CS 538
Jorge Padilla
April 1, 1998

In this lecture, we address the question: Does SAT has small (i.e., polynomial-sized) circuits? In other terms, is $NP \subseteq P/poly$?

We do not have a definite answer to this question. In relation to this question, we have instead the following theorem:

Theorem : $NP \subseteq P/poly \Longrightarrow PH = \Sigma_2^{\mathrm{P}}$

Proof :

Facts

(i) SAT is **self-reducible**. *Explanation:* There are many definitions of self-reducibility. One of them, is the one that follows:

Definition: A is self-reducible if $A \in P^{\mathrm{A}}$, via an oracle TM that on input x, ask queries only about strings $y < x$ (lexicographic order).

SAT satisfies this notion of self-reducibility. We give the following algorithm as a proof of this statement:

on input ϕ
  if ϕ has NO variables
    then return 1 if ϕ evaluates to 1
    and return 0 if ϕ evaluates to 0
  else
    let x be a variable in ϕ
    let ϕ_1 be the result of replacing x by 1
    let ϕ_0 be the result of replacing x by 0
    if $\phi_1 \in SAT$, then return 1
    if $\phi_0 \in SAT$, then return 1
    else return 0 $\Box$

We will use this fact (i) to give a Σ_2^{P} algorithm for Π_2^{P} $(= co - NP^{NP})$. That is, let $A \in \Pi_2^{\mathrm{P}}$ *iff* A is recognized by a *co-NP* nachine M with oracle SAT. We will show : $A \in \Sigma_2^{\mathrm{P}}$. Below, is the proof of this last statement:

Proof :

on input x (with $|x| = n$)
(note that M asks queries only of inputs of $length \leq |x|^k$ for some k.)
  existentially guess a sequence of circuits C_1, C_2,...,C_{n^k}
  using universal moves, do the following:
    1) Simulate $M^{\mathrm{SAT}}(x)$ (answering oracle queries using C_1, C_2,...,C_{n^k})
    2) Verify that each of the circuits C_1, C_2,...,C_{n^k} is computing SAT correctly.
      That is for all strings ϕ with $|\phi| \leq n^k$, $C_\phi(\phi) = 1$, iff :

$[\phi$ has NO variables and evaluates to TRUE] OR
$[(C_{|\phi_0|}(\phi_0) = 1\ OR\ C_{|\phi_1|}(\phi_1) = 1)\ )]$. □

What remains to prove our theorem is this statement:

$\Pi_2^{\mathrm{P}} = \Sigma_2^{\mathrm{P}} \Longrightarrow PH = \Sigma_2^{\mathrm{P}}$

Proof: (*by induction*)

Let $A \in \Sigma_3^{\mathrm{P}}$ then A is recognized by an ATM that begins in existential states then goes to universal states and the goes back to existential states.

Note that :
$B = \{\ (C, x) :\ C$ is a universal configuration of M that is accepting on input $x\ \}$; then: $B \in \Pi_2^{\mathrm{P}} \subseteq \Sigma_2^{\mathrm{P}}$.

Here is the Σ_2^{P} algorithm for A:

on input x
existentially simulate $M(x)$ until it reaches a universal configuration C, then use the Σ_2^{P} algorithm to see if $(C, x) \in B$.

(*Inductive part of the proof*) :

We have $\Sigma_3^{\mathrm{P}} \subseteq \Sigma_2^{\mathrm{P}}$. Assume $\Sigma_i^{\mathrm{P}} \subseteq \Sigma_2^{\mathrm{P}}$. We will show: $\Sigma_{i+1}^{\mathrm{P}} \subseteq \Sigma_2^{\mathrm{P}}$.

$\Sigma_{i+1}^{\mathrm{P}} = NP^{\Sigma_i^{\mathrm{P}}} \subseteq NP^{\Sigma_2^{\mathrm{P}}} = \Sigma_3^{\mathrm{P}} = \Sigma_2^{\mathrm{P}}$. □