This paper presents a proof theoretic framework for obtaining relativized separation results between bounded arithmetic theories. The most well-studied of these theories are the theories S^i_2 and T^i_2. These are axiomatized using a base theory $BASIC$ together with respectively Σ^b_i length induction axioms or Σ^b_i induction axioms and form a hierarchy $S^i_2 \subseteq T^i_2 \subseteq S^{i+1}_2$. Here the predicates definable by Σ^b_i-formulas correspond exactly to the class Σ^p_i of the polynomial hierarchy. Since the theories only have bounded axioms by Parikh's theorem these theories cannot define exponentiation, so length and usual induction may be different. The theories S^i_2 and T^i_2 are studied because of their many connections to open problems in computational complexity [1]. Relativized variants of these theories, $S^i_2(X)$ and $T^i_2(X)$, can be defined by adding an undefined predicate symbol to the language of these theories. In the nonrelativized case, it is known that $S^{i+1}_2 = T^i_2$ implies the collapses of the polynomial hierarchy and $S^i_2 = T^i_2$ would have consequences for bounded query classes; on the other hand, in the relatived case one can show that $S^{i+1}_2(X) \neq T^i_2(X)$ and $S^i_2(X) \neq T^i_2(X)$ [3][2]. The paper under review considers theories $s\Sigma^b_i(X)$-L^mIND which have prenex Σ^b_i induction in the relativized language up to m lengths of a number. The paper computes a so-called "dynamic ordinal" for these theories where m and i satisfy some conditions and uses this to prove relativized separations.

Relativized separations of this type have also been obtained in the reviewer's paper [4] which was written at about the same time as this paper. The proof techniques in the two papers are, however, different. In the reviewer's paper, a generalized conservation result is used to give a characterization of the $\Delta^b_j(X)$-predicates (for $j \leq i$ and m satisfying some conditions) of the theory in question. Then a complexity theoretic oracle result is used to give the separation. The paper under review is inspired by the ordinal theoretic separations of the fragments of Peano Arithmetic, $I\Sigma_n$. The dynamic ordinal of a bounded arithmetic theory is the set of terms up to which the theory can proved bounded order induction for prenex $\Pi^b_1(X)$-formulas. For example, for $T^1_2(X)$ one can show this is the set of terms majorizable by terms of the form $2^{|x|^k}$ for some k. Theories with different dynamic ordinals can be shown to be distinct theories by the order induction principle for some Π^b_1-formula. Computing the dynamic ordinal of a theory is done in two steps: First, a lower bound on the ordinal is obtained by showing, as necessary, order induction for iterated jump formulas of prenex Π^b_i formulas are provable in the theory. This amounts to doing a repeated speed-up of induction argument where one trades-off less induction for formulas with greater quantifier complexity with more induction for formulas with less quantifier complexity. Then an upper bound is obtained by showing an embedding from bounded arithmetic proofs into proofs defined in a semi-formal system introduced in the paper. A lower bound on lengths of proof of order induction in the semi-formal system is shown for proofs where cuts have been eliminated. Using this bound and applying cut-elimination to proofs of order induction that arise from the embedding of bounded arithmetic proofs one gets a bound on the terms the bounded arithmetic can prove order induction to. This argument has as its virtue that its method are "pure"— it does not need to resort to computational complexity results or messy diagonalization arguments. Thus, there is hope that studying variants of this argument can yield insight on nonrelativized separations without necessarily implying hard complexity results.

References

[1] J. Krajíček. Bounded Arithmetic, Propositional Logic, and Complexity Theory. Cambridge. 1995.

[2] J. Krajíček. Fragments of bounded arithmetic and bounded query classes. Transactions of the American Mathematical Society. Vol. 338. pp.587–598. 1993.

[3] J. Krajíček, P. Pudlák, and G.Takeuti. Bounded arithmetic and the polynomial hierarchy. Annals of Pure and Applied Logic. Vol. 52. pp. 143–153. 1991.

[4] C. Pollett Structure and Definability in General Bounded Arithmetic Theories. Annals of Pure and Applied Logic. Vol 100. October 1999. pp.189–245.