- 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. $\geq 1/8$ we would have chosen $B, b$ s.t. $\#\{x \in S \mid h_{B,b}(x) = 0^k\} = 1$.

$\Rightarrow$ With prob. $\geq 1/8n$ 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 — $\oplus$.

- **Defn**: For a boolean formula $\phi(x)$, $\underline{\oplus x,\ \phi(x)}$ is called true if $\#\phi$ is odd.

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

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

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

**Proof sketch**:

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

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

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

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

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

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

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

- Thus,

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

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

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

of success is very 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

$\tau(x, r_i)$

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

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

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

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

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

if $\psi$ 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 $\psi$ 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 $F(\bar{x})$, $F+1$ 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:

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

▷ 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 $\phi'$.

- Next, we remove '$\forall$' by using:

$$\oplus x\ \forall y\ F(x,y) \equiv \oplus x\ \exists y\ \neg F(x,y).$$

⇒ 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 $\psi$ we have $c$ (constant) many quantifiers, we get only a polynomial blowup in the formula size.

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

$\square$

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

- How do we derandomize it?
  <u>Idea:</u> Amplify the (mod 2) value to (mod $2^m$) value, for a larger $m$.