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:

$LIN = \cup_c TIME(n(\log n)^n$.

- Belief: SAT $\notin L$.
- Belief: SAT $\notin LIN$.
- 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 $\mathrm{SAT} \in \mathrm{Time}(n \log n)$ and $\mathrm{SAT} \in L$ 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: ATIME[a,t] $\not\subseteq$ 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: 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,$2^{(s/b)}$,bs] in ATIME[b,$2^{(s/b)}$]

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,$2^{(logt+aloglo}$ which is a contradiction.

Polynomial Hierarchy

Recall definitions

- Σ_i^P = Languages accepted by polynomial time bounded ATM starting in existential state with i alternating quantifiers.
- Π_i^P = Languages accepted by polynomial time bounded ATM starting in universal state with i alternating quantifiers.
- $\mathrm{PH} = \cup_{i|\geq 1}\Sigma_i^P$.
- Convention: $\Sigma_0^P = \Pi_0^P = P$.
- PH "discovered" by Meyer & Stockmeyer.

PH: Simple properties

- $\Pi_i^P = \{L | \overline{L} \in \Sigma_i^P\}$.
- $\Pi_{i-1}^P \subseteq \Sigma_i^P \subseteq \Pi_{i+1}^P$.
- $\mathrm{PH} = \cup_{i\geq 1}\Pi_i^P$.
- 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.
- Σ_i^P Complete problem:

  i-QBF $= \{\phi | \exists \mathbf{x}_1 \forall \mathbf{x}_2 \ldots \phi(\mathbf{x}_1, \ldots, \mathbf{x}_i) = \text{true}\}$.

- $\Sigma_1^P = NP; \Sigma_{i+1}^P = NP^{\Sigma_i^P}$.
- $A \in \Sigma_{i+1}^P \Leftrightarrow \exists B \in \Pi_i^P, c < \infty$ s.t.

$$x \in A \Leftrightarrow \exists y, |y| \leq |x|^c, (x, y) \in B.$$

A non-trivial theorem

Theorem[Umans '2000]: $\textsc{MinDNF}$ is Σ_2^P-complete.

Conjectured since the discovery of PH.

Why PH interests us

- Good question. Should ask about every class.
- Motivation 1: $\textsc{MinDNF}$. 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 NP $\neq P$, NP $\neq$ co-NP etc.
  - Many complexity theoretic assertions can be proved under this belief.

PH collapse hypothesis

Hypothesis: For every i, $\Sigma_i^P \neq \Pi_i^P$.

Proposition: For $i \leq j$,
$\Sigma_i^P = \Pi_i^P \Rightarrow \Sigma_j^P = \Pi_j^P = \Sigma_i^P = \Pi_i^P$.

Proof:

- By induction on j. True for $j = i$. Let $j > i$ and assume true for $j - 1$.
- Let $A \in \Sigma_j^P$ and let $B \in \Pi_{j-1}^P$ s.t.
  $x \in A \Leftrightarrow \exists y$ s.t. $(x, y) \in B$.
- By induction $B \in \Sigma_i^P$ and so $\exists C \in \Pi_{i-1}^P$ s.t. $(x, y) \in B \Leftrightarrow \exists z$ s.t. $(x, y, z) \in C$.
- So $x \in A$ iff $\exists y, z$ s.t. $(x, y, z) \in C$. Thus $A \in \Sigma_i^P$.