- PH & #P are both natural generalizations of NP; one uses <u>alternations</u> & the other <u>counting</u>.

- How do they compare?
  In the 1980s they were thought to be incomparable.

- Eventually, Toda proved in 1989 that $PH \subseteq P^{\#P} = P^{PP}$.

- The proof uses a new paradigm: <u>randomization</u>.

Theorem (Toda 1991): $PH \subseteq P^{\#SAT}$.

- Idea: We will prove this theorem by giving a reduction from Σ_i to a new class $\oplus P$ (parity-P).

- Defn: • A language $L \in \oplus P$ if there is a NDTM M s.t. $\forall x$, $x \in L$ iff $\#$(acc. paths of M on x) is odd.

• $\oplus SAT := \{\phi \mid \phi$ is a boolean formula & $\#\phi$ is odd$\}$.

▷ $\oplus SAT$ is $\oplus P$-complete.

OPEN: $\oplus P \neq P$?

Is it related to $NP \neq P$?

- But something similar is known:
  NP "randomly" reduces to $\oplus P$.

Theorem (Valiant-Vazirani): There is a poly-time TM A s.t.

$$\varphi \in SAT \Rightarrow \Pr_r[A(r,\varphi) \in \oplus SAT] > \frac{1}{8n},$$

$$\& \ \varphi \notin SAT \Rightarrow \Pr_r[A(r,\varphi) \in \oplus SAT] = 0.$$

Proof:

- Given a formula φ we want to transform it to a formula ψ that has 0 resp. 1 satisfying assignment if φ is unsatisfiable resp. satisfiable.

- This we achieve by hashing the 2^k (say) sat. assgn. of φ into 2^k buckets.

[Hashing]

will look random

Claim: For a matrix $B \in \mathbb{F}_2^{k\times n}$ & a vector $b \in \mathbb{F}_2^{k}$, consider the linear transformation $h_{B,b} : \mathbb{F}_2^n \to \mathbb{F}_2^k$.

hash fn.

$$x \mapsto (Bx+b)$$

Falling in a bucket

(1) $\forall x \in \mathbb{F}_2^n$, $\Pr_{B,b}[h_{B,b}(x) = 0^k] = 2^{-k}$.

Two falling in a bucket

(2) $\forall x \neq x' \in \mathbb{F}_2^n$,

$$\Pr_{B,b}[h_{B,b}(x) = h_{B,b}(x') = 0^k] = 2^{-2k}.$$

#(sat. assgn. falling in a bucket)

(3) Let $S \subseteq \mathbb{F}_2^n$ with $2^{k-2} \leq |S| \leq 2^{k-1}$.

Then, $\Pr_{B,b}[\#\{x\in S \mid h_{B,b}(x) = 0^k\} = 1]$

$$> 1/8.$$

Proof: (1)

If we first pick B then the prob. of picking $b = -Bx$ is 2^{-k}.

(2) $\Pr[Bx = -b = Bx'] = \Pr[Bx = -b] \cdot \Pr[Bx' = -b \mid Bx = -b]$

$$= 2^{-k} \cdot \Pr_{B,b}[B(x'-x) = 0^k \mid Bx = -b]$$

$$= 2^{-k} \cdot \Pr_{B}[B(x'-x) = 0^k]$$

$$= 2^{-k} \cdot 2^{-k} \quad [\because x'-x \neq 0^k]$$

(3) • Let N be the random variable $\#\{x \in S \mid h_{B,b}(x) = 0^k\}$.

• Then, by inclusion-exclusion:

$$\Pr_{B,b}[N \geq 1] \geq \sum_{x \in S} \Pr[h_{B,b}(x) = 0^k] - \sum_{x < x' \in S} \Pr[h_{B,b}(x) = h_{B,b}(x') = 0^k]$$

$$\geq |S| \cdot 2^{-k} - \binom{|S|}{2} \cdot 2^{-2k}$$

• Similarly, $\Pr_{B,b}[N \geq 2] \leq \sum_{x < x' \in S} \Pr[h(x) = h(x') = 0^k]$

$$= \binom{|S|}{2} \cdot 2^{-2k}.$$

$$\Rightarrow \Pr_{B,b}[N=1] = \Pr[N \geq 1] - \Pr[N \geq 2]$$

$$\geq |S| \cdot 2^{-k} - 2 \cdot \binom{|S|}{2} \cdot 2^{-2k}$$

$x - x^2$ is an increasing fn. below 1/2

$$\geq (|S| \cdot 2^{-k}) - (|S| \cdot 2^{-k})^2$$

$$\geq \frac{1}{4} - \left(\frac{1}{4}\right)^2 > \frac{1}{8}.$$

$\square$

(Valiant-Vazirani Pf. continues):

- Let the CNF formula ϕ have n variables.
- Randomly pick $k \in \{2, 3, \ldots, n+1\}$, $B \in \mathbb{F}_2^{k \times n}$ & $b \in \mathbb{F}_2^k$.
- Output the boolean formula:

$$\psi(\bar{x}) := \phi(\bar{x}) \wedge [h_{B,b}(x) = 0^k].$$

can be expressed as a boolean formula

- Note that:

If ϕ is unsatisfiable then ψ has zero (so, even) satisfying assignments.

If ϕ is satisfiable then:

- Let $S := \{x \in \{0,1\}^n \mid \Phi(x) = 1\}$.
- With prob. $\geq 1/n$ we would have chosen k s.t. $|S| \in [2^{k-2}, 2^{k-1}]$.
- Conditioned on that, with prob. $> 1/8$ we would have chosen B, b s.t. $\#\{x \in S \mid h_{B,b}(x) = 0^k\} = 1$.

$\Rightarrow$ With prob. $> 1/8n$ we would have k, B, b s.t. $\#\psi = 1$ (so, odd!).

$\square$

- This randomly & efficiently reduces NP to $\oplus$P.

- Now, we will use this idea <u>repeatedly</u> to randomly reduce PH to $\oplus$P.

- We intend to replace $\exists, \forall$ quantifiers by a new quantifier — $\oplus$.

- <u>Defn</u>: For a boolean formula $\phi(x)$, <u>$\oplus x, \phi(x)$</u> is called true if $\#\phi$ is odd.

<u>Lemma 1</u>: Let $c \in \mathbb{N}$ be a <u>constant</u>. There is a poly-time TM A s.t. for every quantified formula ψ with c alternations of $\forall, \exists$ we have:

ψ is true $\Rightarrow \Pr_r[A(r,\psi) \in \oplus SAT] \geq 2/3$

both-sided errors

& ψ is false $\Rightarrow \Pr_r[A(r,\psi) \in \oplus SAT] < 1/3$.

<u>Proof sketch</u>:

- Our aim is to replace the $\forall/\exists$ quantifiers one-by-one by the $\oplus$ quantifier.

- Let us sketch the (inductive) proof for $\psi = \oplus z \in \{0,1\}^{\ell}, \underline{\exists x \in \{0,1\}^n}, \forall w \in \{0,1\}^k \, \phi(z,x,w)$.

- By the Valiant-Vazirani technique, there exists a formula $\tilde{\tau}$ s.t. for a random string r,

$$\Pr_r[\oplus x, (\forall w\ \phi(z,x,w) \wedge \tau(x,r)) \text{ is true}] \geq 1/8n$$

if $\exists x \forall w\ \phi(z,x,w)$ is true, &

$$\Pr_r[\oplus x, (\forall w\ \phi(z,x,w) \wedge \tau(x,r)) \text{ is true}] = 0$$

if $\exists x \forall w\ \phi(z,x,w)$ is false.

- Thus,

$z \in \{0,1\}^\ell$

$$\Pr_r[\oplus z, \oplus x, (\forall w\ \phi \wedge \tau) \text{ is true}] \geq \left(\frac{1}{8n}\right)^{2^\ell}$$

if $\psi = \oplus z, \exists x, \forall w, \phi$ is true.

$\Rightarrow$ We have randomly reduced ψ to $\oplus(z,x), (\forall w\ \phi \wedge \tilde{\tau})$ but the probability

of success is <u>very</u> low.
How to increase it?

- For a fixed z, repeat the transformation $\underline{t}$ times for random strings $r_1, \dots, r_t$:

prob. amplification

$$\Pr_{r_1,\dots,r_t}\left[\bigvee_{i=1}^{t} \oplus x, (\forall w\, \phi \wedge \tau_i) \text{ is true}\right] \geq 1-\left(1-\frac{1}{8n}\right)^t$$

$\tau(x, r_i)$

if $\exists x, \forall w\, \phi$ is true, &

$$\Pr_{r_1,\dots,r_t}[\dots] < \left(1-\frac{1}{8n}\right)^t \text{ otherwise.}$$

- Now considering all $z \in \{0,1\}^\ell$:

$$\Pr_{r_1,\dots,r_t}\left[\oplus z, \bigvee_{i=1}^{t} \oplus x, (\forall w\, \phi \wedge \tau_i) \text{ is true}\right] \geq 1-2^\ell\cdot\left(1-\frac{1}{8n}\right)^t$$

Union bound

if ψ is true; $< 2^\ell \cdot \left(1-\frac{1}{8n}\right)^t$ otherwise.

- Note that for $t = 16n\ell$ we get
$$2^{\ell} \cdot \left(1 - \frac{1}{8n}\right)^{t} = 2^{\ell} \cdot \left(1 - \frac{1}{8n}\right)^{8n \cdot 2\ell}$$
$$\leq 2^{\ell} \cdot (e^{-1})^{2\ell} < 1/3 .$$

- Thus, we randomly reduced ψ to
$$\psi' := \oplus z, \bigvee_{i=1}^{t} \oplus x \, (\forall w \, \phi \wedge \tau_i)$$
$$=: \oplus z, \bigvee_{i=1}^{t} \oplus x \;\; \phi_i(z, x) .$$

- We now want to remove the $\vee$ operator.
- Let us consider a simplified situation:
$(\oplus x \, F_1(x)) \vee (\oplus y \, F_2(y))$.

- We remove the $\vee$ by introducing three new variables u_1, u_2, u_3 & a "+1" operation on formulas:
For a formula $F(\bar{x})$, $\underline{F+1}$ denotes $(u=0 \wedge F(\bar{x})) \vee (u=1 \wedge \bar{x}=0^n)$.

- Clearly, $\#(F+1) = (\#F) + 1$.

- Coming back to $\oplus x\, F_1 \vee \oplus y\, F_2$ we consider:

$$\oplus(x, y, u_1, u_2, u_3)\ \underbrace{(\underbrace{(F_1+1)}_{\text{in}(x,u_1)} \wedge \underbrace{(F_2+1)}_{\text{in}(y,u_2)} + 1)}_{\text{in}(x,y,u_1,u_2,u_3)}.$$

▷ This is true iff $\oplus x\, F_1 \vee \oplus y\, F_2$ is true.

- Thus, by induction, we can randomly reduce $\psi = \oplus z\ \exists x\ \forall w\ \phi(z,x,w)$ to $\oplus z\ \oplus x^*\ \forall w\ \phi'(z,x^*,w)$, for some boolean formula ϕ'.

- Next, we remove '$\forall$' by using:
$\oplus x\ \forall y\ F(x,y) \equiv \oplus x\ \exists y\ \neg F(x,y)$.

$\Rightarrow$ We end up (randomly) with:

$$\oplus z \oplus x^* \oplus w^* \phi''(z, x^*, w^*)$$

which is equivalent to $\psi = \oplus z \exists x \forall w \phi$.

- Since, in a more general ψ we have c (constant) many quantifiers, we get only a polynomial blowup in the formula size.

$\Rightarrow \Sigma_c$Sat randomly reduces to $\oplus$SAT (with an error prob. $< 1/3$).

$\square$

$\triangleright$ We have a <u>randomized</u> poly-time reduction from PH to $\oplus P \subseteq P^{\#P}$.

- How do we derandomize it?

Hensel-lifting inspired

<u>Idea:</u> <u>Amplify</u> the (mod 2) value to (mod 2^m) value, for a larger m.

Lemma 2: Let ψ be a boolean formula & $m \in \mathbb{N}$. Then, there is a poly-time TM T s.t. $\phi = T(\psi, 1^m)$ is a boolean formula satisfying:

$$\#\psi \equiv 1 \pmod 2 \Rightarrow \#\phi \equiv -1 \pmod{2^{m+1}}$$

& $$\#\psi \equiv 0 \pmod 2 \Rightarrow \#\phi \equiv 0 \pmod{2^{m+1}}.$$

Proof: • We build ϕ iteratively using new operations '$+$' & '$*$'.

• For formulas $F(\bar{x})$ & $G(\bar{y})$ define new formulas,

$$(F+G)(\bar{x}, u) := (u=0 \wedge F(\bar{x})) \vee (u=1 \wedge G(\bar{x})).$$

& $$(F*G)(\bar{x}, \bar{y}) := F(\bar{x}) \wedge G(\bar{y}).$$

▷ $\#(F+G) = (\#F) + (\#G)$, &

$\#(FG) = (\#F) \cdot (\#G)$.

• Start with $\phi_0 := \psi$.

• Define $\varphi_{i+1} := 4\varphi_i^3 + 3\varphi_i^4$.

<u>Claim:</u> $\#\varphi_i \equiv -1 \pmod{2^{2^i}}$

(Hensel inspired?)

$\Rightarrow \#\varphi_{i+1} \equiv -1 \pmod{2^{2^{i+1}}}$, &

$\#\varphi_i \equiv 0 \pmod{2^{2^i}}$

$\Rightarrow \#\varphi_{i+1} \equiv 0 \pmod{2^{2^{i+1}}}$.

<u>Proof:</u>

• Observe that $4(-1+2^j \cdot q)^3 + 3(-1+2^j q)^4$

$\equiv 4 \cdot (-1 + 3 \cdot 2^j q) + 3(1 - 4 \cdot 2^j q)$

$\equiv -1 \pmod{2^{2j}}$.

• Also, $4 \cdot (2^j q)^3 + 3 \cdot (2^j q)^4$

$\equiv 0 \pmod{2^{2j}}$. $\square$

• By induction, we deduce that φ_i for $i = O(\lg m)$, will have the properties that we wanted in φ.

(No. of vars. in φ grow by a $\lg m$ factor) $\square$

Proof of Toda's thm.:

- Let $L \in PH$. Let x be a string.
- By Lemmas 1 & 2, we get a poly-time NDTM M & $m = poly(|x|)$ s.t.

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^m}[\#\text{acc.path } M(x,r) \equiv -1 \bmod 2^{m+1}] \geq 2/3, \text{ \&}$$

$$x \notin L \Rightarrow \Pr_r[\ldots] < 1/3.$$

- Further, $\forall x, \forall r$, $\#\text{acc.path } M(x,r) \equiv 0 \text{ or } -1 \bmod 2^{m+1}$.

replace random bits by non-det. ones

- Let us define an NDTM M' that on input x, guesses $r \in \{0,1\}^m$ & accepts iff M accepts (x,r).

$$\Rightarrow \#\text{acc.path } M'(x) = \sum_r \underbrace{\#\text{acc.path } M(x,r)}_{0 \text{ or } -1}$$

- Its value modulo 2^{m+1} is:

$$\begin{cases} \text{between } -\frac{2}{3}\cdot 2^m \ \& \ -2^m, & \text{if } x \in L. \\ \text{between } -\frac{1}{3}\cdot 2^m \ \& \ 0, & \text{if } x \notin L. \end{cases}$$

$\Rightarrow$ Computing #acc. path $M'(x)$ is enough to solve L.

$\Rightarrow$ $PH \subseteq P^{\#P}$ $\square$

notice how the proof used the intermediate class $\oplus P$

- Randomization was a simplifying tool/notion in the above proof, though the theorem statement did not call for randomness at all!

- We will now use randomization to compute.