Last lecture we proved that \( \text{PH} \subseteq \text{BPP}^{\oplus P} \). Here we will prove that:

**Lemma 1.** \( \text{PP}^{\oplus P} \subseteq \text{P}^{\#P} \).

As \( \text{BPP} \subseteq \text{PP} \), both lemmas imply Toda’s theorem, that \( \text{PH} \subseteq \text{P}^{\#P} \).

1 The class \( \text{GapP} \)

**Definition 2.** The class \( \text{GapP} \) is the class of functions \( f \) such that for some NP machine \( M \), \( f(x) \) is the number of accepting paths minus the number of rejecting paths of \( M \) on \( x \).

\( \text{GapP} \) functions are closed under under exponential-size sums and polynomial-size products (we will see this in the exercise). Further:

**Claim 3.** \( \#P \subseteq \text{GapP} \).

**Proof.** Given \( f \in \#P \) corresponding to an NP machine \( M \), let \( N \) be the NP machine that on input \( x \): Simulates \( M(x) \). If it accepted, accept and otherwise branch to an accepting state and a rejecting one.

Let \( a \) and \( r \) be the number of accepting and rejecting paths of \( M \) on \( x \). Thus, the number of accepting paths of \( N \) is \( a + r \) and the number of rejecting paths of \( N \) is \( r \). Thus, the \( \text{GapP} \) function corresponds to \( N \) is \( (a + r) - r = a \), as desired.

**Claim 4.** \( \text{FP}^{\text{GapP}} = \text{FP}^{\#P} \).

**Proof.** (Sketch). The only direction left to prove is \( \text{FP}^{\text{GapP}} \subseteq \text{FP}^{\#P} \). Let \( L \in \text{FP}^{\text{GapP}} \) and assume it makes an oracle call to a function \( f \in \text{GapP} \). We will see in the exercise that every \( \text{GapP} \) function is a difference between a \( \#P \) function and an FP function. Thus, we can compute its output with an oracle to \( \#P \) and an FP computation.

We have the following \( \text{GapP} \) characterization of \( \oplus P \):

**Claim 5.** A language \( L \) is in \( \oplus P \) if and only if there is a \( \text{GapP} \) function \( f \) such that:

- If \( x \in L \) then \( f(x) \equiv 1 \pmod{2} \).
- If \( x \notin L \) then \( f(x) \equiv 0 \pmod{2} \).

**Proof.** The left-to-right direction follows from Claim 3. For the other direction, consider such a \( \text{GapP} \) function with a corresponding NP machine \( M \). Let \( N \) be the following NP machine: On input \( x \), it branches twice, simulating \( M(x) \) on one branch and \( \overline{M}(x) \) on the other. Clearly,

\[
\#\text{acc}_N(x) = \text{acc}_M(x) + \text{rej}_M(x) = (\#\text{acc}_M(x) - \#\text{rej}_M(x)) + 2 \cdot \#\text{rej}_M(x),
\]
so if \( x \in L \) then \( \#\text{acc}_M(x) - \#\text{rej}_M(x) \) is odd and \( \text{acc}_N(x) \) is odd as well, and if \( x \notin L \) then \( \#\text{acc}_M(x) - \#\text{rej}_M(x) \) is even and \( \text{acc}_N(x) \) is even as well. Thus, \( L \in \oplus P \) due to the NP machine \( N \).

2 Characterizing PP\(^{\oplus P}\)

We define PP\(^{A}\) using P\(^A\) predicates.

Claim 6. A language \( L \) is in PP\(^{A}\) if and only if there is a language \( B \in P^A \) and a polynomial \( q \) such that:

- If \( x \in L \) then
  \[ \left| \left\{ y \in \{0, 1\}^{q(|x|)} : (x, y) \in B \right\} \right| \geq \left| \left\{ y \in \{0, 1\}^{q(|x|)} : (x, y) \notin B \right\} \right| \]
- If \( x \notin L \) then
  \[ \left| \left\{ y \in \{0, 1\}^{q(|x|)} : (x, y) \in B \right\} \right| < \left| \left\{ y \in \{0, 1\}^{q(|x|)} : (x, y) \notin B \right\} \right| \]

Proof. The left-to-right direction follows immediately from the definition of PP. For the other direction, consider such a language \( B \) with a corresponding P\(^A\) machine \( M(x, y) \). Let \( N \) be the NP\(^A\) machine that on input \( x \), guesses \( y \in \{0, 1\}^{q(|x|)} \), simulates \( M(x, y) \) and answers accordingly. The correctness easily follows.

Combining the above two claims, and the fact that \( P^{\oplus P} = \oplus P \) implied by what we did last lecture, we have:

Lemma 7. A language \( L \) is in PP\(^{\oplus P}\) if and only if there is a GapP function \( f \) and a polynomial \( q \) such that:

- If \( x \in L \) then
  \[ \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 1 \,(\mod\,2) \right\} \right| \geq \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 0 \,(\mod\,2) \right\} \right| \]
- If \( x \notin L \) then
  \[ \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 1 \,(\mod\,2) \right\} \right| < \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 0 \,(\mod\,2) \right\} \right| \]

3 Proving PP\(^{\oplus P}\) \(\subseteq\) P\(^\# P\)

Our plan is to give a FP\(^{\text{GapP}}\) algorithm to compute
\[ \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 1 \,(\mod\,2) \right\} \right| \]
and
\[ \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 0 \,(\mod\,2) \right\} \right|. \]

With that algorithm, we can prove PP\(^{\oplus P}\) \(\subseteq\) P\(^\# P\).
Proof. Let $L \in \text{PP}^{\oplus \text{P}}$. By Lemma 7, there exists a GapP function $f$ and a polynomial $q$ such that:

- If $x \in L$ then
  \[ \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 1 \, (\text{mod } 2) \right\} \right| \geq \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 0 \, (\text{mod } 2) \right\} \right| \]

- If $x \not\in L$ then
  \[ \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 1 \, (\text{mod } 2) \right\} \right| < \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 0 \, (\text{mod } 2) \right\} \right| \]

We compute in $\text{FP}^{\text{GapP}}$ the above two quantities, and decide accordingly. As $\text{FP}^{\text{GapP}} = \text{FP}^{\#P}$, $L \in \text{P}^{\#P}$.

So, fix a GapP function $f(x, y)$. Consider the polynomial $g(m) = 3m^2 - 2m^3$. One can verify that indeed:

Lemma 8. For all $m$,

1. If $m \equiv 0 \, (\text{mod } 2^j)$ then $g(m) \equiv 0 \, (\text{mod } 2^{2j})$.
2. If $m \equiv 1 \, (\text{mod } 2^j)$ then $g(m) \equiv 1 \, (\text{mod } 2^{2j})$.
3. If $m \equiv 0 \, (\text{mod } 2)$ then $g^{(k)}(m) \equiv 0 \, (\text{mod } 2^{2^k})$.
4. If $m \equiv 1 \, (\text{mod } 2)$ then $g^{(k)}(m) \equiv 1 \, (\text{mod } 2^{2^k})$.

Now, let $h(x, y) = g^{(1 + \log_{2} q(|x|))}(f(x, y))$. As $f$ is a GapP function, and GapP functions are closed under exponential-size sums and polynomial-size products, $h(x, y)$ is itself a GapP function. By the above lemma,

- If $f(x, y) \equiv 1 \, (\text{mod } 2)$ then $h(x, y) \equiv 1 \, (\text{mod } 2^{q(|x|)+1})$.
- If $f(x, y) \equiv 0 \, (\text{mod } 2)$ then $h(x, y) \equiv 0 \, (\text{mod } 2^{q(|x|)+1})$.

Define $r(x)$ as

\[ r(x) = \sum_{y \in \{0, 1\}^{q(|x|)}} h(x, y), \]

which is also a GapP function. We then have:

\[ r(x) \mod 2^{q(|x|)+1} = \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 1 \, (\text{mod } 2) \right\} \right| \]

and

\[ 2^{q(|x|)} - \left( r(x) \mod 2^{q(|x|)+1} \right) = \left| \left\{ y \in \{0, 1\}^{q(|x|)} : f(x, y) \equiv 0 \, (\text{mod } 2) \right\} \right|. \]

The above two computations can be done in $\text{FP}^{\text{GapP}}$, so we are done.