Research Overview

Ilya Volkovich

Department of EECS, CSE Division
University of Michigan
ilyavol@umich.edu

Research Interests

Computational Complexity:

- Algebraic complexity and algebraic problems in computer science
- Derandomization and the role of randomness in computation
- Hardness results for learning algorithms

"The Algebraic World is very structured. Randomness defies structure."

Examples:

- A random set of vectors is independent.
- A random assignment to a polynomial is a non-zero.

Conclusion: algebraic problems are amenable to randomized algorithms.

Polynomial Identity Testing (PIT)

Given an arithmetic circuit C in n variables over some field $\mathbb{F}$, determine whether C computes the (identically) zero polynomial.

- A fundamental problem in algebraic complexity, central to both algorithm design and complexity theory
- One of a handful of problems that have efficient *randomized* algorithms [Zip79, Sch80] but lack *deterministic* ones.
- [KI04, Agr05]: $\mathrm{PIT} \in P \implies$ circuit lowers bounds.
- Our results: deterministic PIT algorithms for several restricted classes of circuits [SV11, KMSV13, SV14, AvMV15]
- Our results: relation between PIT and other algebraic problems: polynomial factorization [SV10], polynomial reconstruction [SV15].

Learning

Revealing a hidden function from a set of examples:
$f(\bar{a}) = 1, f(\bar{b}) = 0, \ldots \; \boxed{f = ?}$
Hardness of learning:

- [FK09]: learning algorithms $\implies$ circuit lower bounds.
- Open problems: randomized learning algorithms and learning algorithms for algebraic concepts?
- Our results: matching lower bounds from randomized learning algorithms [Vol14] and for algebraic concepts [Vol15].
- Open question of [GKL12]: certain learning algorithms for algebraic concepts have a polynomial dependence on $|\mathbb{F}|$. Is it necessary?
- Our results: these algorithms must compute square roots [Vol15].
- Fact: there is no known efficient deterministic root extraction alg.
- Conclusion: certain learning algorithms must be either randomized or have a polynomial dependence on $|\mathbb{F}|$.