LOWER BOUNDS BY RECURSION THEORETIC ARGUMENTS
(Extended Abstract)

Uwe Schöning
EWH Koblenz, Informatik
Rheinau 3-4
D-5400 Koblenz
West Germany

Abstract

Using methods and notions stemming from recursion theory, new lower bounds on the "distance" between certain intractable sets (like NP-complete or EXPTIME-complete sets) and the sets in P are obtained. Here, the distance of two sets A and B is a function on natural numbers that, for each n, gives the number of strings of size n on which A and B differ. Yesha [6] has shown that each NP-complete set has a distance of at least $O(\log \log n)$ from each set in P, assuming $P \neq NP$. Similarly, without an additional assumption, each EXPTIME-complete set has a distance of at least $O(\log \log n)$ from each set in P.

In this paper the following will be shown:

1. Assuming $P \neq NP$, no NP-complete set that is a (weak) $p$-cylinder can be within a distance of $q(n)$ to any set in P where q is any polynomial. (Note that all "naturally known" NP-complete sets have been shown to be $p$-cylinders [3]).

2. No EXPTIME-complete set can be within a distance of $2^{nc}$ to any set in P for some constant $c > 0$.

The second result improves Yesha's by at least two exponentials.
Introduction

Yesha [6] suggested to measure the "distance" of two sets by the census of their symmetric difference.

**Definition.** For two sets \( A \) and \( B \) define the function \( \text{dist}_{A,B} : \mathbb{N} \to \mathbb{N} \) as
\[
\text{dist}_{A,B}(n) = \{|x : |x| = n \text{ and } x \in A \triangle B\}.
\]

If \( A \) is intractable and \( B \) is feasible, then \( B \) could be used to "approximate" \( A \) provided \( \text{dist}_{A,B} \) is a slowly growing function. We will be concerned with proving lower bounds on the distance between certain intractable complete sets and the sets in \( P \).

These notions also play a certain role in the cryptographical security of pseudo-random number generators [5]. If \( A \) is the range of a pseudo-random number generator and \( \text{dist}_{A,B} \) is a slowly growing function for some set \( B \) in \( P \), then the generator is not secure; it does not "pass" the polynomial "statistical test" \( B \) (see [5]). \( B \) can be used to infer \( A \) with high probability. The desirable case in cryptography is that \( \text{dist}_{A,B}(n)/2^n \) is close to 1/2 for sufficiently large \( n \). That is, the "test" \( B \) cannot distinguish \( A \) from a real random source.

The following lower bounds are due to Yesha [6].

**Proposition 1.** If \( P \neq \text{NP} \), then for every \( \text{NP} \)-complete set \( A \) and for every set \( B \) in \( P \), \( \text{dist}_{A,B}(n) \) is not \( O(\log \log n) \).

**Proposition 2.** For every \( \text{EXPTIME} \)-complete set \( A \) and every set \( B \) in \( P \), \( \text{dist}_{A,B}(n) \) is not \( O(\log \log n) \).

These bounds will be improved in the next sections.