A question that is studied in this and other works is: what relations between computational complexity classes are provable in weak theories of bounded arithmetic. While these questions are generally hard, they can sometimes be answered under additional hardness assumptions.

Here, the complexity classes considered are the polynomial time hierarchy PH, in particular its first level NP, and the analogously defined *linear time hierarchy* $LinH$. The theories consideres are PV, the universal theory of the polynomial time functions, and S^1_2, the extension of PV by length induction for NP-predicates.

The hardness assumption used is that there is no probabilistic algorithm that can factor products of two prime numbers in polynomial time. Under this assumption, it is shown consistent with PV that NP is not a subset of $LinH$, and both the following are consistent with S^1_2: 1) NP is not contained in the second level of $LinH$, and 2) the entire PH is contained in $LinH$.

The results are proved by model constructions, making use of the fact that assuming the hardness of factoring, certain forms of the weak pigeonhole principle are unprovable in S^1_2. The scheme $iWPHP$ states that no polynomial time function is an injective mapping from n^2 into n, for every n. Similarly, $sWPHP$ states that there is no polynomial time surjective mapping from n onto n^2. A common generalization is $mWPHP$ stating that no relation in NP is an injective multifunction from n^2 into n. It is known [1] that if factoring is hard, then $S^1_2 + sWHP$ does not prove $iWPHP$, and thus in particular, S^1_2 alone does not prove $mWPHP$.

The precise statement of the results concerns the equivalence of bounded formulas: in the standard model, formulas in the bounded arithmetic hierarchy Σ^b_n define exactly the sets in the corresponding levels of PH, and similarly for linearly bounded formulas Σ^{lin}_n – in which the terms and in particular the bounds on quantifiers are restricted to be polynomials – and $LinH$.

Under the assumption that $PV + sWPHP$ does not prove $iWPHP$, the following are constructed:

- A model of PV in which some Σ^b_1-formula is not equivalent to any Σ^{lin}_∞-formula (with parameters).
- A model of S^1_2 in which some Σ^b_1-formula is not equivalent to any Σ^{lin}_2-formula (with parameters).

Moreover, assuming that S^1_2 does not prove $mWPHP$, a model M of S^1_2 with a $p \in M$ is constructed such that every Σ^b_∞-formula is equivalent in M to a Σ^{lin}_∞-formula with the parameter p.

Finally, it is shown that for $m \geq 1$, in every model of $S^1_2 + \neg mWPHP$ there is a Σ^b_∞-formula not equivalent to any Σ^b_m-formula. In this sense $S^1_2 + \neg mWPHP$ proves that the polynomial time hierarchy is infinite.

References

[1] E. Jeřábek, On independence of variants of the weak pigeonhole principle, J. Logic Comput. **17** (2007), no. 3, 587–604. MR2334518 (2008i:03067)