

Some Connections Between Nonuniform and Uniform Complexity Classes

Ashraf A. Ibrahim

18 April 2008

Objectives For This Talk:

This presentation is a discussion of a paper by R. Karp and R. Lipton with the same title. We are going to summarize all results of related to the complexity class $P/poly$ and introduce some of the techniques used to prove these results.

Definitions and Notations:

Let S be a subset of $\{0, 1\}^*$. Let $h : \mathbb{N} \rightarrow \{0, 1\}^*$, define $S : h = \{wx : x \in S \text{ and } w = h(|x|)\}$.

Let \mathcal{S} be a collection of languages over $\{0, 1\}$ and let \mathcal{F} be a collection of functions from \mathbb{N} to $\{0, 1\}^*$. Define

$$\mathcal{S}/\mathcal{F} = \{S \subset \{0, 1\}^* : \exists h \in \mathcal{F} \text{ s.t. } S : h \in \mathcal{S}\}$$

Definition:

Let $poly$ denote the set of polynomially-bounded functions h from \mathbf{N} to $\{0, 1\}^*$. Then the class $P/poly$ is the collection of languages S such that $S : h \in P$ for some $h \in poly$.

Defintions and Notations:

Let S be any language in over $\{0, 1\}$.

1- Define the following sequence of boolean functions

$$S_n : \{0, 1\}^n \rightarrow \{0, 1\}$$

where $S_n(x_1, \dots, x_n) = 1$ iff $x_1x_2\dots x_n$ is in S .

2- let $L(S_n)$ denote the minimun number of gates in a boolean circuit realizing S_n .

3- We say S has small circuits if $L(S_n)$ is bounded by a polynomial in n .

Theorem 1:

Let $S \subset \{0, 1\}^*$, then the following are equivalent:

- 1- S has small circuits.
- 2- S is in $P/poly$.

The Tournament Method:

A game G is specified by

1- a set $W \subset \{0, 1\}^*$,

2- a pair of length preserving functions F_0 and F_1 , each mapping $\{0, 1\}^* - W$ into $\{0, 1\}^*$, and

3- there is no sequence of moves leading from a position x back to itself.

We can apply nonuniform complexity to games and conclude

Theorem 2:

If $PSPACE \subset P/poly$ then

$$PSPACE = \Sigma_2^p \cap \Pi_2^p.$$

Theorem 3:

$EXPTIME \subset PSPACE/poly$ iff
 $EXPTIME = PSPACE$.

The Methods of Recursive Definition:

Let $K \subset \{0, 1\}^*$ and let $C_K : \{0, 1\}^* \rightarrow \{0, 1\}$ be the characteristic function of K . The recursive definition of C_K is the rule that specifies C_K on a basis set $A \subset \{0, 1\}^*$, and uniquely determines C_K by a recurrence formula of the form $C_K(x) = F(x, C_K(F_1(x)), \dots, C_K(F_t(x)))$ for $x \in \{0, 1\}^* - A$.

Example:

Let G be a game and let S_G be the set of positions from which the player to move can force a win. Then G is uniquely determined by

1- if $x \in W$ then $x \in G$

2- if $x \in \{0, 1\}^* - W$, then

$$x \in G \leftrightarrow f_0(x) \notin G \quad \text{or} \quad f_1(x) \notin G$$

Remark:

When C_K has a simple enough recursive definition, then bounds on the nonuniform complexity of K , yield bounds on its uniform complexity.

Lemma 1:

If $NP \subset P/poly$, then

$$\bigcup_{i=1}^{\infty} \Sigma_i^p \subset P/poly.$$

Theorem 4:

If $NP \subset P/poly$, then

$$\Sigma_2^p = \bigcup_{i=1}^{\infty} \Sigma_i^p.$$

Definition:

let *ZEROS* denote the following decision problem: given a prime q and a set $\{p_1(x), p_2(x), \dots, p_n(x)\}$ of sparse polynomials with integral coefficients to determine whether there exists an integer x such that

$$p_i(x) \equiv 0 \pmod{q} \quad \text{for } i = 1, 2, \dots, n.$$

Corollary 1: (due to Plaisted).

If $ZEROS \in P/poly$, then

$$\bigcup_{i=1}^{\infty} \Sigma_i^p = \Sigma_2^p$$

Theorem 5:

$EXPTIME \subset P/poly$ iff $EXPTIME = \Sigma_2^p$.

We conclude our presentation with following corollary,

Corollary 2:

If $EXPTIME \subset P/poly$ then $P \neq NP$.

Reference:

R. Karp and R. Lipton: *Some connections between nonuniform and uniform complexity classes*, Proc. 12th Annual ACM Symposium on Theory of Computing, pp. 302-309, 1980.