Hardness vs. Randomness

Jorrit de Boer

24 January 2024

Introduction

- *Noam Nisan, Avi Wigderson*: **Hardness vs. Randomness**, J. Comput. Syst. Sci., 49(2):149-167 1994
- *Russell Impagliazzo, Avi Wigderson*: **P=BPP unless E has sub-exponential circuits: Derandomizing the XOR Lemma**, In Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing, STOC '97, pages 220-229, New York, NY, USA, ACM. 1997

Preliminaries

Definition (Probabilistic Turing Machine (PTM))

A probabilistic Turing machine (PTM) is a non-deterministic Turing machine that chooses between the available transitions at each point according to some probability distribution.

Definition (BPP)

The complexity class BPP (*Bounded Probabilistic Polynomial time*) is the class of sets L that are recognized in polynomial time by a PTM M with error probability bounded away from $\frac{1}{2}$, i.e. for some $\epsilon > 0$ and every x

- $x \in L \iff \Pr(M(x) = 1) > \frac{1}{2} + \epsilon$
- $x \notin L \iff \Pr(M(x) = 0) > \frac{1}{2} + \epsilon$

Theorem

$A \in BPP$ if and only if for all polynomials p there is a probabilistic Turing machine recognizing A in polynomial time with error probability $\leq \frac{1}{2^{p(n)}}$.

Preliminaries

Definition (Circuits)

A circuit is a directed acyclic graph in which every node (gate) is either an input node, labeled by one of the n input bits, an AND gate ($\wedge$), an OR gate ($\vee$), or a NOT gate ($\neg$). One of these gates is designated as the output gate. The size of a circuit is the number of gates.

Definition (Family of Circuits Computes a Language)

A family of circuits $\{C_n\}_{n\in\mathbb{N}}$ computes a language $L \subseteq \{0,1\}^*$ if for every length n and every $x \in \{0,1\}^n$,

$$x \in L \iff C_n(x) = 1$$

Main Theorem

Theorem

If there exists a hard to compute function $f \in E = TIME(2^{O(n)})$ *then* $P = BPP$*.*

Definition (Hard to Compute Function)

We say a boolean function f is hard to compute if computing f on input size n requires a circuit of size $2^{\Omega(n)}$.

Overview


Hard to Compute Function
Derandomization
Pseudorandom Generator
P=BPP

Derandomization

Definition (Pseudorandom Generator (PRG))

$G = \{G_n : \{0,1\}^{l(n)} \to \{0,1\}^n\}$, denoted by $G : l \to n$ is called a *pseudorandom generator* if, for any circuit C of size n:

$$|\Pr(C(y) = 1) - \Pr(C(G(x)) = 1)| \leq \frac{1}{n}$$

where y is chosen uniformly in $\{0,1\}^n$ and $x \in \{0,1\}^{l(n)}$.
G is a *quick* pseudorandom generator if $G \in TIME(2^{O(l)})$.

Lemma

If there exists a quick pseudorandom generator $G : l \to n$, then for $A \in BPP$ that can be computed by a PTM in polynomial time $p = p(n)$, A can be computed by a deterministic TM running in time $2^{O(l(p^2))}$.

Derandomization Proof

Definition (Pseudorandom Generator (PRG))

Pseudorandom generator $G : l \to n$: for any circuit C of size n: $|\Pr(C(y) = 1) - \Pr(C(G(x)) = 1)| \leq \frac{1}{n}$ for $y \in \{0,1\}^n$ and $x \in \{0,1\}^l$ uniformly random. G is quick: $G \in TIME(2^{O(l)})$.

Lemma

If there exists a quick PRG $G : l(n) \to n$, then for $A \in BPP$ computed by a PTM in polynomial time $p = p(n)$, then A can be computed by a deterministic TM running in time $2^{O(l(p^2))}$.

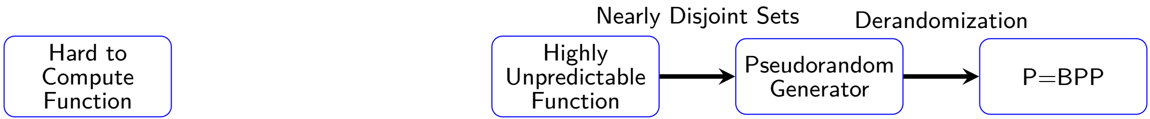
Proof: Take $A \in BPP$ and M_A a PTM that computes it:

- $a \in A \iff \Pr(M_A(a) = 1) > \frac{2}{3}$
- $a \notin A \iff \Pr(M_A(a) = 0) > \frac{2}{3}$

M_A runs in time p, so it uses at most p random bits. $M_A(a) : \{0,1\}^p \to \{0,1\}$. Circuit C of size p^2 that computes $M_A(a)$. So, for $G_{p^2} : \{0,1\}^{l(p^2)} \to \{0,1\}^{p^2}$, $C = M_A(a)$: $|\Pr(C(y) = 1) - \Pr(C(G(x)) = 1)| \leq \frac{1}{p^2}$

$$\Pr(C(G(x)) = 1) \geq \Pr(C(y) = 1) - \frac{1}{p^2} > \frac{2}{3} - \frac{1}{p^2} > \frac{1}{2}$$

Try all inputs $\{0,1\}^{l(p^2)}$ and take a majority. Deterministic and runs in time $2^{l(p^2)} \cdot 2^{O(l(p^2))} = 2^{O(l(p^2))}$. □



Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin. - John von Neumann

Random number generation is too important to be left to chance. - Robert Coveyou

Highly Unpredictable Function

Definition

We say a boolean function $f : \{0,1\}^m \to \{0,1\}$ is Highly Unpredictable if, for some $\epsilon > 0$, for every circuit C of size at most $2^{\epsilon m}$:

$$\left| \Pr\left(C(x) = f(x)\right) - \frac{1}{2} \right| < \frac{1}{2^{\epsilon m}}$$

where x is chosen uniformly random in $\{0,1\}^m$.

Nearly Disjoint Sets

Definition

Collection of sets $S = \{S_1, \ldots, S_n\}$, $S_i \subset \{1, \ldots, l\}$ is called (k, m)-*design* if:

1. For all i:
$$|S_i| = m$$
2. For all $i \neq j$:
$$|S_i \cap S_j| \leq k$$

Nearly Disjoint Sets

Definition

For $f : \{0,1\}^m \to \{0,1\}$ we define $f_S : \{0,1\}^l \to \{0,1\}^n$ as *the bit string of length n computed by applying f to the subsets of the x's denoted by the sets in S:*

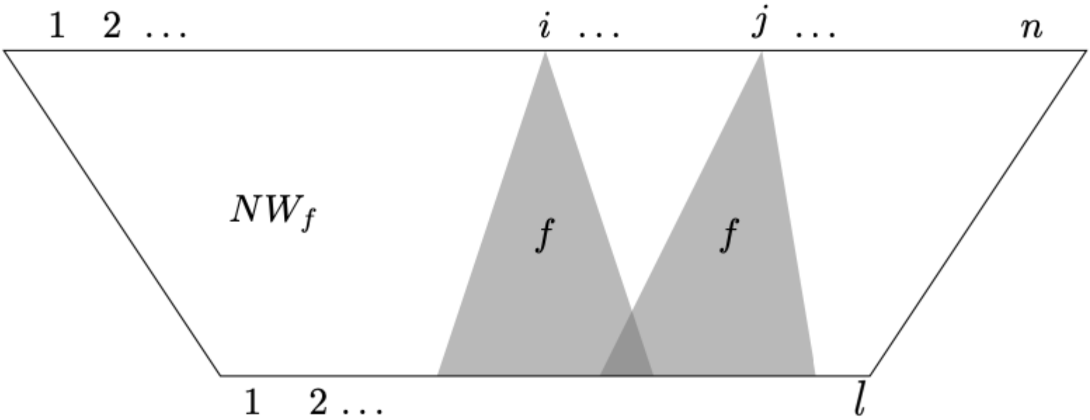
$$f_S(x) = f(x_{S_1})\ f(x_{S_2})\ \dots\ f(x_{S_{n-1}})\ f(x_{S_n})$$

Example

$$S_1 = \{1,3,6,20,23\}, S_2 = \{1,5,9,21,24\} \dots$$

$$f_S(x_1\ x_2\ \dots\ x_{l-1}\ x_l) = f(x_1\ x_3\ x_6\ x_{20}\ x_{23})\ f(x_1\ x_5\ x_9\ x_{21}\ x_{24}) \quad \dots$$

Nearly Disjoint Sets



Nearly Disjoint Sets Make a PRG

Lemma

Let m, n, l *be integers; let* $f : \{0,1\}^m \to \{0,1\}$ *be a "Highly Unpredictable" function:*
For some $\epsilon > 0$, *for every circuit* C *of size at most* $2^{\epsilon m} = n^2$*:*

$$\left| \Pr\left(C(x) = f(x)\right) - \frac{1}{2} \right| < 2^{-\epsilon m} = n^{-2}$$

where x *is chosen uniformly random in* $\{0,1\}^m$.
Let $S = \{S_1, \ldots, S_n\}$, $S_i \subset \{1, \ldots, l\}$ *with* $l = O(\log n)$ *be a* $(\log n, \frac{2}{\epsilon}\log n)$ *design with, i.e.* $|S_i| = m = \frac{2}{\epsilon}\log n$ *and* $|S_i \cap S_j| \leq \log n$.
Then $G : l \to n$ *given by* $G(x) = f_S(x)$ *is a pseudorandom generator.*

Nearly Disjoint Sets Make a PRG Proof

Lemma

Let $f : \{0,1\}^m \rightarrow \{0,1\}$ be a "Highly Unpredictable" function: for every circuit C of size at most n^2: $\left|\Pr\left(C(x) = f(x)\right) - \frac{1}{2}\right| < n^{-2}$ where x is chosen uniformly random in $\{0,1\}^m$.
Let $S = \{S_1, \ldots, S_n\}$, $S_i \subset \{1, \ldots, l\}$ be nearly disjoint sets. Then $G : l \rightarrow n$ given by $G(x) = f_S(x)$ is a pseudorandom generator.

Proof Sketch: Proof by contradiction, G is not a pseudorandom generator, then w.l.o.g. for some circuit C of size n:

$$\Pr(C(y) = 1) - \Pr(C(G(x)) = 1) > 1/n$$

for $y \in \{0,1\}^n$ and $x \in \{0,1\}^l$ chosen uniformly.
Define distribution E_i on $\{0,1\}^n$: the first i bits are from $f_S(x)$ for $x \in \{0,1\}^l$, and the other $n - i$ bits uniformly random. And let $p_i = \Pr(C(z) = 1)$ for $z \in E_i$ uniformly.

$$p_0 - p_n > 1/n$$

so for some i:

$$p_{i-1} - p_i > 1/n^2$$

Construct circuit D which takes $y_1, \ldots, y_{i-1}$ and predicts y_i.

$$\Pr(D(y_1, \ldots, y_{i-1}) = y_i) - \frac{1}{2} > \frac{1}{n^2}$$

Nearly Disjoint Sets Make a PRG Proof

Lemma

Let $f : \{0,1\}^m \to \{0,1\}$ *be a "Highly Unpredictable" function: for every circuit* C *of size at most* n^2*:* $\left|\Pr\left(C(x) = f(x)\right) - \frac{1}{2}\right| < n^{-2}$ *where* x *is chosen uniformly random in* $\{0,1\}^m$*.*
Let $S = \{S_1, \ldots, S_n\}$*,* $S_i \subset \{1, \ldots, l\}$ *be nearly disjoint sets. Then* $G : l \to n$ *given by* $G(x) = f_S(x)$ *is a pseudorandom generator.*

Proof Sketch Continued:

$$\Pr(D(y_1, \ldots, y_{i-1}) = y_i) - \frac{1}{2} > \frac{1}{n^2}$$

$$y_i = f(x_{S_i}) = f(x_1 \ldots x_m)$$

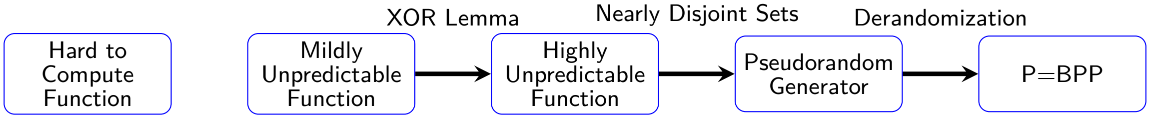
$$\Pr(D(y_1, \ldots, y_{i-1}) = f(x_1 \ldots x_m)) - \frac{1}{2} > \frac{1}{n^2}$$

Circuit D' of size $\leq n^2$:

$$\Pr(D'(x_1 \ldots x_m) = f(x_1 \ldots x_m)) - \frac{1}{2} > \frac{1}{n^2}$$

Contradiction! So G is a PRG. □

Overview


XOR Lemma
Nearly Disjoint Sets
Derandomization
Hard to Compute Function
Mildly Unpredictable Function
Highly Unpredictable Function
Pseudorandom Generator
P=BPP

Mildly Unpredictable Function

Definition (Mildly Unpredictable Function)

We say a boolean function $f : \{0,1\}^n \to \{0,1\}$ is "Mildly Unpredictable" if for all circuits C of size at most $2^{\Omega(n)}$:

$$\Pr(C_n(x) \neq f(x)) > n^{-2}$$

for x chosen uniformly random in $\{0,1\}^n$

XOR Lemma

Lemma (Yao's XOR Lemma)

If $f : \{0,1\}^n \to \{0,1\}$ *is a mildly unpredictable function, i.e. for all circuits* C *of size at most* $2^{\Omega(n)}$*:*

$$\Pr(C_n(x) \neq f(x)) > n^{-2}$$

then $f^{\oplus(k)}$*, which is defined as follows:*

$$f^{\oplus(k)}(x_1, \ldots, x_k) = f(x_1) \oplus \cdots \oplus f(x_k)$$

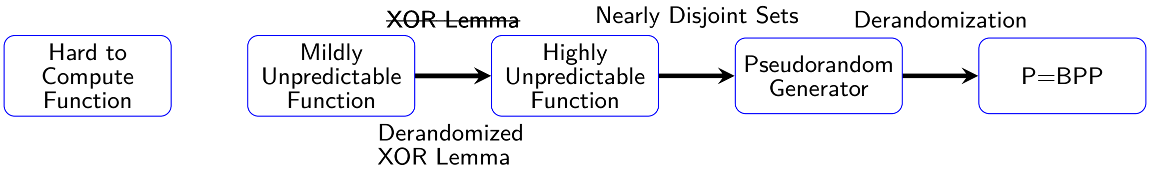
, for $k = O(n^3)$ *is a highly unpredictable function. So, for some* $\epsilon > 0$*, for every circuit* C *of size* $2^{\epsilon n}$*:*

$$\left|\Pr\left(C(x) = f^{\oplus}(x)\right) - 1/2\right| < 2^{\epsilon n}$$

Problem

This XOR Lemma blows up the input by a polynomial amount: $f^{\oplus(k)} : \{0,1\}^{n \cdot O(n^3)} \to \{0,1\}$.

Overview


Hard to Compute Function
Mildly Unpredictable Function
~~XOR Lemma~~
Derandomized XOR Lemma
Highly Unpredictable Function
Nearly Disjoint Sets
Pseudorandom Generator
Derandomization
P=BPP

Derandomized XOR Lemma

Lemma (Derandomized Yao's XOR Lemma)

If $f : \{0,1\}^n \to \{0,1\}$ *is a mildly unpredictable function, i.e. for all circuits* C *of size at most* $2^{\Omega(n)}$*:*

$$\Pr(C_n(x) \neq f(x)) > n^{-2}$$

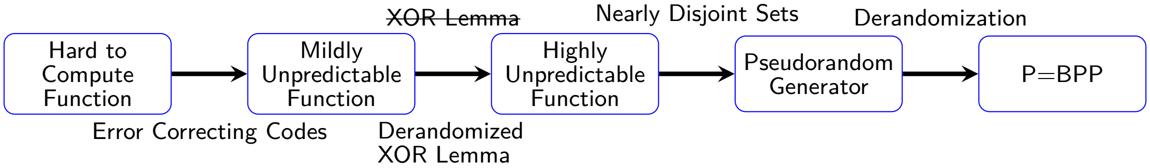
then $f^{\oplus(k)}$*, which is defined as follows:*

$$f^{\oplus(k)}(x_1, \ldots, x_k) = f(x_1) \oplus \cdots \oplus f(x_k)$$

, for $\underline{k = O(1)}$ *is a highly unpredictable function. So, for some* $\epsilon > 0$*, for every circuit* C *of size* $2^{\epsilon n}$*:*

$$\left|\Pr\left(C(x) = f^{\oplus}(x)\right) - 1/2\right| < 2^{\epsilon n}$$

Overview



XOR Lemma
Nearly Disjoint Sets
Derandomization
Hard to Compute Function
Mildly Unpredictable Function
Highly Unpredictable Function
Pseudorandom Generator
P=BPP
Error Correcting Codes
Derandomized XOR Lemma

Error Correcting Codes

Lemma

If there is a hard to compute function $f \in E$, i.e. computing f on input size n requires a circuit of size $2^{\Omega(n)}$, then, there exists a function $h \in E$ that is mildly unpredictable: for every circuit C of size $2^{\Omega(n)}$

$$\Pr(C_n(x) \neq h(x)) > n^{-2}$$

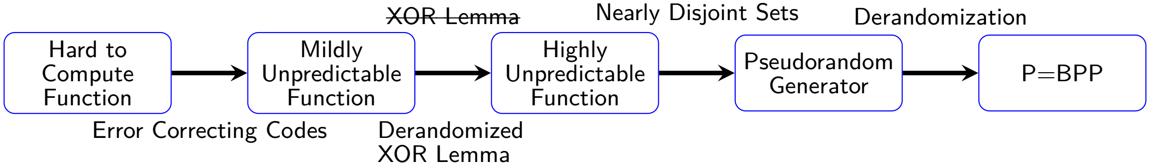
for x chosen uniformly random in $\{0,1\}^n$.

Proof Sketch: View $f : \{0,1\}^n \to \{0,1\}$ as a message of size $L = 2^n$. Apply an error correcting code $ENC : \{0,1\}^L \to \{0,1\}^{\hat{L}}$.

View this new message as a function $\hat{f} : \{0,1\}^{\log \hat{L}} \to \{0,1\}$

Any circuit C trying to compute this function $\hat{f}$ must make n^{-2} mistakes. If not, we can apply the efficient decoder DEC to retrieve f and compute f efficiently.

Overview



Theorem

If there exists a hard to compute function $f \in E = TIME(2^{O(n)})$ *then* $P = BPP$.