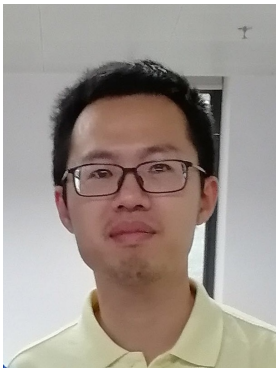
Guangzhou Discrete Mathematics Seminar

(Discrete) mathematics behind interactive proof



Jun Yan

Jinan University, Guangzhou, China

1 June 2018 (Friday), 3pm to 4pm
Room 416, School of Mathematics, Sun Yat-sen University

Interactive proof is an important notion in both complexity theory and cryptography. It incorporates interactiveness and randomness into the canonical mathematical proof, which not only greatly enlarges the scope of what can be proved, but also can achieve a variety of securities. Two inventors of interactive proof (Goldwasser and Micali) were awarded Turing award in 2012 for this great contribution.

In this talk, I will survey interesting (discrete) mathematics behind interactive proof, which includes concepts and techniques from many fields such as number theory, linear/abstract algebra, graph theory, probability theory, mathematical logic, coding theory, and so on. I will also briefly talk about new questions towards interactive proof raised by quantum computation and communication that I have been working on in the past few years.

I will try to avoid going deep into technical details in this talk, while focusing on stating basic results and explaining basic ideas. Nothing is assumed for audiences. All are welcome.

Guangzhou Discrete Mathematics Seminar
Website `http://www.gzdmseminar.cn`
Mirror site `http://www.cantab.net/users/henry.liu/gzdmseminar.htm`

QR code of the seminar series