For a theory T, the finitary consistency statement $Con_T(n)$ states that there is no proof of $0 = 1$ in T of size at most n. A fast consistency prover is a theory T - having a polynomial time decidable axiom system - such that for every consistent polynomial time axiomatized theory S there is a proof of $Con_S(n)$ in T of size at most $p(n)$, for some polynomial $p()$.

Krajíček and Pudlák [1] show that there exists a fast consistency prover if and only if an optimal propositional proof system exists, and thus its existence follows from $NP = co\text{-}NP$. It is an open question whether the converse holds, i.e., whether it is equivalent to $NP = co\text{-}NP$.

The paper under review studies a modified notion of fast consistency prover, where the required bounds on the proof size are uniformly given by a polynomial. It is shown that the existence of fast consistency provers under this modified definition – and of a similarly modified notion of optimal proof system – is indeed equivalent to $NP = co\text{-}NP$.

Moreover it is shown that a related notion of fast consistency prover, where *polynomial time decidable* is replaced by *recursively enumerable*, does not exist.

References

[1] J. Krajíček and P. Pudlák, Propositional proof systems, the consistency of first order theories and the complexity of computations, J. Symbolic Logic **54** (1989), no. 3, 1063–1079. MR1011192 (91e:03053)