_2/c_1}$, the number of integers within $[k_{\min}, k_{\max}]$ is at most $\left\lceil |x|^{c_2/c_1} - |x|^{c_1/c_2} + 1 \right\rceil$, and $|x|$ is one of such integers. Since in algorithm A', k' is selected with uniform distribution from all integers between $k_{\min}$ and $k_{\max}$, we have

$$P(f(A(1^k, f(x))) = f(x) : x \in_U \{0,1\}^k) \le \left\lceil k^{c_2/c_1} - k^{c_1/c_2} + 1 \right\rceil \nu(k).$$

$\nu(k)$ is a negligible function, so is $\left\lceil k^{c_2/c_1} - k^{c_1/c_2} + 1 \right\rceil \nu(k)$. Thus with the property (a) of an SOF′ function, we know that $f \in$ SOF. Thus SOF′ $\subseteq$ SOF.

For any $f \in$ SOF, we can modify it to $f'(x) = (1^{|x|}, 0, f(x))$.* That is, f'(x) first outputs $1^{|x|}$, then one 0, then $f(x)$. Since there is a PPT F such that $F(x) = f(x)$, then obviously there is a PPT $F'(x) = f'(x)$, since outputting $1^{|x|}$ and one 0 is of polynomial complex. And there is a positive constant $c \ge 2$ such that $|f(x)| \le |x|^c$ for $|x| \ge 2$. Thus†

$$|x|^1 < \left|f'(x)\right| \le |x|^c + |x| + 1 < |x|^{c+1}.$$

Since the first 0 in $f'(x)$'s output indicates the length of the prefix 1's, we have $f'(x) = f'(y) \Rightarrow (|x| = |y|) \wedge (f(x) = f(y))$. Thus for every PPT A,

$$P(f'(A(f'(x))) = f'(x) : x \in_U \{0,1\}^k) \le P(f(A(1^k, 0, f(x))) = f(x) : x \in_U \{0,1\}^k).$$

Using similar techniques used above, we can design a PPT A' such that A' first randomly inserts a 0 into the input (the 0 should be inserted after consecutive 1's; no other 0 is before the inserted one) and then calls A to get the output. The number of positions that one 0 can be inserted is less than $|f'(x)|$. Thus

$$P(f(A(1^k, 0, f(x))) = f(x) : x \in_U \{0,1\}^k) \le |x|^{c+1} P(f(A'(1^k, f(x))) = f(x) : x \in_U \{0,1\}^k).$$

For A', since $f \in$ SOF, we know there is a negligible function ν such that

$$P(f(A'(1^k, f(x))) = f(x) : x \in_U \{0,1\}^k) \le \nu(k).$$

Thus we get

$$P(f'(A(f'(x))) = f'(x) : x \in_U \{0,1\}^k) \le |x|^{c+1} \nu(k),$$

where $|x|^{c+1} \nu(k)$ is also a negligible function. So $f'(x) \in$ SOF′.

*Since when $|x| = 1 \Rightarrow |x|^c = 1$ for any c, we can specify $f'(x) = 0$ for $|x| = 1$. This will not destroy the whole proof since SOF or SOF′ only pay attention to input with sufficient large length.

†When $|x| \ge 2$, $c \ge 2$, we have $(|x|^c - 1)(|x| - 1) > 2$, i.e., $|x|^c + |x| + 1 < |x|^{c+1}$.

Ling Li, ling@cs.caltech.edu

10.3 Length-preserving SOF

Assume function $f \in$ SOF. We want to design a length-preserving strong one way function f' from f. First, give three functions and some of their properties:

Append: $\mathcal{C}(x,k)$, where $x \in \{0,1\}^*$ and $k > |x|$, appends x with one 0 and $1^{k-|x|-1}$. If $k = |x|+1$ then no 1's appended. For example, $\mathcal{C}(10,4) = 1001$ and $\mathcal{C}(01,7) = 0101111$. Thus $|\mathcal{C}(x,k)| = k$. Note that $k > |x|$ for $\mathcal{C}(x,k)$. That is, $\mathcal{C}(x,k)$ always appends some 'signature' x. Thus we have (similar to Problem 10.2) $\mathcal{C}(x,k) = \mathcal{C}(x',k') \Leftrightarrow (x = x') \wedge (k = k')$.

AppendR: $\mathcal{C}_R(x,k)$, where $x \in \{0,1\}^*$ and $k > |x|$, append random string of length $(k - |x|)$ to x.

Prefix: $\mathcal{E}(x,k)$, where $x \in \{0,1\}^*$ and $k \in \mathcal{N}$, returns the first k symbols of x. For example, $\mathcal{E}(1001,2) = 10$. It is easy to see $|\mathcal{E}(x,k)| = k$, and $\mathcal{E}(\mathcal{C}_R(x,k'),|x|) = x$.

Since $f \in$ SOF, there exist a constant $c \in \mathcal{N}$ such that $|f(x)| < |x|^c$. For any x with length n^c, we define $f'(x) = \mathcal{C}(f(\mathcal{E}(x,n)), n^c)$. Obviously, f' is length-preserving, and can be calculated in polynomial time. From the properties of append function $\mathcal{C}$, $f'(x) = f'(x') \Leftrightarrow |x| = |x'| \wedge f(\mathcal{E}(x,n)) = f(\mathcal{E}(x',n))$, where $n = |x|^{1/c}$.

For any PPT algorithm A' (that can invert f'), we can design another PPT algorithm (to invert f) $A[1^k, f(x)] = \mathcal{E}(A'[1^{k^c}, \mathcal{C}(f(x),k^c)], k)$, where $k = |x|$. We have

$$\begin{aligned}
P\left(f(A[1^k, f(x)]) = f(x)\right) &= P\left(f(\mathcal{E}(A'[1^{k^c}, \mathcal{C}(f(x),k^c)], k)) = f(\mathcal{E}(\mathcal{C}_R(x,k^c),k)\right) \\
&= P\left(f'(A'[1^{k^c}, \mathcal{C}(f(x),k^c)]) = f'(\mathcal{C}_R(x,k^c))\right) \\
&= P\left(f'(A'[1^{k^c}, f'(\mathcal{C}_R(x,k^c))]) = f'(\mathcal{C}_R(x,k^c))\right).
\end{aligned}$$

The randomness of $\mathcal{C}_R$ assures that

$$P\left(f(A[1^k, f(x)]) = f(x) : x \in_U \{0,1\}^k\right) = P\left(f'(A'[1^{k^c}, f'(x)]) = f'(x) : x \in_U \{0,1\}^{k^c}\right).$$

Thus, since $f \in$ SOF, there exists a negligible function ν such that

$$P\left(f(A[1^k, f(x)]) = f(x) : x \in_U \{0,1\}^k\right) \le \nu(k).$$

Then we have

$$P\left(f'(A'[1^{k^c}, f'(x)]) = f'(x) : x \in_U \{0,1\}^{k^c}\right) \le \nu(k^c),$$

and $\nu(k^c)$ is also a negligible function of k. So f' is a length-preserving strong one-way function.

10.4 BPP

(a) For such PPT A, we can design a PPT $A'(x)$ as:

> Let $K = 18\,|x|^{2b} \cdot t$, where $t = \max\left\{4\frac{2^b}{2^b-1}, 1\right\}$. Run A on x for K times. The number of times that $A(x) = 1$ is $S = \sum_{i=1}^{K} A_i(x)$ where $A_i(x)$ is the output of the i-th run of A. If $S \geq \frac{K}{3}$ then $A'(x) = 1$ otherwise $A'(x) = 0$.

For $x \in L$, $P(A(x) = 1) \geq \frac{1+|x|^{-b}}{3}$. Thus from the Chernoff bound,

$$\begin{aligned} P(A'(x) = 1) = 1 - P\left(S < \frac{K}{3}\right) &\geq 1 - P\left(S < K \cdot (P(A(x) = 1) - \frac{|x|^{-b}}{3})\right) \\ &\geq 1 - P\left(|S - K \cdot P(A(x) = 1)| > \frac{|x|^{-b}}{3} K\right) \\ &\geq 1 - 2e^{-\frac{|x|^{-2b}}{18} K} = 1 - 2e^{-t}. \end{aligned}$$

For $|x| \geq 2$, we have $\frac{4}{1-|x|^{-b}} = 4(1 + \frac{1}{|x|^b - 1}) \leq 4(1 + \frac{1}{2^b-1}) \leq t$. And for $t > 1$, te^{-t} is a decreasing function since $\frac{d(te^{-t})}{dt} = (1-t)e^{-t} < 0$. Thus $te^{-t} \leq e^{-1} < 1$. So we have $\frac{1-|x|^{-b}}{4} \geq \frac{1}{t} > e^{-t}$, or $1 - 2e^{-t} > \frac{1+|x|^{-b}}{2}$. So for $x \in L$, $P(A'(x) = 1) \geq \frac{1+|x|^{-b}}{2}$. (Note: we can not achieve so high a probability when $|x| = 1$, since $P(A(x) = 1) \geq \frac{2}{3}$ can not assure $P(A'(x) = 1) = 1$.)

For $x \notin L$, $P(A(x) = 1) \leq \frac{1-|x|^{-b}}{3}$. Thus from the Chernoff bound,

$$\begin{aligned} P(A'(x) = 1) = P\left(S \geq \frac{K}{3}\right) &\leq P\left(S \geq K \cdot (P(A(x) = 1) + \frac{|x|^{-b}}{3})\right) \\ &\leq P\left(|S - K \cdot P(A(x) = 1)| \geq \frac{|x|^{-b}}{3} K\right) \\ &\leq 2e^{-\frac{|x|^{-2b}}{18} K} = 2e^{-t}. \end{aligned}$$

Since we have proven that for $|x| \geq 2$, $1 - 2e^{-t} > \frac{1+|x|^{-b}}{2}$, we have for $x \notin L$, $P(A'(x) = 1) \leq \frac{1-|x|^{-b}}{2}$. (Note: For $|x| = 1$, this also holds since $P(A(x) = 1) \leq 0$.)

Since A is poly-time computable and K is a polynomial of $|x|$, we have A' is also a PPT.

(b) For such PPT A, we can design a PPT $A'(x)$ as:

> Let $K = 16\,|x|^{2b}$. Run A on x for K times. The number of times that $A(x) = 1$ is $S = \sum_{i=1}^{K} A_i(x)$ where $A_i(x)$ is the output of the i-th run of A. If $S \geq \frac{K}{2}$ then $A'(x) = 1$ otherwise $A'(x) = 0$.

For $x \in L$, $P(A(x)=1) \geq \frac{1+|x|^{-b}}{2}$. Thus from the Chernoff bound,

$$\begin{aligned} P(A'(x)=1) = 1 - P\left(S < \frac{K}{2}\right) &\geq 1 - P\left(S < K \cdot (P(A(x)=1) - \frac{|x|^{-b}}{2})\right) \\ &\geq 1 - P\left(|S - K \cdot P(A(x)=1)| > \frac{|x|^{-b}}{2}K\right) \\ &\geq 1 - 2e^{-\frac{|x|^{-2b}}{8}K} = 1 - 2e^{-2} > \frac{2}{3}. \end{aligned}$$

For $x \notin L$, $P(A(x)=1) \leq \frac{1-|x|^{-b}}{2}$. Thus from the Chernoff bound,

$$\begin{aligned} P(A'(x)=1) = P\left(S \geq \frac{K}{2}\right) &\leq P\left(S \geq K \cdot (P(A(x)=1) + \frac{|x|^{-b}}{2})\right) \\ &\leq P\left(|S - K \cdot P(A(x)=1)| \geq \frac{|x|^{-b}}{2}K\right) \\ &\leq 2e^{-\frac{|x|^{-2b}}{8}K} = 2e^{-2} < \frac{1}{3}. \end{aligned}$$

Since A is poly-time computable and K is a polynomial of $|x|$, we have A' is also a PPT. So $L \in \text{BPP}$.

(c) If $L \in \text{BPP}$, then there exists a PPT algorithm A such that for $x \in L$, $P(A(x)=1) \geq 2/3$ and for $x \notin L$, $P(A(x)=1) \leq 1/3$. Thus we can design a PPT $A'(x)$ as:

> Let $K = 72(|x|+1)$. Run A on x for K times. The number of times that $A(x)=1$ is $S = \sum_{i=1}^{K} A_i(x)$ where $A_i(x)$ is the output of the i-th run of A. If $S \geq \frac{K}{2}$ then $A'(x)=1$ otherwise $A'(x)=0$.

For $x \in L$, $P(A(x)=1) \geq \frac{2}{3}$. Thus from the Chernoff bound,

$$\begin{aligned} P(A'(x)=0) = P\left(S < \frac{K}{2}\right) &\leq P\left(S < K \cdot (P(A(x)=1) - \frac{1}{6})\right) \\ &\leq P\left(|S - K \cdot P(A(x)=1)| > \frac{K}{6}\right) \\ &\leq 2e^{-K/72} = \frac{2}{e}e^{-|x|} < e^{-|x|}. \end{aligned}$$

For $x \notin L$, $P(A(x)=1) \leq \frac{1}{3}$. Thus from the Chernoff bound,

$$\begin{aligned} P(A'(x)=1) = P(S \geq \frac{K}{2}) &\leq P\left(S \geq K \cdot (P(A(x)=1) + \frac{1}{6})\right) \\ &\leq P\left(|S - K \cdot P(A(x)=1)| \geq \frac{K}{6}\right) \\ &\leq 2e^{-K/72} < e^{-|x|}. \end{aligned}$$

Since A is poly-time computable and K is a polynomial of $|x|$, we have A' is also a PPT, and the probability of A' making an error is at most $e^{-|x|}$.

Ling Li, ling@cs.caltech.edu

10.5 SOP

(a) For f a SOP and π a PPT permutation, $\pi \circ f$ is also a PPT permutation, since both f and π are poly-time computable and are permutations. If $\pi \circ f$ is not a SOP, then there exists a PPT A with not negligible probability such that $\pi \circ f(A(\pi \circ f(x))) = \pi \circ f(x)$. We can design $A'(x) = A(\pi(x))$, which is a PPT since A and π are both PPT. Thus for $f(x)$, we have $\pi \circ f(A'(f(x))) = \pi \circ f(x)$ with not negligible probability. Since π is one-to-one, we have $f(A'(f(x))) = f(x)$ with not negligible probability, conflicting with that f is a SOF. So $\pi \circ f$ is also a SOP.

(b) (Collaborate with **Adam Granicz, Ke Yang**) Given a strong one way function f, we can design

$$f_1(x) = (0^{|f(x)|}, f(x)),$$

and

$$f_2(x) = f(\mathcal{E}(x, \left\lceil \frac{|x|}{2} \right\rceil)),$$

where $\mathcal{E}$ is the prefix function defined in Problem 10.3. It is obviously f_1 and f_2 are both one-way functions. However, $f_2 \circ f_1$ is a constant, i.e., $f_2(f_1(x)) = f(0^{|f(x)|})$ is not a one-way function.

Ling Li, ling@cs.caltech.edu

10.6 Poly-time distinguishable

If Q and R are poly-time distinguishable, there exists a PPT test T such that

$$|P_{x\leftarrow Q_n}(T(x)=1) - P_{x\leftarrow R_n}(T(x)=1)|$$

is a nonnegligible function. Let $P_Q^{(n)}$ denote $P_{x\leftarrow Q_n}(T(x)=1)$ and $P_R^{(n)}$ denote $P_{x\leftarrow R_n}(T(x)=1)$ for convenience. Thus $\exists c>0$, $\exists n_0 \in \mathcal{N}$ such that for $n \geq n_0$, $\left|P_Q^{(n)} - P_R^{(n)}\right| > n^{-c}$.

Design a statistical test T': 1. T' has access to random samples from Q and R; 2. T' calculates

$$S_q = \sum_{i=1}^{K} T(q_i), \quad S_r = \sum_{i=1}^{K} T(r_i),$$

and returns $T(x)$ if $S_q \geq S_r$, otherwise returns $1-T(x)$. Here q_i and r_i are samples from Q_n and R_n respectively, and $K = 12n^{3c}$.

- If for $n \geq n_0$, $P_Q^{(n)} - P_R^{(n)} \geq 0$, then $P_Q^{(n)} - P_R^{(n)} > n^{-c}$. Thus from the Chernoff bound,

$$\begin{aligned} P(S_q < S_r) &\leq P\left(S_q < K\cdot(P_Q^{(n)} - \frac{1}{2}n^{-c}) \vee S_r > K\cdot(P_R^{(n)} + \frac{1}{2}n^{-c})\right) \\ &\leq P\left(S_q < K\cdot(P_Q^{(n)} - \frac{1}{2}n^{-c})\right) + P\left(S_r > K\cdot(P_R^{(n)} + \frac{1}{2}n^{-c})\right) \\ &\leq P\left(\left|S_q - K\cdot P_Q^{(n)}\right| > \frac{K}{2}n^{-c}\right) + P\left(\left|S_r - K\cdot P_R^{(n)}\right| > \frac{K}{2}n^{-c}\right) \\ &\leq 4e^{-\frac{n^{-2c}}{4}K} = 4e^{-3n^c} < \frac{1}{4}n^{-c}. \end{aligned}$$

  The last inequality is due to $c>0 \Rightarrow 3n^c > 3 \Rightarrow 16n^c e^{-3n^c} < 16e^{-3} < 1$. So

$$P_{x\leftarrow Q_n}(T'(x)=1) \geq P(S_q \geq S_r)\cdot P_Q^{(n)} \geq \left(1 - \frac{1}{4}n^{-c}\right)P_Q^{(n)} \geq P_Q^{(n)} - \frac{1}{4}n^{-c},$$

  and

$$P_{x\leftarrow R_n}(T'(x)=1) = P(S_q \geq S_r)\cdot P_R^{(n)} + P(S_q < S_r)\cdot(1-P_R^{(n)}) \leq P_R^{(n)} + \frac{1}{4}n^{-c}.$$

  Thus

$$P_{x\leftarrow Q_n}(T'(x)=1) - P_{x\leftarrow R_n}(T'(x)=1) \geq P_Q^{(n)} - P_R^{(n)} - \frac{1}{2}n^{-c} \geq \frac{1}{2}n^{-c}.$$

- If for $n \geq n_0$, $P_Q^{(n)} - P_R^{(n)} < 0$, then $P_R^{(n)} - P_Q^{(n)} > n^{-c}$. Thus from the Chernoff bound,

$$\begin{aligned} P(S_q \geq S_r) &\leq P\left(S_q > K\cdot(P_Q^{(n)} + \frac{1}{2}n^{-c}) \vee S_r \leq K\cdot(P_R^{(n)} - \frac{1}{2}n^{-c})\right) \\ &\leq P\left(S_q > K\cdot(P_Q^{(n)} + \frac{1}{2}n^{-c})\right) + P\left(S_r \leq K\cdot(P_R^{(n)} - \frac{1}{2}n^{-c})\right) \\ &\leq P\left(\left|S_q - K\cdot P_Q^{(n)}\right| > \frac{K}{2}n^{-c}\right) + P\left(\left|S_r - K\cdot P_R^{(n)}\right| \geq \frac{K}{2}n^{-c}\right) \\ &\leq 4e^{-\frac{n^{-2c}}{4}K} = 4e^{-3n^c} < \frac{1}{4}n^{-c}. \end{aligned}$$

So

$$P_{x\leftarrow Q_n}(T'(x)=1) \geq P(S_q < S_r)\cdot(1-P_Q^{(n)}) \geq \left(1-\frac{1}{4}n^{-c}\right)(1-P_Q^{(n)}) \geq 1-P_Q^{(n)}-\frac{1}{4}n^{-c},$$

and

$$P_{x\leftarrow R_n}(T'(x)=1) = P(S_q < S_r)\cdot(1-P_R^{(n)}) + P(S_q \geq S_r)\cdot P_R^{(n)} \leq 1-P_R^{(n)}+\frac{1}{4}n^{-c}.$$

Thus

$$P_{x\leftarrow Q_n}(T'(x)=1) - P_{x\leftarrow R_n}(T'(x)=1) \geq P_R^{(n)} - P_Q^{(n)} - \frac{1}{2}n^{-c} \geq \frac{1}{2}n^{-c}.$$

Thus, for $n \geq n_0$, we always have $P_{x\leftarrow Q_n}(T'(x)=1) - P_{x\leftarrow R_n}(T'(x)=1) \geq \frac{1}{2}n^{-c}$, positive and nonnegligible.