Derandomization (II)

Yijia Chen

Shanghai Jiao Tong University

November 18, 2012

Hardness

Worst-case hardness

Definition

Let $f : \{0,1\}^* \to \{0,1\}$ be a function. The *worst-case hardness* of f is defined by

$$H_{\mathrm{wrs}}(f)(n) := \max\Big\{S \in \mathbb{N} \;\Big|\; \text{every circuit } C \text{ of size at most } S \text{ fails to compute } f \text{ on some input in } \{0,1\}^n\Big\}$$

for every $n \in \mathbb{N}$.

Equivalently,

$$H_{\mathrm{wrs}}(f)(n) := \max\Big\{S \in \mathbb{N} \;\Big|\; \Pr_{x \in \{0,1\}^n}[C(x) = f(x)] < 1 \text{ for every circuit } C \text{ with } |C| \le S\Big\}$$

Definition

Let $f : \{0,1\}^* \to \{0,1\}$ be a function. The *average-case hardness* of f is defined by

$$H_{\mathrm{avg}}(f)(n) := \max\left\{ S \in \mathbb{N} \;\middle|\; \Pr_{x \in \{0,1\}^n}[C(x) = f(x)] < \frac{1}{2} + \frac{1}{S} \text{ for every circuit } C \text{ with } |C| \leq S \right\}$$

for every $n \in \mathbb{N}$.

Examples

1. If $f \in$ **BPP** then, since **BPP** $\subseteq$ **P/poly**, both $\mathsf{H}_{\mathsf{wrs}}(f)$ and $\mathsf{H}_{\mathsf{avg}}(f)$ are bounded by some polynomial.
2. It is conjectured that $3\textsc{Sat}$ has exponential worst-case hardness, i.e., $\mathsf{H}_{\mathsf{wrs}}(3\textsc{Sat}) \geq 2^{\omega(n)}$. On the other hand, $\mathsf{H}_{\mathsf{avg}}(3\textsc{Sat})$ is unclear.
3. If we trust the security of current cryptosystems, then we do believe that **NP** contains functions that are hard on the average.

Pseudorandom Generators

Theorem (Nisan and Wigderson, 1988)

For every time-constructible and nondecreasing function $S : \mathbb{N} \to \mathbb{N}$*, if there exists a Boolean function* $f \in \mathbf{DTIME}(2^{O(n)})$ *such that* $H_{\mathrm{avg}}(f) \geq S(n)$ *for every* $n \in \mathbb{N}$*, then there exists an* $S(\delta \cdot \ell)^{\delta}$*-pseudorandom generator for some constant* $\delta > 0$*.*

Corollary

If there exists a Boolean function $f \in \mathbf{E} = \mathbf{DTIME}(2^{O(n)})$ *and* $\varepsilon > 0$ *such that*

$$H_{\mathrm{avg}}(f) \geq 2^{\varepsilon \cdot n},$$

then there exists a $2^{\lceil \ell / a \rceil}$*-pseudorandom generator. Consequently,* $\mathbf{BPP} = \mathbf{P}$*.*

Yao's Theorem

Theorem (Yao, 1982)

Let Y be a distribution over $\{0,1\}^m$. Suppose that there exists an $S > 10 \cdot n$ and an $\varepsilon > 0$ such that for every circuit C of size at most $2 \cdot S$ and $i \in [m]$,

$$\Pr_{r \in_R Y} \left[C(r_1, \ldots, r_{i-1}) = r_i \right] \leq \frac{1}{2} + \frac{\varepsilon}{m}.$$

Then, Y is (S, ε)-pseudorandom.

Proof (1)

Let $i \in [0, m]$ and consider the distribution Y_i on $\{0, 1\}^m$ generated by the following process.

1. `Choose` $r_1, \ldots, r_m$ `according to the distribution` Y.
2. `Choose` $y_{i+1}, \ldots, y_m \in \{0, 1\}$ `independently and uniformly in random.`
3. `Output` $(r_1, \ldots, r_i, y_{i+1}, \ldots, y_m)$.

Observe that

$$Y_0 = U_m \quad \text{and} \quad Y_m = Y.$$

Proof (2)

Now assume that Y is not (S, ε)-pseudorandom, i.e., there exists a circuit D of size at most S such that

$$\left| \Pr[D(Y) = 1] - \Pr[D(U_m) = 1] \right| \geq \varepsilon.$$

We deduce

$$\begin{aligned}
&\sum_{i \in [m]} \left| \Pr[D(Y_i) = 1] - \Pr[D(Y_{i-1}) = 1] \right| \\
&\qquad \geq \left| \sum_{i \in [m]} \Pr[D(Y_i) = 1] - \Pr[D(Y_{i-1}) = 1] \right| \\
&\qquad = \left| \Pr[D(Y) = 1] - \Pr[D(U_m) = 1] \right| \geq \varepsilon.
\end{aligned}$$

Thus, there is a $k \in [m]$ with

$$\left| \Pr[D(Y_k) = 1] - \Pr[D(Y_{k-1}) = 1] \right| \geq \frac{\varepsilon}{m}.$$

Proof (3)

Without loss of generality we assume

$$\Pr[D(Y_k) = 1] - \Pr[D(Y_{k-1}) = 1] \geq \frac{\varepsilon}{m}.$$

Roughly, it says that r_k is more easy to satisfy D then y_k.

We consider the following randomized algorithm $\mathbb{C}(r_1, \ldots, r_{k-1})$

1. `Choose` $y_k, \ldots, y_m \in \{0, 1\}$ `independently and uniformly in random.`
2. `Simulate the circuit` D `on input` $(r_1, \ldots, r_{k-1}, y_k. \ldots, y_m)$.
3. `If the simulation outputs 1, then output` y_k, `otherwise` $1 - y_k$.

We want to calculate

$$\Pr\left[\mathbb{C}(r_1, \ldots, r_{k-1}) = r_k\right]$$

where the probability is taken over $(r_1, \ldots, r_{k-1}, r_k, \ldots, r_m) \in_R Y$ and the internal coin tosses of $\mathbb{C}$ (i.e., $y_k, \ldots, y_m$ in Line 1).

Proof (4)

Observe that the event E of $\mathbb{C}(r_1, \ldots, r_{k-1}) = r_k$ happens if and only if one of the following events happens:

(E_1) $D(r_1, \ldots, r_{k-1}, y_k, \ldots, y_m) = 1$ and $r_k = y_k$.

(E_2) $D(r_1, \ldots, r_{k-1}, y_k, \ldots, y_m) = 0$ and $r_k \neq y_k$.

Thus, $\Pr[E] = \Pr[E_1] + \Pr[E_2]$.

Then, we rewrite

$$
\begin{aligned}
\Pr[E_1] &= 1/2 \cdot \Pr\left[D(r_1, \ldots, r_{k-1}, y_k, \ldots, y_m) = 1 \;\middle|\; r_k = y_k\right] \\
&= 1/2 \cdot \Pr\left[D(r_1, \ldots, r_{k-1}, r_k, y_{k+1}, \ldots, y_m) = 1\right] \\
&= 1/2 \cdot \Pr\left[D(Y_k) = 1\right],
\end{aligned}
$$

and

$$
\begin{aligned}
\Pr[E_2] &= 1/2 \cdot \Pr\left[D(r_1, \ldots, r_{k-1}, y_k, \ldots, y_m) = 0 \;\middle|\; r_k \neq y_k\right] \\
&= 1/2 \cdot (1 - \Pr\left[D(r_1, \ldots, r_{k-1}, y_k, \ldots, y_m) = 1 \;\middle|\; r_k \neq y_k\right]).
\end{aligned}
$$

Proof (5)

On the other hand, we observe

$$\begin{aligned}
\Pr[D(Y_{k-1}) = 1] &= \Pr\left[D(r_1, \ldots, r_{k-1}, y_k, \ldots, y_m) = 1\right] \\
&= 1/2 \cdot \Pr\left[D(r_1, \ldots, r_{k-1}, y_k, \ldots, y_m) = 1 \;\middle|\; r_k = y_k\right] \\
&\quad + 1/2 \cdot \Pr\left[D(r_1, \ldots, r_{k-1}, y_k, \ldots, y_m) = 1 \;\middle|\; r_k \neq y_k\right] \\
&= \Pr[E_1] + 1/2 - \Pr[E_2].
\end{aligned}$$

Put all the pieces together:

$$\begin{aligned}
\Pr[E] &= \Pr[E_1] + \Pr[E_2] \\
&= 1/2 + 2 \cdot \Pr[E_1] - \Pr[D(Y_{k-1}) = 1] \\
&= 1/2 + \Pr[D(Y_k) = 1] - \Pr[D(Y_{k-1}) = 1] \geq 1/2 + \varepsilon/m.
\end{aligned}$$

Proof (6)

Now we know

$$\Pr\left[\mathbb{C}(r_1,\dots,r_{k-1}) = r_k\right] \geq \frac{1}{2} + \frac{\varepsilon}{m}.$$

Recall the randomized algorithm $\mathbb{C}$:

1. `Choose` $y_k,\dots,y_m \in \{0,1\}$ `independently and uniformly in random.`
2. `Simulate the circuit` D `on input` $(r_1,\dots,r_{k-1},y_k.\dots,y_m)$`.`
3. `If the simulation outputs 1, then output` y_k`, otherwise` $1-y_k$`.`

Thus there must exist some fixed $z_k,\dots,z_m \in \{0,1\}$ such that

$$\Pr[D(r_1,\dots,r_{k-1},z_k\dots,z_m) = r_k] \geq \frac{1}{2} + \frac{\varepsilon}{m}.$$

This is a contradiction, as $D(\_,\dots,\_,z_k,\dots,z_m)$ is a circuit of size at most $2 \cdot S$. □

Lemma (One-bit generator)

If there exists an $f \in \mathbf{E}$ *with* $H_{\text{avg}}(f) \geq n^4$*, then there is an* $(\ell + 1)$*-pseudorandom generator.*

Proof.

Let

$$G(z) = z \circ f(z).$$

By Yao's lemma, it suffices to show that there does not exist a circuit C of size $2 \cdot (\ell + 1)^3 < \ell^4$ and a number $i \in [\ell + 1]$ such that

$$\Pr_{r = G(U_\ell)} \left[C(r_1, \ldots, r_{i-1}) = r_i \right] > \frac{1}{2} + \frac{1}{10 \cdot (\ell + 1)}.$$

Assume $i = \ell + 1$, otherwise trivial.

$$\Pr_{z \in_R \{0,1\}^\ell} \left[C(z) = f(z) \right] > \frac{1}{2} + \frac{1}{10 \cdot (\ell + 1)} > \frac{1}{2} + \frac{1}{\ell^4},$$

which cannot hold under the assumption that $\mathrm{H}_{\text{avg}}(f) \geq n^4$. □

Second toy example

Lemma (Two-bit generator)

If there exists an $f \in \mathbf{E}$ with $H_{\text{avg}}(f) \geq n^4$, then there is an $(\ell + 2)$-pseudorandom generator.

Proof (1)

Let

$$G(z) = z_1 \dots z_{\lceil \ell/2 \rceil} \circ f(z_1, \dots, z_{\lceil \ell/2 \rceil}) \circ z_{\lceil \ell/2 \rceil + 1} \dots z_\ell \circ f(z_{\lceil \ell/2 \rceil}, \dots, z_\ell).$$

By Yao's lemma, it suffices to show that there does not exist a circuit C of size $2 \cdot (\ell + 2)^3$ and a number $i \in [\ell + 2]$ such that

$$\Pr_{r = G(U_\ell)} \left[C(r_1, \dots, r_{i-1}) = r_i \right] > \frac{1}{2} + \frac{1}{10 \cdot (\ell + 2)}.$$

Trivial for $i \neq \lceil \ell/2 + 1 \rceil$ and $i \neq \ell + 2$.

The case of $i = \lceil \ell/2 \rceil + 1$ is the same as the 1-bit case.

Proof (2)

Now consider $i = \ell + 2$ and assume

$$\Pr_{r \in_R \{0,1\}^{\lceil \ell/2 \rceil}, r' \in_R \{0,1\}^{\lfloor \ell/2 \rfloor}} \left[C(r \circ f(r) \circ r') = f(r') \right] > \frac{1}{2} + \frac{1}{10 \cdot (\ell + 2)}.$$

The Averaging Principle: If A is some event depending on two independent random variables X, Y, then there exists some x in the range of X such that

$$\Pr_Y [A(x, Y)] \geq \Pr_{X,Y} [A(X, Y)].$$

Thus for some fixed $r \in \{0, 1\}^{\lceil \ell/2 \rceil}$

$$\Pr_{r' \in_R \{0,1\}^{\lfloor \ell/2 \rfloor}} \left[C(r \circ f(r) \circ r') = f(r') \right] > \frac{1}{2} + \frac{1}{10 \cdot (\ell + 2)}.$$

Proof (3)

Let

$$D(r') \mapsto C(r \circ f(r) \circ r')$$

be a circuit of size

$$2 \cdot (\ell + 1)^3 + \lceil \ell/2 \rceil + 1 \leq (\ell/2)^4.$$

Hence,

$$\Pr_{r' \in_R \{0,1\}^{\lfloor \ell/2 \rfloor}} \left[D(r') = f(r') \right] > \frac{1}{2} + \frac{1}{10 \cdot (\ell + 2)} > \frac{1}{2} + \frac{1}{(\ell/2)^4},$$

contradicting the hardness of f. □

Thank you