Quantum Computing: the Good, the Bad and the (not so) Ugly

Vladimir Zamdzhiev

Department of Computer Science
University of Oxford

7 June 2016

Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world

Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world, however, wrong for macro/micro world

Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world, however, wrong for macro/micro world
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.)

Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world, however, wrong for macro/micro world
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.), but wrong for micro world

Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world, however, wrong for macro/micro world
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.), but wrong for micro world
- Quantum Mechanics – describes the micro world (photons, electrons, etc.)

Physical Theories

Currently, there are three main physical theories:

- Classical Mechanics – describes the moderately sized world, however, wrong for macro/micro world
- General Relativity – works for moderately sized and macro world (stars, galaxies, black holes, etc.), but wrong for micro world
- Quantum Mechanics – describes the micro world (photons, electrons, etc.), never proven false
  - However, mostly useless for anything outside micro world

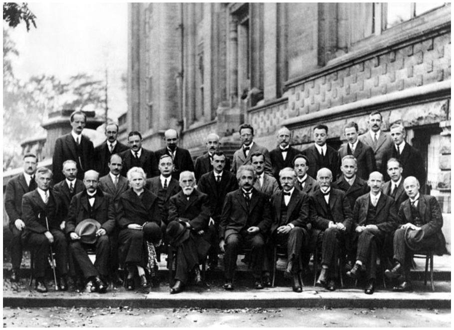


Figure: The 1927 Solvay Conference in Brussels

Computer Design

- Modern computers operate by manipulating electromagnetic processes in electronic circuits
- 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?

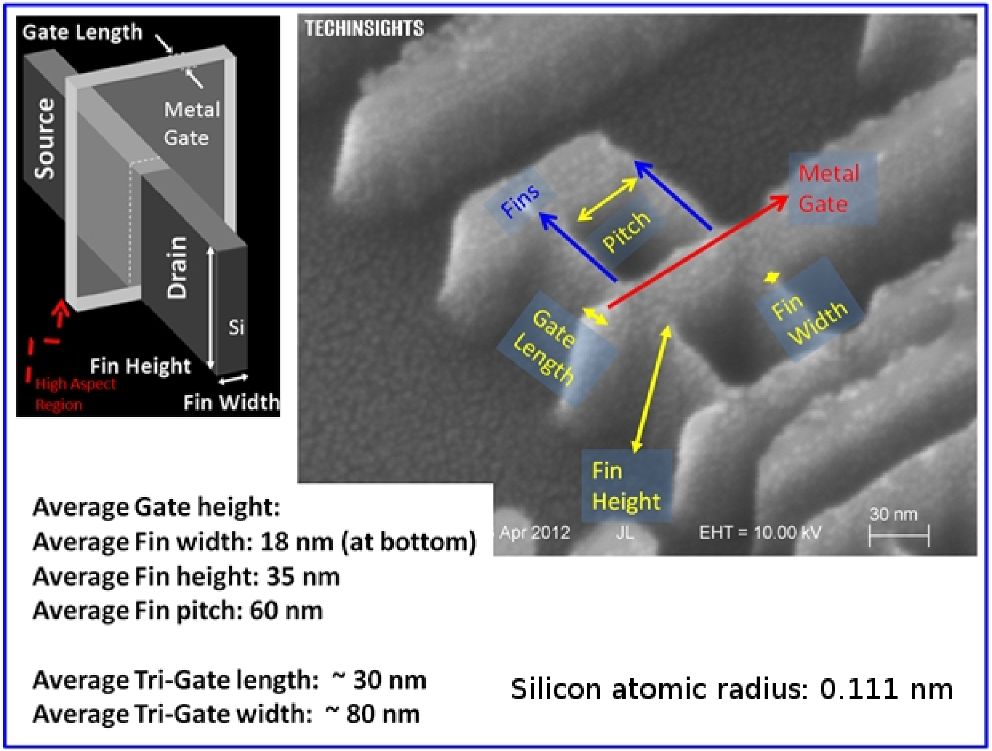


Figure: Intel 22-nm Tri-Gate device

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

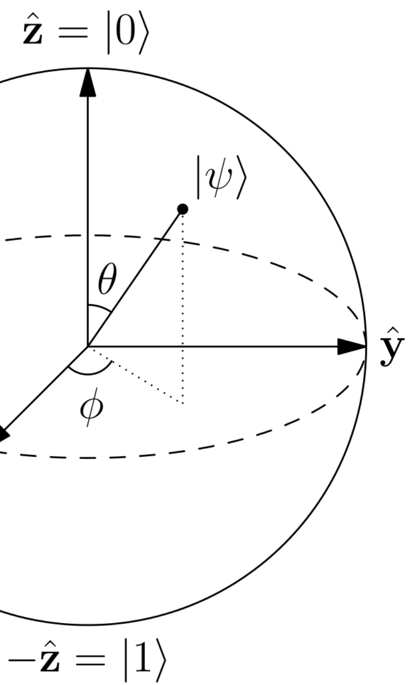


Figure: Bloch-sphere representation of a qubit state

Quantum Entanglement – important resource

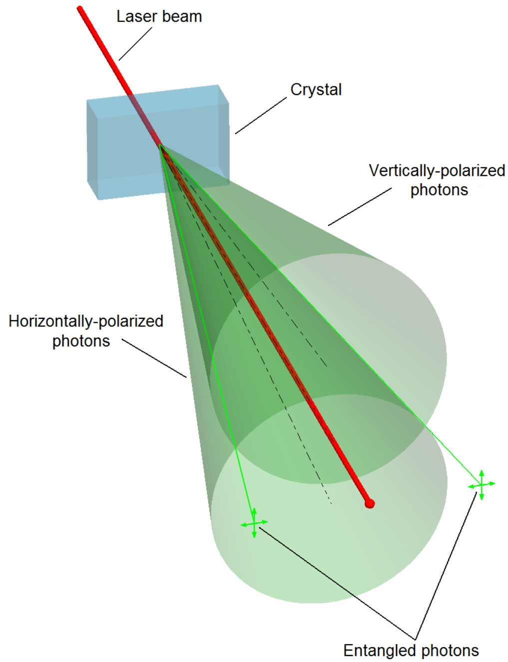
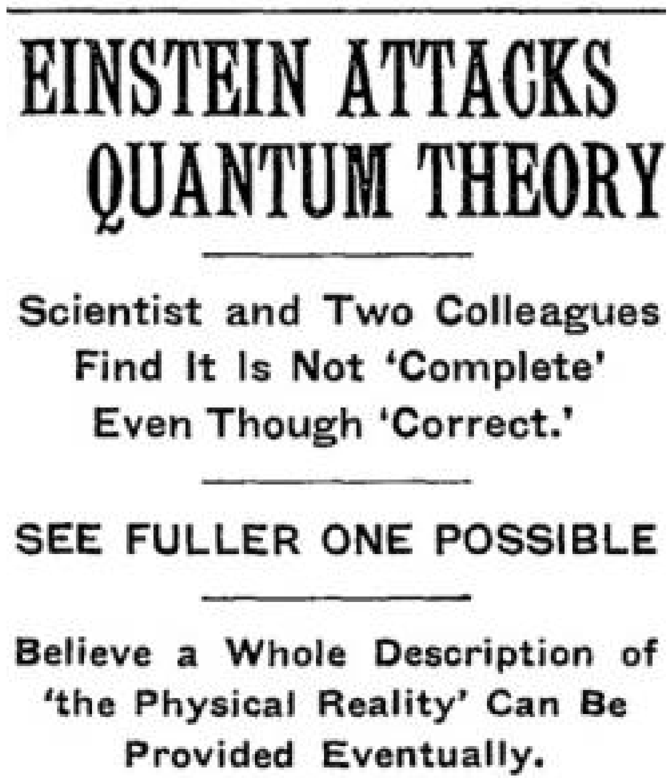


Figure: Illustration of quantum optics experiment which produces entanglement

Quantum Entanglement – important resource



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

Figure: May 4, 1935 *New York Times* article headline regarding the imminent EPR paper

Quantum Entanglement – important resource

- Quantum entanglement is a special kind of correlation between systems which allows them to exhibit similar properties, even when space-time seperated
- Einstein famously referred to it as: "Spooky action at a distance"
- Schrödinger described it as: "I would not call entanglement one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."
- Quantum entanglement is a crucial resource for quantum computing and also for many quantum information security protocols.

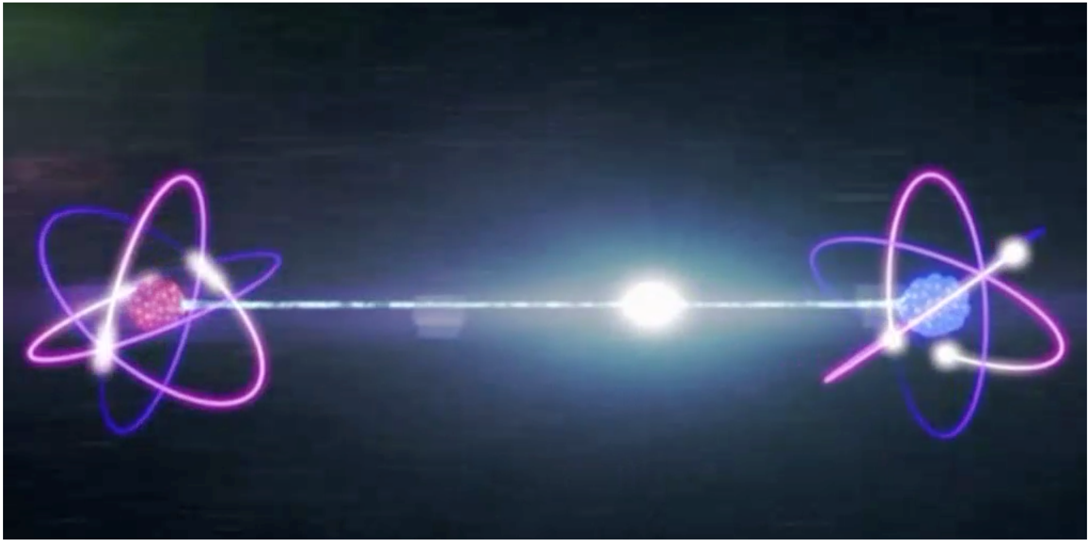


Figure: A most likely inaccurate illustration of quantum entanglement

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 (this is the case for encryption)

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 (this is the case for encryption)
- 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 (this is the case for encryption)
- 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

Quantum Superposition – important resource

A quantum system may be in many different states at the same time.

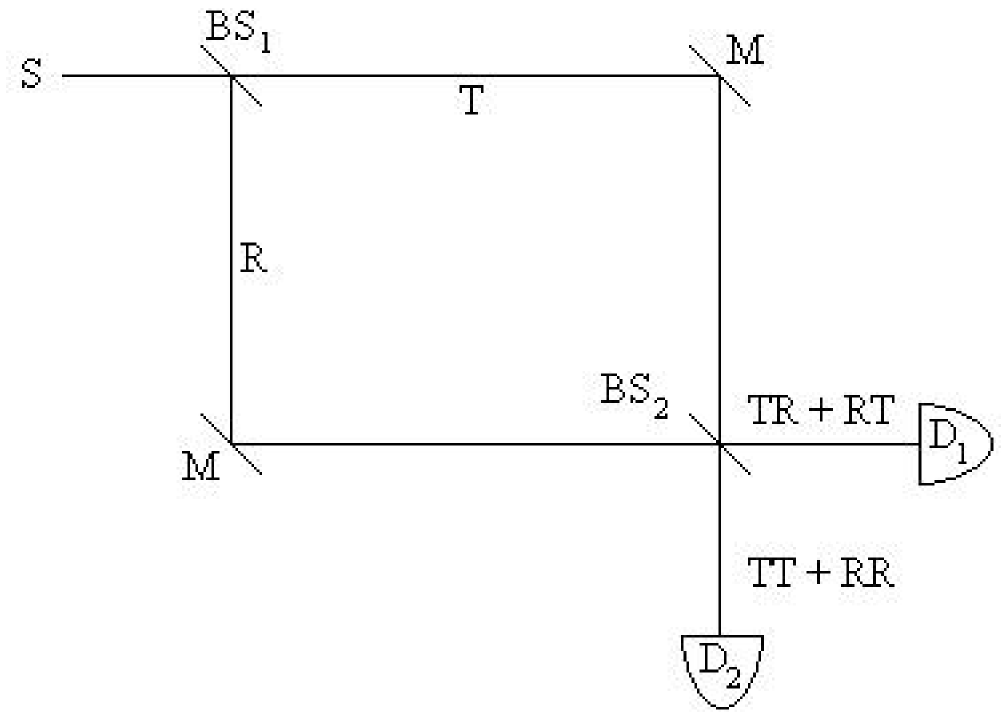


Figure: single-photon interference performed with a Mach-Zehnder interferometer

- Very rough analogy: allows for exponential parallelism
- Crucial for computational speedup

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.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
  - Decent speedup, but not mind-blowing
  - 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.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
  - Decent speedup, but not mind-blowing
  - This results in improved computational complexity for many practical problems
- Shor's algorithm:
  - An algorithm which can perform integer factorization exponentially faster than the best known classical algorithms

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.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
  - Decent speedup, but not mind-blowing
  - This results in improved computational complexity for many practical 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

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.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
  - Decent speedup, but not mind-blowing
  - This results in improved computational complexity for many practical 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

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.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
  - Decent speedup, but not mind-blowing
  - This results in improved computational complexity for many practical 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.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
  - Decent speedup, but not mind-blowing
  - This results in improved computational complexity for many practical 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
- 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.

- Grover's algorithm:
  - An algorithm which can search an unsorted database with a quadratic speedup over the best classical algorithm
  - Decent speedup, but not mind-blowing
  - This results in improved computational complexity for many practical 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
- 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

How soon will quantum computers be able to crack encryption?

Here's what the Information Assurance Directorate (IAD) of the National Security Agency (NSA) of the United States has to say on the matter:

- "IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer...
- ...Until this new suite is developed and products are available implementing the quantum resistant suite, we will rely on current algorithms. For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition."

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
- Consider the following simple question: What happens when we apply a Hadamard gate to the second qubit of a Bell state and measure in the computational basis?

Quantum computing is difficult

- Quantum Physics is highly unintuitive
- Quantum programming is very difficult
- Discovering efficient quantum algorithms is extremely hard
- Consider the following simple question: What happens when we apply a Hadamard gate to the second qubit of a Bell state and measure in the computational basis?
- Answer using the traditional formalism:

the Hadamard gate on the second. The resulting operation is, with scaling factor s,

$$I \otimes H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = s \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

Now, you can pass your entangled state, $\begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}^T$ for $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, through the gate and get

$$s \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix}$$

Which is the state

$$|00\rangle + |01\rangle + |10\rangle - |11\rangle.$$

And measurement of the first qubit or the second qubit would be 0 or 1 with equal probability, and give no information on the state of the other qubit.

Quantum computing is difficult

What can be done about this?

Quantum computing is difficult

What can be done about this?

- Design higher-level mathematical models which ignore some of the complexity

Quantum computing is difficult

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

Quantum computing is difficult

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
- Replace linear algebra with category theory (very abstract mathematical theory)

Quantum computing is difficult

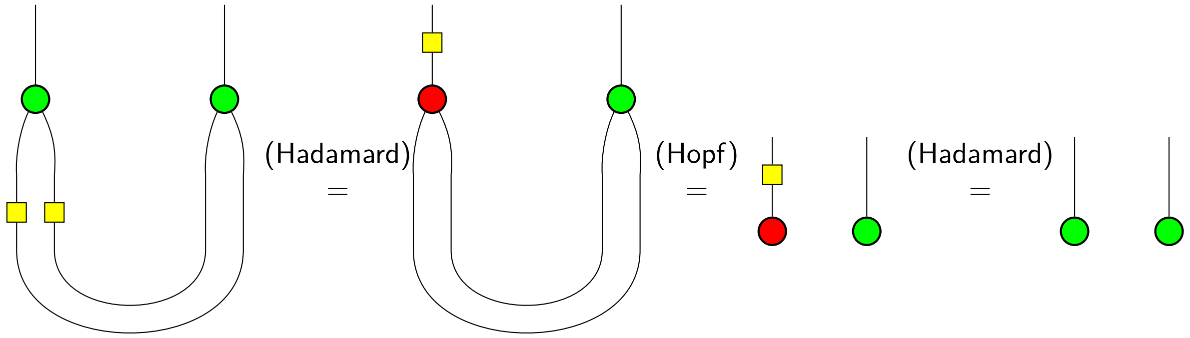
What can be done about this?

- Design higher-level mathematical models which ignore some of the complexity
- Similar to the idea of higher-level vs lower-level programming languages
- Replace linear algebra with category theory (very abstract mathematical theory)
- Then, we can perform reasoning by either term rewriting or diagram rewriting (both amenable to computer-assisted reasoning)

Quantum computing is difficult

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
- Replace linear algebra with category theory (very abstract mathematical theory)
- Then, we can perform reasoning by either term rewriting or diagram rewriting (both amenable to computer-assisted reasoning)



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
- This approach is difficult to utilise in computer systems

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
- This approach is difficult to utilise in computer systems
- I've been working on rewriting of quantum circuits using the higher-level approach

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
- This approach is difficult to utilise in computer systems
- I've been working on rewriting of quantum circuits using the higher-level approach
- I've shown how to perform equational reasoning on certain families of quantum circuits which is formal enough for computers to do

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
- This approach is difficult to utilise in computer systems
- I've been working on rewriting of quantum circuits using the higher-level approach
- I've shown how to perform equational reasoning on certain families of quantum circuits which is formal enough for computers to do
- 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
- This approach is difficult to utilise in computer systems
- I've been working on rewriting of quantum circuits using the higher-level approach
- I've shown how to perform equational reasoning on certain families of quantum circuits which is formal enough for computers to do
- This has applications in:
  - Verification of quantum protocols and algorithms

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
- This approach is difficult to utilise in computer systems
- I've been working on rewriting of quantum circuits using the higher-level approach
- I've shown how to perform equational reasoning on certain families of quantum circuits which is formal enough for computers to do
- This has applications in:
  - Verification of quantum protocols and algorithms
  - 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
- This approach is difficult to utilise in computer systems
- I've been working on rewriting of quantum circuits using the higher-level approach
- I've shown how to perform equational reasoning on certain families of quantum circuits which is formal enough for computers to do
- This has applications in:
  - Verification of quantum protocols and algorithms
  - Compiler optimisation for quantum programming languages
- After DPhil: postdoc in designing quantum programming languages (in particular, working on mathematical models for quantum programs)

Thank you for your attention!