UNIVERSITY OF TORONTO
FACULTY OF ARTS & SCIENCE | Department of Mathematics

# Departmental PhD Thesis Exam

Wednesday, June 12th, 2024 at 11:00 a.m. (sharp)
via Zoom / BA6183

PhD Candidate : Adrian She

Supervisor : Toniann Pitassi, Henry Yuen

Thesis title : Algebraic Methods in Query and Proof Complexity


## Abstract

Algebraic methods have become a powerful tool for analyzing the complexity of various computational models, including low-depth circuits, algebraic proofs, and quantum query algorithms. In particular, the complexity of computing a function in these models is related to whether or not the function admits a low-degree polynomial approximation. In this thesis, we present two novel applications of algebraic methods in computational complexity theory.

In the first part of the thesis, we study unitary property testing, where a quantum algorithm is given query access to a black-box unitary and has to decide whether or not it satisfies some property. In addition to containing the classical query complexity model as a special case, this model also contains "inherently quantum" problems that have no classical analogue. Our main contribution is a generalized polynomial method for analyzing the complexity of unitary property testing problems. By leveraging connections with invariant theory, we apply this method to obtain lower bounds on problems such as determining recurrence times of unitaries, approximating the dimension of a subspace, and approximating the entanglement entropy of a state. We also present a candidate problem towards an oracle separation of $\mathsf{QMA}$ and $\mathsf{QMA}(2)$, a long standing open question in quantum complexity theory.

In the second part of the thesis, we study the tensor isomorphism problem (TI), which has recently emerged as having connections to multiple areas of research, including quantum information theory, post-quantum cryptography, and computational algebra. However, the current best upper bound is essentially the brute force algorithm. Being an algebraic problem, the study of tensor isomorphism naturally lends itself to algebraic and semi-algebraic proof systems such as the polynomial calculus (PC) and sum-of-squares (SoS). We show a $\Omega(n)$ lower bound on PC degree or SoS degree for tensor isomorphism and a non-trivial upper bound for testing isomorphism of tensors of bounded rank. Along the way, we also show that PC cannot perform basic linear algebra in sublinear degree, such as comparing the rank of two matrices. We introduce a strictly stronger proof system, called PC + Inv, which enables linear algebra to be done in low degree. We conjecture that even PC + Inv cannot solve TI in polynomial time either, and highlight many other open questions about proof complexity approaches to TI.