COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

SHANG-EN HUANG

Dynamic Connectivity, Hopsets, and Byzantine Agreement

Friday, April 29, 2022
9:30 – 11:30am
4941 BBB

ABSTRACT: We study three fun algorithmic challenges and apply graph algorithms and data structures to improve them.

The first challenge is to design a data structure that solves the fully dynamic graph connectivity problem. For any sequence of edge insertions and deletions to a graph, our data structure performs updates in amortized randomized $O(\log n(\log \log n)^2)$ time, improving Thorup's result by a $O(\log \log n)$ factor since 2000. Our result leaves a small $O((\log \log n)^2)$ gap to the $\Omega(\log n)$ lower bound given by Pătraşcu and Demaine in 2006.

The second topic we study includes various structures on graphs concerning distances and reachability, such as spanners, emulators, hopsets and shortcutting sets. A (β, ε)-hopset is a set of weighted edges added to an undirected weighted graph such that distances between any pair of vertices can then be $(1+\varepsilon)$-approximated using a path with at most β edges (hops). We applied Thorup and Zwick's sublinear additive emulator construction to build an optimal hopset, where optimal tradeoff is established by the work of Abboud, Bodwin, and Pettie. A shortcutting set is a reachability-preserving set of directed edges whose addition to a directed unweighted graph reduces the diameter. We give a $\Omega(n^{1/6})$ diameter lower bound on any $O(n)$-size shortcutting set. The techniques can also be applied to undirected weighted graphs such as $O(n)$-size spanners and emulators.

The third problem we solve is the asynchronous Byzantine agreement (ABA) problem. In distributed computing, reaching consensus among all n processes is a challenging task, especially when a subset of processes are secretly corrupted and malicious behavior may occur. We propose a protocol that solves ABA in an asynchronous distributed network with a fully-connected authenticated p2p channels. The protocol works against a full-information (no crypto for hiding information) and adaptive (corrupting processes over time) adversary, and allows up to (n-1)/4 faulty processes, improving King and Saia's 2013 result from $(1.14 \times 10^{-9})n$ faulty processes. Unlike the first two topics in this thesis, ABA is not obviously related to graphs. But interestingly, one building block in our protocol is a fractional matching algorithm with a continuous Lipschitz guarantee.

CHAIR: Prof. Seth Pettie