Rahul B S
Roll No - 160540
CSE, IIT Kanpur

Quantum Proofs for Classical Theorems

13th March 2019

MOTIVATION

Theoretical concepts and techniques used in quantum computation for quantum algorithms, quantum complexity theory has been found useful in obtaining results in diverse classical (non-quantum) areas, such as coding theory, communication complexity, and polynomial approximations. This paper surveys these results and quantum toolbox they use. Finally it concludes by saying “thinking quantumly” can be a source of insight and of charming, surprising proofs, even when a scalable quantum computer is not built.

INTRODUCTION

Many mathematical results can be proved by reasoning from different domain perspective than originally proposed one. For example from high school math, real-valued identities in trigonometry like - $\cos(x + y) = \cos x \cos y - \sin x \sin y$. If we use concepts from complex numbers then : $e^{ix} = \cos x + i \sin x$ we have $e^{i(x+y)} = \cos (x+y) + i \sin (x+y) = e^{ix}e^{iy} = (\cos x + i \sin x)(\cos y + i \sin y) = (\cos x \cos y - \sin x \sin y) + i (\sin x \cos y + \cos x \sin y)$, taking real parts gives the result.

Similarly another example is of *probabilistic method*, associated with Paul Erdos : Idea here is to prove the existence of an object with a specific desirable property P by choosing such an object at random, and showing that it satisfies P with positive probability.

QUANTUM TOOLBOX

Here toolbox used for proving subsequent results are introduced.

- ➔ Basics of quantum computation - qubits, superposition, measurements. Then quantum query model and some quantum query algorithms are discussed
- ➔ Quantum information theory - results like communication lower bound for inner product, Lower bounds on locally decodable codes, rigidity of hadamard matrices are introduced.

PROVING RESULTS IN POLYNOMIALS

The previous quantum toolbox is used in proving results like :

- ➔ ε-approximating polynomials for symmetric boolean functions : upper bound on degree on the error ε is made tighter by using quantum theoretical concepts than previously obtained (due to De Wolf)
- ➔ Robust polynomials and Closure properties of PP are discussed
- ➔ Jackson theorem : this is a result from approximation theory - approximating complex functions can be done by polynomials (due to Weierstrass's Theorem). Bernstein gave a simple construction of such polynomials, which can be described in a probabilistic way. Jackson gave tighter upper bound to the error in approximation. Original proof used trigonometric ideas. New proof (due to Drucker, De Wolf) closely follows Bernstein idea, but replaces his classical estimation procedure with the quantum counting algorithm.

OTHER APPLICATIONS

Here we have examples of classical results that were both inspired by earlier quantum proofs, but do not explicitly use quantum techniques :

- ➔ The relational adversary : result due to Aaronson is given
- ➔ Proof systems for the shortest vector problem : A lattice is an additive subgroup of R^n consisting of all integer combinations of a linearly independent set of n vectors. Here the problem is to find $\lambda(L)>0$ (can be shown to exist) the minimum (Euclidean) distance of the lattice L, such that: (i) any two distinct $x, y \in L$ are at distance at least $\lambda(L)$ from each other, (ii) there exists $x \in L$ such that $||x|| = \lambda(L)$. Results in building proof system are discussed. Applications of this problem include cryptography.

Further many other classical results are listed which can be proved using quantum techniques.

REFERENCES

Andrew Drucker, Ronald de Wolf : Quantum Proofs for Classical Theorems [link]