Drexel Analysis Seminar

May 12, 2017

12-12:50 PM, Korman 245

Speaker: Jianxin Chen (University of Maryland)

Title: Quantum algorithm for multivariate polynomial interpolation

Abstract: How many quantum queries are required to determine the coefficients of a degree-d polynomial in n variables? We present and analyze quantum algorithms for this multivariate polynomial interpolation problem over the fields $\mathbb{F}_q$, $\mathbb{R}$, and $\mathbb{C}$. We show that $k_{\mathbb{C}}$ and $2k_{\mathbb{C}}$ queries suffice to achieve probability 1 for $\mathbb{C}$ and $\mathbb{R}$, respectively, where $k_{\mathbb{C}} = \lceil \frac{1}{n+1}\binom{n+d}{d} \rceil$ except for $d = 2$ and four other special cases. For $\mathbb{F}_q$, we show that $\lceil \frac{d}{n+d}\binom{n+d}{d} \rceil$ queries suffice to achieve probability approaching 1 for large field order q. The classical query complexity of this problem is $\binom{n+d}{d}$, so our result provides a speedup by a factor of $n+1$, $\frac{n+1}{2}$, and $\frac{n+d}{d}$ for $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{F}_q$, respectively. Thus we find a much larger gap between classical and quantum algorithms than the univariate case, for which the speedup is by a factor of 2. For the case of $\mathbb{F}_q$, we conjecture that $2k_{\mathbb{C}}$ queries also suffice to achieve probability approaching 1 for large field order q, although we leave this as an open problem.