HARDNESS HYPOTHESES, DERANDOMIZATION, AND CIRCUIT COMPLEXITY

JOHN M. HITCHCOCK AND A. PAVAN

Abstract. We consider hypotheses about nondeterministic computation that have been studied in different contexts and shown to have interesting consequences:

- The measure hypothesis: NP does not have p-measure 0.
- The pseudo-NP hypothesis: there is an NP language that can be distinguished from any DTIME($2^{n^\epsilon}$) language by an NP refuter.
- The NP-machine hypothesis: there is an NP machine accepting 0$^*$ for which no $2^{n^\epsilon}$-time machine can find infinitely many accepting computations.

We show that the NP-machine hypothesis is implied by each of the first two. Previously, no relationships were known among these three hypotheses. Moreover, we unify previous work by showing that several derandomizations and circuit-size lower bounds that are known to follow from the first two hypotheses also follow from the NP-machine hypothesis. In particular, the NP-machine hypothesis becomes the weakest known uniform hardness hypothesis that derandomizes AM. We also consider UP versions of the above hypotheses as well as related immunity and scaled dimension hypotheses.

Keywords. Circuit complexity, derandomization, resource-bounded measure and scaled dimension.

Subject classification. 68Q15, 68Q17, and 68Q30.

1. Introduction

The following uniform hardness hypotheses are known to imply full derandomization of Arthur–Merlin games (NP = AM):

- The measure hypothesis: NP does not have p-measure 0 (Impagliazzo & Moser 2003).
The pseudo-NP hypothesis: NP has a language that can be distinguished from any DTIME(2^{n^c}) language by an NP refuter (Lu 2001).

NE ∩ coNE cannot infinitely-often be decided in 2^{n^c} time (Impagliazzo et al. 2002).

While the hypotheses are quite different, each of these results rely on the ingenious “easy witness method” of Kabanets (2001): try to show that the hypothesis is false by searching for an easy witness, a witness that has low circuit complexity when viewed as the truth-table of a Boolean function. If the hypothesis is true, we can show that this search must fail. Therefore there are no easy witnesses and we can use the mechanism in the hypothesis to nondeterministically generate witnesses of high circuit complexity that are sufficient for derandomizing AM (Klivans & van Melkebeek 2002; Miltersen & Vinodchandran 2005).

Given the similarity in the proofs, it is natural to ask how much more these hypotheses have in common. We show that all three of the above hypotheses imply the following NP-machine hypothesis:

There is an NP machine accepting 0^* for which no 2^{n^c}-time machine can find infinitely many accepting computations.

Roughly speaking, this hypothesis says that there is an NP search problem that cannot be solved in subexponential time. This hypothesis and several variations have been used a few times in complexity theory (Fenner et al. 2003; Glaßer et al. 2004; Hemaspaandra et al. 1997; Pavan & Selman 2002). The NP-machine hypothesis in this form is due to Pavan & Selman (2002), who showed that it implies a separation of NP-completeness notions.

The easy witness method readily applies to show that the NP-machine hypothesis also implies NP = AM. Therefore we have the following picture:

\[
\begin{array}{c}
\text{Measure Hypothesis} \\
\text{Pseudo-NP Hypothesis} \Rightarrow \text{NP-Machine Hypothesis} \Rightarrow \text{NP = AM} \\
\text{NE ∩ coNE Hypothesis}
\end{array}
\]

Thus the NP-machine hypothesis becomes the weakest known “uniform hardness” hypothesis that derandomizes AM.