Lecture 11
Hardness vs Randomness

Rafael Oliveira
rafael.oliveira.teaching@gmail.com
University of Waterloo

CS 860 - Graduate Complexity Theory
Fall 2022

Overview

- Nisan-Wigderson (NW) Generators

Pseudorandom Generators

Definition 1 (Pseudorandom Distributions)

A distribution R over $\{0,1\}^m$ is (s,ε)-pseudorandom if for every circuit C such that $S(C) \leq s$

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

where U_m is the uniform distribution over $\{0,1\}^m$.

Pseudorandom Generators

Definition 1 (Pseudorandom Distributions)

A distribution R over $\{0,1\}^m$ is (s, ε)-pseudorandom if for every circuit C such that $S(C) \leq s$

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

where U_m is the uniform distribution over $\{0,1\}^m$.

- We say that $G : \{0,1\}^\ell \to \{0,1\}^m$ is (s, ε)-pseudorandom if the distribution $G(U_\ell)$ is (s, ε)-pseudorandom.

Constructing PRGs

- It seems to be very hard to construct PRGs unconditionally
- Today: one can use hard boolean functions to construct PRGs
- Idea:
  1. unpredictability equivalent to pseudorandomness (**[Yao 1982]**)
  2. a hard function should be hard to predict

Nisan-Wigderson PRG

Definition 2 (Average-Case Hardness)

Given $f : \{0,1\}^n \to \{0,1\}$, its average-case hardness, denoted by $H(f)$, is the smallest $s \in \mathbb{N}$ such that

$$\forall C \text{ circuit } \text{ s.t. } S(C) \leq s \Rightarrow \Pr_x[C(x) = f(x)] \leq 1/2 + 1/s$$

Nisan-Wigderson PRG

Definition 2 (Average-Case Hardness)

Given $f : \{0,1\}^n \to \{0,1\}$, its average-case hardness, denoted by $H(f)$, is the smallest $s \in \mathbb{N}$ such that

$$\forall C \text{ circuit } \text{ s.t. } S(C) \leq s \Rightarrow \Pr_x[C(x) = f(x)] \leq 1/2 + 1/s$$

Theorem 3 (Special case of **[NW 1994]**)

If there is $L \in E$ and $\delta > 0$ such that for all sufficiently large n, $H(L_n) \geq 2^{\delta n}$, then there is constant $c > 0$ and family of PRGs $G_m : \{0,1\}^{c \log m} \to \{0,1\}^m$ which are computable in poly(m) *time and are $(2m, 1/8)$-pseudorandom.*

Nisan-Wigderson PRG

Definition 2 (Average-Case Hardness)

Given $f : \{0,1\}^n \to \{0,1\}$, its average-case hardness, denoted by $H(f)$, is the smallest $s \in \mathbb{N}$ such that

$$\forall C \text{ circuit s.t. } S(C) \leq s \Rightarrow \Pr_x[C(x) = f(x)] \leq 1/2 + 1/s$$

Theorem 3 (Special case of **[NW 1994]**)

If there is $L \in$ E and $\delta > 0$ such that for all sufficiently large n, $H(L_n) \geq 2^{\delta n}$, then there is constant $c > 0$ and family of PRGs $G_m : \{0,1\}^{c \log m} \to \{0,1\}^m$ which are computable in poly(m) *time and are $(2m, 1/8)$-pseudorandom.*

- In particular, the above implies P $=$ BPP.

Combinatorial designs

Definition 4 (Combinatorial designs)

Given integers $t > \ell > d > 0$, the family $\{S_1, \ldots, S_m\}$ of subsets of $[t]$ is a (t, ℓ, d)-design if

1. $|S_i| = \ell$ for all $i \in [m]$
2. $|S_i \cap S_j| \leq d$ for all $i \neq j$

Combinatorial designs

Definition 4 (Combinatorial designs)

Given integers $t > \ell > d > 0$, the family $\{S_1, \ldots, S_m\}$ of subsets of $[t]$ is a (t, ℓ, d)-design if

1. $|S_i| = \ell$ for all $i \in [m]$
2. $|S_i \cap S_j| \leq d$ for all $i \neq j$

Proposition 5

For every $\ell \in \mathbb{N}^*$ and $\gamma \in (0, 1)$, there is $t = O(\gamma^{-1}\ell)$ such that a $(t, \ell, \gamma\ell)$-design $\{S_1, \ldots, S_m\}$, where $m := 2^{\gamma\ell}$, can be constructed in $O(2^t \cdot tm^2)$ time.

NW generators: construction

- Notation: if $x \in \{0,1\}^t$ and $S \subseteq [t]$, let $x_S \in \{0,1\}^{|S|}$ be the string obtained by selecting the bits of S (in order) from x

Definition 6 (NW generators)

For a boolean function $f : \{0,1\}^\ell \to \{0,1\}$ and a design $\mathcal{S} := \{S_1, \ldots, S_m\}$ over $[t]$, the NW-generator is given by

$$NW_{f,\mathcal{S}}(x) := f_1(x) \circ \cdots \circ f_m(x)$$

where $f_i(x) := f(x_{S_i})$

Proof of Pseudorandomness

Follows from the following lemma:

Lemma 7

Let t, ℓ, γ as in Proposition 5 and $m := 2^{\gamma\ell}$. If $f : \{0,1\}^\ell \to \{0,1\}$ and $\mathcal{S} := \{S_1, \ldots, S_m\}$ be a $(t, \ell, \log m)$-design over $[t]$.
If $D : \{0,1\}^m \to \{0,1\}$ is s.t.

$$|\Pr_r[D(r) = 1] - \Pr_x[D(NW_{f,\mathcal{S}}(x)) = 1]| > \varepsilon$$

then there is a circuit C with $S(C) = O(m^2)$ s.t.

$$|\Pr_x[D(C(x)) = f(x)] - 1/2| > \varepsilon/m.$$

Proof of Pseudorandomness

Follows from the following lemma:

Lemma 7

Let t, ℓ, γ *as in Proposition 5 and* $m := 2^{\gamma\ell}$. *If* $f : \{0,1\}^\ell \to \{0,1\}$ *and* $\mathcal{S} := \{S_1, \ldots, S_m\}$ *be a* $(t, \ell, \log m)$*-design over* $[t]$.
If $D : \{0,1\}^m \to \{0,1\}$ *is s.t.*

$$|\Pr_r[D(r) = 1] - \Pr_x[D(NW_{f,\mathcal{S}}(x)) = 1]| > \varepsilon$$

then there is a circuit C *with* $S(C) = O(m^2)$ *s.t.*

$$|\Pr_x[D(C(x)) = f(x)] - 1/2| > \varepsilon/m.$$

- Above lemma shows that a distinguisher for the generator yields a distinguisher for f

Proof of Lemma 7

Main idea: if D distinguishes $NW_{f,\mathcal{S}}$ from uniform, then can find a bit of output of $NW_{f,\mathcal{S}}$ where we can notice this difference. From this bit, we can non-trivially predict f.

Main tool: hybrid argument.

Proof of Lemma 7

Main idea: if D distinguishes $NW_{f,\mathcal{S}}$ from uniform, then can find a bit of output of $NW_{f,\mathcal{S}}$ where we can notice this difference. From this bit, we can non-trivially predict f.

Main tool: hybrid argument.

Define distributions $H_0, \ldots, H_m$ over $\{0,1\}^m$ as follows:

- Sample $u \sim U_m$ and $v \sim NW_{f,\mathcal{S}}(U_t)$
- H_i given by $v_{[i]} \circ u_{[m]\setminus[i]}$

Proof of Lemma 7

Main idea: if D distinguishes $NW_{f,\mathcal{S}}$ from uniform, then can find a bit of output of $NW_{f,\mathcal{S}}$ where we can notice this difference. From this bit, we can non-trivially predict f.

Main tool: hybrid argument.

Define distributions $H_0, \ldots, H_m$ over $\{0,1\}^m$ as follows:

- Sample $u \sim U_m$ and $v \sim NW_{f,\mathcal{S}}(U_t)$
- H_i given by $v_{[i]} \circ u_{[m] \setminus [i]}$
- $H_0 = U_m$ and $H_m = NW_{f,\mathcal{S}}(U_t)$

Proof of Lemma 7

Main idea: if D distinguishes $NW_{f,\mathcal{S}}$ from uniform, then can find a bit of output of $NW_{f,\mathcal{S}}$ where we can notice this difference. From this bit, we can non-trivially predict f.

Main tool: hybrid argument.

Define distributions $H_0, \ldots, H_m$ over $\{0,1\}^m$ as follows:

- Sample $u \sim U_m$ and $v \sim NW_{f,\mathcal{S}}(U_t)$
- H_i given by $v_{[i]} \circ u_{[m]\setminus[i]}$
- $H_0 = U_m$ and $H_m = NW_{f,\mathcal{S}}(U_t)$

By hypothesis of lemma, there is $b_0 \in \{0,1\}$ s.t.

$$\Pr_x[D'(NW_{f,\mathcal{S}}(x)) = 1] - \Pr_r[D'(r) = 1] > \varepsilon$$

where $D'(x) = b_0 \oplus D(x)$.

Proof of Lemma 7

- Note

$$
\begin{aligned}
\varepsilon &< \Pr_x[D'(NW_{f,\mathcal{S}}(x)) = 1] - \Pr_r[D'(r) = 1] \\
&= \Pr[D'(H_m) = 1] - \Pr[D'(H_0) = 1] \\
&= \sum_{i=1}^{m} (\Pr[D'(H_i) = 1] - \Pr[D'(H_{i-1}) = 1])
\end{aligned}
$$

Proof of Lemma 7

- Note

$$\begin{aligned}\varepsilon &< \Pr_x[D'(NW_{f,\mathcal{S}}(x)) = 1] - \Pr_r[D'(r) = 1] \\ &= \Pr[D'(H_m) = 1] - \Pr[D'(H_0) = 1] \\ &= \sum_{i=1}^{m}(\Pr[D'(H_i) = 1] - \Pr[D'(H_{i-1}) = 1])\end{aligned}$$

- There is $i \in [m]$ such that

$$\Pr[D'(H_i) = 1] - \Pr[D'(H_{i-1}) = 1] > \varepsilon/m$$

Proof of Lemma 7

- Note

$$\begin{aligned}\varepsilon &< \Pr_x[D'(NW_{f,\mathcal{S}}(x)) = 1] - \Pr_r[D'(r) = 1] \\ &= \Pr[D'(H_m) = 1] - \Pr[D'(H_0) = 1] \\ &= \sum_{i=1}^{m} (\Pr[D'(H_i) = 1] - \Pr[D'(H_{i-1}) = 1])\end{aligned}$$

- There is $i \in [m]$ such that

$$\Pr[D'(H_i) = 1] - \Pr[D'(H_{i-1}) = 1] > \varepsilon/m$$

- Assume $S_i = [\ell]$ and let $\{0,1\}^t = \{0,1\}^\ell \times \{0,1\}^{t-\ell}$ s.t. $x = (y, z)$

Proof of Lemma 7

- Note

$$\begin{aligned}\varepsilon &< \Pr_x[D'(NW_{f,\mathcal{S}}(x)) = 1] - \Pr_r[D'(r) = 1] \\ &= \Pr[D'(H_m) = 1] - \Pr[D'(H_0) = 1] \\ &= \sum_{i=1}^{m} (\Pr[D'(H_i) = 1] - \Pr[D'(H_{i-1}) = 1])\end{aligned}$$

- There is $i \in [m]$ such that

$$\Pr[D'(H_i) = 1] - \Pr[D'(H_{i-1}) = 1] > \varepsilon/m$$

- Assume $S_i = [\ell]$ and let $\{0,1\}^t = \{0,1\}^\ell \times \{0,1\}^{t-\ell}$ s.t. $x = (y, z)$
- Above inequality $\Rightarrow$ good distinguisher for $f : \{0,1\}^\ell \to \{0,1\}$

Distinguisher for f

Consider following algorithm A:

- **Input**: $y \in \{0,1\}^\ell$
- **Output**: $b \in \{0,1\}$ (guess for $f(y)$)

Distinguisher for f

Consider following algorithm A:

- **Input**: $y \in \{0,1\}^\ell$
- **Output**: $b \in \{0,1\}$ (guess for $f(y)$)

1. pick random $z \in \{0,1\}^{t-\ell}$ and $r \in \{0,1\}^{m-i+1}$
2. compute $f_1(x), \ldots, f_{i-1}(x)$ ($x = (y,z)$, $f_i(x) := f(x_{S_i})$)

Distinguisher for f

Consider following algorithm A:

- **Input**: $y \in \{0,1\}^\ell$
- **Output**: $b \in \{0,1\}$ (guess for $f(y)$)

1. pick random $z \in \{0,1\}^{t-\ell}$ and $r \in \{0,1\}^{m-i+1}$
2. compute $f_1(x), \ldots, f_{i-1}(x)$ ($x = (y,z)$, $f_i(x) := f(x_{S_i})$)
3. If $D'(f_1(x), \ldots, f_{i-1}(x), r_i, \ldots, r_m) = 1$, output r_i.
   Else, output $1 - r_i$.

Distinguisher for f

Consider following algorithm A:

- **Input**: $y \in \{0,1\}^\ell$
- **Output**: $b \in \{0,1\}$ (guess for $f(y)$)

1. pick random $z \in \{0,1\}^{t-\ell}$ and $r \in \{0,1\}^{m-i+1}$
2. compute $f_1(x), \ldots, f_{i-1}(x)$ $\quad (x = (y,z),\ f_i(x) := f(x_{S_i}))$
3. If $D'(f_1(x), \ldots, f_{i-1}(x), r_i, \ldots, r_m) = 1$, output r_i.
   Else, output $1 - r_i$.

Claim: $\Pr_{y,z,r}[A(y) = f(y)] > 1/2 + \varepsilon/m$

Same proof as last lecture's.

Distinguisher for f

Consider following algorithm A:

- **Input**: $y \in \{0,1\}^\ell$
- **Output**: $b \in \{0,1\}$ (guess for $f(y)$)

1. pick random $z \in \{0,1\}^{t-\ell}$ and $r \in \{0,1\}^{m-i+1}$
2. compute $f_1(x), \ldots, f_{i-1}(x)$ $(x = (y,z),\ f_i(x) := f(x_{S_i}))$
3. If $D'(f_1(x), \ldots, f_{i-1}(x), r_i, \ldots, r_m) = 1$, output r_i.
   Else, output $1 - r_i$.

Claim: $\Pr_{y,z,r}[A(y) = f(y)] > 1/2 + \varepsilon/m$

Same proof as last lecture's.

By averaging, there are fixed z, r such that A when given z, r approximates f well.

Efficiency of A

- Seems like we computed f many times to try to compute f!

  Design property!

Efficiency of A

- Seems like we computed f many times to try to compute f!
- By design property, $i \neq j \Rightarrow |S_i \cap S_j| \leq \log m$.
  $f_j(y, z) = f_j(x) = f(x_{S_j})$ depends on $\leq \log m$ bits of y!

Efficiency of A

- Seems like we computed f many times to try to compute f!
- By design property, $i \neq j \Rightarrow |S_i \cap S_j| \leq \log m$.
  $f_j(y,z) = f_j(x) = f(x_{S_j})$ depends on $\leq \log m$ bits of y!
- Since we have fixed z, r

  $$f_j \text{ computed by circuit of size } O(m)$$

  So all m bits can be computed by a $O(m^2)$ sized circuit!

Proof of Theorem 3

- Let $f_\ell : \{0,1\}^\ell \to \{0,1\}$ be given by $f(x) := L_\ell(x)$.
- Let $G_m := NW_{f,\mathcal{S}}$ with the parameters ℓ, γ, t and $m = 2^{\gamma\ell}$ from Proposition 5 (design)

Proof of Theorem 3

- Let $f_\ell : \{0,1\}^\ell \to \{0,1\}$ be given by $f(x) := L_\ell(x)$.
- Let $G_m := NW_{f,\mathcal{S}}$ with the parameters ℓ, γ, t and $m = 2^{\gamma\ell}$ from Proposition 5 (design)
- By Definition 1, G_m is not $(2m, 1/8)$-pseudorandom $\Rightarrow$ exists cicuit D with $S(D) \leq 2m$ s.t.

$$|\Pr[D(G_m(U_\ell)) = 1] - \Pr[D(U_m) = 1]| < 1/8$$

Proof of Theorem 3

- Let $f_\ell : \{0,1\}^\ell \to \{0,1\}$ be given by $f(x) := L_\ell(x)$.
- Let $G_m := NW_{f,\mathcal{S}}$ with the parameters ℓ, γ, t and $m = 2^{\gamma\ell}$ from Proposition 5 (design)
- By Definition 1, G_m is not $(2m, 1/8)$-pseudorandom $\Rightarrow$ exists cicuit D with $S(D) \leq 2m$ s.t.

$$|\Pr[D(G_m(U_\ell)) = 1] - \Pr[D(U_m) = 1]| < 1/8$$

- By Lemma 7, there is circuit Φ of size $O(m^2)$ such that

$$\Pr_x[\Phi(x) = f(x)] > 1/2 + 1/8m = 1/2 + 2^{-\gamma\ell-3}$$

which contradicts $H(L_\ell) \geq 2^{\delta\ell}$ when $\gamma < \delta/3$

Construction of combinatorial designs

- Take p to be a prime number and consider $\mathbb{F}_p$ finite field with p elements. Let $t = p^2$.
- Take all polynomials of degree $\leq d = \gamma\ell$ in $\mathbb{F}_p[z]$

Construction of combinatorial designs

- Take p to be a prime number and consider $\mathbb{F}_p$ finite field with p elements. Let $t = p^2$.
- Take all polynomials of degree $\leq d = \gamma\ell$ in $\mathbb{F}_p[z]$
- For each polynomial $q(z) \in \mathbb{F}_p[z]$, let

$$S_q := \{(i, q(i)) \mid i \in [\ell]\}$$

Construction of combinatorial designs

- Take p to be a prime number and consider $\mathbb{F}_p$ finite field with p elements. Let $t = p^2$.
- Take all polynomials of degree $\leq d = \gamma\ell$ in $\mathbb{F}_p[z]$
- For each polynomial $q(z) \in \mathbb{F}_p[z]$, let

$$S_q := \{(i, q(i)) \mid i \in [\ell]\}$$

- Note that if $f \not\equiv g$ then $|S_f \cap S_g| \leq d$

Construction of combinatorial designs

- Take p to be a prime number and consider $\mathbb{F}_p$ finite field with p elements. Let $t = p^2$.
- Take all polynomials of degree $\leq d = \gamma\ell$ in $\mathbb{F}_p[z]$
- For each polynomial $q(z) \in \mathbb{F}_p[z]$, let

$$S_q := \{(i, q(i)) \mid i \in [\ell]\}$$

- Note that if $f \not\equiv g$ then $|S_f \cap S_g| \leq d$
- There are p^{d+1} polynomials of degree $\leq d$

References I

Arora, Sanjeev and Barak, Boaz (2009)
Computational Complexity, A Modern Approach — Chapter 20
Cambridge University Press

Papadimitriou, C (1994)
Computational Complexity
Addison-Wesley

Trevisan, Luca (2002)
Lecture notes — Lectures 23, 24
See webpage

Goldreich, Oded (2006)
Computational complexity: a conceptual perspective. — Chapter 6
https://www.wisdom.weizmann.ac.il/~oded/cc-drafts.html

References II

Babai, L and Fortnow, L and Nisan, N and Wigderson, A (1993)
BPP has subexponential time simulations unless EXPTIME has publishable proofs
Computational Complexity

Impagliazzo, Russell (1995)
Hard-core distributions for somewhat hard problems
FOCS

Impagliazzo, Russell and Wigderson, Avi (1997)
P = BPP unless E has subexponential circuits
STOC

Impagliazzo, Russell and Wigderson, Avi (1998)
Randomness vs Time: Derandomization under a uniform assumption
FOCS

References III

Nisan, Noam and Wigderson, Avi (1994)
Hardness vs Randomness
Journal of Computer and System Sciences

Yao, Andrew C. (1982)
Theory and applications of trapdoor functions
FOCS