Meta Complexity

Lecture 4

Ronald de Haan
me@ronalddehaan.eu

University of Amsterdam

June 3, 2025

What will we cover in this lecture?

- (Cryptographic and complexity-theoretic) pseudorandom generators
- Hardness amplification
- Derandomization

(Cryptographic) pseudorandom generators (PRGs)

Definition

Let $G : \{0,1\}^* \to \{0,1\}$ be a polynomial-time computable function. Let $\ell : \mathbb{N} \to \mathbb{N}$ be a polynomial-time computable function such that $\ell(n) > n$ for every n. Then G is a *secure pseudorandom generator of stretch* $\ell(n)$ if:

- $|G(x)| = \ell(|x|)$ for every $x \in \{0,1\}^*$; and
- for every probabilistic polynomial-time algorithm A there exists a negligible function $\epsilon : \mathbb{N} \to [0,1]$ such that for every $n \in \mathbb{N}$:

$$\left|\Pr[A(G(U_n)) = 1] - \Pr[A(U_{\ell(n)}) = 1\right| < \epsilon(n)$$

(here U_n denotes the uniform distribution over $\{0,1\}^n$).

Theorem (Haastad, Impagliazzo, Levin, Luby 1999)

If OWFs exist, then for every $c \in \mathbb{N}$,
there exists a secure pseudorandom generator with stretch $\ell(n) = n^c$.

(Complexity-theoretic) pseudorandom generators (PRGs)

Definition

A distribution R over $\{0,1\}^m$ is (S,ϵ)-pseudorandom (for $S \in \mathbb{N}, \epsilon > 0$) if for every circuit C of size at most S:

$$|\Pr[C(R) = 1] - \Pr[C(U_m) = 1]| < \epsilon.$$

Definition

Let $S : \mathbb{N} \to \mathbb{N}$ be some function. A 2^n-time computable function $G : \{0,1\}^* \to \{0,1\}^*$ is an $S(\ell)$-*pseudorandom generator* if:

- $|G(z)| = S(|z|)$ for every $z \in \{0,1\}^*$; and
- for every $\ell \in \mathbb{N}$ the distribution $G(U_\ell)$ is $(S(\ell)^3, 1/10)$-pseudorandom.

Derandomization using PRGs

- Suppose that there exists an $S(\ell)$-pseudorandom generator for a time-constructible nondecreasing $S : \mathbb{N} \to \mathbb{N}$.

  Then for every polynomial-time computable function $\ell : \mathbb{N} \to \mathbb{N}$ it holds that $\mathsf{BPTIME}(S(\ell(n))) \subseteq \mathsf{DTIME}(2^{c\ell(n)})$ for some constant c.

- In particular, if there exists a $2^{\epsilon\ell}$-pseudorandom generator for some constant $\epsilon > 0$, then $\mathsf{BPP} = \mathsf{P}$.

Worst-case and average-case hardness (repeated)

Definition

For $f : \{0,1\}^n \to \{0,1\}$ and $\rho \in [0,1]$ we define the *ρ-average-case hardness of f*, denoted $\mathrm{H}^{\rho}_{\mathrm{avg}}(f)$, to be the largest S such that for every circuit of size S:

$$\mathop{\mathbb{P}}_{x \in_R \{0,1\}^n}[C(x) = f(x)] < \rho.$$

We define the *worst-case hardness of f*, denoted $\mathrm{H}_{\mathrm{wrs}}(f)$, to equal $\mathrm{H}^{1}_{\mathrm{avg}}(f)$.

We define the *average-case hardness of f*, denoted $\mathrm{H}_{\mathrm{avg}}(f)$, to equal:

$$\max\left\{S : \mathrm{H}^{1/2+1/S}_{\mathrm{avg}}(f) \geq S\right\}.$$

Hardness amplification

- Let $f \in \mathsf{E}$ be such that $\mathrm{H}_{\mathrm{wrs}}(f)(n) \geq S(n)$ for some time-constructible nondecreasing function $S : \mathbb{N} \to \mathbb{N}$.

  Then there exists a function $g \in E$ and a constant $c > 0$ such that $\mathrm{H}_{\mathrm{avg}}(g)(n) \geq S(n/c)^{1/c}$ for sufficiently large n.

PRGs from average-case hardness

- Let $S : \mathbb{N} \to \mathbb{N}$ be time-constructible and nondecreasing.

  If there exists $f \in \mathsf{E}$ such that $\mathrm{H}_{\mathrm{avg}}(f)(n) \geq S(n)$ for every n,
  then there exists an $S(\delta\ell)^{\delta}$-pseudorandom generator for some constant $\delta > 0$.

Derandomization under worst-case assumptions

- Let $S : \mathbb{N} \to \mathbb{N}$ be time-constructible and nondecreasing.

  If there exists $f \in \mathsf{E}$ such that $\mathsf{H}_{\mathsf{wrs}}(f)(n) \geq S(n)$ for every n,
  then there exists an $S(\delta\ell)^{\delta}$-pseudorandom generator for some constant $\delta > 0$.

- In particular, if there exists $f \in \mathsf{E}$ and $\epsilon > 0$ such that $\mathsf{H}_{\mathsf{wrs}}(f)(n) \geq 2^{\epsilon n}$ for every n, then $\mathsf{BPP} = \mathsf{P}$.

Summary

- (Cryptographic and complexity-theoretic) pseudorandom generators
- Hardness amplification
- Derandomization