# Lecture 4: Pseudorandomness

# Last Lecture

- Example of Reduction

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function
  - (Intuition) Weak One-Way Func. $\implies$ Strong One-Way Func.

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function
  - (Intuition) Weak One-Way Func. $\implies$ Strong One-Way Func.
- Ensemble of Probability Distribution

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function
  - (Intuition) Weak One-Way Func. $\implies$ Strong One-Way Func.
- Ensemble of Probability Distribution
  - $\{X_n\}_{n\in\mathbb{N}}$: $\forall n \in \mathbb{N}$, $X_n$ is a probability distribution over $\{0,1\}^{\ell(n)}$ for some polynomial $\ell(\cdot)$

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function
  - (Intuition) Weak One-Way Func. $\implies$ Strong One-Way Func.
- Ensemble of Probability Distribution
  - $\{X_n\}_{n \in \mathbb{N}}$: $\forall n \in \mathbb{N}$, $X_n$ is a probability distribution over $\{0,1\}^{\ell(n)}$ for some polynomial $\ell(\cdot)$
- Computational Indistinguishability

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function
  - (Intuition) Weak One-Way Func. $\implies$ Strong One-Way Func.
- Ensemble of Probability Distribution
  - $\{X_n\}_{n \in \mathbb{N}}$: $\forall n \in \mathbb{N}$, $X_n$ is a probability distribution over $\{0,1\}^{\ell(n)}$ for some polynomial $\ell(\cdot)$
- Computational Indistinguishability
  - Any n.u. PPT $D$ can distinguish $\{X_n\}$ from $\{Y_n\}$ with only negligible probability

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function
  - (Intuition) Weak One-Way Func. $\implies$ Strong One-Way Func.
- Ensemble of Probability Distribution
  - $\{X_n\}_{n\in\mathbb{N}}$: $\forall n \in \mathbb{N}$, $X_n$ is a probability distribution over $\{0,1\}^{\ell(n)}$ for some polynomial $\ell(\cdot)$
- Computational Indistinguishability
  - Any n.u. PPT $D$ can distinguish $\{X_n\}$ from $\{Y_n\}$ with only negligible probability
- Property 1: Closure under Efficient Operations

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function
  - (Intuition) Weak One-Way Func. $\implies$ Strong One-Way Func.
- Ensemble of Probability Distribution
  - $\{X_n\}_{n\in\mathbb{N}}$: $\forall n \in \mathbb{N}$, $X_n$ is a probability distribution over $\{0,1\}^{\ell(n)}$ for some polynomial $\ell(\cdot)$
- Computational Indistinguishability
  - Any n.u. PPT $D$ can distinguish $\{X_n\}$ from $\{Y_n\}$ with only negligible probability
- Property 1: Closure under Efficient Operations
  - Efficient processing cannot help distinguish computationally indistinguishable distributions

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function
  - (Intuition) Weak One-Way Func. $\implies$ Strong One-Way Func.
- Ensemble of Probability Distribution
  - $\{X_n\}_{n\in\mathbb{N}}$: $\forall n \in \mathbb{N}$, $X_n$ is a probability distribution over $\{0,1\}^{\ell(n)}$ for some polynomial $\ell(\cdot)$
- Computational Indistinguishability
  - Any n.u. PPT $D$ can distinguish $\{X_n\}$ from $\{Y_n\}$ with only negligible probability
- Property 1: Closure under Efficient Operations
  - Efficient processing cannot help distinguish computationally indistinguishable distributions
- Property 2: Transitivity (aka, the "Hybrid Lemma")

# Last Lecture

- Example of Reduction
  - Hardness of Factoring $\implies$ Weak One-Way Function
  - (Intuition) Weak One-Way Func. $\implies$ Strong One-Way Func.
- Ensemble of Probability Distribution
  - $\{X_n\}_{n\in\mathbb{N}}$: $\forall n \in \mathbb{N}$, $X_n$ is a probability distribution over $\{0,1\}^{\ell(n)}$ for some polynomial $\ell(\cdot)$
- Computational Indistinguishability
  - Any n.u. PPT $D$ can distinguish $\{X_n\}$ from $\{Y_n\}$ with only negligible probability
- Property 1: Closure under Efficient Operations
  - Efficient processing cannot help distinguish computationally indistinguishable distributions
- Property 2: Transitivity (aka, the "Hybrid Lemma")
  - If first and last hybrids are comp. distinguishable, then at least a pair of consecutive hybrids are comp. distinguishable

# Distinguishing vs Prediction

# Distinguishing vs Prediction

**Definition (Prediction Advantage)**

$$\max_{\mathcal{A}} \Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : \mathcal{A}(t) = b] - \frac{1}{2}$$

# Distinguishing vs Prediction

**Definition (Prediction Advantage)**

$$\max_{\mathcal{A}} \Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : \mathcal{A}(t) = b] - \frac{1}{2}$$

- Comp. Indistinguishability $\iff$ Negl. Prediction Advantage

# Distinguishing vs Prediction

**Definition (Prediction Advantage)**

$$\max_{\mathcal{A}} \Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : \mathcal{A}(t) = b] - \frac{1}{2}$$

- Comp. Indistinguishability $\iff$ Negl. Prediction Advantage
  - Think: Comp. Indistinguishability $\Rightarrow$ Negl. Prediction Advantage?

# Distinguishing vs Prediction

**Definition (Prediction Advantage)**

$$\max_{\mathcal{A}} \Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : \mathcal{A}(t) = b] - \frac{1}{2}$$

- Comp. Indistinguishability $\iff$ Negl. Prediction Advantage
  - Think: Comp. Indistinguishability $\Rightarrow$ Negl. Prediction Advantage?
  - Think: Comp. Indistinguishability $\Leftarrow$ Negl. Prediction Advantage?

# Distinguishing vs Prediction (contd.)

**Lemma (Prediction Lemma)**

*Let $\{X_n^0\}$ and $\{X_n^1\}$ be ensembles of probability distributions. Let $D$ be a n.u. PPT that $\varepsilon(\cdot)$-distinguishes $\{X_n^0\}$ and $\{X_n^1\}$ for infinitely many $n \in \mathbb{N}$. Then, $\exists$ n.u. PPT $\mathcal{A}$ s.t.*

$$\Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : \mathcal{A}(t) = b] - \frac{1}{2} \geqslant \frac{\varepsilon(n)}{2}$$

*for infinitely many $n \in \mathbb{N}$.*

# Distinguishing vs Prediction (contd.)

**Lemma (Prediction Lemma)**

*Let $\{X_n^0\}$ and $\{X_n^1\}$ be ensembles of probability distributions. Let $D$ be a n.u. PPT that $\varepsilon(\cdot)$-distinguishes $\{X_n^0\}$ and $\{X_n^1\}$ for infinitely many $n \in \mathbb{N}$. Then, $\exists$ n.u. PPT $\mathcal{A}$ s.t.*

$$\Pr[b \xleftarrow{\$} \{0,1\}, t \leftarrow X_n^b : \mathcal{A}(t) = b] - \frac{1}{2} \geqslant \frac{\varepsilon(n)}{2}$$

*for infinitely many $n \in \mathbb{N}$.*

- Think: Proof?

# Pseudorandom Distributions

# Pseudorandom Distributions

- How to test that a string is "random-looking?"

# Pseudorandom Distributions

- How to test that a string is “random-looking?”
  - Roughly same number of 0s and 1s

# Pseudorandom Distributions

- How to test that a string is “random-looking?”
  - Roughly same number of 0s and 1s
  - Roughly same number of 00s and 11s

# Pseudorandom Distributions

- How to test that a string is "random-looking?"
  - Roughly same number of 0s and 1s
  - Roughly same number of 00s and 11s
  - Given any prefix, hard to guess next bit

# Pseudorandom Distributions

- How to test that a string is "random-looking?"
  - Roughly same number of 0s and 1s
  - Roughly same number of 00s and 11s
  - Given any prefix, hard to guess next bit
  - Given any prefix, hard to guess next sequence

# Pseudorandom Distributions

- How to test that a string is "random-looking?"
  - Roughly same number of 0s and 1s
  - Roughly same number of 00s and 11s
  - Given any prefix, hard to guess next bit
  - Given any prefix, hard to guess next sequence
  - ...

# Pseudorandom Distributions

- How to test that a string is "random-looking?"
  - Roughly same number of 0s and 1s
  - Roughly same number of 00s and 11s
  - Given any prefix, hard to guess next bit
  - Given any prefix, hard to guess next sequence
  - ...

<u>*Want*</u>*: Strings that pass* **all** *efficient tests*

# Pseudorandom Distributions (contd.)

- Uniform Distribution

# Pseudorandom Distributions (contd.)

- Uniform Distribution
  - $U_{\ell(n)}$ denotes uniform distribution over $\{0,1\}^{\ell(n)}$

# Pseudorandom Distributions (contd.)

- Uniform Distribution
  - $U_{\ell(n)}$ denotes uniform distribution over $\{0,1\}^{\ell(n)}$
- Pseudorandomness

# Pseudorandom Distributions (contd.)

- Uniform Distribution
  - $U_{\ell(n)}$ denotes uniform distribution over $\{0,1\}^{\ell(n)}$
- Pseudorandomness
  - Intuition: A distribution is pseudorandom if it "looks like" a uniform distribution to any efficient test

# Pseudorandom Distributions (contd.)

- Uniform Distribution
  - $U_{\ell(n)}$ denotes uniform distribution over $\{0,1\}^{\ell(n)}$
- Pseudorandomness
  - Intuition: A distribution is pseudorandom if it "looks like" a uniform distribution to any efficient test

# Pseudorandom Distributions (contd.)

- Uniform Distribution
  - $U_{\ell(n)}$ denotes uniform distribution over $\{0,1\}^{\ell(n)}$
- Pseudorandomness
  - Intuition: A distribution is pseudorandom if it "looks like" a uniform distribution to any efficient test

**Definition (Pseudorandom Ensembles)**

An ensemble $\{X_n\}$, where $X_n$ is a distribution over $\{0,1\}^{\ell(n)}$, is said to be pseudorandom if:

$$\{X_n\} \approx \{U_{\ell(n)}\}$$

# Pseudorandom Distributions (contd.)

- Uniform Distribution
  - $U_{\ell(n)}$ denotes uniform distribution over $\{0,1\}^{\ell(n)}$
- Pseudorandomness
  - Intuition: A distribution is pseudorandom if it "looks like" a uniform distribution to any efficient test

**Definition (Pseudorandom Ensembles)**

An ensemble $\{X_n\}$, where $X_n$ is a distribution over $\{0,1\}^{\ell(n)}$, is said to be pseudorandom if:

$$\{X_n\} \approx \{U_{\ell(n)}\}$$

- Think: How to show indistinguishability against *all* efficient tests?

# Next-bit Unpredictability

# Next-bit Unpredictability

**Definition (Next-bit Unpredictability)**

An ensemble of distributions $\{X_n\}$ over $\{0,1\}^{\ell(n)}$ is next-bit unpredictable if, for all $0 \leqslant i < \ell(n)$ and n.u. PPT $\mathcal{A}$, $\exists$ negligible function $\nu(\cdot)$ s.t.:

$$\Pr[t = t_1 \dots t_{\ell(n)} \leftarrow X_n \colon \mathcal{A}(t_1 \dots t_i) = t_{i+1}] \leqslant \frac{1}{2} + \nu(n)$$

# Next-bit Unpredictability

**Definition (Next-bit Unpredictability)**

An ensemble of distributions $\{X_n\}$ over $\{0,1\}^{\ell(n)}$ is next-bit unpredictable if, for all $0 \leqslant i < \ell(n)$ and n.u. PPT $\mathcal{A}$, $\exists$ negligible function $\nu(\cdot)$ s.t.:

$$\Pr[t = t_1 \dots t_{\ell(n)} \leftarrow X_n \colon \mathcal{A}(t_1 \dots t_i) = t_{i+1}] \leqslant \frac{1}{2} + \nu(n)$$

**Theorem (Completeness of Next-bit Test)**

*If $\{X_n\}$ is next-bit unpredictable then $\{X_n\}$ is pseudorandom.*

# Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{ x \leftarrow X_n, u \leftarrow U_n \colon x_1 \dots x_i u_{i+1} \dots u_{\ell(n)} \right\}$$

# Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)}\right\}$$

- First Hybrid: $H_n^0$ is the uniform distribution $U_{\ell(n)}$

# Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \ldots x_i u_{i+1} \ldots u_{\ell(n)}\right\}$$

- First Hybrid: $H_n^0$ is the uniform distribution $U_{\ell(n)}$
- Last Hybrid: $H_n^{\ell(n)}$ is the distribution $X_n$

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)}\right\}$$

- First Hybrid: $H_n^0$ is the uniform distribution $U_{\ell(n)}$
- Last Hybrid: $H_n^{\ell(n)}$ is the distribution $X_n$
- Suppose $H_n^{(\ell(n))}$ is next-bit unpredictable but not pseudorandom

# Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)}\right\}$$

- First Hybrid: $H_n^0$ is the uniform distribution $U_{\ell(n)}$
- Last Hybrid: $H_n^{\ell(n)}$ is the distribution $X_n$
- Suppose $H_n^{(\ell(n))}$ is next-bit unpredictable but not pseudorandom
- $H_n^{(0)} \not\approx H_n^{(\ell(n))} \implies \exists\ i \in [\ell(n) - 1]$ s.t. $H_n^{(i)} \not\approx H_n^{(i+1)}$

# Next-bit Unpredictability $\implies$ Pseudorandomness

$$H_n^{(i)} := \left\{x \leftarrow X_n, u \leftarrow U_n : x_1 \dots x_i u_{i+1} \dots u_{\ell(n)}\right\}$$

- First Hybrid: $H_n^0$ is the uniform distribution $U_{\ell(n)}$
- Last Hybrid: $H_n^{\ell(n)}$ is the distribution $X_n$
- Suppose $H_n^{(\ell(n))}$ is next-bit unpredictable but not pseudorandom
- $H_n^{(0)} \not\approx H_n^{(\ell(n))} \implies \exists\ i \in [\ell(n)-1]$ s.t. $H_n^{(i)} \not\approx H_n^{(i+1)}$
- Now, next bit unpredictability is violated

# Pseudorandom Generators

# Pseudorandom Generators

**Definition (Pseudorandom Generator)**

A pseudorandom generator (PRG) $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is an efficiently computable function, where $\ell(\cdot)$ is a suitable polynomial s.t. $\ell(n) > n$, such that:

$$\{G(U_n)\} \approx \{U_{\ell(n)}\}$$

# Pseudorandom Generators

**Definition (Pseudorandom Generator)**

A pseudorandom generator (PRG) $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is an efficiently computable function, where $\ell(\cdot)$ is a suitable polynomial s.t. $\ell(n) > n$, such that:

$$\{G(U_n)\} \approx \{U_{\ell(n)}\}$$

1. Stretches $n$ random bits into $\ell(n)$ pseudorandom bits

# Pseudorandom Generators

## Definition (Pseudorandom Generator)

A pseudorandom generator (PRG) $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is an efficiently computable function, where $\ell(\cdot)$ is a suitable polynomial s.t. $\ell(n) > n$, such that:

$$\{G(U_n)\} \approx \{U_{\ell(n)}\}$$

1. Stretches $n$ random bits into $\ell(n)$ pseudorandom bits
2. Impossible unconditionally (need comp. indistinguishability)

# Pseudorandom Generators

**Definition (Pseudorandom Generator)**

A pseudorandom generator (PRG) $G\colon \{0,1\}^n \to \{0,1\}^{\ell(n)}$ is an efficiently computable function, where $\ell(\cdot)$ is a suitable polynomial s.t. $\ell(n) > n$, such that:

$$\{G(U_n)\} \approx \{U_{\ell(n)}\}$$

1. Stretches $n$ random bits into $\ell(n)$ pseudorandom bits
2. Impossible unconditionally (need comp. indistinguishability)
3. How to construct PRGs?

# Hardcore Predicate

# Hardcore Predicate

- Let $f$ be a one-way function

# Hardcore Predicate

- Let $f$ be a one-way function
- Intuition: $h(\cdot)$ is hardcore for $f$ if $h(x)$ is hard to predict even if $f(x)$ is given to the adversary

# Hardcore Predicate

- Let $f$ be a one-way function
- Intuition: $h(\cdot)$ is hardcore for $f$ if $h(x)$ is hard to predict even if $f(x)$ is given to the adversary

**Definition (Hardcore Predicate)**

The predicate $h\colon \{0,1\}^n \to \{0,1\}$ is hardcore for $f : \{0,1\}^n \to \{0,1\}^m$ if $\forall$ n.u. PPT adversary $\mathcal{A}$, $\exists$ negligible function $\mu(\cdot)$ such that:

$$\Pr\left[x \xleftarrow{\$} \{0,1\}^n \colon \mathcal{A}(1^n, f(x)) = h(x)\right] \leqslant \frac{1}{2} + \mu(n)$$

# Hardcore Predicate

- Let $f$ be a one-way function
- Intuition: $h(\cdot)$ is hardcore for $f$ if $h(x)$ is hard to predict even if $f(x)$ is given to the adversary

**Definition (Hardcore Predicate)**

The predicate $h\colon \{0,1\}^n \to \{0,1\}$ is hardcore for $f : \{0,1\}^n \to \{0,1\}^m$ if $\forall$ n.u. PPT adversary $\mathcal{A}$, $\exists$ negligible function $\mu(\cdot)$ such that:

$$\Pr\left[x \xleftarrow{\$} \{0,1\}^n \colon \mathcal{A}(1^n, f(x)) = h(x)\right] \leqslant \frac{1}{2} + \mu(n)$$

- Hardcore Predicate suffices to construct PRG

# Construction Outline: PRG from OWF

- Step 1: OWF (OWP) $\implies$ Hardcore Predicate for OWF (OWP)

# Construction Outline: PRG from OWF

- Step 1: OWF (OWP) $\implies$ Hardcore Predicate for OWF (OWP)
- Step 2: Hardcore Predicate for OWF (OWP) $\implies$ One-bit stretch PRG

# Construction Outline: PRG from OWF

- Step 1: OWF (OWP) $\implies$ Hardcore Predicate for OWF (OWP)
- Step 2: Hardcore Predicate for OWF (OWP) $\implies$ One-bit stretch PRG
- Step3: One-bit stretch PRG $\implies$ Poly-stretch PRG

# Construction Outline: PRG from OWF

- Step 1: OWF (OWP) $\implies$ Hardcore Predicate for OWF (OWP)
- Step 2: Hardcore Predicate for OWF (OWP) $\implies$ One-bit stretch PRG
- Step3: One-bit stretch PRG $\implies$ Poly-stretch PRG
- Today: Step 2 for OWP and Step 3

# Construction Outline: PRG from OWF

- Step 1: OWF (OWP) $\implies$ Hardcore Predicate for OWF (OWP)
- Step 2: Hardcore Predicate for OWF (OWP) $\implies$ One-bit stretch PRG
- Step3: One-bit stretch PRG $\implies$ Poly-stretch PRG
- Today: Step 2 for OWP and Step 3
- Step 1 in next lecture

# Hardcore Predicate for OWP $\implies$ One-bit stretch PRG

- Construction: $G(s) = f(s) \parallel h(s)$

# Hardcore Predicate for OWP $\implies$ One-bit stretch PRG

- Construction: $G(s) = f(s) \parallel h(s)$
- Think: Proof?

# One-bit stretch PRG $\implies$ Poly-stretch PRG

Intuition: Iterate the one-bit stretch PRG poly times

Construction of $G_{poly} : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$:

# One-bit stretch PRG $\implies$ Poly-stretch PRG

Intuition: Iterate the one-bit stretch PRG poly times

Construction of $G_{poly} : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$:

- Let $G_1 : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ be a one-bit stretch PRG

# One-bit stretch PRG $\implies$ Poly-stretch PRG

Intuition: Iterate the one-bit stretch PRG poly times

Construction of $G_{poly} : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$:

- Let $G_1 : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ be a one-bit stretch PRG
- $X_0 \leftarrow s$

# One-bit stretch PRG $\implies$ Poly-stretch PRG

Intuition: Iterate the one-bit stretch PRG poly times

Construction of $G_{poly} : \{0,1\}^n \to \{0,1\}^{\ell(n)}$:

- Let $G_1 : \{0,1\}^n \to \{0,1\}^{n+1}$ be a one-bit stretch PRG
- $X_0 \leftarrow s$
- $X_1 \| b_1 \leftarrow G_1(X_0)$

# One-bit stretch PRG $\implies$ Poly-stretch PRG

Intuition: Iterate the one-bit stretch PRG poly times

Construction of $G_{poly} : \{0,1\}^n \to \{0,1\}^{\ell(n)}$:

- Let $G_1 : \{0,1\}^n \to \{0,1\}^{n+1}$ be a one-bit stretch PRG
- $X_0 \leftarrow s$
- $X_1 \| b_1 \leftarrow G_1(X_0)$
- $X_2 \| b_2 \leftarrow G_1(X_1)$

# One-bit stretch PRG $\implies$ Poly-stretch PRG

Intuition: Iterate the one-bit stretch PRG poly times

Construction of $G_{poly} : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$:

- Let $G_1 : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ be a one-bit stretch PRG
- $X_0 \leftarrow s$
- $X_1 \| b_1 \leftarrow G_1(X_0)$
- $X_2 \| b_2 \leftarrow G_1(X_1)$
- $X_3 \| b_3 \leftarrow G_1(X_2)$

# One-bit stretch PRG $\implies$ Poly-stretch PRG

Intuition: Iterate the one-bit stretch PRG poly times

Construction of $G_{poly} : \{0,1\}^n \to \{0,1\}^{\ell(n)}$:

- Let $G_1 : \{0,1\}^n \to \{0,1\}^{n+1}$ be a one-bit stretch PRG
- $X_0 \leftarrow s$
- $X_1 \| b_1 \leftarrow G_1(X_0)$
- $X_2 \| b_2 \leftarrow G_1(X_1)$
- $X_3 \| b_3 \leftarrow G_1(X_2)$
- $X_i \| b_i \leftarrow G_1(X_{i-1})$

# One-bit stretch PRG $\implies$ Poly-stretch PRG

Intuition: Iterate the one-bit stretch PRG poly times

Construction of $G_{poly} : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$:

- Let $G_1 : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ be a one-bit stretch PRG
- $X_0 \leftarrow s$
- $X_1 \| b_1 \leftarrow G_1(X_0)$
- $X_2 \| b_2 \leftarrow G_1(X_1)$
- $X_3 \| b_3 \leftarrow G_1(X_2)$
- $X_i \| b_i \leftarrow G_1(X_{i-1})$
- $G_{poly}(s) := b_1 \ldots b_{\ell(n)}$

# One-bit stretch PRG $\implies$ Poly-stretch PRG

Intuition: Iterate the one-bit stretch PRG poly times

Construction of $G_{poly} : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$:

- Let $G_1 : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ be a one-bit stretch PRG
- $X_0 \leftarrow s$
- $X_1 \| b_1 \leftarrow G_1(X_0)$
- $X_2 \| b_2 \leftarrow G_1(X_1)$
- $X_3 \| b_3 \leftarrow G_1(X_2)$
- $X_i \| b_i \leftarrow G_1(X_{i-1})$
- $G_{poly}(s) := b_1 \dots b_{\ell(n)}$
- Proof?