Lower Bounds Related to Polynomial Identity Testing, Circuit Minimization, and Inversion Minimization

By

Andrew Morgan

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
(Computer Sciences)

at the
UNIVERSITY OF WISCONSIN–MADISON

2022

Date of final oral examination: 01/21/2022

The dissertation is approved by the following members of the Final Oral Committee:
   Dieter van Melkebeek, Professor, Computer Sciences
   Eric Allender, Professor, Computer Science at Rutgers University
   Jin-Yi Cai, Professor, Computer Sciences
   Daniel Erman, Associate Professor, Mathematics
Abstract

Computational complexity theory aims to provide a mathematically rigorous understanding of the resources necessary to solve computational problems. This dissertation develops complexity lower bounds in three settings.

*Polynomial Identity Testing.* Given two arithmetic formulas, do they compute the same multivariate polynomial? This basic problem has an efficient randomized algorithm and plays a central role in the area of derandomization. We propose a pseudorandom generator based on evaluations of univariate rational functions and characterize its power through its vanishing ideal. We construct an explicit Groebner basis, yielding tight bounds on the minimum sparsity, degree, and partition class size of set multilinearity in the vanishing ideal. We develop a membership test inspired by the theory of alternating algebras and give a proof of concept of its usefulness in the model of read-once oblivious algebraic branching programs. Via an equivalence with the Shpilka–Volkovich generator, computational lower bounds for polynomials in the vanishing ideal follow from existing derandomization results.

*Circuit Minimization.* Given a truth table, what is the minimum size of a Boolean circuit computing it? This fundamental problem and a descriptive Kolmogorov variant known as MKTP have thus far resisted classification as solvable in polynomial time or NP-complete. We show that the complexity of MKTP is no less than that of isomorphism problems with respect to zero-error randomized reductions. Our reduction is related to
the known interactive proofs of nonisomorphism and hinges on a near-optimal encoding for samples of flat, samplable distributions.

**Inversion Minimization.** Given a rooted tree and a ranking of its leaves, what is the minimum number of inversions of the leaves that can be attained by ordering the tree? We study the number of comparisons necessary to solve this problem by considering notions of connectivity and sensitivity with respect to adjacent-rank transpositions. We show that for many tree shapes the problem is essentially as hard as sorting.