# Higher-order rewriting of Quantum Circuits

Vladimir Zamdzhiev

Department of Computer Science
University of Oxford

13 March 2016

## Physical Theories

Currently, there are three main physical theories:

- Quantum Mechanics – describes the micro world (photons, electrons, etc.)
- General Relativity – describes the macro world (stars, galaxies, black holes, etc.)
- Classical Physics – describes the "moderately" sized world

All of them are inconsistent with each other.

## Physical Theories

Currently, there are three main physical theories:

- Quantum Mechanics – describes the micro world (photons, electrons, etc.)
- General Relativity – describes the macro world (stars, galaxies, black holes, etc.)
- Classical Physics – describes the "moderately" sized world

All of them are inconsistent with each other.

- Modern computers operate by manipulating electromagnetic processes in electronic circuits
- Physical processes traditionally described by classical physics
- However, electronic circuits become smaller and smaller and start exhibiting quantum phenomena
- What happens when our computational hardware becomes so small that it is "fully" quantum?

## Quantum Computing

Classical computing:

- Classical computers (laptops, phones, etc.) manipulate classical information (bits) in order to perform computation
- Classical information is described using classical information theory which is a mathematical model that assumes the world is explained using classical physics.
- This is a perfectly reasonable assumption to make for our current hardware

## Quantum Computing

Classical computing:

- Classical computers (laptops, phones, etc.) manipulate classical information (bits) in order to perform computation
- Classical information is described using classical information theory which is a mathematical model that assumes the world is explained using classical physics.
- This is a perfectly reasonable assumption to make for our current hardware

Quantum Computing:

- Consider a computer so small that it can manipulate simple quantum systems called qubits (quantum bits)
- The underlying mathematical model is now different as it is based on quantum physics
- Processing of quantum information (qubits) is as a result fundamentally different
- The speed of certain computations is also provably faster in some cases

## Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution"

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions

## Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution"

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions
- Two kinds of security for this problem:

## Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution"

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time

## Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution"

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is

## Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution"

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is
- In the classical case where all actors have classical computers and use classical communication channels, we get computational security

## Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution"

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is
- In the classical case where all actors have classical computers and use classical communication channels, we get computational security
- In the quantum case where all actors have quantum computers and use quantum communication channels, we get unconditional security

## Security, Classical and Quantum Communication

One of the most important problems in communication security is "Key Distribution"

- The problem involves two parties agreeing on a key in such a way that any third party is unable to obtain it under reasonable assumptions
- Two kinds of security for this problem:
  - Computational security – the two parties have a (severe) computational advantage over any third party, but the third party is guaranteed to recover their secrets given enough time
  - Unconditional security (or information-theoretic security) – any third party does not have enough information to recover the secret (regardless of computational power) and can at best guess what it is
- In the classical case where all actors have classical computers and use classical communication channels, we get computational security
- In the quantum case where all actors have quantum computers and use quantum communication channels, we get unconditional security
- In the quantum case eavesdropping can be detected, but in the classical case it cannot

## Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

# Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Shor's algorithm:
  - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms
  - This destroys all of the widely used public-key encryption systems
  - Online banking, internet commerce, private communication over the internet – dead
  - New encryption systems will be needed to solve this problem
  - Improved computational complexity for many practical problems

# Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Shor's algorithm:
    - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms
    - This destroys all of the widely used public-key encryption systems
    - Online banking, internet commerce, private communication over the internet – dead
    - New encryption systems will be needed to solve this problem
    - Improved computational complexity for many practical problems
- Grover's algorithm:
    - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
    - The speedup is not as significant as Shor's algorithm, but still nice
    - This results in improved computational complexity for many practical problems

# Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Shor's algorithm:
  - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms
  - This destroys all of the widely used public-key encryption systems
  - Online banking, internet commerce, private communication over the internet – dead
  - New encryption systems will be needed to solve this problem
  - Improved computational complexity for many practical problems
- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
  - The speedup is not as significant as Shor's algorithm, but still nice
  - This results in improved computational complexity for many practical problems
- Many other improved algorithms are known, but the above two are the most famous

## Computational advantages

Quantum computing has attracted a lot of interest because it offers computational speedups over some of the best known classical algorithms for important problems.

- Shor's algorithm:
  - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms
  - This destroys all of the widely used public-key encryption systems
  - Online banking, internet commerce, private communication over the internet – dead
  - New encryption systems will be needed to solve this problem
  - Improved computational complexity for many practical problems
- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
  - The speedup is not as significant as Shor's algorithm, but still nice
  - This results in improved computational complexity for many practical problems
- Many other improved algorithms are known, but the above two are the most famous
- Overall appeal is the decreased computational time for many problems which will result in better technologies in all kinds of fields

# Quantum computing is difficult

## Quantum computing is difficult

- Quantum Physics is highly unintuitive

# Quantum computing is difficult

- Quantum Physics is highly unintuitive
- Quantum programming is very difficult

## Quantum computing is difficult

- Quantum Physics is highly unintuitive
- Quantum programming is very difficult
- Discovering efficient quantum algorithms is extremely hard

# Quantum computing is difficult

- Quantum Physics is highly unintuitive
- Quantum programming is very difficult
- Discovering efficient quantum algorithms is extremely hard

What can be done about this?

## Quantum computing is difficult

- Quantum Physics is highly unintuitive
- Quantum programming is very difficult
- Discovering efficient quantum algorithms is extremely hard

What can be done about this?

- Design higher-level mathematical models which ignore some of the complexity
- Similar to the idea of higher-level vs lower-level programming languages

## So, what am I doing?

- Quantum algorithms and protocols are described in terms of families (or sets) of quantum circuits

## So, what am I doing?

- Quantum algorithms and protocols are described in terms of families (or sets) of quantum circuits
- Proving the correctness of an algorithm or protocol usually involves a mixture of linear algebra and rewriting of circuits

## So, what am I doing?

- Quantum algorithms and protocols are described in terms of families (or sets) of quantum circuits
- Proving the correctness of an algorithm or protocol usually involves a mixture of linear algebra and rewriting of circuits
- The above approach is not formal enough for automation

## So, what am I doing?

- Quantum algorithms and protocols are described in terms of families (or sets) of quantum circuits
- Proving the correctness of an algorithm or protocol usually involves a mixture of linear algebra and rewriting of circuits
- The above approach is not formal enough for automation
- I've been working on rewriting of quantum circuits

## So, what am I doing?

- Quantum algorithms and protocols are described in terms of families (or sets) of quantum circuits
- Proving the correctness of an algorithm or protocol usually involves a mixture of linear algebra and rewriting of circuits
- The above approach is not formal enough for automation
- I've been working on rewriting of quantum circuits
- I've shown how to perform equational reasoning on certain families of quantum circuits which is formal enough for computers to assist with the reasoning

## So, what am I doing?

- Quantum algorithms and protocols are described in terms of families (or sets) of quantum circuits
- Proving the correctness of an algorithm or protocol usually involves a mixture of linear algebra and rewriting of circuits
- The above approach is not formal enough for automation
- I've been working on rewriting of quantum circuits
- I've shown how to perform equational reasoning on certain families of quantum circuits which is formal enough for computers to assist with the reasoning
- This has applications in:

## So, what am I doing?

- Quantum algorithms and protocols are described in terms of families (or sets) of quantum circuits
- Proving the correctness of an algorithm or protocol usually involves a mixture of linear algebra and rewriting of circuits
- The above approach is not formal enough for automation
- I've been working on rewriting of quantum circuits
- I've shown how to perform equational reasoning on certain families of quantum circuits which is formal enough for computers to assist with the reasoning
- This has applications in:
  - Compiler optimisation for quantum programming languages

## So, what am I doing?

- Quantum algorithms and protocols are described in terms of families (or sets) of quantum circuits
- Proving the correctness of an algorithm or protocol usually involves a mixture of linear algebra and rewriting of circuits
- The above approach is not formal enough for automation
- I've been working on rewriting of quantum circuits
- I've shown how to perform equational reasoning on certain families of quantum circuits which is formal enough for computers to assist with the reasoning
- This has applications in:
  - Compiler optimisation for quantum programming languages
  - Verification of quantum protocols and algorithms

Thank you for your attention!