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

Coherence in Property Testing: Quantum-Classical Separations

Dr. Pei Wu

Weizmann Institute of Science

Host：姜少峰 助理教授
2024年7月17日 星期三 14:00
静园五院204室

Abstract

Property testing is a fundamental task both classically and quantumly. There is a wealth of results investigating property testing of classical probability distributions, where a tester is given samples of a distribution typically over a large domain, say $\{0,1\}^n$ for large n. A central classical result is that to verify the support size of an unknown distribution requires $O(2^n/n)$ (Valiant&Valiant, STOC11) . In fact, to distinguish vastly different support sizes of flat distributions is hard: even given $2^{n/16}$ samples, no tester can distinguish between flat distributions of support size $2^{n/8}$ from $2^{n/4}$ with probability better than $2^{-\theta(n)}$.

In the quantum setting, quantum states can be in a coherent superposition of many states of $\{0,1\}^n$, in particular, allowing a more global description of probability distributions. One can then ask how much coherence helps property testing. A natural way to encode a flat distribution is via subset states, $|\phi_S\rangle = 1/\sqrt{|S|} \sum_{i \in S}|i\rangle$. We show that coherence alone is not enough to improve the testability of support size, (1) Even given $2^{n/16}$ copies, no tester can distinguish between subset states of size $2^{n/8}$ from $2^{n/4}$ with probability better than $2^{-\theta(n)}$. In fact, we obtain a more general result showing that subset states are indistinguishable from Haar random states provided the support size is not too small nor too large. This also provides new constructions of pseudorandom (PRS) and pseudoentangled states.

Given that standard property testing fails badly here, we enhance these models by allowing multiple provers. In particular, we show that even interacting with multiple AM provers, classical property testing still fails, (2) Even given $2^{\Omega(n)}$ samples from a classical distributions and interacting with $2^{\Omega(n)}$ AM provers in $2^{\Omega(n)}$ rounds, no classical tester can estimate the support size up to factors $2^{\Omega(n)}$ with probability better than $2^{-\theta(n)}$. We obtain this classical lower bound via a curious reduction to fast mixing of high-dimensional expanders.

In contrast, we show that coherent subset state proofs suffice to improve testability exponentially, (3) With just polynomially many copies and subset state proofs, a tester can, with high probability, approximate the support size of a subset state of arbitrary size, or detect that the certificates are malicious. Our results show some of the power and limitations of coherence in property testing for a natural property and establish quantum-classical separations that are exponential in various parameters.

Biography

Pei Wu obtained his PhD from UCLA. He is currently is a postdoc research fellow at the Weizmann Institute of Science. His research interest lies in theoretical computer science. He will start as an assistant professor at Pennsylvania State University, Fall 2024.