$\Rightarrow \#P \subseteq FP^{\text{per on } 0/1}$. □

Theorem (Valiant 1979): per, on 0/1 matrices, is #P-complete.

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

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

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

- The proof uses a new paradigm: randomization.

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 $\#(\text{acc. paths of } M \text{ on } x)$ 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 $\oplus P$.

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

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

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

<u>Proof:</u>

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

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

Claim: For a matrix $B \in \mathbb{F}_2^{k \times n}$ & a vector $b \in \mathbb{F}_2^k$, consider the linear transformation $h_{B,b} : \mathbb{F}_2^n \to \mathbb{F}_2^k$. ($h_{B,b}$ ← 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 $1/2$

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

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

□

(Valiant-Vazirani Pf. continues):

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

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

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: