

Provably Total Search Problems in Fragments of Bounded Arithmetic Below Polynomial-time

Jean-Jose Razafindrakoto¹ and Arnold Beckmann²

Swansea University {466199, a.beckmann@swansea.ac.uk}

Abstract. In bounded arithmetic, a host of theories have been developed and which correspond to complexity classes within the polynomial hierarchy and below polynomial-time (see [1] for an overview). Recent research has tried to characterize the provably total NP search problems in such theories, where a total NP search problem is provably total in a theory T if it can be formalized in the language of T and T can prove that, for each instance, there exists a solution to the search problem. For example, Buss and Krajíček [2] showed that the class of provably total NP search problems in a certain bounded arithmetic theory (denoted T_2^1 in [3] and TV^1 in [1]) is characterized by PLS [4]. Further characterizations for theories above T_2^1 were later discovered. To the best of our knowledge, no such characterizations are known for the theories below T_2^1 until this work.

Given a class S of provably total NP search problems for some theory, the general aim of our research project is to identify some specific provably total NP search problem class (usually defined via some specific combinatorial principle) which is complete within S under AC^0 -many-one reduction; completeness should be proven using AC^0 -reasoning only, i.e. formalizable in V^0 (see [1]). For example, it was shown by Cook and Nguyen [1] that PLS, where the neighborhood function and the initial point are given by AC^0 -functions, is complete in the above sense for the class of provably total NP search problems in T_2^1 .

For the theory related to polynomial-time, we identify the search problem class Inflationary Iteration (IITER) which serves our above described aim. A function F (defined on finite strings) is inflationary if X is a subset of $F(X)$ (under the natural identification of strings with finite sets). An IITER principle is defined as a special case of the iteration principle [5], in which the iterated function has to be AC^0 -computable and inflationary.

Cook and Nguyen [1] have a generic way of defining a bounded arithmetic theory VC for complexity classes C below polynomial-time. For such theory VC , we define a search problem class $KPT[C]$ which serves our above described aim. These problems are based on a version of Herbrand's theorem proven by Krajíček, Pudlák and Takeuti [6].

References

1. Cook, S., Nguyen, P.: Logical Foundations of Proof Complexity. 1st edn. Cambridge University Press, New York, NY, USA (2010)

2. Buss, S.R., Krajíček, J.: An application of boolean complexity to separation problems in bounded arithmetic. In: Proc. London Math. Society. (1994) 1–21
3. Buss, S.R.: Bounded Arithmetic. ProQuest LLC, Ann Arbor, MI (1985) Thesis (Ph.D.)–Princeton University.
4. Johnson, D.S., Papadimitriou, C.H., Yannakakis, M.: How easy is local search? J. Comput. System Sci. **37**(1) (1988) 79–100 26th IEEE Conference on Foundations of Computer Science (Portland, OR, 1985).
5. Chiari, M., Krajíček, J.: Witnessing functions in bounded arithmetic and search problems. J. Symbolic Logic **63**(3) (1998) 1095–1115
6. Krajíček, J., Pudlák, P., Takeuti, G.: Bounded arithmetic and the polynomial hierarchy. Ann. Pure Appl. Logic **52**(1-2) (1991) 143–153 International Symposium on Mathematical Logic and its Applications (Nagoya, 1988).