Today

- Fortnow’s time/space lower bound on SAT.
- PH: Complete problems and a hypothesis.

Power of Alternation

- Basic notion.
- Captures Time/Space differently.
- Next application shows how powerful it is.

Fortnow’s theorem

For today, will use LIN to mean the class of computations in NEARLY-LINEAR TIME:

\[ LIN = \bigcup_c TIME(n (\log n)^n) \]

- Belief: SAT \(\not\in L\).
- Belief: SAT \(\not\in LIN\).
- Can’t prove any of the above.
- Fortnow’s theorem: Both can not be false!

Proof of Fortnow’s theorem

- For simplicity we’ll prove that if SAT \(\in Time(n \log n)\) and SAT \(\in L\) then we reach a contradiction.
- Won’t give full proof: But rather give main steps, leaving steps as exercises.
Main ideas

- Alternation simulates small space computations in little time. (Savitch).
- If NTIME(t) in co-NTIME(t log t), then alternation is not powerful.
- Formal contradiction derived from: \( \text{ATIME}[a, t] \not\subseteq \text{ATIME}[a-1, t/\log t] \).

Fortnow: Step 1

Fact 1: If \( L \) in NTIME(t), and \( x \) of length \( n \), then can construct SAT instance \( \phi \) of size \( t(n) \log t(n) \) such that \( x \in L \) iff \( \phi \) in SAT.

Reference: a 70’s paper of Cook.

Proof: Left as exercise.

Fortnow: Step 2

Fix \( a(n) = \sqrt{\log n} \).

Fact 2: \( \text{ATIME}[a, t] \) is contained in NTIME[t (log t)^2a]

Proof: Induction on \#alternations + Fact 1.

Fortnow: Step 3

Fact 3: If SAT in \( L \), then NTIME[t (log t)^2a] in SPACE(log t + a log log t).

Proof: Padding
Fortnow: Step 4

Fact 4: SPACE[s] in ATISP[b, 2^{O(s/b)}], bs in ATIME[b, 2^{O(s/b)}]

Proof: Exercise 3 of PS 1.

Whither contradiction?

- If we set $b = a - 1$ (approximated by $a$ in our calculations), then ...
- ATIME[a, t] is contained in ATIME[b, 2^{(log t + a \log t)}],
  which is a contradiction.

Polynomial Hierarchy

Recall definitions

- $\Sigma^P_i$ = Languages accepted by polynomial time bounded ATM starting in existential state with $i$ alternating quantifiers.
- $\Pi^P_i$ = Languages accepted by polynomial time bounded ATM starting in universal state with $i$ alternating quantifiers.
- $\text{PH} = \bigcup_{i \geq 1} \Sigma^P_i$.
- Convention: $\Sigma^P_0 = \Pi^P_0 = P$.
- PH “discovered” by Meyer & Stockmeyer.

PH: Simple properties

- $\Pi^P_i = \{L|\overline{L} \in \Sigma^P_i\}$.
- $\Pi^P_{i-1} \subseteq \Sigma^P_i \subseteq \Pi^P_{i+1}$.
- $\text{PH} = \bigcup_{i \geq 1} \Pi^P_i$.
- As in assertion “TQBF is complete for PSPACE”, can postpone all computations to the end; and can assume final computation simply verifies if a 3-CNF formula is satisfied.
- $\Sigma^P_i$ Complete problem:

  $i$-QBF = $\{\phi|\exists x_1 \forall x_2 \ldots \phi(x_1, \ldots, x_i) = \text{true}\}$. 
\[ \Sigma^P_1 = NP; \Sigma^P_{i+1} = NP^{\Sigma^P_i}. \]

- \( A \in \Sigma^P_{i+1} \iff \exists B \in \Pi^P_i, \exists c < \infty \text{ s.t.} \]
  \[ x \in A \iff \exists y, |y| \leq |x|^c, (x, y) \in B. \]

**A non-trivial theorem**

Theorem [Umans '2000]: \( \text{MinDNF} \) is \( \Sigma^P_2 \) complete.

Conjectured since the discovery of PH.

---

**Why PH interests us**

- Good question. Should ask about every class.
- Motivation 1: \( \text{MinDNF} \). But why consider the entire infinite hierarchy.
- Motivation 2:
  - Tests our ability to work with alternation.
  - We know a lot about quantifiers, but don’t know how to eliminate even one quantifier!
  - Belief: Can not remove quantifiers!
  - A stronger belief than \( \text{NP} \neq \text{P}, \text{NP} \neq \text{co-NP} \) etc.
  - Many complexity theoretic assertions can be proved under this belief.

---

**PH collapse hypothesis**

Hypothesis: For every \( i \), \( \Sigma^P_i \neq \Pi^P_i \).

Proposition: For \( i \leq j \),
\[ \Sigma^P_i = \Pi^P_i \Rightarrow \Sigma^P_j = \Pi^P_j = \Sigma^P_i = \Pi^P_i. \]

Proof:

- By induction on \( j \). True for \( j = i \). Let \( j > i \) and assume true for \( j - 1 \).
- Let \( A \in \Sigma^P_j \) and let \( B \in \Pi^P_{j-1} \) s.t.
  \[ x \in A \iff \exists y \text{ s.t. } (x, y) \in B. \]
- By induction \( B \in \Sigma^P_i \) and so \( \exists C \in \Pi^P_{i-1} \) s.t.
  \[ (x, y, z) \in C. \]
- So \( x \in A \iff \exists y, z \text{ s.t. } (x, y, z) \in C. \text{ Thus } A \in \Sigma^P_i. \]