

# 2016 Theory Day in Taiwan

<http://theoryday.github.io>

Date: Saturday, 26 March, 2016

Location: Auditorium 105 at EE Building 2,  
National Taiwan University, Taipei



The Theory Day in Taiwan is an experimental one-day event that aims to stimulate interaction and discussion for TCS researchers in Taiwan and nearby countries. We invited 4 hour-long talks in general TCS area with long breaks for interaction and discussion. The meeting is free and open to everyone; in particular, students are encouraged to attend.

## Program

9.20 – 9.30	Registration
9.30 - 10.30	Anthony Man-Cho So (The Chinese University of Hong Kong) <b>A Unified Framework for Establishing Error Bounds for Structured Convex Optimization Problems</b>
10.30 - 11.00	Break and Discussion
11.00 - 12.00	Po-An Chen (National Chiao Tung University) <b>How Much of a Person Influencing the Others and Being Influenced Matters in Opinion Formation Games</b>
12.00 - 2.00	Lunch (on your own)
2.00 - 3.00	Shengyu Zhang (The Chinese University of Hong Kong) <b>Sensitivity Conjecture and Log-rank Conjecture for Functions with Small Alternating Numbers</b>
3.00 - 3.30	Break and Discussion
3.30 - 4.30	Yunghsiang S. Han (National Taiwan University of Science and Technology) <b>Novel FFT over Binary Finite Fields and Its Application to Reed-Solomon Erasure Codes</b>

## Abstracts

### **A Unified Framework for Establishing Error Bounds for Structured Convex Optimization Problems**

Anthony Man-Cho So (The Chinese University of Hong Kong)

In recent years, we have witnessed a widespread use of first-order methods (FOMs) to solve large-scale structured convex optimization problems. It is well known that many FOMs will converge linearly if the problem at hand possesses a certain Lipschitzian error bound. In this talk, we shall present a new framework for establishing such error bounds for a host of structured convex optimization problems. Our framework makes essential use of the notions of calmness and metric subregularity from variational analysis. It not only unifies and simplifies the proofs of several existing error bounds but also leads to a new error bound for structured convex optimization with nuclear norm regularization. We believe that our techniques will have further applications in the development of error bounds and convergence rate analysis of first-order methods.

### **How Much of a Person Influencing the Others and Being Influenced Matters in Opinion Formation Games**

Po-An Chen (National Chiao Tung University)

The opinion forming process in a social network could be naturally modeled as opinion influencing and updating dynamics. This already attracted researchers' interest a while ago in mathematical sociology, and recently in theoretical computer science. In so-called "opinion formation games", when underlying networks are directed, a bounded price of anarchy is only known for weighted Eulerian graphs, which may not be the most general class of directed graphs that give a bounded price of anarchy. Thus, we aim to bound the price of anarchy for games with directed graphs more general than weighted Eulerian graphs in this work.

We first bound the price of anarchy for a more general class of directed graphs with conditions intuitively meaning that each node does not influence the others more than she is influenced by herself and the others, where the bounds depend on such influence difference (in a ratio). This generalizes the previous results on directed graphs, and recovers and matches the previous bounds in some specific classes of (directed) Eulerian graphs. We then show that there exists an example that just slightly violates the conditions with an unbounded price of anarchy. We further propose more directions along this line of research.

## **Sensitivity Conjecture and Log-rank Conjecture for Functions with Small Alternating Numbers**

Shengyu Zhang (The Chinese University of Hong Kong)

The Sensitivity Conjecture and the Log-rank Conjecture are among the most important and challenging problems in concrete complexity. Incidentally, the Sensitivity Conjecture is known to hold for monotone functions, and so is the Log-rank Conjecture for  $f(x \wedge y)$  and  $f(x \oplus y)$  with monotone functions  $f$ , where  $\wedge$  and  $\oplus$  are bit-wise AND and XOR, respectively. In this paper, we extend these results to functions  $f$  which alternate values for a relatively small number of times on any monotone path from all-0 input to all-1 input. These deepen our understandings of the two conjectures, and contribute to the recent line of research on functions with small alternating numbers.

## **Novel FFT over Binary Finite Fields and Its Application to Reed-Solomon Erasure Codes**

Yunghsiang S. Han (National Taiwan University of Science and Technology)

A fundamental issue in algebra is to reduce the computational complexities of arithmetic operations over polynomials. Many fast polynomial-related algorithms, such as encoding/decoding of Reed-Solomon codes, are based on fast Fourier transforms (FFT). However, it is algorithmically harder as the traditional fast Fourier transform (FFT) cannot be applied directly over characteristic-2 finite fields. To the best of our knowledge, no existing algorithm for characteristic-2 finite field FFT/polynomial multiplication has provably achieved  $O(h \log_2(h))$  operations. In this talk, we present a new basis of polynomial over finite fields of characteristic-2 and then apply it to the encoding/decoding of Reed-Solomon erasure codes. The proposed polynomial basis allows that  $h$ -point polynomial evaluation can be computed in  $O(h \log_2(h))$  finite field operations with small leading constant. As compared with the canonical polynomial basis, the proposed basis improves the arithmetic complexity of addition, multiplication, and the determination of polynomial degree from  $O(h \log_2(h) \log_2 \log_2(h))$  to  $O(h \log_2(h))$ . Based on this basis, we then develop the encoding and erasure decoding algorithms for the  $(n = 2^r, k)$  Reed-Solomon codes. Thanks to the efficiency of transform based on the polynomial basis, the encoding can be completed in  $O(n \log_2(k))$  finite field operations, and the erasure decoding in  $O(n \log_2(n))$  finite field operations. To the best of our knowledge, this is the first approach supporting Reed-Solomon erasure codes over characteristic-2 finite fields while achieving a complexity of  $O(n \log_2(n))$ , in both additive and multiplicative complexities. As the complexity of leading factor is small, the algorithms are advantageous in practical applications. This work was presented at the 55th Annual Symposium on Foundations of Computer Science (FOCS 2014).