In-Class September 9 2019

1 Pseudorandom Generators

2. Let $G : \{0,1\}^n \to \{0,1\}^{p(n)}$ be a pseudorandom generator with expansion factor $p(n) > 2n$. Namely, for any n, on input a seed of size n, G outputs a string of size $p(n)$. If G' is a pseudorandom generator, give a proof (by reduction); if not show an efficient distinguisher and its probability of success.

(a) $G'(s) \stackrel{def}{=} s||G(s)$ is NOT a PRG. Show a distinguisher. Let D be a distinguisher for G' with the following algorithm:

1. On input y, parse y as $y = y_1, \ldots, y_n, y_{n+1}, y_{p(n)+n}$.
2. Calculate $z = G(y_1, \ldots, y_n)$.
3. Return

$$D(y) = \begin{cases} 1 & \text{if } z = y_{n+1}, \ldots, y_{p(n)+n}, \\ 0 & \text{otherwise.} \end{cases}$$

Case Analysis:

1. If $y = y_1, \ldots, y_n, y_{n+1}, \ldots, y_{n+p(n)}$ is chosen uniformly at random, then for any $y_1, \ldots, y_n$ there is one possible string $y_{n+1}, \ldots, y_{n+p(n)}$ needs to be. The length of this string is $p(n)$, so the probability of occurrence is $2^{-p(n)}$.
$$Pr[D(y) = 1 | y \xleftarrow{R} \{0,1\}^{n+p(n)}] = 2^{-p(n)}.$$
2. If $y = G'(s)$ for some s, then $y = s||G(s)$.
$$Pr[D(y) = 1 | y = G'(s)] = 1.$$

Thus, the difference is

$$|Pr[D(y) = 1 | y \xleftarrow{R} \{0,1\}^{n+p(n)}] = 2^{-p(n)} - Pr[D(y) = 1 | y = G'(s)]| = 1 - 2^{-p(n)},$$

which is non-negligible.

(b) $G'(s) \stackrel{def}{=} f(G(f(s)))$, where $f(x)$ is a function that takes as input a string of size l (with $l > 1$) and outputs a string of size $l - 1$ with the least significant bit of x removed. (For inputs of length 1, you can ignore the fact that $G'(s)$ is not defined.)

Theorem. *If G is a PRG, then $G' \stackrel{def}{=} f(G(f(s)))$ is a PRG.*

Proof. Assume G' is not a PRG. Then there is a distinguisher D who distinguishes:

$$|Pr[D(y) = 1|y = G'(s) - Pr[D(y) = 1|y \leftarrow^{R} \{0,1\}^{p(n)}]]| = q(n),$$

where $q(n)$ is a non-negligible function.

Now, we will create a new distinguisher D' which will simulate D.

1. Given input y to D', $|y| = p(\ell)$. Remove the least significant bit of y to create $y' = y_1, \dots, y_{p(\ell)-1}$.
2. Give y' to D to distinguish.
3. Output $D(y')$. That is, output whatever D outputs on y' as the result for y.

Case Analysis:

1. If $y = G(x)$ for some seed x, then $y = G(f(s))$ where $s = x||b$. This is because x and $f(s)$ will have the same distribution.

   When D' removes the least significant bit of y, it is applying the function $y' = f(y)$ as defined above. Then $f(y) = f(G(x))$ for some random input $x \in \{0,1\}^n \implies f(y) = f(G(f(s)))$ for $s \in \{0,1\}^{n+1}$.

   $$y' = f(y) \implies f(y) = f(G(x)) \implies$$
   $$y = G(x) \implies y = G(f(s)) \text{ for some } s$$

   Because D' outputs the same as D:

   $$Pr[D(y') = 1|y' = G'(x)] = Pr[D(f(y)) = 1|y = G(f(s))] =$$
   $$Pr[D'(y) = 1|y = G(f(s))]$$

2. If $y \leftarrow^{r} \{0,1\}^{p(n)}$, then y' will also be random. Then because D' outputs the same as D:

   $$Pr[D(y') = 1|y' \leftarrow \{0,1\}^{p(n)-1}] = Pr[D(f(y)) = 1|y \leftarrow \{0,1\}^{p(n)}] =$$
   $$Pr[D'(y) = 1|y \leftarrow \{0,1\}^{p(n)}]$$

Thus, the difference is:

$$|Pr[D'(y) = 1|y = G(f(s))] - Pr[D'(y) = 1|y \leftarrow \{0,1\}^{p(n)}]| = q(n).$$

Since we assumed $q(n)$ was a non-negligible function, this means D' is a distinguisher for G that distinguishes with non-negligible probability. Since G is a PRG, this is a contradiction.

□