Toda Theorem
Part 1

\[ \text{PH} \subseteq \text{BPP}^{\oplus P} \]
Basic Definitions

• Language L belongs to class PP if exists polynomial NTM such that
  \[ x \in L \iff P\{M(x) = 1\} > 0.5 \]

• Language L belongs to class BPP if exists probabilistic polynomial algorithm such that x from L is accepted with probability more than 0.75 and x not from L is declined with the same probability.
⊕ \( P \) Class

• Language L belongs to class \( \oplus P \) (parity P) if exists polynomial-time non-deterministic Turing machine, such x lies in L is equivalent to that fact, that number of accepting computations is odd (or, exists polynomially checked relation R such that the number of \( y(R(x, y) = 1) \) ) is odd.

• It can be quickly checked that \( \oplus SAT \) is complete for \( \oplus P \)
Polynomial hierarchy

\[ \Sigma^0 P = P \]

\[ \Sigma^{i+1} P = NP^{\Sigma^i P} \]

\[ \text{PH} = \bigcup_{i \geq 0} \Sigma^i P \]

-Polynomial Hierarchy
General Idea of proof

\( NP \subseteq BPP^{\oplus P} \quad NP \subseteq RP^{\oplus P} \)

\( NP^A \subseteq BPP^{\oplus P^A} \)

- because of Valiant-Vazirani Lemma \( \forall i \in N \ \Sigma^i P \subseteq BPP^{\oplus P} \)
- because Valiant-Vazirani Lemma can be relativised

- We will prove, that by the mathematical induction. It will prove, that

- Base \( i = 1 \) is obvious
Idea of Proof

- Lemma 2: $\oplus P^{BPP^A} \subseteq BPP^{\oplus P^A}$
- Lemma 3: $\oplus P^{\oplus P} \subseteq \oplus P$
- Lemma 4: $BPP^{BPP^A} \subseteq BPP^A$

So, considering this Lemmas being truth we’ll receive

$$\Sigma^{k+1} P = NP^{\Sigma^k P} \subseteq NP^{BPP^{\oplus P}} \subseteq BPP^{\oplus P^{BPP^{\oplus P}}} \subseteq BPP^{BPP^{\oplus P^{\oplus P}}} \subseteq BPP^{BPP^{\oplus P}} \subseteq BPP^{\oplus P}$$

and the first part of Toda’s Theorem will be proved.
Lemma 4

- In definition of BPP we can use, instead of $(1-3/4)2^{-p_i}$ where $p_i$ is a polynomially function of input length
- $M$ uses $L$ as oracle, $M$ is wrong with $\Pr = 2^{-e(n)}$ $L \in \text{BPP}^A$
- We can consider, that the lengths of all branches of NTM $L$ are equal and the number of its accesses to $L$ is equal to $l(n)$ in all branches
- We can replace every access to oracle $L$ by the branch of machine $N$ (from the definition of BPP) with the probability of mistake
- The number $2^{-i(n)}$ of branches, which status will change is equal to $2^{-e(n)}$ that can be made (less than) 0.25
Lemma 2

- $L \in \oplus P^{BPPA}$ so exists NTM with oracle $B^A \in BPP^A$ accepting every $x \in \{0,1\}^n$ for odd number of $y$. $y \in \{0,1\}^{\gamma(n)}$

R is corresponding relationship

\[ R \in P^{B^A} \in P^{BPP^A} \in BPP^{BPP^A} \in BPP^A \]

- So $L = \{x | \#\{y : \#\{z : (x, y, z) \in L(\Pi^A)\} \geq (1 - 2^{-\pi(n)})2^{\varsigma(n)}\} \text{ is odd}\}$

- And we need:

\[ L = \{x | \#\{z : \#\{y : (x, y, z) \in L(\Pi^A)\} \text{ is odd}\} \geq 0.75 \times 2^{\varsigma(n)}\} \]
Lemma 2- end

- We can consider a table, (for fixed x, WLOG x is in L), in (y, z) we’ll put result of $\Pi$ for given (y, z). The number of rows with more than $\binom{1-2^{-\pi(n)}}{2^\gamma(n)}$ ones is odd and the number of columns, which have 1 in intersection with this columns is more than

$$2^{\xi(n)} - 2^{-\pi(n)} \times 2^{\xi(n)} \times 2^{\gamma(n)}$$

- In other rows is not many 1, so the number of ‘good’ rows is

$$2^{\xi(n)} - 2^{-\pi(n)} \times 2^{\xi(n)} \times 2^{\gamma(n)} - 2^{-\pi(n)} \times 2^{\xi(n)} \times 2^{\gamma(n)} \geq 0.75 \times 2^{\xi(n)}$$

for

$$\pi(n) \geq \gamma(n) + 3$$
Lemma 5

\[ \oplus P = co - \bigoplus P \]