

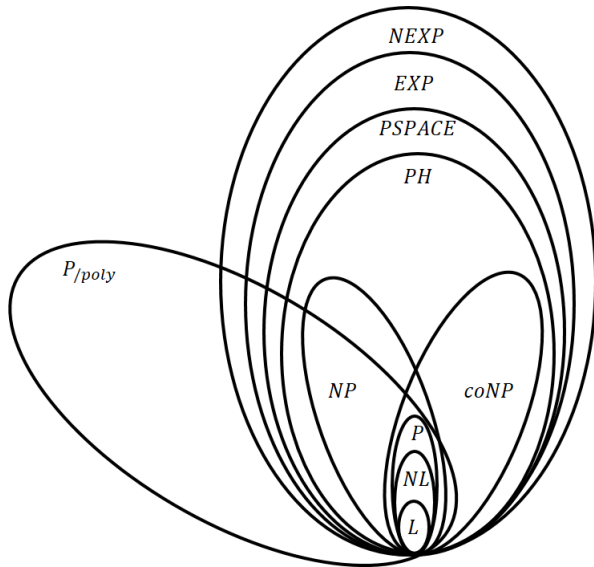
CSL853: Complexity Theory

Ragesh Jaiswal, CSE, IIT Delhi

Complexity Diagram

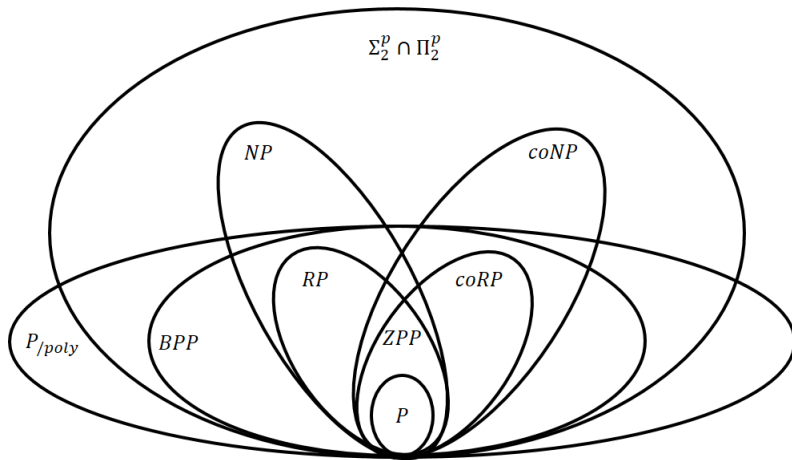
Complexity Diagram

Our current view of complexity classes



Complexity Diagram

Randomized Computation



Complexity of Counting

Complexity of Counting

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}$$

Theorem (Toda, 1991)

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}.$$

- **Proof plan:** Show that $\text{PH} \subseteq \oplus\text{P}$.
- We will start by showing that for every language $L \in \text{NP}$, there exists a language $L' \in \oplus\text{P}$ such that $L \leq_r L'$. This is known as the *Valiant-Vazirani Theorem* (1986).

Definition (Unique SAT)

$\text{USAT} = \{\psi : \psi \text{ is a Boolean formula that has a unique satisfying assignment}\}.$

Theorem (Valiant, Vazirani, 1986)

There exists a polynomial-time algorithm f such that for every n -variable Boolean formula ψ

$$\psi \in \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{USAT}] \geq \frac{1}{8n}$$

$$\psi \notin \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{SAT}] = 0$$

Complexity of Counting

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}$$

Theorem (Toda, 1991)

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}.$$

- **Proof plan:** Show that $\text{PH} \subseteq \oplus\text{P}$.
- We will start by showing that for every language $L \in \text{NP}$, there exists a language $L' \in \oplus\text{P}$ such that $L \leq_r L'$. This is known as the *Valiant-Vazirani Theorem* and was proved in 1986.

Definition (Unique SAT)

$\text{USAT} = \{\psi : \psi \text{ is a Boolean formula that has a unique satisfying assignment}\}.$

Theorem (Valiant, Vazirani, 1986)

There exists a polynomial-time algorithm f such that for every n -variable Boolean formula ψ

$$\psi \in \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{USAT}] \geq \frac{1}{8n}$$

$$\psi \notin \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{SAT}] = 0$$

Corollary (Corollary of Valiant-Vazirani Theorem)

There exists a polynomial-time algorithm f such that for every n -variable Boolean formula ψ

$$\psi \in \text{SAT} \Rightarrow \Pr[f(\psi) \in \oplus\text{SAT}] \geq \frac{1}{8n}$$

$$\psi \notin \text{SAT} \Rightarrow \Pr[f(\psi) \in \oplus\text{SAT}] = 0$$

Complexity of Counting

Valiant-Vazirani Theorem

Theorem (Valiant, Vazirani, 1986)

There exists a polynomial-time algorithm f such that for every n -variable Boolean formula ψ

$$\psi \in \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{USAT}] \geq \frac{1}{8n}$$

$$\psi \notin \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{SAT}] = 0$$

Proof.

Lemma (Valiant-Vazirani Lemma)

Let $\mathcal{H}_{n,k}$ be a family of pairwise independent hash function family from $\{0,1\}^n$ to $\{0,1\}^k$ and $S \subseteq \{0,1\}^n$ such that $2^{k-2} \leq |S| \leq 2^{k-1}$. Then

$$\Pr_{h \in \mathcal{H}_{n,k}} \left[\text{there is a unique } x \in S \text{ satisfying } h(x) = 0^k \right] \geq 1/8.$$

Complexity of Counting

Valiant-Vazirani Theorem

Theorem (Valiant, Vazirani, 1986)

There exists a polynomial-time algorithm f such that for every n -variable Boolean formula ψ

$$\psi \in \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{USAT}] \geq \frac{1}{8n}$$

$$\psi \notin \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{SAT}] = 0$$

Proof.

Lemma (Valiant-Vazirani Lemma)

Let $\mathcal{H}_{n,k}$ be a family of pairwise independent hash function family from $\{0,1\}^n$ to $\{0,1\}^k$ and $S \subseteq \{0,1\}^n$ such that $2^{k-2} \leq |S| \leq 2^{k-1}$. Then

$$\Pr_{h \in \mathcal{H}_{n,k}} \left[\text{there is a unique } x \in S \text{ satisfying } h(x) = 0^k \right] \geq 1/8.$$

- Given a Boolean formula ψ on n variables, pick $k \in \{2, 3, \dots, n+1\}$ and $h \in \mathcal{H}_{n,k}$ at random and consider the formula

$$\psi(x) \wedge (h(x) = 0^k).$$



Complexity of Counting

Valiant-Vazirani Theorem

Theorem (Valiant, Vazirani, 1986)

There exists a polynomial-time algorithm f such that for every n -variable Boolean formula ψ

$$\psi \in \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{USAT}] \geq \frac{1}{8n}$$

$$\psi \notin \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{SAT}] = 0$$

- Claim: If $\text{USAT} \in \text{P}$, then $\text{NP} = \text{RP}$.
- Open question: Is it possible to amplify the probability in the above theorem?

Complexity of Counting

Valiant-Vazirani Theorem

Theorem (Valiant, Vazirani, 1986)

There exists a polynomial-time algorithm f such that for every n -variable Boolean formula ψ

$$\psi \in \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{USAT}] \geq \frac{1}{8n}$$

$$\psi \notin \text{SAT} \Rightarrow \Pr[f(\psi) \in \text{SAT}] = 0$$

- Claim: If $\text{USAT} \in \text{P}$, then $\text{NP} = \text{RP}$.
- Open question: Is it possible to amplify the probability in the above theorem?
Not known.
- However, the following theorem can be proven.

Theorem (Randomized reduction from PH to $\oplus\text{SAT}$)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Complexity of Counting

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}$$

Theorem (Toda, 1991)

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}.$$

- Proof plan: Show that $\text{PH} \subseteq \oplus\text{P}$.
- If we can *derandomize* the following theorem, then we are done.

Theorem (Randomized reduction from PH to $\oplus\text{SAT}$)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

- Proof sub-plan: We will first prove the above theorem, and then try to *derandomize* it.

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

- We will need some tools and definitions.

Definition ($\#\psi$ and $\oplus\psi$)

Given a boolean formula ψ over n variables, $\#\psi$ denotes the number of satisfying assignments of ψ and $\oplus\psi = \#\psi \pmod{2}$.

Lemma

There are polynomial time algorithms A, B that, given formulas ϕ in n variables and ψ in m variables, output formulas $\phi \circ \psi$ in $(m + n)$ variables and $\phi \upharpoonright \psi$ in $\max(n, m) + 1$ variables such that $\#(\phi \circ \psi) = (\#\phi) \cdot (\#\psi)$ and $\#(\phi \upharpoonright \psi) = (\#\phi) + (\#\psi)$ respectively.

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Lemma

There are polynomial time algorithms A, B that, given formulas ϕ in n variables and ψ in m variables, output formulas $\phi \circ \psi$ in $(m + n)$ variables and $\phi \dagger \psi$ in $\max(n, m) + 1$ variables such that $\#(\phi \circ \psi) = (\#\phi) \cdot (\#\psi)$ and $\#(\phi \dagger \psi) = (\#\phi) + (\#\psi)$ respectively.

Lemma

Let ϕ and ψ be Boolean formulas and $\mathbf{1}$ denote some canonical Boolean formula that has exactly one satisfying assignment. Then the following hold:

- ① $(\oplus_x \phi(x)) \wedge (\oplus_y \psi(y)) \Leftrightarrow \oplus_{x,y} (\phi \circ \psi)(x, y).$
- ② $\neg(\oplus_x \phi(x)) \Leftrightarrow \oplus_{x,z} (\phi \dagger \mathbf{1})(x, z).$
- ③ $(\oplus_x \phi(x) \vee (\oplus_y \psi(y))) \Leftrightarrow \oplus_{x,y,z} ((\phi \dagger \mathbf{1}) \circ (\psi \dagger \mathbf{1}) \dagger \mathbf{1})(x, y, z).$

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Lemma

Let ϕ and ψ be Boolean formulas and $\mathbf{1}$ denote some canonical Boolean formula that has exactly one satisfying assignment. Then the following hold:

- ① $(\oplus_x \phi(x)) \wedge (\oplus_y \psi(y)) \Leftrightarrow \oplus_{x,y} (\phi \circ \psi)(x, y).$
- ② $\neg(\oplus_x \phi(x)) \Leftrightarrow \oplus_{x,z} (\phi \dagger \mathbf{1})(x, z).$
- ③ $(\oplus_x \phi(x) \vee (\oplus_y \psi(y))) \Leftrightarrow \oplus_{x,y,z} ((\phi \dagger \mathbf{1}) \circ (\psi \dagger \mathbf{1}) \dagger \mathbf{1})(x, y, z).$

- The following lemma follows from the previous one.

Lemma (Randomized reduction from NP to $\oplus$ SAT)

There exists a probabilistic polynomial-time algorithm A that given a parameter m and any Boolean formula ψ of size n , runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \in \text{SAT} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \notin \text{SAT} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Proof.

- Claim: It is sufficient to show that theorem for formulas that begin with the $\exists$ quantifier.

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Proof.

- Claim: It is sufficient to show that theorem for formulas that begin with the $\exists$ quantifier.
- The proof is by induction on the number of alternations c of the quantified Boolean formula.
- The base case ($c = 1$)?

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Proof.

- Claim: It is sufficient to show that theorem for formulas that begin with the $\exists$ quantifier.
- The proof is by induction on the number of alternations c of the quantified Boolean formula.
- The base case ($c = 1$) follows from the previous lemma.

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Proof.

- Claim: It is sufficient to show that theorem for formulas that begin with the $\exists$ quantifier.
- The proof is by induction on the number of alternations c of the quantified Boolean formula.
- The base case ($c = 1$) follows from the previous lemma.
- Let $\psi = \exists x_1 \forall x_2 \dots \phi$. For any value of x_2 , let $\psi(x_1)$ denote the quantified formula where x_1 is fixed.

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Proof.

- Claim: It is sufficient to show that theorem for formulas that begin with the $\exists$ quantifier.
- The proof is by induction on the number of alternations c of the quantified Boolean formula.
- The base case ($c = 1$) follows from the previous lemma.
- Let $\psi = \exists x_1 \forall x_2 \dots \phi$. For any value of x_2 , let $\psi(x_1)$ denote the quantified formula where x_1 is fixed.
- By the induction hypothesis, there is an efficient reduction that outputs a $\oplus$ SAT formula $\beta(x_1)$ that is equivalent to $\psi(x_1)$ with probability at least $(1 - 2^{-(m+2)})$.

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Proof.

- Claim: It is sufficient to show that theorem for formulas that begin with the $\exists$ quantifier.
- The proof is by induction on the number of alternations c of the quantified Boolean formula.
- The base case ($c = 1$) follows from the previous lemma.
- Let $\psi = \exists x_1 \forall x_2 \dots \phi$. For any value of x_2 , let $\psi(x_1)$ denote the quantified formula where x_1 is fixed.
- By the induction hypothesis, there is an efficient reduction that outputs a $\oplus$ SAT formula $\beta(x_1)$ that is equivalent to $\psi(x_1)$ with probability at least $(1 - 2^{-(m+2)})$.
- Consider $\alpha = \bigvee_{j=1}^K (\tau_j \wedge \beta(x_1))$, where $(\tau_j \wedge \beta(x_1))$ is the output of the reduction in the Valiant-Vazirani corollary given input $\beta(x_1)$.

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Proof.

- Claim: It is sufficient to show that theorem for formulas that begin with the $\exists$ quantifier.
- The proof is by induction on the number of alternations c of the quantified Boolean formula.
- The base case ($c = 1$) follows from the previous lemma.
- Let $\psi = \exists x_1 \forall x_2 \dots \phi$. For any value of x_2 , let $\psi(x_1)$ denote the quantified formula where x_1 is fixed.
- By the induction hypothesis, there is an efficient reduction that outputs a $\oplus$ SAT formula $\beta(x_1)$ that is equivalent to $\psi(x_1)$ with probability at least $(1 - 2^{-(m+2)})$.
- Consider $\alpha = \bigvee_{j=1}^K (\tau_j \wedge \beta(x_1))$, where $(\tau_j \wedge \beta(x_1))$ is the output of the reduction in the Valiant-Vazirani corollary given input $\beta(x_1)$.
- Claim: For large enough K , if $\exists x_1 \beta(x_1)$ is true, then $\Pr[\alpha \text{ is true}] \geq (1 - 2^{-O(m)})$ and the probability of 0 otherwise.

Complexity of Counting

Randomized reduction from PH to $\oplus$ SAT

Theorem (Randomized reduction from PH to $\oplus$ SAT)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Proof.

- Claim: It is sufficient to show that theorem for formulas that begin with the $\exists$ quantifier.
- The proof is by induction on the number of alternations c of the quantified Boolean formula.
- The base case ($c = 1$) follows from the previous lemma.
- Let $\psi = \exists x_1 \forall x_2 \dots \phi$. For any value of x_2 , let $\psi(x_1)$ denote the quantified formula where x_1 is fixed.
- By the induction hypothesis, there is an efficient reduction that outputs a $\oplus$ SAT formula $\beta(x_1)$ that is equivalent to $\psi(x_1)$ with probability at least $(1 - 2^{-(m+2)})$.
- Consider $\alpha = \bigvee_{j=1}^K (\tau_j \wedge \beta(x_1))$, where $(\tau_j \wedge \beta(x_1))$ is the output of the reduction in the Valiant-Vazirani corollary given input $\beta(x_1)$.
- Claim: For large enough K , if $\exists x_1 \beta(x_1)$ is true, then $\Pr[\alpha \text{ is true}] \geq (1 - 2^{-O(m)})$ and the probability of 0 otherwise.
- Finally, α may be converted to an equivalent $\oplus$ SAT formula. □

Complexity of Counting

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}$$

Theorem (Toda, 1991)

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}.$$

- Proof plan: Show that $\text{PH} \subseteq \oplus\text{P}$.
- Proof sub-plan: Derandomize the following theorem.

Theorem (Randomized reduction from PH to $\oplus\text{SAT}$)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Theorem

There is a polynomial time algorithm B that, on input $(\psi, 1^l)$ outputs a formula such that

$$\psi \in \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv -1 \pmod{2^{l+1}}$$

$$\psi \notin \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv 0 \pmod{2^{l+1}}$$

Complexity of Counting

$\text{PH} \subseteq \text{P}^{\#\text{SAT}}$

Theorem

There is a polynomial time algorithm B that, on input $(\psi, 1^l)$ outputs a formula such that

$$\psi \in \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv -1 \pmod{2^{l+1}}$$

$$\psi \notin \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv 0 \pmod{2^{l+1}}$$

Proof.

Lemma

Let $p(x) = 3x^4 + 4x^3$. For any integers x and n :

$$x \equiv -1 \pmod{n} \Rightarrow p(x) \equiv -1 \pmod{n^2}$$

$$x \equiv 0 \pmod{n} \Rightarrow p(x) \equiv 0 \pmod{n^2}$$

Complexity of Counting

$\text{PH} \subseteq \text{P}^{\#\text{SAT}}$

Theorem

There is a polynomial time algorithm B that, on input $(\psi, 1^l)$ outputs a formula such that

$$\psi \in \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv -1 \pmod{2^{l+1}}$$

$$\psi \notin \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv 0 \pmod{2^{l+1}}$$

Proof.

Lemma

Let $p(x) = 3x^4 + 4x^3$. For any integers x and n :

$$x \equiv -1 \pmod{n} \Rightarrow p(x) \equiv -1 \pmod{n^2}$$

$$x \equiv 0 \pmod{n} \Rightarrow p(x) \equiv 0 \pmod{n^2}$$

- Set $\psi_0 = \psi$, $\forall i, \psi_{i+1} = 4 \circ \psi_i^3 + 3 \circ \psi_i^4$, and $B(\psi) = \psi_{\lceil \log l + 1 \rceil}$. □

Complexity of Counting

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}$$

Theorem (Toda, 1991)

$$\text{PH} \subseteq \text{P}^{\#\text{SAT}}.$$

Proof.

Theorem (Randomized reduction from PH to $\oplus\text{SAT}$)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Theorem

There is a polynomial time algorithm B that, on input (ψ, l) outputs a formula such that $\psi \in \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv -1 \pmod{2^{l+1}}$ and $\psi \notin \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv 0 \pmod{2^{l+1}}$

- Let $m = 2$ and ψ be a quantified Boolean formula (with constant number of alternations).
- Let the randomized algorithm use R random coin tosses and let the output of A with random coins $r \in \{0, 1\}^R$ be denoted by $A(\psi, r)$.
- Claim 1: Let $f(\psi) = \sum_{r \in \{0, 1\}^R} \#B(A(\psi, r))$. $f \in \#P$.

Complexity of Counting

$\text{PH} \subseteq \text{P}^{\#\text{SAT}}$

Theorem (Toda, 1991)

$\text{PH} \subseteq \text{P}^{\#\text{SAT}}$.

Proof.

Theorem (Randomized reduction from PH to $\oplus\text{SAT}$)

Let $c \in \mathbb{N}$ be some constant. There exists a probabilistic polynomial-time algorithm A that given a parameter m and any quantified Boolean formula ψ of size n and c levels of alternations, runs in $\text{poly}(n, m)$ time and satisfies

$$\psi \text{ is true} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \geq 1 - 2^{-m}$$

$$\psi \text{ is false} \Rightarrow \Pr[A(\psi) \in \oplus\text{SAT}] \leq 2^{-m}$$

Theorem

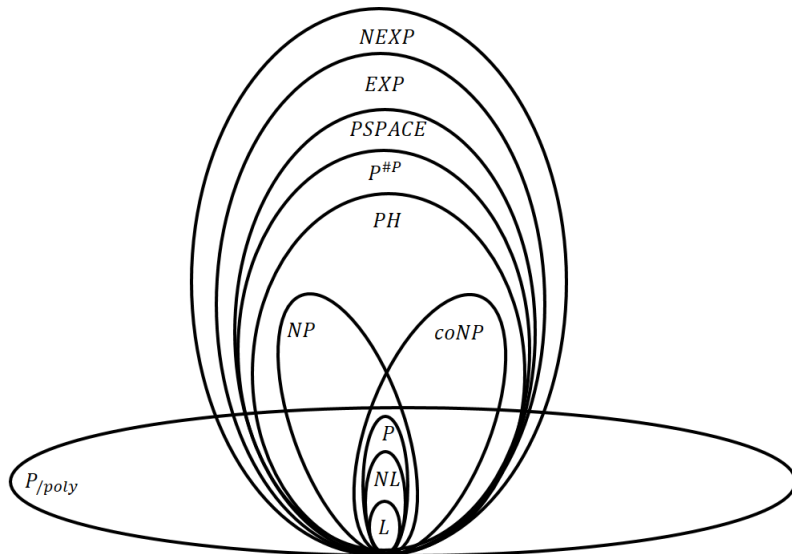
There is a polynomial time algorithm B that, on input $(\psi, 1^l)$ outputs a formula such that $\psi \in \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv -1 \pmod{2^{l+1}}$ and $\psi \notin \oplus\text{SAT} \Rightarrow \#(B(\psi)) \equiv 0 \pmod{2^{l+1}}$

- Let $m = 2$ and ψ be a quantified Boolean formula (with constant number of alternations).
- Let the randomized algorithm use R random coin tosses and let the output of A with random coins $r \in \{0, 1\}^R$ be denoted by $A(\psi, r)$.
- Claim 1: Let $f(\psi) = \sum_{r \in \{0, 1\}^R} \#B(A(\psi, r))$. $f \in \#P$.
- Claim 2: If ψ is true, then $-2^R \leq f(\psi) \leq -\lceil(3/4)2^R\rceil$ and if ψ is false, then $-\lceil(1/4)2^R\rceil \leq f(\psi) \leq 0$.
- The proof follows from observing that the range is disjoint for $2^{l+1} > 2^{R+2}$. $\square$

Complexity Diagram

Complexity Diagram

Our current view of complexity classes



End