The polynomial and linear time hierarchies in weak arithmetic

Leszek Aleksander Kołodziejczyk
Institute of Mathematics
Warsaw University
Banacha 2, 02-097 Warszawa, Poland.

Neil Thapen
Mathematical Institute
Academy of Sciences of the Czech Republic
Žitná 25, CZ-115 67 Praha 1.

May 15, 2007

Abstract

We prove a number of conditional independence results concerning the relationship between the linear and polynomial time hierarchies in PV and S^1_2. Our general assumption is that integer factoring is hard, in the sense that there does not exist a probabilistic polynomial time algorithm for factoring. Under this assumption, we show that there exists a model of PV in which the two hierarchies differ. The proof technique cannot be extended to S^1_2, but can be modified to yield a model of S^1_2 in which NP is not contained in the second level of the linear hierarchy. We then show that there exists a model of S^1_2 in which the hierarchies are equal. As a corollary of the proof, we obtain the existence of a model of S^1_2 in which PH (defined in terms of so-called strict Σ^b_n classes) does not collapse.

Our methods are model-theoretic and rely on the analysis of variants of the weak pigeonhole principle for polynomial time functions. A separate, though similar, model-theoretic argument shows unconditionally that there is a model of the very weak theory V^0 in which the linear and polynomial hierarchies are different.