The Polynomial Hierarchy

- Optimization problems
- The class \( \text{DP} \)
- The classes \( \text{P}^{\text{NP}} \) and \( \text{FP}^{\text{NP}} \)
- The classes \( \text{FP}^{\text{NP}[\log n]} \) and \( \text{FP}^{\text{NP[\parallel]}} \)
- The polynomial hierarchy

(C. Papadimitriou: Computational Complexity, Chapter 17)

Optimization Problems—cont’d

- The four variants can be ordered in “increasing complexity” by reductions: \( \text{TSP(D)} ; \text{EXACT TSP} ; \text{TSP COST} ; \text{TSP} \)
- All the four variants of TSP are *polynomially equivalent*: there is a polynomial-time algorithm for one iff there is one for all four (because \( \text{TSP(D)} \) and \( \text{TSP} \) are).
- Reductions and completeness provide a more refined and interesting characterization of problems.
- For example, the other three versions of TSP are complete for some very natural extensions of \( \text{NP} \).

The Class \( \text{DP} \)

- \( \text{EXACT TSP in \text{NP}}? \) Most probably not but closely related to \( \text{NP} \) and \( \text{coNP} \).
- A language \( L \) is in the class \( \text{DP} \) iff there are two languages \( L_1 \in \text{NP} \) and \( L_2 \in \text{coNP} \) such that \( L = L_1 \cap L_2 \).
- \( \text{EXACT TSP in \text{DP}} \) because the length of the shortest tour equal to \( B \) iff
  - there is a tour of length at most \( B \) (a TSP(D) problem) and
  - there is a no tour of length at most \( B - 1 \) (a TSP(D) COMPLEMENT problem).
- Note \( \text{DP is not \text{NP} \cap \text{coNP}} \)!
  (Most likely \( \text{DP} \) is not contained even in \( \text{NP} \cup \text{coNP} \).)
The Class DP—cont’d

➤ SAT-UNSAT: given two Boolean expressions \( \phi, \phi' \) both in CNF with three literals per clause. Is it true that \( \phi \) is satisfiable and \( \phi' \) is not?

➤ SAT-UNSAT is DP-complete.

➤ EXACT TSP is DP-complete.

➤ “Exact cost” versions of NP-complete optimization problems (INDEPENDENT SET, KNAPSACK, MAX-CUT, MAX SAT, …) can be shown DP-complete.

The Classes \( P^{NP} \) and \( FP^{NP} \)

➤ DP: the class of languages decided by two queries to an NP (SAT) oracle.

➤ A generalization of this idea: allow a polynomial number of adaptive SAT oracle calls: class \( P^{SAT} \).

➤ Since SAT is NP-complete, \( P^{SAT} = P^{NP} (\Delta_2P) \).

➤ \( FP^{NP} \): the corresponding functional problem functions computable using a polynomial number of adaptive NP oracle queries.

The Class DP—cont’d

➤ Also other types of problems are in DP.

➤ CRITICAL SAT: Given a Boolean expression \( \phi \), is it true that \( \phi \) is unsatisfiable but deleting any clause makes it satisfiable?

➤ UNIQUE SAT: Given a Boolean expression \( \phi \), is it true that \( \phi \) has a unique satisfying truth assignment?

➤ CRITICAL HAMILTON PATH: Given a graph, is it true that it has no Hamilton path but addition of any edge creates a Hamilton path?

➤ CRITICAL 3-COLORABILITY: Given a graph, is it true that it has no 3-coloring but deletion of any node makes it 3-colorable?

☞ “Critical” versions are known to be DP-complete.

The Class FP

➤ There are several natural \( FP^{NP} \)-complete problems

➤ MAX-WEIGHT SAT: Given a set of clauses each with an integer weight, find a truth assignment that satisfies a set of clauses with the most total weight.

➤ MAX OUTPUT: Given a nondeterministic Turing machine \( N \) and its input \( 1^n \) such that \( N \) halts on input \( 1^n \) in \( O(n) \) steps with a binary string of length \( n \) on its output string, determine the largest output (considered as a binary integers) of any computation of \( N \) on \( 1^n \).

➤ MAX OUTPUT is \( FP^{NP} \)-complete

➤ MAX-WEIGHT SAT is \( FP^{NP} \)-complete
**TSP**

**INSTANCE:** $n$ cities $1, \ldots, n$ and a nonnegative integer distance $d_{ij}$ between any two cities $i$ and $j$ (such that $d_{ij} = d_{ji}$).

**QUESTION:** What is the shortest tour of the cities?

**Theorem.** TSP is $\text{FP}^{\text{NP}}$-complete.

**Proof.**

- TSP $\in$ $\text{FP}^{\text{NP}}$: use binary search and the $\text{NP}$ oracle for TSP(D): is there a tour of length at most $B$?
- Completeness: reduction $(R, S)$ from MAX-WEIGHT SAT to TSP: Given a set $\Sigma$ of clauses with weights, $R(\Sigma)$ is a set of cities with distances such that if $t$ is the shortest tour for $R(\Sigma)$, then $S(t)$ is the truth assignment satisfying clauses with the most total weight.

**Corollary.** TSP COST is $\text{FP}^{\text{NP}}$-complete.

- Other $\text{FP}^{\text{NP}}$-complete problems: KNAPSACK, WEIGHTED MAX CUT, WEIGHTED BISECTION WIDTH
- What about CLIQUE SIZE, UNARY TSP, MAX SAT, MAX CUT, BISECTION WIDTH?
- For these only $\log n$ oracle calls are needed: cost polynomially large (logarithmically many bits)
- **CLIQUE SIZE:** Given a graph, determine the size of its largest clique. Use binary search with oracle: is the largest clique larger than $k$? Only $\log n$ queries are needed where $n$ is the number of nodes.
The polynomial hierarchy is a sequence of classes:

- $\Delta_0 \mathsf{P} = \Sigma_0 \mathsf{P} = \Pi_0 \mathsf{P} = \mathsf{P}$
- $i \geq 0$:
  - $\Delta_{i+1} \mathsf{P} = \Sigma_{i+1} \mathsf{P}$
  - $\Sigma_{i+1} \mathsf{P} = \mathsf{NP}^{\Sigma_i \mathsf{P}}$
  - $\Pi_{i+1} \mathsf{P} = \mathsf{coNP}^{\Sigma_i \mathsf{P}}$

- Cumulative polynomial hierarchy: $\mathsf{PH} = \bigcup_{i \geq 0} \Sigma_i \mathsf{P}$

In the literature also the following notation is used: $\Delta^p_i$, $\Sigma^p_i$, $\Pi^p_i$
The polynomial hierarchy—cont’d

Properties:
- \( \Delta_1^P = \Sigma_0^P = P \)
- \( \Sigma_1^P = \text{NP}^\Sigma_0^P = \text{NP} \)
- \( \Pi_1^P = \text{coNP}^\Sigma_0^P = \text{coNP} \)
- \( \Delta_2^P = \Sigma_1^P = \text{P}^\Sigma_0^P = \text{NP} \)
- \( \Sigma_2^P = \text{NP}^\Sigma_1^P = \text{NP}^\text{NP} \)
- \( \Pi_2^P = \text{coNP}^\Sigma_1^P = \text{coNP}^\text{NP} \)

- \( \Delta_i^P \subseteq \Sigma_{i+1}^P \subseteq \Pi_{i+1}^P \subseteq \Delta_{i+2}^P \)

Certificates—cont’d

- A relation \( R \subseteq (\Sigma^*)_{i+1} \) is said to be polynomially balanced if whenever \((x, y_1, \ldots, y_i) \in R\), it holds that \(|y_1|, \ldots, |y_i| \leq |x|^k\) for some \(k\).

- Let \( L \) be a language and \( i \geq 1 \). Then \( L \in \Sigma_i^P \) iff there is a polynomially balanced, polynomial-time decidable \((i+1)\)-ary relation \( R \) such that

\[
L = \{ x \mid \exists y_1 \forall y_2 \exists y_3 \cdots Qy_i \text{ such that } (x, y_1, \ldots, y_i) \in R \}
\]

where \( Q \) is \( \forall \) if \( i \) is even and \( \exists \) if \( i \) is odd.

Certificates

- Let \( L \) be a language and \( i \geq 1 \). Then \( L \in \Sigma_i^P \) iff there is a polynomially balanced relation \( R \) such that the language \( \{x, y \mid (x, y) \in R\} \) is in \( \Pi_{i-1}^P \) and

\[
L = \{ x \mid \text{there is a } y \text{ such that } (x, y) \in R \}
\]

- Let \( L \) be a language and \( i \geq 1 \). Then \( L \in \Pi_i^P \) iff there is a polynomially balanced relation \( R \) such that the language \( \{x, y \mid (x, y) \in R\} \) is in \( \Sigma_{i-1}^P \) and

\[
L = \{ x \mid \text{for all } y \text{ with } |y| \leq |x|^k, (x, y) \in R \}
\]

PH is fragile

- If for some \( i \geq 1 \), \( \Sigma_i^P = \Pi_i^P \), then for all \( j > i \),

\[
\Delta_j^P = \Sigma_j^P = \Pi_j^P = \Sigma_i^P.
\]

(The polynomial hierarchy is said to collapse to the \(i\)th level.)

- If \( P = \text{NP} \), or if \( \text{NP} = \text{coNP} \), then the polynomial hierarchy collapses to the first level.

- \( P = \text{NP} \) iff \( P = \text{PH} \).

- Notice that it can be the case that \( P \neq \text{NP} \) and \( \text{NP} \neq \text{coNP} \) but the polynomial hierarchy collapses to the second level (not expected to happen, though).
Complete problems

- **QSAT\(_i\)** (quantified satisfiability with \(i\) alternations of quantifiers):
  - Given a Boolean expression \(\phi\) with the Boolean variables partitioned into \(i\) sets \(X_1, \ldots, X_i\), is it true that there is a partial truth assignment for the variables \(X_1\) such that for all partial truth assignments for \(X_2\) there is a partial truth assignment for \(X_3\) \(
\ldots \phi\) is satisfied by the overall truth assignment?

- **QSAT\(_i\)**: Is the following quantified Boolean expression true
  \[ \exists X_1 \forall X_2 \exists X_3 \cdots QX_i \phi \]
  where \(Q\) is \(\forall\) if \(i\) is even and \(\exists\) if \(i\) is odd.

Theorem. For all \(i \geq 1\), **QSAT\(_i\)** is \(\Sigma_i P\)-complete.

Example. **MINIMUM CIRCUIT**: Given a Boolean circuit \(C\), is it true that there is no circuit with fewer gates that computes the same Boolean function?

**MINIMUM CIRCUIT** \(\in \Pi_2 P\).

Example. **MINIMAL MODEL SAT**: Given a set of clauses \(S\) and an atom \(a\), is it true that there is a (subset) minimal model of \(S\) with \(a\) true?

**MINIMAL MODEL SAT** is \(\Sigma_2 P\)-complete.

Complete problems—cont’d

- **PH** \(\subseteq\) **PSPACE**
  - \(L \in \text{PH}\) if \(L \in \Sigma_i P\) if \(L = \{x \mid \exists y_1 \forall y_2 \cdots Qy_i \text{ s.t. } (x, y_1, \ldots, y_i) \in R\}\)
  - It is open whether **PH** = **PSPACE**.
    - If **PH** = **PSPACE**, then the polynomial hierarchy collapses to some finite level. (There are **PSPACE**-complete problems.)
    - If **PH** does not collapse, problems are strictly harder in an upper level when compared to the lower level: if \(L\) is a \(\Sigma_{i+1} P\)-complete language and \(L \in \Sigma_i P\), then **PH** collapses to the level \(i\).

Example. Consider a \(\Sigma_3 P\)-complete problem. It cannot be solved with a polynomial overhead on top of a procedure for a problem in **NP** (unless **PH** collapses to the level 1).
BPP and polynomial circuits

**Theorem.** $\text{BPP} \subseteq \Sigma_2^P$

**Corollary.** $\text{BPP} \subseteq \Sigma_2^P \cap \Pi_2^P$

Proof. $\text{BPP}$ is closed under complement. Hence, if $L \in \text{BPP}$, $\overline{L} \in \text{BPP} \subseteq \Sigma_2^P$ implying $L \in \Pi_2^P$.

**Theorem.** If SAT has polynomial circuits, then the polynomial hierarchy collapses to the second level.

---

**Learning Objectives**

- The classes $\text{DP}$, $\text{P}^{\text{NP}}$, $\text{FP}^{\text{NP}}$, $\text{FP}^{\text{NP}[\log n]}$ and $\text{FP}^{\text{NP}}$
- Classification of optimization problems into these classes
- The concept of the polynomial hierarchy