Quantum query complexity and distributed computing
Röhrig, H.P.

Citation for published version (APA):
Abstract

In complexity theory, the strengths and limitations of computers are investigated on abstract models of computation. The choice of these models is governed by three considerations: (1) how close is the model to existing computers or computers that could be built in principle? (2) how well does it lend itself to proving interesting properties of computers? (3) how elegant is the model mathematically?

Quantum computation appeals to all three criteria. In functional analysis, quantum mechanics has a beautiful mathematical underpinning, which benefits quantum computing through new applications of linear algebra and matrix analysis. Nowadays it is a widely-held belief that the physical theory of “quantum mechanics” describes reality accurately at very small scales of length, time, and energy. Where classical probabilistic Turing machines may be seen as capturing the power of computers operating according to finite-precision classical physics, the computational model of “quantum circuits” aims at modeling what realistic computers in a quantum mechanical world can do. Query complexity, a variant of time complexity, has a close analogue for quantum computers; as in the classical case, our current mathematical tools are more amenable to this restricted complexity measure than to general time complexity. Sometimes, the implications of quantum query complexity shed new light even on classical complexity theory.

This thesis investigates the properties and applications of quantum query complexity and the related quantum communication complexity. It suggests new cryptographic protocols and new experiments for probing the predictions of quantum mechanics. Quantum states are very sensitive; this thesis examines ways to deal with imperfections and errors in a number of different situations.
Quantum Query Complexity  In query complexity, we are concerned with the number of times an algorithm reads a bit of the input. A celebrated result of quantum computing is Grover's algorithm, which allows an entry to be found in an unordered database with significantly less queries than any classical computer. We studied quantum search and its generalizations, particularly in the presence of imperfections.

“Property testing” drew a lot of attention in recent years, both for theoretical applications in relation to the PCP theorem and for practical applications on large data sets. The premise is that the input is so large that it is not possible to consider it in its entirety, only sampling from it in a few places instead. For most properties, sampling is not sufficient to tell whether the input has that property or whether it differs from each input with the property in at least a single bit position. However, a relaxed notion of checking the property is still conceivable: we would like to know whether or not the input differs from all inputs with the property in many bit positions. “Property testing” is concerned with algorithms that distinguish between the two cases of being close or far from having a given property. Our contribution is to translate this concept to quantum computation: we prove that quantum computers can be exponentially more efficient than classical computers in testing certain properties and we also show that there are properties that are untestable even by quantum computers.

Building quantum computers will be a challenging task. Errors in the quantum memory and quantum operations are unavoidable and need to be dealt with either by hardware or software. Surprisingly, a chain of landmark results showed that the fragile quantum state can be protected against certain types of errors and it is even possible to perform fault-tolerant quantum computation, provided the noise is of a certain kind and the noise level not too high. Together with recent experimental progress, this improves the prospects of real-world quantum computers. However, the fault-tolerance constructions do not apply to errors in the query-complexity model caused by distorted access to the input. Errors of this type are of interest because they arise in the composition of quantum algorithms and because they model real-world errors in accesses to quantum memory. We formalize the notion of noisy access to the input by proposing models of “noisy queries.” We show that for one such model (which corresponds to composing quantum algorithms) some quantum algorithms can actually be made robust at less cost than classical algorithms. We also extend the concept of approximating Boolean functions by polynomials to polynomials “robustly” approximating Boolean functions.

Quantum Distributed Computing  Nonlocality is a feature of quantum mechanics that was not explicitly incorporated by its inventors. Instead, Ein-
stein and others remarked that the axioms of quantum mechanics predict that two distant objects can be in an “entangled” state where manipulations of one object have an immediate effect on the other object, no matter how far apart. At first, this effect was discounted as an unrealistic and hence undesirable property, which needed to be eliminated by a theory replacing or amending quantum mechanics. When it became technologically feasible to conduct experiments probing nonlocality, it turned out that the results do not contradict quantum mechanics. However, due to the difficulty of conducting such experiments, they are hampered by practical limitations. Taking noise into account, it is possible to explain the data from all experiments conducted up to now using contrived classical theories. Consequently, there is an ongoing effort to devise and conduct “loophole-free” nonlocality experiments. Using combinatorial techniques developed originally for the study of quantum communication complexity, we present abstract experiments that are resistant to the most common type of error, detector inefficiency, as well as some level of more general noise.

Distributed computing studies computational tasks to be accomplished by a group of people. Examples include voting and broadcasting the same message to many parties over point-to-point channels in presence of disabled or malevolent participants. These problems share many properties and techniques with cryptography. Problems such as the impossible quantum bit commitment can be relaxed to approximate coin tossing, which can be used for two-party leader election. We develop the notion of a quantum broadcast channel, introduce a new two-party protocol, and apply it to multiparty coin-flipping with an overwhelming majority of “bad” parties. We show that the new multiparty protocol is asymptotically optimal.