The Needs of the Many vs The Needs of the One

Known $3\mathrm{SAT}$ is NP-complete.

The Needs of the Many vs The Needs of the One

Known $3\mathrm{SAT}$ is NP-complete.
So we think $3\mathrm{SAT} \notin \mathrm{P}$.

The Needs of the Many vs The Needs of the One

Known $3\mathrm{SAT}$ is NP-complete.
So we think $3\mathrm{SAT} \notin \mathrm{P}$.

Def $\#\phi$ is the **number of satisfying assignments** for ϕ.

The Needs of the Many vs The Needs of the One

Known $3\mathrm{SAT}$ is NP-complete.
So we think $3\mathrm{SAT} \notin \mathrm{P}$.

Def $\#\phi$ is the **number of satisfying assignments** for ϕ.

Our Question Given ϕ where you are **promised** that $\#\phi \le 1$, determine $\#\phi$. We call this problem **VV** (for Valiant-Vazirani).

The Needs of the Many vs The Needs of the One

Known $3\mathrm{SAT}$ is NP-complete.
So we think $3\mathrm{SAT} \notin \mathrm{P}$.

Def $\#\phi$ is the **number of satisfying assignments** for ϕ.

Our Question Given ϕ where you are **promised** that $\#\phi \le 1$, determine $\#\phi$. We call this problem **VV** (for Valiant-Vazirani).
Vote

The Needs of the Many vs The Needs of the One

Known 3SAT is NP-complete.
So we think $3\text{SAT} \notin \text{P}$.

Def $\#\phi$ is the **number of satisfying assignments** for ϕ.

Our Question Given ϕ where you are **promised** that $\#\phi \le 1$, determine $\#\phi$. We call this problem **VV** (for Valiant-Vazirani).
Vote
1) **VV** $\in \text{P}$.

The Needs of the Many vs The Needs of the One

Known $3\mathrm{SAT}$ is NP-complete.
So we think $3\mathrm{SAT} \notin \mathrm{P}$.

Def $\#\phi$ is the **number of satisfying assignments** for ϕ.

Our Question Given ϕ where you are **promised** that $\#\phi \le 1$, determine $\#\phi$. We call this problem **VV** (for Valiant-Vazirani).
Vote
1) **VV** $\in \mathrm{P}$.
2) If **VV** $\in \mathrm{P}$ then $\mathrm{P} = \mathrm{NP}$.

The Needs of the Many vs The Needs of the One

Known $3\mathrm{SAT}$ is NP-complete.
So we think $3\mathrm{SAT} \notin \mathrm{P}$.

Def $\#\phi$ is the **number of satisfying assignments** for ϕ.

Our Question Given ϕ where you are **promised** that $\#\phi \le 1$, determine $\#\phi$. We call this problem **VV** (for Valiant-Vazirani).
Vote
1) **VV** $\in \mathrm{P}$.
2) If **VV** $\in \mathrm{P}$ then $\mathrm{P} = \mathrm{NP}$.
3) If **VV** $\in \mathrm{P}$ then something else unlikely happens.

The Needs of the Many vs The Needs of the One

Known $3SAT$ is NP-complete.
So we think $3SAT \notin P$.

Def $\#\phi$ is the **number of satisfying assignments** for ϕ.

Our Question Given ϕ where you are **promised** that $\#\phi \le 1$, determine $\#\phi$. We call this problem **VV** (for Valiant-Vazirani).
Vote
1) **VV** $\in P$.
2) If **VV** $\in P$ then $P = NP$.
3) If **VV** $\in P$ then something else unlikely happens.
The answer is 3.

The Needs of the Many vs The Needs of the One

Known $3\mathrm{SAT}$ is NP-complete.
So we think $3\mathrm{SAT} \notin \mathrm{P}$.

Def $\#\phi$ is the **number of satisfying assignments** for ϕ.

Our Question Given ϕ where you are **promised** that $\#\phi \le 1$, determine $\#\phi$. We call this problem **VV** (for Valiant-Vazirani).
Vote
1) **VV** $\in \mathrm{P}$.
2) If **VV** $\in \mathrm{P}$ then $\mathrm{P} = \mathrm{NP}$.
3) If **VV** $\in \mathrm{P}$ then something else unlikely happens.
The answer is 3.

If **VV** $\in \mathrm{P}$ then SAT is in randomized poly time (RP).

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

What We Can't Say

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

What We Can't Say $\phi \in \mathrm{SAT} \rightarrow \mathrm{ALG}(\phi)$ accepts

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

What We Can't Say $\phi \in \mathrm{SAT} \rightarrow \mathrm{ALG}(\phi)$ accepts
What We Can't Say

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

What We Can't Say $\phi \in \mathrm{SAT} \rightarrow \mathrm{ALG}(\phi)$ accepts
What We Can't Say $\phi \in \mathrm{SAT}$ iff $\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1$.

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

What We Can't Say $\phi \in \mathrm{SAT} \rightarrow \mathrm{ALG}(\phi)$ accepts
What We Can't Say $\phi \in \mathrm{SAT}$ iff $\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1$.

What We Can Say

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

What We Can't Say $\phi \in \mathrm{SAT} \rightarrow \mathrm{ALG}(\phi)$ accepts
What We Can't Say $\phi \in \mathrm{SAT}$ iff $\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1$.

What We Can Say $\phi \in \mathrm{SAT} \rightarrow \Pr(\mathrm{ALG}(\phi) = 0) \leq \frac{1}{4}$.

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

What We Can't Say $\phi \in \mathrm{SAT} \rightarrow \mathrm{ALG}(\phi)$ accepts
What We Can't Say $\phi \in \mathrm{SAT}$ iff $\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1$.

What We Can Say $\phi \in \mathrm{SAT} \rightarrow \Pr(\mathrm{ALG}(\phi) = 0) \leq \frac{1}{4}$.
What We Can Say

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

What We Can't Say $\phi \in \mathrm{SAT} \rightarrow \mathrm{ALG}(\phi)$ accepts
What We Can't Say $\phi \in \mathrm{SAT}$ iff $\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1$.

What We Can Say $\phi \in \mathrm{SAT} \rightarrow \Pr(\mathrm{ALG}(\phi) = 0) \le \frac{1}{4}$.
What We Can Say
$\phi \in \mathrm{SAT} \rightarrow \Pr(\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1 \ge \frac{1}{n}$.
$\phi \notin \mathrm{SAT} \rightarrow \Pr(\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1) = 0$

Randomized Algorithms

Def A **Randomized Algorithm** is an algorithm that will, in some of its step, flip a coin; the next instruction is based on that coin.

Let ALG be a rand Alg and x be an input.

What We Can't Say $\phi \in \mathrm{SAT} \rightarrow \mathrm{ALG}(\phi)$ accepts
What We Can't Say $\phi \in \mathrm{SAT}$ iff $\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1$.

What We Can Say $\phi \in \mathrm{SAT} \rightarrow \Pr(\mathrm{ALG}(\phi) = 0) \leq \frac{1}{4}$.
What We Can Say
$\phi \in \mathrm{SAT} \rightarrow \Pr(\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1 \geq \frac{1}{n}$.
$\phi \notin \mathrm{SAT} \rightarrow \Pr(\#\mathrm{SAT}(\mathrm{ALG}(\phi)) = 1) = 0$
When is a Rand Alg Useful? When it is fast and has a high probability of being correct.

A Useful Rand Alg: Preparation

Consider the following matrix of polynomials:

A Useful Rand Alg: Preparation

Consider the following matrix of polynomials:

$$M(x) = \begin{pmatrix} x & x-1 & 3x+4 \\ 17x^2+x-1 & x^2+17 & -12x^2+4x-3 \\ x^3+x^2-5 & x^3+x^2+x-77 & x^3-84x^2+8x-100 \end{pmatrix}$$

A Useful Rand Alg: Preparation

Consider the following matrix of polynomials:

$$M(x) = \begin{pmatrix} x & x-1 & 3x+4 \\ 17x^2+x-1 & x^2+17 & -12x^2+4x-3 \\ x^3+x^2-5 & x^3+x^2+x-77 & x^3-84x^2+8x-100 \end{pmatrix}$$

Imagine taking its determinant.

A Useful Rand Alg: Preparation

Consider the following matrix of polynomials:

$$M(x) = \begin{pmatrix} x & x-1 & 3x+4 \\ 17x^2+x-1 & x^2+17 & -12x^2+4x-3 \\ x^3+x^2-5 & x^3+x^2+x-77 & x^3-84x^2+8x-100 \end{pmatrix}$$

Imagine taking its determinant.

It would be a mess!

A Useful Rand Alg: Preparation

Consider the following matrix of polynomials:

$$M(x) = \begin{pmatrix} x & x-1 & 3x+4 \\ 17x^2+x-1 & x^2+17 & -12x^2+4x-3 \\ x^3+x^2-5 & x^3+x^2+x-77 & x^3-84x^2+8x-100 \end{pmatrix}$$

Imagine taking its determinant.

It would be a mess! Or not.

A Useful Rand Alg: Preparation

Consider the following matrix of polynomials:

$$M(x) = \begin{pmatrix} x & x-1 & 3x+4 \\ 17x^2+x-1 & x^2+17 & -12x^2+4x-3 \\ x^3+x^2-5 & x^3+x^2+x-77 & x^3-84x^2+8x-100 \end{pmatrix}$$

Imagine taking its determinant.

It would be a mess! Or not. It could be 0.

A Useful Rand Alg: Preparation

Consider the following matrix of polynomials:

$$M(x) = \begin{pmatrix} x & x-1 & 3x+4 \\ 17x^2+x-1 & x^2+17 & -12x^2+4x-3 \\ x^3+x^2-5 & x^3+x^2+x-77 & x^3-84x^2+8x-100 \end{pmatrix}$$

Imagine taking its determinant.

It would be a mess! Or not. It could be 0.

If it were 0 then the **intermediary calculations** would be a mess even though the final answer is not.

A Useful Rand Alg: Preparation

Consider the following matrix of polynomials:

$$M(x) = \begin{pmatrix} x & x-1 & 3x+4 \\ 17x^2+x-1 & x^2+17 & -12x^2+4x-3 \\ x^3+x^2-5 & x^3+x^2+x-77 & x^3-84x^2+8x-100 \end{pmatrix}$$

Imagine taking its determinant.

It would be a mess! Or not. It could be 0.

If it were 0 then the **intermediary calculations** would be a mess even though the final answer is not.

If it were 0 then plugging in any number for x and doing the det (which is easy) would yields 0.

A Useful Rand Alg: Preparation

Consider the following matrix of polynomials:

$$M(x) = \begin{pmatrix} x & x-1 & 3x+4 \\ 17x^2+x-1 & x^2+17 & -12x^2+4x-3 \\ x^3+x^2-5 & x^3+x^2+x-77 & x^3-84x^2+8x-100 \end{pmatrix}$$

Imagine taking its determinant.

It would be a mess! Or not. It could be 0.

If it were 0 then the **intermediary calculations** would be a mess even though the final answer is not.

If it were 0 then plugging in any number for x and doing the det (which is easy) would yields 0.

Is the Det of the above matrix 0? I do not know but I doubt it.

A Useful Rand Alg for DETPOLYZERO

Def Let DETPOLYZERO be the set of all square matrices $M(x)$ of polynomials in one variable over the integers such that the $\mathrm{DET}(M(x)) = 0$.

A Useful Rand Alg for DETPOLYZERO

Def Let DETPOLYZERO be the set of all square matrices $M(x)$ of polynomials in one variable over the integers such that the $\mathrm{DET}(M(x)) = 0$.

$$M_1(x) = \begin{pmatrix} x & x-1 \\ x+1 & x^2-1 \end{pmatrix}$$

is NOT in DETPOLYZERO since Det is

$$x(x^2-1)-(x-1)(x+1) = x^3-x-(x^2-1) = x^3-x^2-x+1 \not\equiv 0.$$

A Useful Rand Alg for DETPOLYZERO

Def Let DETPOLYZERO be the set of all square matrices $M(x)$ of polynomials in one variable over the integers such that the $\mathrm{DET}(M(x)) = 0$.

$$M_1(x) = \begin{pmatrix} x & x-1 \\ x+1 & x^2-1 \end{pmatrix}$$

is NOT in DETPOLYZERO since Det is

$$x(x^2-1)-(x-1)(x+1) = x^3-x-(x^2-1) = x^3-x^2-x+1 \not\equiv 0.$$

$$M_2(x) = \begin{pmatrix} 1 & x-1 \\ x+1 & x^2-1 \end{pmatrix}$$

is IN DETPOLYZERO since the determinant is

$$x^2-1-(x-1)(x+1) = x^2-1-(x^2-1) = 0.$$

DETPOLYZERO is in RP

Here is a rand algorithm for DETPOLYZERO.

DETPOLYZERO is in RP

Here is a rand algorithm for DETPOLYZERO.

1. Input $M(x)$ ($n \times n$ matrix of polys of degree $\leq d$).

DETPOLYZERO is in RP

Here is a rand algorithm for DETPOLYZERO.

1. Input $M(x)$ ($n \times n$ matrix of polys of degree $\leq d$).
2. Pick prime $(dn)^2 \leq p \leq 2(dn)^2$ and $a \in \{0, \ldots, p-1\}$.

DETPOLYZERO is in RP

Here is a rand algorithm for DETPOLYZERO.

1. Input $M(x)$ ($n \times n$ matrix of polys of degree $\le d$).
2. Pick prime $(dn)^2 \le p \le 2(dn)^2$ and $a \in \{0, \ldots, p-1\}$.
3. $d = \mathrm{DET}(M(a)) \pmod{p}$. If $d \ne 0$ output NO!!, else YES??

DETPOLYZERO is in RP

Here is a rand algorithm for DETPOLYZERO.

1. Input $M(x)$ ($n \times n$ matrix of polys of degree $\le d$).
2. Pick prime $(dn)^2 \le p \le 2(dn)^2$ and $a \in \{0, \ldots, p-1\}$.
3. $d = \mathrm{DET}(M(a)) \pmod{p}$. If $d \ne 0$ output NO!!, else YES??

If $\mathrm{DET}(M(x)) = 0$ then $d = 0$.

DETPOLYZERO is in RP

Here is a rand algorithm for DETPOLYZERO.

1. Input $M(x)$ ($n \times n$ matrix of polys of degree $\le d$).
2. Pick prime $(dn)^2 \le p \le 2(dn)^2$ and $a \in \{0, \ldots, p-1\}$.
3. $d = \mathrm{DET}(M(a)) \pmod{p}$. If $d \ne 0$ output NO!!, else YES??

If $\mathrm{DET}(M(x)) = 0$ then $d = 0$.
If $\mathrm{DET}(M(x)) \ne 0$ then likely $d \ne 0$. (Proof next slide.)

DETPOLYZERO is in RP

Here is a rand algorithm for DETPOLYZERO.

1. Input $M(x)$ ($n \times n$ matrix of polys of degree $\le d$).
2. Pick prime $(dn)^2 \le p \le 2(dn)^2$ and $a \in \{0, \ldots, p-1\}$.
3. $d = \mathrm{DET}(M(a)) \pmod{p}$. If $d \ne 0$ output NO!!, else YES??

If $\mathrm{DET}(M(x)) = 0$ then $d = 0$.
If $\mathrm{DET}(M(x)) \ne 0$ then likely $d \ne 0$. (Proof next slide.)
Note In the above algorithm, we use "mod p" so that the intermediate values do not get so large.

Prob of Error

If $\mathrm{DET}(M(x)) \neq 0$ then $\mathrm{DET}(M(x))$ is a poly of degree $\leq dn$.

Prob of Error

If $\mathrm{DET}(M(x)) \neq 0$ then $\mathrm{DET}(M(x))$ is a poly of degree $\leq dn$.

View $\mathrm{DET}(M(x))$ as a poly in mod p. It has $\leq dn$ roots mod p.

Prob of Error

If $\mathrm{DET}(M(x)) \neq 0$ then $\mathrm{DET}(M(x))$ is a poly of degree $\leq dn$.

View $\mathrm{DET}(M(x))$ as a poly in mod p. It has $\leq dn$ roots mod p.

$a \in \{0, \ldots, p-1\}$ where $p \sim (dn)^2$ is picked at random.

Prob of Error

If $\mathrm{DET}(M(x)) \neq 0$ then $\mathrm{DET}(M(x))$ is a poly of degree $\leq dn$.

View $\mathrm{DET}(M(x))$ as a poly in mod p. It has $\leq dn$ roots mod p.

$a \in \{0, \ldots, p-1\}$ where $p \sim (dn)^2$ is picked at random.

Prob($\mathrm{DET}(M(a)) \equiv 0 \pmod{p}$)=Prob($a$ is a root):

$$\frac{dn}{d^2n^2} = \frac{1}{dn} \leq \frac{1}{n} \text{ which is small!.}$$

Can We Reduce the Probability of Error?

Lets say we had a Rand Alg for A with Prob of error $\leq \frac{1}{4}$.

Can We Reduce the Probability of Error?

Lets say we had a Rand Alg for A with Prob of error $\leq \frac{1}{4}$.

$$\begin{aligned} x \in A \rightarrow \Pr(\mathrm{ALG}(x) = 0) &\leq \tfrac{1}{4} \\ x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) &= 1 \end{aligned}$$

Can We Reduce the Probability of Error?

Lets say we had a Rand Alg for A with Prob of error $\leq \frac{1}{4}$.

$$
\begin{array}{ll}
x \in A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & \leq \frac{1}{4} \\
x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & = 1
\end{array}
$$

Can we get the probability of being right higher? Discuss

Can We Reduce the Probability of Error?

Lets say we had a Rand Alg for A with Prob of error $\leq \frac{1}{4}$.

$$\begin{aligned} x \in A \rightarrow \Pr(\mathrm{ALG}(x) = 0) &\leq \frac{1}{4} \\ x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) &= 1 \end{aligned}$$

Can we get the probability of being right higher? Discuss

ALG2: Run it twice!

Can We Reduce the Probability of Error?

Lets say we had a Rand Alg for A with Prob of error $\leq \frac{1}{4}$.

$$\begin{array}{ll} x \in A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & \leq \frac{1}{4} \\ x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & = 1 \end{array}$$

Can we get the probability of being right higher? Discuss

ALG2: Run it twice!
If either time is says 1, then output 1. Else output 0

Can We Reduce the Probability of Error?

Lets say we had a Rand Alg for A with Prob of error $\leq \frac{1}{4}$.

$$\begin{array}{ll} x \in A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & \leq \frac{1}{4} \\ x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & = 1 \end{array}$$

Can we get the probability of being right higher? Discuss

ALG2: Run it twice!
If either time is says 1, then output 1. Else output 0

$$\begin{array}{ll} x \in A \rightarrow \Pr(\mathrm{ALG2}(x) = 0) & \leq \frac{1}{4^2} \\ x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & = 1 \end{array}$$

Can We Reduce the Probability of Error?

Lets say we had a Rand Alg for A with Prob of error $\leq \frac{1}{4}$.

$$\begin{array}{ll} x \in A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & \leq \frac{1}{4} \\ x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & = 1 \end{array}$$

Can we get the probability of being right higher? Discuss

ALG2: Run it twice!
If either time is says 1, then output 1. Else output 0

$$\begin{array}{ll} x \in A \rightarrow \Pr(\mathrm{ALG2}(x) = 0) & \leq \frac{1}{4^2} \\ x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & = 1 \end{array}$$

Run n times to get Prob of error $\leq \frac{1}{4^n}$.

Can We Reduce the Probability of Error?

Lets say we had a Rand Alg for A with Prob of error $\le \frac{1}{4}$.

$$\begin{array}{ll} x \in A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & \le \frac{1}{4} \\ x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & = 1 \end{array}$$

Can we get the probability of being right higher? Discuss

$\mathrm{ALG2}$: Run it twice!
If either time is says 1, then output 1. Else output 0

$$\begin{array}{ll} x \in A \rightarrow \Pr(\mathrm{ALG2}(x) = 0) & \le \frac{1}{4^2} \\ x \notin A \rightarrow \Pr(\mathrm{ALG}(x) = 0) & = 1 \end{array}$$

Run n times to get Prob of error $\le \frac{1}{4^n}$.

Moral If have 1-sided error and Prob of error < 1 then can iterate to get error very small.

Rand Poly Time (RP)

Def A set A is in **Randomized Polynomial Time (RP)** if there exists a randomized algorithm ALG that runs in poly time such that:

$$\begin{array}{ll} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) = 0) \leq \frac{1}{4} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) = 0) = 1 \end{array}$$

1) Equiv to def where replace $\frac{1}{4}$ by $\frac{1}{2^{|x|}}$

Rand Poly Time (RP)

Def A set A is in **Randomized Polynomial Time (RP)** if there exists a randomized algorithm ALG that runs in poly time such that:

$$\begin{aligned} x \in A &\rightarrow \Pr(\mathrm{ALG}(x) = 0) \leq \frac{1}{4} \\ x \notin A &\rightarrow \Pr(\mathrm{ALG}(x) = 0) = 1 \end{aligned}$$

1) Equiv to def where replace $\frac{1}{4}$ by $\frac{1}{2^{|x|}}$
2) Our RP is 1-sided error. 2-sided error classes have been defined.

Rand Poly Time (RP)

Def A set A is in **Randomized Polynomial Time (RP)** if there exists a randomized algorithm ALG that runs in poly time such that:

$$\begin{aligned} x \in A &\rightarrow \Pr(\mathrm{ALG}(x) = 0) \le \tfrac{1}{4} \\ x \notin A &\rightarrow \Pr(\mathrm{ALG}(x) = 0) = 1 \end{aligned}$$

1) Equiv to def where replace $\frac{1}{4}$ by $\frac{1}{2^{|x|}}$
2) Our RP is 1-sided error. 2-sided error classes have been defined.
3) Very few problems in RP that are not known to be in P. DETPOLYZERO is one of them.

Rand Poly Time (RP)

Def A set A is in **Randomized Polynomial Time (RP)** if there exists a randomized algorithm ALG that runs in poly time such that:

$$\begin{array}{ll} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) = 0) \le \frac{1}{4} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) = 0) = 1 \end{array}$$

1) Equiv to def where replace $\frac{1}{4}$ by $\frac{1}{2^{|x|}}$
2) Our RP is 1-sided error. 2-sided error classes have been defined.
3) Very few problems in RP that are not known to be in P. DETPOLYZERO is one of them.
4) RP is thought to be feasible.

Famous and Motivating Example

$\mathrm{PRIMES} \in \mathrm{RP}.$

Famous and Motivating Example

$\mathrm{PRIMES} \in \mathrm{RP}$.

1. This was an early example of a problem in RP. (A 1967 paper sort-of has it, but a 1977 paper has it, and the algorithm actually used is 1980.)

Famous and Motivating Example

$\text{PRIMES} \in \text{RP}$.

1. This was an early example of a problem in RP. (A 1967 paper sort-of has it, but a 1977 paper has it, and the algorithm actually used is 1980.)
2. This result may have motivated the definition of RP.

Famous and Motivating Example

$\mathrm{PRIMES} \in \mathrm{RP}$.

1. This was an early example of a problem in RP. (A 1967 paper sort-of has it, but a 1977 paper has it, and the algorithm actually used is 1980.)
2. This result may have motivated the definition of RP.
3. The $\mathrm{PRIMES} \in \mathrm{RP}$ algorithm is very fast and actually used for many cryptography protocols.

Famous and Motivating Example

$\mathrm{PRIMES} \in \mathrm{RP}$.

1. This was an early example of a problem in RP. (A 1967 paper sort-of has it, but a 1977 paper has it, and the algorithm actually used is 1980.)
2. This result may have motivated the definition of RP.
3. The $\mathrm{PRIMES} \in \mathrm{RP}$ algorithm is very fast and actually used for many cryptography protocols.
4. In 2002 $\mathrm{PRIMES} \in \mathrm{P}$ was proven. The algorithm is much slower than the randomized algorithm; however, it is interesting that the problem is in P.

Famous and Motivating Example

$\text{PRIMES} \in \text{RP}$.

1. This was an early example of a problem in RP. (A 1967 paper sort-of has it, but a 1977 paper has it, and the algorithm actually used is 1980.)
2. This result may have motivated the definition of RP.
3. The $\text{PRIMES} \in \text{RP}$ algorithm is very fast and actually used for many cryptography protocols.
4. In 2002 $\text{PRIMES} \in \text{P}$ was proven. The algorithm is much slower than the randomized algorithm; however, it is interesting that the problem is in P.
5. There are reasons to think $\text{P} = \text{RP}$.

Randomized Reductions: Intuition

The following would be a good definition but it is **not** our definition.

Randomized Reductions: Intuition

The following would be a good definition but it is **not** our definition.

$$\begin{aligned} x \in A &\rightarrow \Pr(\mathrm{ALG}(x) \in B) \geq \tfrac{3}{4} \\ x \notin A &\rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{aligned}$$

Randomized Reductions: Intuition

The following would be a good definition but it is **not** our definition.

$$\begin{array}{ll} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) \in B) \geq \frac{3}{4} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{array}$$

We **demand less!** of our reductions.
Def $A \leq_r B$ if there is an alg ALG and a poly q such that

Randomized Reductions: Intuition

The following would be a good definition but it is **not** our definition.

$$\begin{aligned} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) \in B) \geq \frac{3}{4} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{aligned}$$

We **demand less!** of our reductions.
Def $A \leq_r B$ if there is an alg ALG and a poly q such that

$$\begin{aligned} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) \in B) \geq \frac{1}{q(n)} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{aligned}$$

Randomized Reductions: Intuition

The following would be a good definition but it is **not** our definition.

$$\begin{array}{ll} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{3}{4} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{array}$$

We **demand less!** of our reductions.
Def $A \le_r B$ if there is an alg ALG and a poly q such that

$$\begin{array}{ll} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{1}{q(n)} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{array}$$

How Odd! We seem to be allowing a large prob of error!

Randomized Reductions: Intuition

The following would be a good definition but it is **not** our definition.

$$\begin{array}{ll} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{3}{4} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{array}$$

We **demand less!** of our reductions.
Def $A \le_r B$ if there is an alg ALG and a poly q such that

$$\begin{array}{ll} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{1}{q(n)} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{array}$$

How Odd! We seem to be allowing a large prob of error!

Plan This small prob of success will get us all we need.

$A \leq_r B$ and $B \in \mathrm{P} \rightarrow A \in \mathrm{RP}$

$A \leq_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

$A \le_r B$ and $B \in \mathrm{P} \to A \in \mathrm{RP}$

$A \le_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

1. Input x. Let $|x| = n$.

$A \leq_r B$ and $B \in \mathrm{P} \rightarrow A \in \mathrm{RP}$

$A \leq_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

1. Input x. Let $|x| = n$.
2. Run $\mathrm{ALG}(x)$ $2q(n)$ times to get $y_1, \ldots, y_{2q(n)}$.

$A \leq_r B$ and $B \in \mathrm{P} \rightarrow A \in \mathrm{RP}$

$A \leq_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

1. Input x. Let $|x| = n$.
2. Run $\mathrm{ALG}(x)$ $2q(n)$ times to get $y_1, \ldots, y_{2q(n)}$.
3. For $1 \leq i \leq 2q(n)$ ask if $y_i \in B$. If any of the answers are YES, then output YES. Otherwise output NO.

$A \leq_r B$ and $B \in \mathrm{P} \rightarrow A \in \mathrm{RP}$

$A \leq_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

1. Input x. Let $|x| = n$.
2. Run $\mathrm{ALG}(x)$ $2q(n)$ times to get $y_1, \ldots, y_{2q(n)}$.
3. For $1 \leq i \leq 2q(n)$ ask if $y_i \in B$. If any of the answers are YES, then output YES. Otherwise output NO.

$x \in A \rightarrow \Pr(y_i \in B) \geq \frac{1}{q(|x|)}$, hence

$A \le_r B$ and $B \in \mathrm{P} \rightarrow A \in \mathrm{RP}$

$A \le_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

1. Input x. Let $|x| = n$.
2. Run $\mathrm{ALG}(x)$ $2q(n)$ times to get $y_1, \ldots, y_{2q(n)}$.
3. For $1 \le i \le 2q(n)$ ask if $y_i \in B$. If any of the answers are YES, then output YES. Otherwise output NO.

$x \in A \rightarrow \Pr(y_i \in B) \ge \frac{1}{q(|x|)}$, hence

$$\Pr((\forall i)[y_i \notin B]) \le \left(1 - \frac{1}{q(n)}\right)^{2q(n)}$$

$A \le_r B$ and $B \in \mathrm{P} \rightarrow A \in \mathrm{RP}$

$A \le_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

1. Input x. Let $|x| = n$.
2. Run $\mathrm{ALG}(x)$ $2q(n)$ times to get $y_1, \ldots, y_{2q(n)}$.
3. For $1 \le i \le 2q(n)$ ask if $y_i \in B$. If any of the answers are YES, then output YES. Otherwise output NO.

$x \in A \rightarrow \mathrm{Pr}(y_i \in B) \ge \frac{1}{q(|x|)}$, hence

$$\begin{aligned}
\mathrm{Pr}((\forall i)[y_i \notin B]) &\le \left(1 - \frac{1}{q(n)}\right)^{2q(n)} \\
&\le (e^{-1/q(n)})^{2q(n)} \le (e^{-1})^2 \le \frac{1}{4}
\end{aligned}$$

$A \le_r B$ and $B \in \mathrm{P} \rightarrow A \in \mathrm{RP}$

$A \le_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

1. Input x. Let $|x| = n$.
2. Run $\mathrm{ALG}(x)$ $2q(n)$ times to get $y_1, \ldots, y_{2q(n)}$.
3. For $1 \le i \le 2q(n)$ ask if $y_i \in B$. If any of the answers are YES, then output YES. Otherwise output NO.

$x \in A \rightarrow \Pr(y_i \in B) \ge \frac{1}{q(|x|)}$, hence

$$\begin{aligned} \Pr((\forall i)[y_i \notin B]) &\le \left(1 - \frac{1}{q(n)}\right)^{2q(n)} \\ &\le (e^{-1/q(n)})^{2q(n)} \le (e^{-1})^2 \le \frac{1}{4} \end{aligned}$$

Hence $\Pr((\exists i)[y_i \in B]) \ge 1 - \frac{1}{4} = \frac{3}{4}$.

$A \leq_r B$ and $B \in \mathrm{P} \rightarrow A \in \mathrm{RP}$

$A \leq_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

1. Input x. Let $|x| = n$.
2. Run $\mathrm{ALG}(x)$ $2q(n)$ times to get $y_1, \ldots, y_{2q(n)}$.
3. For $1 \leq i \leq 2q(n)$ ask if $y_i \in B$. If any of the answers are YES, then output YES. Otherwise output NO.

$x \in A \rightarrow \Pr(y_i \in B) \geq \frac{1}{q(|x|)}$, hence

$$\begin{aligned}\Pr((\forall i)[y_i \notin B]) &\leq \left(1 - \frac{1}{q(n)}\right)^{2q(n)} \\ &\leq (e^{-1/q(n)})^{2q(n)} \leq (e^{-1})^2 \leq \frac{1}{4}\end{aligned}$$

Hence $\Pr((\exists i)[y_i \in B]) \geq 1 - \frac{1}{4} = \frac{3}{4}$.
So $x \in A \rightarrow$ Prob Alg says YES is $\geq \frac{3}{4}$.

$A \leq_r B$ and $B \in \mathrm{P} \rightarrow A \in \mathrm{RP}$

$A \leq_r B$ via f and polynomial q. Here is Alg for $A \in \mathrm{RP}$.

1. Input x. Let $|x| = n$.
2. Run $\mathrm{ALG}(x)$ $2q(n)$ times to get $y_1, \ldots, y_{2q(n)}$.
3. For $1 \leq i \leq 2q(n)$ ask if $y_i \in B$. If any of the answers are YES, then output YES. Otherwise output NO.

$x \in A \rightarrow \Pr(y_i \in B) \geq \frac{1}{q(|x|)}$, hence

$$\begin{aligned}\Pr((\forall i)[y_i \notin B]) &\leq \left(1 - \frac{1}{q(n)}\right)^{2q(n)} \\ &\leq (e^{-1/q(n)})^{2q(n)} \leq (e^{-1})^2 \leq \frac{1}{4}\end{aligned}$$

Hence $\Pr((\exists i)[y_i \in B]) \geq 1 - \frac{1}{4} = \frac{3}{4}$.
So $x \in A \rightarrow$ Prob Alg says YES is $\geq \frac{3}{4}$.

$x \notin A \rightarrow (\forall i)[y_i \notin B]$ hence Rand Alg says NO.

Our Plan (This is what Valiant-Vazirani did)

Given ϕ we produce a formula ζ such that

$$\begin{aligned} \phi \in SAT &\rightarrow \#(\zeta) = 1 \text{ with high probability;} \\ \phi \notin SAT &\rightarrow \#(\zeta) = 0. \end{aligned}$$

Our Plan (This is what Valiant-Vazirani did)

Given ϕ we produce a formula ζ such that

$$\begin{aligned} \phi \in SAT &\quad \rightarrow \#(\zeta) = 1 \text{ with high probability;} \\ \phi \notin SAT &\quad \rightarrow \#(\zeta) = 0. \end{aligned}$$

A formula is a set of satisfying assignments!

Our Plan (This is what Valiant-Vazirani did)

Given ϕ we produce a formula ζ such that

$$\begin{aligned} \phi \in SAT &\quad \rightarrow \#(\zeta) = 1 \text{ with high probability;} \\ \phi \notin SAT &\quad \rightarrow \#(\zeta) = 0. \end{aligned}$$

A formula is a set of satisfying assignments!

We want to **map** this set to a much **smaller set**.

Our Plan (This is what Valiant-Vazirani did)

Given ϕ we produce a formula ζ such that

$$\begin{aligned} \phi \in SAT &\rightarrow \#(\zeta) = 1 \text{ with high probability;} \\ \phi \notin SAT &\rightarrow \#(\zeta) = 0. \end{aligned}$$

A formula is a set of satisfying assignments!
We want to **map** this set to a much **smaller set**.
How do computer scientists map large sets to small sets? Discuss

Our Plan (This is what Valiant-Vazirani did)

Given ϕ we produce a formula ζ such that

$$\begin{aligned} \phi \in SAT &\rightarrow \#(\zeta) = 1 \text{ with high probability;} \\ \phi \notin SAT &\rightarrow \#(\zeta) = 0. \end{aligned}$$

A formula is a set of satisfying assignments!
We want to **map** this set to a much **smaller set**.
How do computer scientists map large sets to small sets? Discuss Hash Functions!

Hash Functions

Hash Functions: Motivation

Hash Functions: Motivation

If a set is **large** then a randomly chosen hash function will likely map some element to 0^k.

Hash Functions: Motivation

If a set is **large** then a randomly chosen hash function will likely map some element to 0^k.

If a set is **small** then a randomly chosen hash function is unlikely to map some element to 0^k.

Probability Review

Probability Review

1. A **sample space** is the set of things that could happen. In our case it will be the set of possible hash functions that could be produced.

Probability Review

1. A **sample space** is the set of things that could happen. In our case it will be the set of possible hash functions that could be produced.
2. A **random variable** is a mapping from the sample space to numbers. In our case it will be mapping the hash function h to the number $|\{x : h(x) = 0^k\}|$.

Probability Review

1. A **sample space** is the set of things that could happen. In our case it will be the set of possible hash functions that could be produced.
2. A **random variable** is a mapping from the sample space to numbers. In our case it will be mapping the hash function h to the number $|\{x : h(x) = 0^k\}|$.
3. If S is a random variable then $E(S)$ is its expected value and $Var(S)$ is its variance. It is known that $Var(S) = E((S - E(S))^2) = E(S^2) - E(S)^2$.

Probability Review

1. A **sample space** is the set of things that could happen. In our case it will be the set of possible hash functions that could be produced.
2. A **random variable** is a mapping from the sample space to numbers. In our case it will be mapping the hash function h to the number $|\{x : h(x) = 0^k\}|$.
3. If S is a random variable then $E(S)$ is its expected value and $Var(S)$ is its variance. It is known that $Var(S) = E((S - E(S))^2) = E(S^2) - E(S)^2$.

Convention Whenever we have a 0-1 valued matrix apply to a vector we do all of the calculations mod 2.

Lemma

Let $k, n \in \mathbb{N}$ with $0 \leq k \leq n$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Lemma

Let $k, n \in \mathbb{N}$ with $0 \leq k \leq n$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$. Consider the following random variable:

Lemma

Let $k, n \in \mathbb{N}$ with $0 \le k \le n$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M.

Lemma

Let $k, n \in \mathbb{N}$ with $0 \leq k \leq n$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M.

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Lemma

Let $k, n \in \mathbb{N}$ with $0 \le k \le n$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M.

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.

Lemma

Let $k, n \in \mathbb{N}$ with $0 \le k \le n$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M.

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.

Then

Lemma

Let $k, n \in \mathbb{N}$ with $0 \le k \le n$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M.

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.

Then

1. $E(S) = 2^{-k}|X|$

Lemma

Let $k, n \in \mathbb{N}$ with $0 \le k \le n$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M.

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.

Then

1. $E(S) = 2^{-k}|X|$
2. $Var(S) \le 2^{-k}|X|$.

Lemma

Let $k, n \in \mathbb{N}$ with $0 \le k \le n$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M.

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.

Then

1. $E(S) = 2^{-k}|X|$
2. $Var(S) \le 2^{-k}|X|$.

Note $E(S)$ and $Var(S)$ do not depends on n, just on k and $|X|$.

Proof of Lemma: R_x

Before looking at $E(S)$ and $Var(S)$ we will need to look at E of some easier random variables:

Proof of Lemma: R_x

Before looking at $E(S)$ and $Var(S)$ we will need to look at E of some easier random variables:

Let $x, y \in X$. Let R_x be the **random variable**

Proof of Lemma: R_x

Before looking at $E(S)$ and $Var(S)$ we will need to look at E of some easier random variables:

Let $x, y \in X$. Let R_x be the **random variable**

$$R_x = \begin{cases} 1 & \text{if } M(x) = 0^k; \\ 0 & \text{if } M(x) \neq 0^k. \end{cases} \tag{1}$$

Proof of Lemma: R_x

Before looking at $E(S)$ and $Var(S)$ we will need to look at E of some easier random variables:
Let $x, y \in X$. Let R_x be the **random variable**

$$R_x = \begin{cases} 1 & \text{if } M(x) = 0^k; \\ 0 & \text{if } M(x) \neq 0^k. \end{cases} \quad (1)$$

Let R_y be similar.

Proof of Lemma: R_x

Before looking at $E(S)$ and $Var(S)$ we will need to look at E of some easier random variables:
Let $x, y \in X$. Let R_x be the **random variable**

$$R_x = \begin{cases} 1 & \text{if } M(x) = 0^k; \\ 0 & \text{if } M(x) \neq 0^k. \end{cases} \tag{1}$$

Let R_y be similar.
Let $M_i(x)$ be the ith element of the vector $M(x)$.

Proof of Lemma: R_x

Before looking at $E(S)$ and $Var(S)$ we will need to look at E of some easier random variables:
Let $x, y \in X$. Let R_x be the **random variable**

$$R_x = \begin{cases} 1 & \text{if } M(x) = 0^k; \\ 0 & \text{if } M(x) \neq 0^k. \end{cases} \tag{1}$$

Let R_y be similar.
Let $M_i(x)$ be the ith element of the vector $M(x)$.

$$E(R_x) = \prod_{i=1}^{k} \Pr(M_i(x) = 0) = \frac{1}{2^k}$$

Proof of Lemma: R_x

Before looking at $E(S)$ and $Var(S)$ we will need to look at E of some easier random variables:
Let $x, y \in X$. Let R_x be the **random variable**

$$R_x = \begin{cases} 1 & \text{if } M(x) = 0^k; \\ 0 & \text{if } M(x) \neq 0^k. \end{cases} \tag{1}$$

Let R_y be similar.
Let $M_i(x)$ be the ith element of the vector $M(x)$.

$$E(R_x) = \prod_{i=1}^{k} \Pr(M_i(x) = 0) = \frac{1}{2^k}$$

We also have

Proof of Lemma: R_x

Before looking at $E(S)$ and $Var(S)$ we will need to look at E of some easier random variables:
Let $x, y \in X$. Let R_x be the **random variable**

$$R_x = \begin{cases} 1 & \text{if } M(x) = 0^k; \\ 0 & \text{if } M(x) \neq 0^k. \end{cases} \quad (1)$$

Let R_y be similar.
Let $M_i(x)$ be the ith element of the vector $M(x)$.

$$E(R_x) = \prod_{i=1}^{k} \Pr(M_i(x) = 0) = \frac{1}{2^k}$$

We also have

$$E(R_x^2) = \prod_{i=1}^{k} \Pr(M_i(x) = 0) = \frac{1}{2^k}$$

Proof of Lemma: $R_x R_y$

We now compute $E(R_x R_y)$.

Proof of Lemma: $R_x R_y$

We now compute $E(R_x R_y)$.

$$E(R_x R_y) = \Pr(M(x) = 1 \wedge M(y) = 1) = \frac{1}{2^k} \times \frac{1}{2^k} = \frac{1}{4^k}.$$

Proof of Lemma $E(S), V(S)$

$$E(S) = E(\sum_{x \in X} R_x) = \sum_{x \in X} E(R_x) = \frac{1}{2^k}|X|.$$

Proof of Lemma $E(S), V(S)$

$$E(S) = E(\sum_{x \in X} R_x) = \sum_{x \in X} E(R_x) = \frac{1}{2^k}|X|.$$

Recall that $Var(S) = E(S^2) - (E(S))^2$.

Proof of Lemma $E(S), V(S)$

$$E(S) = E(\sum_{x \in X} R_x) = \sum_{x \in X} E(R_x) = \frac{1}{2^k}|X|.$$

Recall that $Var(S) = E(S^2) - (E(S))^2$.

$$\begin{aligned}
\mathbf{E(S^2)} &= \mathbf{E((\textstyle\sum_{x \in X} R_x)(\textstyle\sum_{y \in X} R_y));} \\
&= \textstyle\sum_{x \in X} \sum_{y \in X} E(R_x R_y); \\
&= \textstyle\sum_{x \in X} E(R_x^2) + \sum_{x \neq y} E(R_x R_y); \\
&= \textstyle\sum_{x \in X} \frac{1}{2^k} + \sum_{x \neq y} \frac{1}{4^k}; \\
&= \mathbf{\tfrac{1}{2^k}|X| + \tfrac{1}{4^k}|X|(|X| - 1);}
\end{aligned}$$

Proof of Lemma $E(S), V(S)$

$$E(S) = E(\sum_{x \in X} R_x) = \sum_{x \in X} E(R_x) = \frac{1}{2^k}|X|.$$

Recall that $Var(S) = E(S^2) - (E(S))^2$.

$$\begin{aligned}
\mathbf{E(S^2)} &= \mathbf{E((\textstyle\sum_{x \in X} R_x)(\sum_{y \in X} R_y));} \\
&= \textstyle\sum_{x \in X} \sum_{y \in X} E(R_x R_y); \\
&= \textstyle\sum_{x \in X} E(R_x^2) + \sum_{x \neq y} E(R_x R_y); \\
&= \textstyle\sum_{x \in X} \frac{1}{2^k} + \sum_{x \neq y} \frac{1}{4^k}; \\
&= \mathbf{\tfrac{1}{2^k}|X| + \tfrac{1}{4^k}|X|(|X| - 1);}
\end{aligned}$$

$$\begin{aligned}
\mathbf{Var(S)} &= \mathbf{E(S^2) - (E(S))^2} \\
&= \tfrac{1}{2^k}|X| + \tfrac{1}{4^k}|X|(|X| - 1) - \tfrac{1}{4^k}|X|^2 \\
&= \tfrac{1}{2^k}|X| + \tfrac{1}{4^k}|X|^2 - \tfrac{1}{4^k}|X| - \tfrac{1}{4^k}|X|^2 \\
&= \tfrac{1}{2^k}|X| - \tfrac{1}{4^k}|X| \\
&\leq \mathbf{\tfrac{1}{2^k}|X|}
\end{aligned}$$

What if $k = 0$?

Recall we had:

What if $k = 0$?

Recall we had:
Let $k, n \in \mathbb{N}$ with $0 \leq k \leq n$.

What if $k = 0$?

Recall we had:
Let $k, n \in \mathbb{N}$ with $0 \leq k \leq n$.

Pick a random $k \times n$ 0-1 valued matrix M.

What if $k = 0$?

Recall we had:

Let $k, n \in \mathbb{N}$ with $0 \leq k \leq n$.

Pick a random $k \times n$ 0-1 valued matrix M.

We allowed $k = 0$.

What if $k = 0$?

Recall we had:

Let $k, n \in \mathbb{N}$ with $0 \leq k \leq n$.

Pick a random $k \times n$ 0-1 valued matrix M.

We allowed $k = 0$.

What is a $0 \times n$ *matrix?*

What if $k = 0$?

Recall we had:

Let $k, n \in \mathbb{N}$ with $0 \leq k \leq n$.

Pick a random $k \times n$ 0-1 valued matrix M.

We allowed $k = 0$.

What is a $0 \times n$ matrix?

What is the sound of one hand clapping?

What if $k = 0$?

Recall we had:
Let $k, n \in \mathbb{N}$ with $0 \leq k \leq n$.

Pick a random $k \times n$ 0-1 valued matrix M.

We allowed $k = 0$.

What is a $0 \times n$ matrix?

What is the sound of one hand clapping?

The matrix question is easier: By convention the $0 \times n$ matrix has no effect. So

$$X = \{x \in X : M(x) = 0^k\}.$$

Plan

Def Let $\ell \in \mathbb{N}$. Then SAT_ℓ is

$$\{\phi : 1 \le \#(\phi) \le \ell\}.$$

Plan

Def Let $\ell \in \mathbb{N}$. Then SAT_ℓ is

$$\{\phi : 1 \le \#(\phi) \le \ell\}.$$

Plan

1) $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$. (Why 12? We'll see later.)

Plan

Def Let $\ell \in \mathbb{N}$. Then SAT_ℓ is

$$\{\phi : 1 \le \#(\phi) \le \ell\}.$$

Plan
1) $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$. (Why 12? We'll see later.)
2) $\mathrm{SAT}_{12} \le_r \mathrm{SAT}_1$. (Not Quite- this reduction will only be correct if the input comes from the first reduction.)

$$\mathrm{SAT} \leq_r \mathrm{SAT}_{12}$$

Chebyshev's inequality

If S is any random variable and $a > 0$ then

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Chebyshev's inequality

If S is any random variable and $a > 0$ then

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Intuitively this is saying that the probability that S is far away from $E(S)$ is small, and how small depends on $Var(S)$.

Chebyshev's inequality

If S is any random variable and $a > 0$ then

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Intuitively this is saying that the probability that S is far away from $E(S)$ is small, and how small depends on $Var(S)$.

Chebyshev proved it so we don't have to :-)

Before We Prove $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Recall

Def Let A and B be two sets. We say that $A \le_r B$ if there exists fast Rand Alg ALG and poly q:

Before We Prove $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Recall

Def Let A and B be two sets. We say that $A \le_r B$ if there exists fast Rand Alg ALG and poly q:

$$\begin{aligned} x \in A &\rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{1}{q(n)} \\ x \notin A &\rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{aligned}$$

Before We Prove $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Recall

Def Let A and B be two sets. We say that $A \le_r B$ if there exists fast Rand Alg ALG and poly q:

$$\begin{array}{ll} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{1}{q(n)} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{array}$$

We will get a reduction ϕ to ψ where

Before We Prove $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Recall

Def Let A and B be two sets. We say that $A \le_r B$ if there exists fast Rand Alg ALG and poly q:

$$\begin{aligned} x \in A &\rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{1}{q(n)} \\ x \notin A &\rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{aligned}$$

We will get a reduction ϕ to ψ where
$\phi \in \mathrm{SAT} \rightarrow \Pr(1 \le \#\psi \le 12) \ge \frac{1}{2n}$.

Before We Prove $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Recall

Def Let A and B be two sets. We say that $A \le_r B$ if there exists fast Rand Alg ALG and poly q:

$$\begin{aligned} x \in A &\rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{1}{q(n)} \\ x \notin A &\rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{aligned}$$

We will get a reduction ϕ to ψ where
$\phi \in \mathrm{SAT} \rightarrow \Pr(1 \le \#\psi \le 12) \ge \frac{1}{2n}$. **Key** Not much to ask for!

Before We Prove $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Recall

Def Let A and B be two sets. We say that $A \le_r B$ if there exists fast Rand Alg ALG and poly q:

$$\begin{array}{ll} x \in A & \rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{1}{q(n)} \\ x \notin A & \rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{array}$$

We will get a reduction ϕ to ψ where

$\phi \in \mathrm{SAT} \rightarrow \Pr(1 \le \#\psi \le 12) \ge \frac{1}{2n}$. **Key** Not much to ask for!

$\phi \notin \mathrm{SAT} \rightarrow \#\psi = 0$.

Before We Prove $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Recall

Def Let A and B be two sets. We say that $A \le_r B$ if there exists fast Rand Alg ALG and poly q:

$$\begin{aligned} x \in A &\rightarrow \Pr(\mathrm{ALG}(x) \in B) \ge \frac{1}{q(n)} \\ x \notin A &\rightarrow \Pr(\mathrm{ALG}(x) \notin B) = 1 \end{aligned}$$

We will get a reduction ϕ to ψ where

$\phi \in \mathrm{SAT} \rightarrow \Pr(1 \le \#\psi \le 12) \ge \frac{1}{2n}$. **Key** Not much to ask for!

$\phi \notin \mathrm{SAT} \rightarrow \#\psi = 0$. **Key** This will be easy.

$\mathrm{SAT} \leq_r \mathrm{SAT}_{12}$

Here is the randomized reduction.

$\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Here is the randomized reduction.

1. Input $\phi(\vec{x})$. Let n be the number of variables in ϕ.

SAT $\leq_r$ SAT$_{12}$

Here is the randomized reduction.

1. Input $\phi(\vec{x})$. Let n be the number of variables in ϕ.
2. Evaluate $\phi(\vec{0})$. If T then output $x \in \mathrm{SAT}_{12}$.

$\text{SAT} \le_r \text{SAT}_{12}$

Here is the randomized reduction.

1. Input $\phi(\vec{x})$. Let n be the number of variables in ϕ.
2. Evaluate $\phi(\vec{0})$. If T then output $x \in \text{SAT}_{12}$.
   If FALSE then goto next step. **Note** If X is the set of satisfying assignments then $0^n \notin X$.

SAT $\leq_r$ SAT$_{12}$

Here is the randomized reduction.

1. Input $\phi(\vec{x})$. Let n be the number of variables in ϕ.
2. Evaluate $\phi(\vec{0})$. If T then output $x \in \mathrm{SAT}_{12}$.
   If FALSE then goto next step. **Note** If X is the set of satisfying assignments then $0^n \notin X$.
3. Pick a random $k \in \{0, \ldots, n-1\}$ (uniformly).

$\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Here is the randomized reduction.

1. Input $\phi(\vec{x})$. Let n be the number of variables in ϕ.
2. Evaluate $\phi(\vec{0})$. If T then output $x \in \mathrm{SAT}_{12}$.
   If FALSE then goto next step. **Note** If X is the set of satisfying assignments then $0^n \notin X$.
3. Pick a random $k \in \{0, \ldots, n-1\}$ (uniformly).
4. Pick a random $k \times n$ 0-1 valued matrix M.

SAT $\leq_r$ SAT$_{12}$

Here is the randomized reduction.

1. Input $\phi(\vec{x})$. Let n be the number of variables in ϕ.
2. Evaluate $\phi(\vec{0})$. If T then output $x \in \mathrm{SAT}_{12}$.
   If FALSE then goto next step. **Note** If X is the set of satisfying assignments then $0^n \notin X$.
3. Pick a random $k \in \{0, \ldots, n-1\}$ (uniformly).
4. Pick a random $k \times n$ 0-1 valued matrix M.
5. Output the Boolean formula $\psi(\vec{x}) = \phi(x) \wedge (M(x) = 0^k)$.

$\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Here is the randomized reduction.

1. Input $\phi(\vec{x})$. Let n be the number of variables in ϕ.
2. Evaluate $\phi(\vec{0})$. If T then output $x \in \mathrm{SAT}_{12}$.
   If FALSE then goto next step. **Note** If X is the set of satisfying assignments then $0^n \notin X$.
3. Pick a random $k \in \{0, \ldots, n-1\}$ (uniformly).
4. Pick a random $k \times n$ 0-1 valued matrix M.
5. Output the Boolean formula $\psi(\vec{x}) = \phi(x) \wedge (M(x) = 0^k)$.

Clearly if $\phi \notin \mathrm{SAT}$ then $\psi \notin \mathrm{SAT}_{12}$.

$\mathrm{SAT} \le_r \mathrm{SAT}_{12}$

Here is the randomized reduction.

1. Input $\phi(\vec{x})$. Let n be the number of variables in ϕ.
2. Evaluate $\phi(\vec{0})$. If T then output $x \in \mathrm{SAT}_{12}$.
   If FALSE then goto next step. **Note** If X is the set of satisfying assignments then $0^n \notin X$.
3. Pick a random $k \in \{0, \ldots, n-1\}$ (uniformly).
4. Pick a random $k \times n$ 0-1 valued matrix M.
5. Output the Boolean formula $\psi(\vec{x}) = \phi(x) \wedge (M(x) = 0^k)$.

Clearly if $\phi \notin \mathrm{SAT}$ then $\psi \notin \mathrm{SAT}_{12}$.
Need that if $\phi \in \mathrm{SAT}$ then $\Pr(1 \le \#\psi \le 12) \ge \frac{1}{2n}$.

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \leq 12$?

If k is assigned to 0 at random then

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \leq 12$?

If k is assigned to 0 at random then

$$\phi = \psi \in \mathrm{SAT}_{12}$$

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \leq 12$?

If k is assigned to 0 at random then

$$\phi = \psi \in \mathrm{SAT}_{12}$$

$\Pr(k = 0) = \frac{1}{n} \geq \frac{1}{2n}$.

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \geq 13$?

m is such that $2^m < \#(\phi) \leq 2^{m+1}$. **Note** $m \in \{3, \ldots, n-1\}$.)

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \geq 13$?

m is such that $2^m < \#(\phi) \leq 2^{m+1}$. **Note** $m \in \{3, \ldots, n-1\}$.)

$$\Pr(k = m - 2) = \frac{1}{n}.$$

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \geq 13$?

m is such that $2^m < \#(\phi) \leq 2^{m+1}$. **Note** $m \in \{3, \ldots, n-1\}$.)

$$\Pr(k = m - 2) = \frac{1}{n}.$$

We will show If $k = m - 2$ then

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \geq 13$?

m is such that $2^m < \#(\phi) \leq 2^{m+1}$. **Note** $m \in \{3, \ldots, n-1\}$.)

$$\Pr(k = m - 2) = \frac{1}{n}.$$

We will show If $k = m - 2$ then

$$\Pr(1 \leq \#\psi \leq 12) \geq \frac{1}{2}$$

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \geq 13$?

m is such that $2^m < \#(\phi) \leq 2^{m+1}$. **Note** $m \in \{3, \ldots, n-1\}$.)

$$\Pr(k = m - 2) = \frac{1}{n}.$$

We will show If $k = m - 2$ then

$$\Pr(1 \leq \#\psi \leq 12) \geq \frac{1}{2}$$

We will then have

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \geq 13$?

m is such that $2^m < \#(\phi) \leq 2^{m+1}$. **Note** $m \in \{3, \ldots, n-1\}$.)

$$\Pr(k = m - 2) = \frac{1}{n}.$$

We will show If $k = m - 2$ then

$$\Pr(1 \leq \#\psi \leq 12) \geq \frac{1}{2}$$

We will then have

$$\Pr(1 \leq \#\psi \leq 12) \geq \frac{1}{n} \times \frac{1}{2} = \frac{1}{2n}.$$

What if $\phi \in \mathrm{SAT}$ and $\#(\phi) \geq 13$?

m is such that $2^m < \#(\phi) \leq 2^{m+1}$. **Note** $m \in \{3, \ldots, n-1\}$.)

$$\Pr(k = m - 2) = \frac{1}{n}.$$

We will show If $k = m - 2$ then

$$\Pr(1 \leq \#\psi \leq 12) \geq \frac{1}{2}$$

We will then have

$$\Pr(1 \leq \#\psi \leq 12) \geq \frac{1}{n} \times \frac{1}{2} = \frac{1}{2n}.$$

That is all we need to show!

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

X is the set of sat assignments of ϕ. $0^n \notin X$. $2^m < |X| \leq 2^{m+1}$.

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

X is the set of sat assignments of ϕ. $0^n \notin X$. $2^m < |X| \leq 2^{m+1}$.
Random hash function $h : \{0,1\}^n \to \{0,1\}^k$.

$2^m < \#\phi \le 2^{m+1}$ and $k = m - 2$

X is the set of sat assignments of ϕ. $0^n \notin X$. $2^m < |X| \le 2^{m+1}$.
Random hash function $h : \{0,1\}^n \to \{0,1\}^k$.

$$\#\psi = S = |\{x \in X : h(x) = 0^k\}|.$$

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

X is the set of sat assignments of ϕ. $0^n \notin X$. $2^m < |X| \leq 2^{m+1}$.
Random hash function $h : \{0,1\}^n \rightarrow \{0,1\}^k$.

$$\#\psi = S = |\{x \in X : h(x) = 0^k\}|.$$

We know

$$E(S) = 2^{-k}|X| = 2^{-(m-2)}|X|$$

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

X is the set of sat assignments of ϕ. $0^n \notin X$. $2^m < |X| \leq 2^{m+1}$.
Random hash function $h : \{0,1\}^n \to \{0,1\}^k$.

$$\#\psi = S = |\{x \in X : h(x) = 0^k\}|.$$

We know

$$E(S) = 2^{-k}|X| = 2^{-(m-2)}|X|$$

$$Var(S) \leq 2^{-(m-2)}|X|.$$

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

X is the set of sat assignments of ϕ. $0^n \notin X$. $2^m < |X| \leq 2^{m+1}$.
Random hash function $h : \{0,1\}^n \to \{0,1\}^k$.

$$\#\psi = S = |\{x \in X : h(x) = 0^k\}|.$$

We know

$$E(S) = 2^{-k}|X| = 2^{-(m-2)}|X|$$

$$Var(S) \leq 2^{-(m-2)}|X|.$$

Hence

$$2^{-(m-2)+m} < E(S) \leq 2^{-(m-2)+m+1},$$

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

X is the set of sat assignments of ϕ. $0^n \notin X$. $2^m < |X| \leq 2^{m+1}$.
Random hash function $h : \{0,1\}^n \to \{0,1\}^k$.

$$\#\psi = S = |\{x \in X : h(x) = 0^k\}|.$$

We know

$$E(S) = 2^{-k}|X| = 2^{-(m-2)}|X|$$

$$Var(S) \leq 2^{-(m-2)}|X|.$$

Hence

$$2^{-(m-2)+m} < E(S) \leq 2^{-(m-2)+m+1},$$

so

$$4 < E(S) \leq 8$$

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

X is the set of sat assignments of ϕ. $0^n \notin X$. $2^m < |X| \leq 2^{m+1}$.
Random hash function $h : \{0,1\}^n \to \{0,1\}^k$.

$$\#\psi = S = |\{x \in X : h(x) = 0^k\}|.$$

We know

$$E(S) = 2^{-k}|X| = 2^{-(m-2)}|X|$$

$$Var(S) \leq 2^{-(m-2)}|X|.$$

Hence

$$2^{-(m-2)+m} < E(S) \leq 2^{-(m-2)+m+1},$$

so

$$4 < E(S) \leq 8$$

and

$$Var(S) < 8.$$

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

Recap:

$$4 < E(S) \leq 8$$

and

$$Var(S) < 8.$$

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

Recap:

$$4 < E(S) \leq 8$$

and

$$Var(S) < 8.$$

Want $\Pr(|S| \notin \{1, \ldots, 12\}) \leq \frac{1}{2}$.

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

Recap:

$$4 < E(S) \leq 8$$

and

$$Var(S) < 8.$$

Want $\Pr(|S| \notin \{1, \ldots, 12\}) \leq \frac{1}{2}$.

By Chebyshev's inequality

$$\Pr(|S - E(S)| \geq 4) \leq \frac{Var(S)}{4^2} \leq \frac{8}{16} = \frac{1}{2}.$$

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

Recap:

$$4 < E(S) \leq 8$$

and

$$Var(S) < 8.$$

Want $\Pr(|S| \notin \{1, \ldots, 12\}) \leq \frac{1}{2}$.
By Chebyshev's inequality

$$\Pr(|S - E(S)| \geq 4) \leq \frac{Var(S)}{4^2} \leq \frac{8}{16} = \frac{1}{2}.$$

Since $4 < E(S) \leq 8$ this yields

$2^m < \#\phi \leq 2^{m+1}$ and $k = m - 2$

Recap:

$$4 < E(S) \leq 8$$

and

$$Var(S) < 8.$$

Want $\Pr(|S| \notin \{1, \ldots, 12\}) \leq \frac{1}{2}$.
By Chebyshev's inequality

$$\Pr(|S - E(S)| \geq 4) \leq \frac{Var(S)}{4^2} \leq \frac{8}{16} = \frac{1}{2}.$$

Since $4 < E(S) \leq 8$ this yields
$\Pr(S \in \{1, \ldots, 12\}) > 1 - \frac{1}{2} = \frac{1}{2}$.

$$\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$$

Not Quite

What We Really Need

Recall that we have a reduction that maps ϕ to ψ such that

$$\begin{aligned} \phi \in \mathrm{SAT} &\rightarrow \Pr(\psi \in \mathrm{SAT}_{12}) \geq \frac{1}{2n} \\ \phi \notin \mathrm{SAT} &\rightarrow \psi \notin \mathrm{SAT} \text{ hence } \psi \notin \mathrm{SAT}_{12} \end{aligned}$$

What We Really Need

Recall that we have a reduction that maps ϕ to ψ such that

$$\begin{array}{ll} \phi \in \mathrm{SAT} & \rightarrow \Pr(\psi \in \mathrm{SAT}_{12}) \geq \frac{1}{2n} \\ \phi \notin \mathrm{SAT} & \rightarrow \psi \notin \mathrm{SAT} \text{ hence } \psi \notin \mathrm{SAT}_{12} \end{array}$$

Let ψ be the output of this reduction. Then (with high prob)

$$\#\psi \in \{0, \ldots, 12\}.$$

What We Really Need

Recall that we have a reduction that maps ϕ to ψ such that

$$\begin{array}{ll} \phi \in \mathrm{SAT} & \rightarrow \Pr(\psi \in \mathrm{SAT}_{12}) \geq \frac{1}{2n} \\ \phi \notin \mathrm{SAT} & \rightarrow \psi \notin \mathrm{SAT} \text{ hence } \psi \notin \mathrm{SAT}_{12} \end{array}$$

Let ψ be the output of this reduction. Then (with high prob)

$$\#\psi \in \{0, \ldots, 12\}.$$

We do not need $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$.

What We Really Need

Recall that we have a reduction that maps ϕ to ψ such that

$$\begin{aligned} \phi \in \mathrm{SAT} &\rightarrow \Pr(\psi \in \mathrm{SAT}_{12}) \geq \frac{1}{2n} \\ \phi \notin \mathrm{SAT} &\rightarrow \psi \notin \mathrm{SAT} \text{ hence } \psi \notin \mathrm{SAT}_{12} \end{aligned}$$

Let ψ be the output of this reduction. Then (with high prob)

$$\#\psi \in \{0, \ldots, 12\}.$$

We do not need $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$.

We need $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$ where the input ψ has

$$\#\psi \in \{0, \ldots, 12\}.$$

What We Really Need

Recall that we have a reduction that maps ϕ to ψ such that

$$\begin{array}{ll} \phi \in \mathrm{SAT} & \rightarrow \Pr(\psi \in \mathrm{SAT}_{12}) \geq \frac{1}{2n} \\ \phi \notin \mathrm{SAT} & \rightarrow \psi \notin \mathrm{SAT} \text{ hence } \psi \notin \mathrm{SAT}_{12} \end{array}$$

Let ψ be the output of this reduction. Then (with high prob)

$$\#\psi \in \{0, \ldots, 12\}.$$

We do not need $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$.

We need $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$ where the input ψ has

$$\#\psi \in \{0, \ldots, 12\}.$$

We will get (with restricted input)

$$\begin{array}{ll} \psi \in \mathrm{SAT}_{12} & \rightarrow \Pr(\zeta \in \mathrm{SAT}_1) \geq \frac{1}{12} \\ \psi \notin \mathrm{SAT} & \rightarrow \zeta \notin \mathrm{SAT} \text{ hence } \zeta \notin \mathrm{SAT}_1 \end{array}$$

What We Really Need

Recall that we have a reduction that maps ϕ to ψ such that

$$\begin{array}{ll} \phi \in \mathrm{SAT} & \rightarrow \Pr(\psi \in \mathrm{SAT}_{12}) \geq \frac{1}{2n} \\ \phi \notin \mathrm{SAT} & \rightarrow \psi \notin \mathrm{SAT} \text{ hence } \psi \notin \mathrm{SAT}_{12} \end{array}$$

Let ψ be the output of this reduction. Then (with high prob)

$$\#\psi \in \{0, \ldots, 12\}.$$

We do not need $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$.

We need $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$ where the input ψ has

$$\#\psi \in \{0, \ldots, 12\}.$$

We will get (with restricted input)

$$\begin{array}{ll} \psi \in \mathrm{SAT}_{12} & \rightarrow \Pr(\zeta \in \mathrm{SAT}_1) \geq \frac{1}{12} \\ \psi \notin \mathrm{SAT} & \rightarrow \zeta \notin \mathrm{SAT} \text{ hence } \zeta \notin \mathrm{SAT}_1 \end{array}$$

Compose the two prob reductions to get $\mathrm{SAT} \leq_r \mathrm{SAT}_1$.

Notation

X_1 will be a vector of n variables.

Notation

X_1 will be a vector of n variables.

X_2 will be another vector of n variables, disjoint from X_1

Notation

X_1 will be a vector of n variables.

X_2 will be another vector of n variables, disjoint from X_1

X_3 will be another vector of n variables, disjoint from X_1 and X_2.

Notation

X_1 will be a vector of n variables.

X_2 will be another vector of n variables, disjoint from X_1

X_3 will be another vector of n variables, disjoint from X_1 and X_2.

$\vdots$

The Reduction We Need

The Reduction We Need

1. Input(ψ). (Can assume $\#\psi \in \{0, \ldots, 12\}$.)

The Reduction We Need

1. Input(ψ). (Can assume $\#\psi \in \{0, \ldots, 12\}$.)
2. Pick a random $m \in \{1, \ldots, 12\}$.

The Reduction We Need

1. Input(ψ). (Can assume $\#\psi \in \{0, \ldots, 12\}$.)
2. Pick a random $m \in \{1, \ldots, 12\}$.
3. Output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

The Reduction We Need

1. Input(ψ). (Can assume $\#\psi \in \{0, \dots, 12\}$.)
2. Pick a random $m \in \{1, \dots, 12\}$.
3. Output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

(ζ has nm variables.)

The Reduction We Need

1. Input(ψ). (Can assume $\#\psi \in \{0, \ldots, 12\}$.)
2. Pick a random $m \in \{1, \ldots, 12\}$.
3. Output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

(ζ has nm variables.)

Analysis on next slide.

Analysis of Reduction

Case 1 $\#(\psi) \in \mathrm{SAT}_{12}$. Let $\#\psi = i \in \{1, \ldots, 12\}$.

Analysis of Reduction

Case 1 $\#(\psi) \in \mathrm{SAT}_{12}$. Let $\#\psi = i \in \{1, \ldots, 12\}$.
If $m = i$ then ψ has m different satisfying assignments $B_1, \ldots, B_m$.

Analysis of Reduction

Case 1 $\#(\psi) \in \mathrm{SAT}_{12}$. Let $\#\psi = i \in \{1, \ldots, 12\}$.
If $m = i$ then ψ has m different satisfying assignments $B_1, \ldots, B_m$.
We output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

Analysis of Reduction

Case 1 $\#(\psi) \in \mathrm{SAT}_{12}$. Let $\#\psi = i \in \{1, \ldots, 12\}$.
If $m = i$ then ψ has m different satisfying assignments $B_1, \ldots, B_m$.
We output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

This only has one satisfying assignment:

Analysis of Reduction

Case 1 $\#(\psi) \in \mathrm{SAT}_{12}$. Let $\#\psi = i \in \{1, \ldots, 12\}$.
If $m = i$ then ψ has m different satisfying assignments $B_1, \ldots, B_m$.
We output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

This only has one satisfying assignment:

$$\psi(B_1) \wedge \cdots \wedge \psi(B_m) \wedge (B_1 < \cdots < B_m) = T.$$

Analysis of Reduction

Case 1 $\#(\psi) \in \mathrm{SAT}_{12}$. Let $\#\psi = i \in \{1, \ldots, 12\}$.
If $m = i$ then ψ has m different satisfying assignments $B_1, \ldots, B_m$.
We output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

This only has one satisfying assignment:

$$\psi(B_1) \wedge \cdots \wedge \psi(B_m) \wedge (B_1 < \cdots < B_m) = T.$$

Hence $\#(\zeta) = 1$

Analysis of Reduction

Case 1 $\#(\psi) \in \mathrm{SAT}_{12}$. Let $\#\psi = i \in \{1, \ldots, 12\}$.
If $m = i$ then ψ has m different satisfying assignments $B_1, \ldots, B_m$.
We output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

This only has one satisfying assignment:

$$\psi(B_1) \wedge \cdots \wedge \psi(B_m) \wedge (B_1 < \cdots < B_m) = T.$$

Hence $\#(\zeta) = 1$
Prob that $m = i$ is $\frac{1}{12}$.

Analysis of Reduction

Case 1 $\#(\psi) \in \mathrm{SAT}_{12}$. Let $\#\psi = i \in \{1, \ldots, 12\}$.
If $m = i$ then ψ has m different satisfying assignments $B_1, \ldots, B_m$.
We output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

This only has one satisfying assignment:

$$\psi(B_1) \wedge \cdots \wedge \psi(B_m) \wedge (B_1 < \cdots < B_m) = T.$$

Hence $\#(\zeta) = 1$

Prob that $m = i$ is $\frac{1}{12}$.

Case 2 $\phi \notin \mathrm{SAT}$. Then clearly $\zeta \notin \mathrm{SAT}$.

Analysis of Reduction

Case 1 $\#(\psi) \in \mathrm{SAT}_{12}$. Let $\#\psi = i \in \{1, \ldots, 12\}$.
If $m = i$ then ψ has m different satisfying assignments $B_1, \ldots, B_m$.
We output

$$\zeta = \psi(X_1) \wedge \cdots \wedge \psi(X_m) \wedge (X_1 < \cdots < X_m).$$

This only has one satisfying assignment:

$$\psi(B_1) \wedge \cdots \wedge \psi(B_m) \wedge (B_1 < \cdots < B_m) = T.$$

Hence $\#(\zeta) = 1$

Prob that $m = i$ is $\frac{1}{12}$.

Case 2 $\phi \notin \mathrm{SAT}$. Then clearly $\zeta \notin \mathrm{SAT}$.
We are done!

Recap

Recap

1) We defined $A \leq_r B$. This definition is **key** since if $x \in A$ only demand that the prob $y \in B$ be bounded below by $\frac{1}{q(n)}$.

Recap

1) We defined $A \leq_r B$. This definition is **key** since if $x \in A$ only demand that the prob $y \in B$ be bounded below by $\frac{1}{q(n)}$.

2) Using Random Hash Functions and Chebyshev's inequality we get $\mathrm{SAT} \leq_r \mathrm{SAT}_{12}$.

Recap

1) We defined $A \leq_r B$. This definition is **key** since if $x \in A$ only demand that the prob $y \in B$ be bounded below by $\frac{1}{q(n)}$.

2) Using Random Hash Functions and Chebyshev's inequality we get $\mathrm{SAT} \leq_r \mathrm{SAT}_{12}$.

3) Using Lex ordering we get $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$ where the input formula ϕ has $\#\phi \leq 12$.

Recap

1) We defined $A \leq_r B$. This definition is **key** since if $x \in A$ only demand that the prob $y \in B$ be bounded below by $\frac{1}{q(n)}$.

2) Using Random Hash Functions and Chebyshev's inequality we get $\mathrm{SAT} \leq_r \mathrm{SAT}_{12}$.

3) Using Lex ordering we get $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$ where the input formula ϕ has $\#\phi \leq 12$.

4) Compose the two rand reductions to get $\mathrm{SAT} \leq_r \mathrm{SAT}_1$.

Recap

1) We defined $A \le_r B$. This definition is **key** since if $x \in A$ only demand that the prob $y \in B$ be bounded below by $\frac{1}{q(n)}$.

2) Using Random Hash Functions and Chebyshev's inequality we get $\mathrm{SAT} \le_r \mathrm{SAT}_{12}$.

3) Using Lex ordering we get $\mathrm{SAT}_{12} \le_r \mathrm{SAT}_1$ where the input formula ϕ has $\#\phi \le 12$.

4) Compose the two rand reductions to get $\mathrm{SAT} \le_r \mathrm{SAT}_1$.

5) By Lemma, if $\mathrm{SAT}_1 \in \mathrm{P}$ then $\mathrm{SAT} \in \mathrm{RP}$.

Recap

1) We defined $A \leq_r B$. This definition is **key** since if $x \in A$ only demand that the prob $y \in B$ be bounded below by $\frac{1}{q(n)}$.

2) Using Random Hash Functions and Chebyshev's inequality we get $\mathrm{SAT} \leq_r \mathrm{SAT}_{12}$.

3) Using Lex ordering we get $\mathrm{SAT}_{12} \leq_r \mathrm{SAT}_1$ where the input formula ϕ has $\#\phi \leq 12$.

4) Compose the two rand reductions to get $\mathrm{SAT} \leq_r \mathrm{SAT}_1$.

5) By Lemma, if $\mathrm{SAT}_1 \in \mathrm{P}$ then $\mathrm{SAT} \in \mathrm{RP}$.

6) One can modify to get: if $\mathrm{SAT}_1 \in \mathrm{RP}$ then $\mathrm{SAT} \in \mathrm{RP}$.

Take Away

1) If $\mathrm{SAT}_1 \in \mathrm{P}$ then $\mathrm{SAT} \in \mathrm{RP}$.

Take Away

1) If $\mathrm{SAT}_1 \in \mathrm{P}$ then $\mathrm{SAT} \in \mathrm{RP}$.

2) We think $\mathrm{SAT} \notin \mathrm{RP}$.

Take Away

1) If $\mathrm{SAT}_1 \in \mathrm{P}$ then $\mathrm{SAT} \in \mathrm{RP}$.

2) We think $\mathrm{SAT} \notin \mathrm{RP}$.

3) Hence we think $\mathrm{SAT}_1 \notin \mathrm{P}$.

Take Away

1) If $\mathrm{SAT}_1 \in \mathrm{P}$ then $\mathrm{SAT} \in \mathrm{RP}$.

2) We think $\mathrm{SAT} \notin \mathrm{RP}$.

3) Hence we think $\mathrm{SAT}_1 \notin \mathrm{P}$.

4) If $\mathrm{SAT}_1 \in \mathrm{RP}$ then $\mathrm{SAT} \in \mathrm{RP}$.

Take Away

1) If $\mathrm{SAT}_1 \in \mathrm{P}$ then $\mathrm{SAT} \in \mathrm{RP}$.

2) We think $\mathrm{SAT} \notin \mathrm{RP}$.

3) Hence we think $\mathrm{SAT}_1 \notin \mathrm{P}$.

4) If $\mathrm{SAT}_1 \in \mathrm{RP}$ then $\mathrm{SAT} \in \mathrm{RP}$.

2) We think $\mathrm{SAT} \notin \mathrm{RP}$.

Take Away

1) If $\mathrm{SAT}_1 \in \mathrm{P}$ then $\mathrm{SAT} \in \mathrm{RP}$.

2) We think $\mathrm{SAT} \notin \mathrm{RP}$.

3) Hence we think $\mathrm{SAT}_1 \notin \mathrm{P}$.

4) If $\mathrm{SAT}_1 \in \mathrm{RP}$ then $\mathrm{SAT} \in \mathrm{RP}$.

2) We think $\mathrm{SAT} \notin \mathrm{RP}$.

3) Hence we think $\mathrm{SAT}_1 \notin \mathrm{RP}$.