北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
青 年 讲 座

Efficiently Batching Unambiguous Interactive Proofs

Matthew Man-Hou Hong

MIT

Host：刘天任 助理教授
2026年1月15日 星期四 3:00pm
静园五院204室

Abstract

We show that if a language $\mathcal{L}$ admits a public-coin unambiguous interactive proof (UIP) with round complexity ℓ where a bits are communicated per round, then the *batch language* $\mathcal{L}^{\otimes\kappa}$, i.e. the set of k-tuples of statements all belonging to $\mathcal{L}$, has an unambiguous interactive proof with round complexity $\ell\cdot$ polylog (k) , per-round communication of $a\cdot\ell\cdot$polylog(k) +poly(ℓ) bits, assuming the verifier in the UIP has depth bounded by polylog(k). Prior to this work, the best known batch UIP for $\mathcal{L}^{\otimes\kappa}$ required communication complexity at least (poly$(a)\cdot k^{\epsilon}+k)\cdot\ \ell^{1/\epsilon}$ for any arbitrarily small constant $\epsilon>0$ (Reingold-Rothblum-Rothblum, STOC 2016).

As a corollary of our result, we obtain a *doubly efficient proof system*, that is, a proof system whose proving overhead is polynomial in the time of the underlying computation, for any language computable in polynomial space and in time at most $n^{O\left(\sqrt{\frac{\log n}{\log\log n}}\right)}$. This expands the state of the art of doubly efficient proof systems: prior to our work, such systems were known for languages computable in polynomial space and in time $n^{(logn)^{\delta}}$ for a small $\delta>0$ significantly smaller than $1/2$ (Reingold-Rothblum-Rothblum, STOC 2016).

Based on joint work with Bonnie Berger, Rohan Goyal, and Yael Tauman Kalai.

Biography

Matthew Man-Hou Hong is a fifth-year Ph.D. candidate at MIT advised by Bonnie Berger and Yael Tauman Kalai. He is interested in applied and theoretical cryptography, and theoretical computer science (TCS). He received his B.Eng. from the Institute for Interdisciplinary Sciences at Tsinghua University, China.

http: //cfcs.pku.edu.cn/