Abstract

In recent years, we have seen several approaches to the graph isomorphism problem based on "generic" mathematical programming or algebraic (Gröbner basis) techniques. For most of these, lower bounds have been established. In fact, it has been shown that the pairs of non-isomorphic CFI-graphs (introduced by Cai, Fürer, and Immerman in 1992 as hard examples for the combinatorial Weisfeiler-Leman algorithm) cannot be distinguished by these mathematical algorithms. A notable exception were the algebraic algorithms over the field $\mathbb{F}_2$, for which no lower bound was known. Another, in some way even stronger, approach to graph isomorphism testing is based on solving systems of linear Diophantine equations (that is, linear equations over the integers), which is known to be possible in polynomial time. So far, no lower bounds for this approach were known. Lower bounds for the algebraic algorithms can best be proved in the framework of proof complexity, where they can be phrased as lower bounds for algebraic proof systems such as Nullstellensatz or the (more powerful) polynomial calculus. We give new hard examples for these systems: families of pairs of non-isomorphic graphs that are hard to distinguish by polynomial calculus proofs simultaneously over all prime fields, including $\mathbb{F}_2$, as well as examples that are hard to distinguish by the systems-of-linear-Diophantine-equations approach. In a previous paper, we observed that the CFI-graphs are closely related to what we call "group CSPs": constraint satisfaction problems where the constraints are membership tests in some coset of a subgroup of a cartesian power of a base group ($\mathbb{Z}_2$ in the case of the classical CFI-graphs). Our new examples are also based on group CSPs (for Abelian groups), but here we extend the CSPs by a few non-group constraints to obtain even harder instances for graph isomorphism.