COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Alexandra Veliche

Codes & Lattices: Computational Complexity and Constructions

Tuesday, May 27, 2025
9:30am – 11:30am
3725 Beyster / Hybrid – Zoom

ABSTRACT: Linear codes and point lattices are two mathematical objects that play a fundamental role in many areas of computer science. Perhaps most notably, in cryptography the computational hardness of problems for codes and lattices is used as a security assumption for most cryptographic schemes proposed to be post-quantum. Understanding the complexity of these problems, and how techniques for codes and lattices are related, is crucial for understanding the security of the corresponding cryptosystems. With this motivation, we explore both the computational complexity and algorithmic sides of coding problems and lattice problems.

We study the computational complexity of two key problems relevant to cryptography: Learning With Errors (LWE) and Code Equivalence (CE).

For problems like LWE, we introduce an alternative measure of computational hardness: the maximum success probability achievable by any probabilistic polynomial-time algorithm. This measure more accurately models the security goals of cryptosystems based on these problems. Under this new perspective, we study the worst-case to average-case hardness of LWE and prove a tight Turing reduction from the Bounded Distance Decoding (BDD) problem to both search and decision variants of LWE. Our reduction improves well-known previous reductions by using only a few oracle calls and explicitly quantifying the loss in success probability.

The CE problem has several variants, including Permutation Code Equivalence (PCE), Signed Permutation Code Equivalence (SPCE), and Linear Code Equivalence (LCE). We prove polynomial-time Karp reductions from PCE to both LCE and SPCE. Along with a known Karp reduction from SPCE to the Lattice Isomorphism Problem (LIP), our second result implies a reduction from PCE to LIP.

On the algorithmic side, we use lattices and Fourier analytic techniques to construct an algorithm that list-decodes Generalized Reed-Solomon (GRS) codes from worst-case or average-case errors over any -(quasi)norm where . This is based on the Guruswami-Sudan soft-decision decoding algorithm. Our algorithm applies to a broader family of codes and (quasi)norms than was previously known and outperforms previous algorithms for the - and -norms for most rate-distance regimes.

CHAIR: Prof. Mahdi Cheraghachi