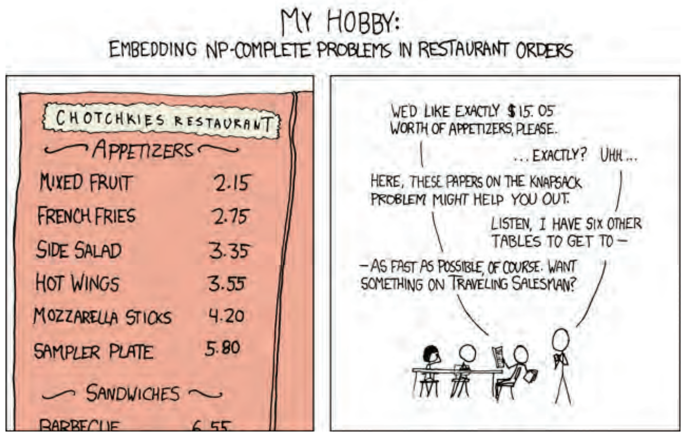
Research@CSE Theory of Computation



Source: xkcd.com

The Theory Group at the University of Michigan conducts research across many areas of theoretical computer science, such as combinatorial optimization, data structures, cryptography, quantum information and computation, parallel and distributed computation, algorithmic game theory, graph theory, geometry, and combinatorics. Listed here is a representative sample of our research projects.

DESIGN AND ANALYSIS OF ALGORITHMS

Faculty: Seth Pettie, Martin Strauss, Quentin Stout, Grant Schoenebeck, Kevin Compton, Yaoyun Shi

Modern applications of computer science ultimately depend on having highly efficient algorithms for solving basic computational tasks; some examples are searching and summarizing a large corpus of textual data, finding optimal routes in networks, or finding an optimal solution to a set of linear inequalities. Efficiency is a fine goal, but what is it exactly? We try to characterize, in a mathematically rigorous way, the computational resources (running time, storage space, communication, energy, etc.) required to solve various combinatorial and optimization problems. We also investigate how changing the model of computation affects the complexity of solving specific problems. For example, we now know that quantum computers could solve some problems exponentially faster than a classical computer and that many other, but not all, problems can be solved significantly faster on a parallel computer.

Algorithms research at Michigan spans across many areas, including network optimization, approximation algorithms, the design and analysis of data structures, combinatorial problems in geometry, analysis of social networks, and algorithms for various parallel, distributed, and streaming models of computation.

QUANTUM INFORMATION PROCESSING

Faculty: Yaoyun Shi, Igor Markov

Our goal is to sharpen the boundaries between the classical and the quantum worlds with respect to information processing. We investigate the following questions within the mathematical framework of quantum information science:

- For which kind of computational tasks can quantum computers dramatically outperform classical computers?
- To what degree can classical physics simulate and approximate quantum physics?
- How can one leverage quantum information to achieve higher efficiency and better security in communication?

COMPUTER SCIENCE
AND ENGINEERING
UNIVERSITY OF MICHIGAN

Bob and Betty Beyster Building
2260 Hayward Street, Ann Arbor, MI 48109-2121
cse.umich.edu

Research@CSE Theory of Computation

MASSIVE DATASETS

Faculty: Martin Strauss, Quentin Stout

Massive datasets abound in a wide variety of application such as observations of the heavens and earth, genomic analyses, voice and data networks, and transactional data arising from commerce and medical care.

In many applications, the size of the dataset is much larger than the size of the useful information in the dataset. A typical class of problem is called "heavy hitters," in which we must track the most significant k items out of n >> k. We will want to use resources (time, space, communication) polynomial in k but much less than n. Typically, we present randomized approximation algorithms that, with high probability, give a solution that may be less than optimal but is provably close to optimal. We may also need to satisfy additional constraints, such as privacy constraints in cryptographic contexts.

Another research direction is developing algorithms to analyze large data collections using map-reduce operations, such as in Hadoop, and other scalable operations for distributed memory systems.

In some cases we are looking for specific structures, such as cliques in cellphone calling records, and in other cases are applying learning algorithms in parallel to more rapidly look for unknown structure.

SECURE CRYPTOGRAPHIC PROTOCOLS

Faculty: Kevin Compton, Yaoyun Shi, Martin Strauss

Cryptography is essential to electronic financial transactions and private communication so it is imperative that our cryptographic systems be truly secure against a variety of attacks. Below are two ongoing projects to (dis)prove the security cryptographic systems.

The first project deals with side channel attacks on cryptosystems. Small computing devices, such as smart cards, leak information through voltage fluctuations, radiation and other channels other than the standard input and output channels. It turns out that in some cases this side channel information reveals keys and other types of information stored on the smart card. The group is currently looking at different attacks and measures to protect against them.

The second project deals with cryptographic protocol security. When you buy something over the internet or log onto a remote site, you use various protocols where encrypted and secured information is sent over an open channel. Are these protocols secure? We are looking at different models of security and investigating new ways to automate the process of proving a protocol secure.

Yet another set of challenges are posed by quantum information technologies: how can we ensure that classical cryptographic protocols are secure against quantum adversaries, and how can we make use of quantum information to achieve unconditional security? We have developed methods for generating and distributing random numbers securely against all-powerful quantum adversaries, and are exploring many frontiers in quantum cryptography and post-quantum classical cryptography.

PARALLEL AND DISTRIBUTED COMPUTATION

Faculty: Quentin Stout, Seth Pettie

For decades, the speed of processors was growing exponentially, but this has abruptly stopped. Instead, now the number of processor cores on a chip is growing exponentially. A graphics processing unit (GPU) in a laptop may have 100 cores, and supercomputers may have 1,000,000. At Michigan, we are developing algorithms and data structures that use parallelism to help solve large problems such as climate modeling and the design of ethical clinical trials.

Abstract models of parallelism are also investigated, such as having a large number of small entities (cores on a chip, smart dust, ants, robots) working together on the same problem. Algorithms may need to take physical location into account, where communicating with entities far away takes more time and energy. We also study abstract models of distributed computation, where a large number of independent, unsynchronized computers are arranged in a (possibly unknown) network and must solve a problem only through local communication.

COMPLEXITY THEORY

Faculty: Grant Schoenebeck, Yaoyun Shi

Some computational tasks seem resilient to efficient solutions or even efficient approximation. When can we show that no efficient algorithm exists? What types of inputs are particularly difficult and why? What are the limits of quantum computing and parallelism? Besides the mathematical beauty of these questions, they have important applications to cryptography.

Research@CSE Theory of Computation

THE INTERSECTION OF COMPUTER SCIENCE AND ECONOMICS

Faculty: Jacob Abernethy, Grant Schoenebeck, Satinder Singh Baveja, Michael Wellman

In today's online environments, computational agents engage with each other in commerce and other economically important activities. In such environments, agents must not reason only about their own actions, but also the actions of other agents. How can we design strategic agents that perform in dynamic and uncertain environments? Additionally markets are being designed to allocate goods such as CPU time or advertising slots. How can we design new markets with desirable properties such as allocating goods to agents that most desire them? Market design can be thought of as an optimization problem where the inputs need to be elicited.

There are deep applications to social networks which can be viewed as a distributed system where each node operates in a local, autonomous, and, possibly, self-interested way. How can we reason about processes over such networks and what goals can be accomplished by such a network?

OPTIMIZING ENERGY CONSUMPTION

Faculty: Quentin Stout, Martin Strauss

We look at parallel algorithms that adapt as power reductions constrain the speed or number of cores that can be turned on, or as the number of entities available to work together changes. How can they be made to use less energy for computation and for heat removal?

In a smart grid, the grid operator can sense what appliances are in use and possibly turn them off. How can we ensure privacy and security of customer interest? How can we ensure stability of this large dynamical system, while accommodating variable green energy sources like solar and wind? Can we design auctions to encourage off-peak use and guarantee stability?

Another aspect is making algorithms themselves more energy efficient. For example, we have developed power-aware parallel algorithms that change their behavior as the available power changes. In supercomputers there may be hotspots, forcing some regions of the system to slow down relative to the other regions even though they are all working together. How can our algorithms dynamically adjust to this?

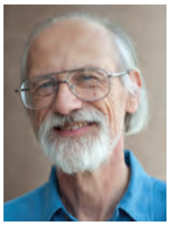
FACULTY IN THEORY OF COMPUTATION

Kevin Compton
Associate Professor
kjc
3603 Beyster Bldg

Seth Pettie
Associate Professor
pettie
3628 Beyster Bldg

Grant Schoenebeck
Assistant Professor
schoeneb
3640 Beyster Bldg

Yaoyun Shi
Associate Professor
shiyy
3632 Beyster Bldg



Quentin Stout
Professor
qstout
3605 Beyster Bldg

Martin Strauss
Professor
martinjs
3633 Beyster Bldg

AFFILIATED FACULTY

Jacob Abernethy - Computer Science and Engineering, Artificial Intelligence

Satinder Singh Baveja - Computer Science and Engineering, Artificial Intelligence

Andreas Blass - Mathematics

Anna Gilbert - Mathematics

Jeffrey Lagarias - Mathematics

Igor Markov - Computer Science and Engineering, Computer Architecture

Carl Miller - Computer Science and Engineering

Michael Wellman - Computer Science and Engineering, Artificial Intelligence