The One Way to Quantum Computation

Vincent Danos

Elham Kashefi

Prakash Panangaden

CNRS Paris

IQC Waterloo

McGill University

The “One-Way” Quantum Computer

- A new model of quantum computation based on **measurements** as the driving force of the computation. [Raussendorff and Briegel PRL 2001]

The “One-Way” Quantum Computer

- A new model of quantum computation based on **measurements** as the driving force of the computation. [Raussendorff and Briegel PRL 2001]
- The usual (circuit) model is based on reversible transformations (unitaries) with measurements only at the end.

The “One-Way” Quantum Computer

- A new model of quantum computation based on **measurements** as the driving force of the computation. [Raussendorff and Briegel PRL 2001]
- The usual (circuit) model is based on reversible transformations (unitaries) with measurements only at the end.
- In Quantum Mechanics measurements are irreversible;

The “One-Way” Quantum Computer

- A new model of quantum computation based on **measurements** as the driving force of the computation. [Raussendorff and Briegel PRL 2001]
- The usual (circuit) model is based on reversible transformations (unitaries) with measurements only at the end.
- In Quantum Mechanics measurements are irreversible;
- hence the name “One-way quantum computer.”

Outline of the Talk

- Manifesto and slogans.

Outline of the Talk

- Manifesto and slogans.
- Brief overview of quantum mechanics.

Outline of the Talk

- Manifesto and slogans.
- Brief overview of quantum mechanics.
- Brief overview of quantum computation.

Outline of the Talk

- Manifesto and slogans.
- Brief overview of quantum mechanics.
- Brief overview of quantum computation.
- Entanglement and Teleportation.

Outline of the Talk

- Manifesto and slogans.
- Brief overview of quantum mechanics.
- Brief overview of quantum computation.
- Entanglement and Teleportation.
- Measurement-based computation.

Outline of the Talk

- Manifesto and slogans.
- Brief overview of quantum mechanics.
- Brief overview of quantum computation.
- Entanglement and Teleportation.
- Measurement-based computation.
- Measurement Calculus.

Outline of the Talk

- Manifesto and slogans.
- Brief overview of quantum mechanics.
- Brief overview of quantum computation.
- Entanglement and Teleportation.
- Measurement-based computation.
- Measurement Calculus.
- Standardization.

Outline of the Talk

- Manifesto and slogans.
- Brief overview of quantum mechanics.
- Brief overview of quantum computation.
- Entanglement and Teleportation.
- Measurement-based computation.
- Measurement Calculus.
- Standardization.
- Conclusions.

Manifesto and slogans

- Given all the exceedingly clever quantum algorithms that people have invented it is time to study the **structure** of quantum computation.

Manifesto and slogans

- Given all the exceedingly clever quantum algorithms that people have invented it is time to study the **structure** of quantum computation.
- This means understanding:

Manifesto and slogans

- Given all the exceedingly clever quantum algorithms that people have invented it is time to study the **structure** of quantum computation.
- This means understanding:
  - How computations compose

Manifesto and slogans

- Given all the exceedingly clever quantum algorithms that people have invented it is time to study the **structure** of quantum computation.
- This means understanding:
  - How computations compose
  - The type structure of computations

Manifesto and slogans

- Given all the exceedingly clever quantum algorithms that people have invented it is time to study the **structure** of quantum computation.
- This means understanding:
  - How computations compose
  - The type structure of computations
- Ideas from the semantics/concurrency/type theory community will prove useful.

Intuitions about quantum mechanics

- The notion of state is subtle.

Intuitions about quantum mechanics

- The notion of state is subtle.
- Systems can be in *superpositions* of states. Thus the state space must have a notion of addition: a vector space; in fact also an inner product to measure how different states are.

Intuitions about quantum mechanics

- The notion of state is subtle.
- Systems can be in *superpositions* of states. Thus the state space must have a notion of addition: a vector space; in fact also an inner product to measure how different states are.
- The results of measurements are probabilistic: we cannot model physical observables as functions.

Intuitions about quantum mechanics

- The notion of state is subtle.
- Systems can be in *superpositions* of states. Thus the state space must have a notion of addition: a vector space; in fact also an inner product to measure how different states are.
- The results of measurements are probabilistic: we cannot model physical observables as functions.
- Measurements disturb the system, they have to be operators of some kind and they may fail to commute with each other.

Intuitions about quantum mechanics

- The notion of state is subtle.
- Systems can be in *superpositions* of states. Thus the state space must have a notion of addition: a vector space; in fact also an inner product to measure how different states are.
- The results of measurements are probabilistic: we cannot model physical observables as functions.
- Measurements disturb the system, they have to be operators of some kind and they may fail to commute with each other.

Probability in quantum mechanics

- The probabilistic behaviour of quantum mechanics is inherent.

Probability in quantum mechanics

- The probabilistic behaviour of quantum mechanics is inherent.
- It is not possible to explain the probabilities as an abstraction of some hidden deterministic behaviour.

Probability in quantum mechanics

- The probabilistic behaviour of quantum mechanics is inherent.
- It is not possible to explain the probabilities as an abstraction of some hidden deterministic behaviour.
- More precisely: there is no theory that is

Probability in quantum mechanics

- The probabilistic behaviour of quantum mechanics is inherent.
- It is not possible to explain the probabilities as an abstraction of some hidden deterministic behaviour.
- More precisely: there is no theory that is
  - local,

Probability in quantum mechanics

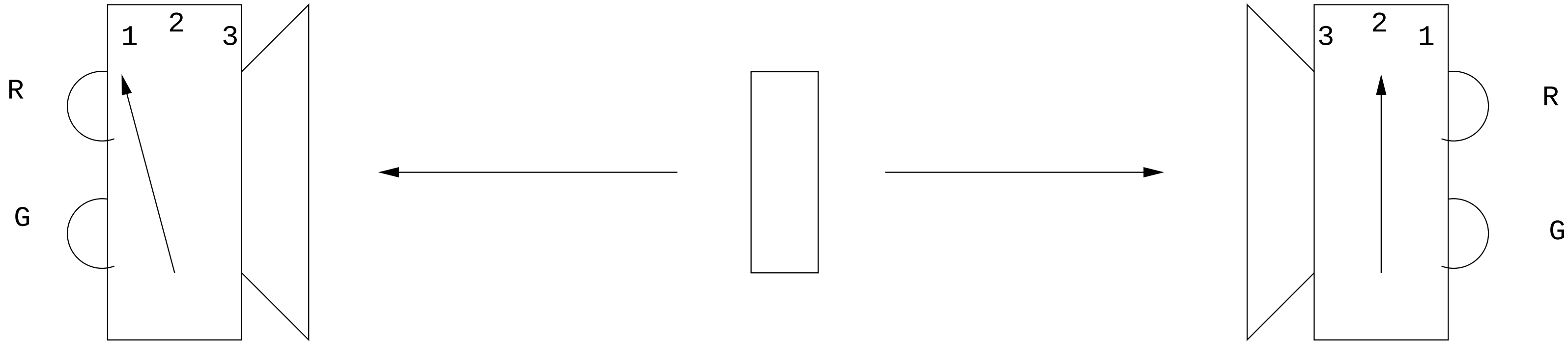
- The probabilistic behaviour of quantum mechanics is inherent.
- It is not possible to explain the probabilities as an abstraction of some hidden deterministic behaviour.
- More precisely: there is no theory that is
  - local,
  - causal,

Probability in quantum mechanics

- The probabilistic behaviour of quantum mechanics is inherent.
- It is not possible to explain the probabilities as an abstraction of some hidden deterministic behaviour.
- More precisely: there is no theory that is
  - local,
  - causal,
  - based on a deterministic state.

Mermin's example I

A simple version of Bell's inequality that can be understood easily.

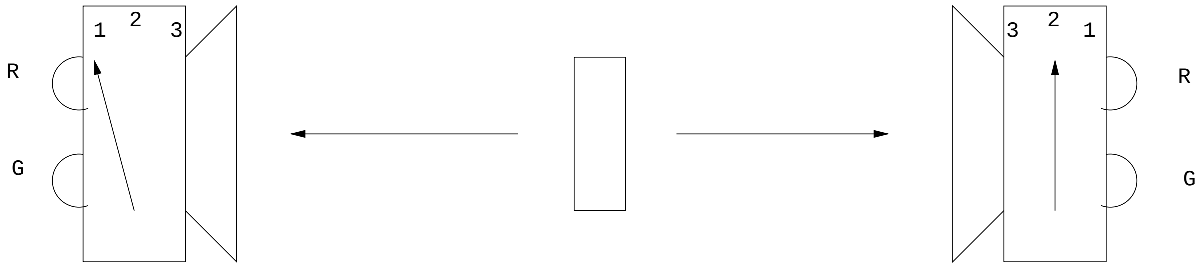


Two detectors each with 3 settings and 2 indicators (Red and Green). The detectors are set independently and uniformly at random.

The detectors are not connected to each other or to the source.

Source of correlated particles in the middle.

Mermin's Example II



Whatever the setting on a detector, the red or the green lights flash with equal probability, but never both at the same time.

When the settings are the same the two detectors **always** agree.

When the settings are different the detectors agree $\frac{1}{4}$ of the time!

Why is this strange?: 1

- How could the detectors **always** agree when the settings are the same, even though the actual colour seems to be chosen at random?

Why is this strange?: 1

- How could the detectors **always** agree when the settings are the same, even though the actual colour seems to be chosen at random?
- There must be some "hidden" property of the particles that determines which colour is chosen for each setting; the two correlated particles must be identical with respect to this property, *whether or not the switches are set the same way.*

Why is this strange?: 1

- How could the detectors **always** agree when the settings are the same, even though the actual colour seems to be chosen at random?
- There must be some “hidden” property of the particles that determines which colour is chosen for each setting; the two correlated particles must be identical with respect to this property, *whether or not the switches are set the same way.*
- Let us write GGR mean that for the three settings, $1, 2, 3$, the detectors flash green, green and red respectively for a type GGR particle.

Why is this strange?: 2

- Suppose that the settings are different and we have an RRG particle:

Why is this strange?: 2

- Suppose that the settings are different and we have an RRG particle:
- then for two of the possible settings ($1, 2$ and $2, 1$) the same colour flashes and for the other four settings the colours are different. Thus $\frac{1}{3}$ of the time the colours must match.

Why is this strange?: 2

- Suppose that the settings are different and we have an RRG particle:
- then for two of the possible settings ($1, 2$ and $2, 1$) the same colour flashes and for the other four settings the colours are different. Thus $\frac{1}{3}$ of the time the colours must match.
- This applies for any of the combinations: $RRG, RGR, GRR, GGR, GRG, RGG$.

Why is this strange?: 2

- Suppose that the settings are different and we have an RRG particle:
- then for two of the possible settings ($1, 2$ and $2, 1$) the same colour flashes and for the other four settings the colours are different. Thus $\frac{1}{3}$ of the time the colours must match.
- This applies for any of the combinations: $RRG, RGR, GRR, GGR, GRG, RGG$.
- For particles of type RRR and GGG the colours **always** match whatever the settings.

The inescapable conclusion

Thus *whatever the distribution of particle types* the probability that the lights match when the settings are different is at least $\frac{1}{3}$!.

This just ain't what we see in nature!

assumptions about detectors

- What happens at one detector cannot alter what happens at the other: local

assumptions about detectors

- What happens at one detector cannot alter what happens at the other: local
- a detector cannot predict the future sequence of particles and alter its behaviour: causal.

assumptions about detectors

- What happens at one detector cannot alter what happens at the other: local
- a detector cannot predict the future sequence of particles and alter its behaviour: causal.
- no ordinary probabilistic automaton or MDP can reproduce the observed behaviour without breaking locality or causality.

Bell's inequality

The inequality,

$$Prob(\text{lights agree}|\text{settings different}) \geq \frac{1}{3},$$

is a simple special case of Bell's inequality.

Bell's inequality

- Quantum mechanics predicts that this inequality is violated.

Bell's inequality

- Quantum mechanics predicts that this inequality is violated.
- Bell's inequality has been **experimentally tested** and it is plainly violated

The Point of this discussion

The probabilistic nature of quantum mechanics does not arise as an abstraction of things that could be known. State is not enough to predict the outcomes of measurements; **state is enough to predict evolution to new states.**

If you want to know where the $\frac{1}{4}$ comes from and a description of the "real" experiment, see me later.

Postulates of quantum mechanics

- States form a Hilbert Space $\mathcal{H}$

Postulates of quantum mechanics

- States form a Hilbert Space $\mathcal{H}$
- The evolution of an *isolated* system is governed by a *unitary* transformation. This is determinate evolution.

Postulates of quantum mechanics

- States form a Hilbert Space $\mathcal{H}$
- The evolution of an *isolated* system is governed by a *unitary* transformation. This is determinate evolution.
- Measurements are described by Hermitian operators. Why operators?

The Effect of a Measurement

- For a measurement described by M the possible outcomes are the *eigenvalues* of M.

The Effect of a Measurement

- For a measurement described by M the possible outcomes are the *eigenvalues* of M.
- If M is an observable with eigenvalues λ_i and eigenvectors ϕ_i and $\psi = \sum_i c_i \phi_i$ is any state then, $Pr(\lambda_i|\psi) = |c_i|^2$

The Effect of a Measurement

- For a measurement described by M the possible outcomes are the *eigenvalues* of M.
- If M is an observable with eigenvalues λ_i and eigenvectors ϕ_i and $\psi = \sum_i c_i \phi_i$ is any state then, $Pr(\lambda_i | \psi) = |c_i|^2$
- If M is measured and λ_i is obtained the system gets knocked into a eigenstate of M with eigenvalue λ_i.

The Effect of a Measurement

- For a measurement described by M the possible outcomes are the *eigenvalues* of M.
- If M is an observable with eigenvalues λ_i and eigenvectors ϕ_i and $\psi = \sum_i c_i \phi_i$ is any state then, $Pr(\lambda_i|\psi) = |c_i|^2$
- If M is measured and λ_i is obtained the system gets knocked into a eigenstate of M with eigenvalue λ_i.
- If we measure M immediately again then we will certainly get the value λ_i again.

Unitary Evolution

- If a system in state ψ is subjected to interactions and evolves it does so by a unitary operator U; $\psi \mapsto U\psi$.

Unitary Evolution

- If a system in state ψ is subjected to interactions and evolves it does so by a unitary operator U; $\psi \mapsto U\psi$.
- This is in stark contrast to what happens during a measurement.

Unitary Evolution

- If a system in state ψ is subjected to interactions and evolves it does so by a unitary operator U; $\psi \mapsto U\psi$.
- This is in stark contrast to what happens during a measurement.
- Typically quantum computation is presented in terms of circuits that implement various unitaries.

Combining Systems

- When two systems are put together their individual Hilbert spaces, $\mathcal{H}_1$ and $\mathcal{H}_2$ are combined to give $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Combining Systems

- When two systems are put together their individual Hilbert spaces, $\mathcal{H}_1$ and $\mathcal{H}_2$ are combined to give $\mathcal{H}_1 \otimes \mathcal{H}_2$.
- There is no *à priori* reason why this should happen; this is what we see in nature.

Combining Systems

- When two systems are put together their individual Hilbert spaces, $\mathcal{H}_1$ and $\mathcal{H}_2$ are combined to give $\mathcal{H}_1 \otimes \mathcal{H}_2$.
- There is no *à priori* reason why this should happen; this is what we see in nature.
- The “size” (dimensionality) of the combined state space grows *exponentially*.

Combining Systems

- When two systems are put together their individual Hilbert spaces, $\mathcal{H}_1$ and $\mathcal{H}_2$ are combined to give $\mathcal{H}_1 \otimes \mathcal{H}_2$.
- There is no *à priori* reason why this should happen; this is what we see in nature.
- The “size” (dimensionality) of the combined state space grows *exponentially*.
- This is what gives quantum computation its power.

Notation for Quantum Computation

- The basic unit is a two-dimensional state space called a **qubit**. The basis states are typically written $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$. Note that $|0\rangle$ is not the zero of the vector space!

Notation for Quantum Computation

- The basic unit is a two-dimensional state space called a **qubit**. The basis states are typically written $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$. Note that $|0\rangle$ is not the zero of the vector space!
- Tensor product is denoted by juxtaposition: $|0\rangle \otimes |0\rangle = |00\rangle$.

Notation for Quantum Computation

- The basic unit is a two-dimensional state space called a **qubit**. The basis states are typically written $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$. Note that $|0\rangle$ is not the zero of the vector space!
- Tensor product is denoted by juxtaposition: $|0\rangle \otimes |0\rangle = |00\rangle$.
- We can measure in the computational basis by using the Hermitian operator $|0\rangle\langle 0| + |1\rangle\langle 1|$.

Universality

- A quantum computation is the implementation of a transformation on a collection of qubits based on some given set of primitive transformations.

Universality

- A quantum computation is the implementation of a transformation on a collection of qubits based on some given set of primitive transformations.
- The primitive building blocks are called “gates” and the combinations are called “circuits.”

Universality

- A quantum computation is the implementation of a transformation on a collection of qubits based on some given set of primitive transformations.
- The primitive building blocks are called “gates” and the combinations are called “circuits.”
- A few basic gates are enough to approximate all the possible unitary operations: universality.

Universality

- A quantum computation is the implementation of a transformation on a collection of qubits based on some given set of primitive transformations.
- The primitive building blocks are called “gates” and the combinations are called “circuits.”
- A few basic gates are enough to approximate all the possible unitary operations: universality.
- The basic gates are certain one-qubit operations plus a particular two-qubit operation: CNOT.

Some example gates

The Pauli matrices:

$$\sigma_x \text{ or just } X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y \text{ or just } Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_z \text{ or just } Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The Hadamard matrix

The Hadamard matrix:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

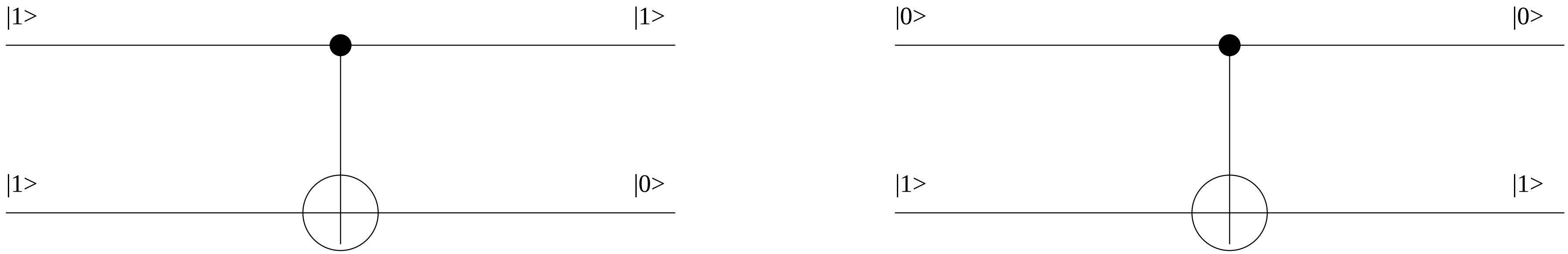
We have

$$H|0\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle$$

and

$$H|1\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle$$

The CNOT gate



It acts as follows

$$|xy\rangle \mapsto |x(x \oplus y)\rangle.$$

The x bit controls whether a **not** is applied to the second bit.

Entanglement

- Consider two qubit states, a basis is given by: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

Entanglement

- Consider two qubit states, a basis is given by: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.
- Some states, e.g. $|00\rangle + |01\rangle = |0\rangle \otimes (|0\rangle + |1\rangle)$ are tensor products while others, e.g. $|01\rangle + |10\rangle$ are not. These are called “entangled” states.

Entanglement

- Consider two qubit states, a basis is given by: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.
- Some states, e.g. $|00\rangle + |01\rangle = |0\rangle \otimes (|0\rangle + |1\rangle)$ are tensor products while others, e.g. $|01\rangle + |10\rangle$ are not. These are called “entangled” states.
- There are many notions of entanglement and proposed measures of how entangled two states are. For two qubits the state $|01\rangle + |10\rangle$ is maximally entangled, as is, e.g. $|00\rangle + |11\rangle$. They are called Bell states or Bell pairs.

CNOT entangles

When $CNOT$ is applied to $H|0\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle$ we get $\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$.

Controlled versions of other one-qubit gates are possible.

Thus CZ stands for controlled Z. *This is also an entangler*.

Measuring a Bell Pair

- Suppose that we prepare the state $|01\rangle + |10\rangle$ and separate the two qubits but preserve the entanglement. We have two experimenters *sharing an entangled pair*.

Measuring a Bell Pair

- Suppose that we prepare the state $|01\rangle + |10\rangle$ and separate the two qubits but preserve the entanglement. We have two experimenters *sharing an entangled pair*.
- Suppose that one of them performs a measurement to determine the state. He will get the outcome $|0\rangle$ or $|1\rangle$ with equal probability.

Measuring a Bell Pair

- Suppose that we prepare the state $|01\rangle + |10\rangle$ and separate the two qubits but preserve the entanglement. We have two experimenters *sharing an entangled pair*.
- Suppose that one of them performs a measurement to determine the state. He will get the outcome $|0\rangle$ or $|1\rangle$ with equal probability.
- The other observer will detect the same outcomes and by themselves these outcomes will seem random. However, the two sets of outcomes will be perfectly correlated.

Teleportation

- Suppose that two agents A and B share a Bell pair. Then there is a way for A to communicate a one-qubit state $|\psi\rangle$ to B by sending just two classical bits.

Teleportation

- Suppose that two agents A and B share a Bell pair. Then there is a way for A to communicate a one-qubit state $|\psi\rangle$ to B by sending just two classical bits.
- Let A's portion of the entangled pair be $|a\rangle$; A measures the state $|\psi\rangle \otimes |a\rangle$ in the Bell basis $|01\rangle \pm |10\rangle$ and $|00\rangle \pm |11\rangle$.

Teleportation

- Suppose that two agents A and B share a Bell pair. Then there is a way for A to communicate a one-qubit state $|\psi\rangle$ to B by sending just two classical bits.
- Let A's portion of the entangled pair be $|a\rangle$; A measures the state $|\psi\rangle \otimes |a\rangle$ in the Bell basis $|01\rangle \pm |10\rangle$ and $|00\rangle \pm |11\rangle$.
- She sends to B the outcome of the measurement (2 bits).

Teleportation

- Suppose that two agents A and B share a Bell pair. Then there is a way for A to communicate a one-qubit state $|\psi\rangle$ to B by sending just two classical bits.
- Let A's portion of the entangled pair be $|a\rangle$; A measures the state $|\psi\rangle \otimes |a\rangle$ in the Bell basis $|01\rangle \pm |10\rangle$ and $|00\rangle \pm |11\rangle$.
- She sends to B the outcome of the measurement (2 bits).
- B applies a unitary transformation to his state and it ends up being $|\psi\rangle$.

The algebra behind teleportation*

- Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,
  the shared state is $\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$.

The algebra behind teleportation*

- Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,
  the shared state is $\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$.
- The Bell basis states are $(|00\rangle + |11\rangle)$, $(|00\rangle - |11\rangle)$, $(|10\rangle + |01\rangle)$ and $(|10\rangle - |01\rangle)$.

The algebra behind teleportation*

- Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,
  the shared state is $\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$.
- The Bell basis states are $(|00\rangle + |11\rangle)$, $(|00\rangle - |11\rangle)$, $(|10\rangle + |01\rangle)$ and $(|10\rangle - |01\rangle)$.
- After combining $|\psi\rangle$ with her state the combined system is in

$$\frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)],$$

The algebra behind teleportation cont.*

which equals

$$\frac{1}{2\sqrt{2}}[(|00\rangle + |11\rangle)(\alpha|0\rangle + \beta|1\rangle) + (|00\rangle - |11\rangle)(\alpha|0\rangle - \beta|1\rangle)$$

$$+(|10\rangle + |01\rangle)(\beta|0\rangle + \alpha|1\rangle) + (|10\rangle - |01\rangle)(\beta|0\rangle - \alpha|1\rangle)$$

If A gets the first basis state she tells this to B and he knows that he now has $|\psi\rangle$. If A gets the second result, B has to fix up his state to get $|\psi\rangle$, and so on. This "fixing up" amounts to applying Pauli operations.

The Point of Teleportation

- The result of a measurement tells you what unitary to apply

The Point of Teleportation

- The result of a measurement tells you what unitary to apply
- in order to get a determinate result.

The Point of Teleportation

- The result of a measurement tells you what unitary to apply
- in order to get a determinate result.
- It did not matter that the measurement outcome is indeterminate, the whole procedure is determinate.

The Point of Teleportation

- The result of a measurement tells you what unitary to apply
- in order to get a determinate result.
- It did not matter that the measurement outcome is indeterminate, the whole procedure is determinate.
- This is a computation - of the identity function (!) - that is guided by measurement outcomes.

The Point of Teleportation

- The result of a measurement tells you what unitary to apply
- in order to get a determinate result.
- It did not matter that the measurement outcome is indeterminate, the whole procedure is determinate.
- This is a computation - of the identity function (!) - that is guided by measurement outcomes.
- Can we compute more interesting functions?

Computing by Measurements

- Teleporting is *compositional*. If $|\psi\rangle$ is entangled with something else then the teleported version will have the same entanglement.

Computing by Measurements

- Teleporting is *compositional*. If $|\psi\rangle$ is entangled with something else then the teleported version will have the same entanglement.
- One can modify the teleportation protocol to implement an arbitrary one-qubit unitary and some selected two-qubit unitaries: this is enough to get universality [Gottesman and Chuang 1999].

Computing by Measurements

- Teleporting is *compositional*. If $|\psi\rangle$ is entangled with something else then the teleported version will have the same entanglement.
- One can modify the teleportation protocol to implement an arbitrary one-qubit unitary and some selected two-qubit unitaries: this is enough to get universality [Gottesman and Chuang 1999].
- Teleportation looks like it involves two-qubit measurements but it can be reduced to one-qubit measurements.

The Measurement-based Slogan

Measurements, followed by unitary corrections which may depend on the measurement outcomes can implement determinate quantum computations.

The One Way Quantum Computer

- Use measurements to guide the computation; use Pauli corrections to eliminate the indeterminacy.

The One Way Quantum Computer

- Use measurements to guide the computation; use Pauli corrections to eliminate the indeterminacy.
- One-qubit measurements and one-qubit corrections suffice [Raussendorf and Briegel 2001]

The One Way Quantum Computer

- Use measurements to guide the computation; use Pauli corrections to eliminate the indeterminacy.
- One-qubit measurements and one-qubit corrections suffice [Raussendorf and Briegel 2001]
- provided one has the “right” entanglement to start with.

The One Way Quantum Computer

- Use measurements to guide the computation; use Pauli corrections to eliminate the indeterminacy.
- One-qubit measurements and one-qubit corrections suffice [Raussendorf and Briegel 2001]
- provided one has the “right” entanglement to start with.
- One standard type of entangled state suffices and further entanglement is not necessary.

Basic Ideas

- There is a “cluster” of qubits arranged in a grid; each adjacent pair is entangled: cluster states.

Basic Ideas

- There is a “cluster” of qubits arranged in a grid; each adjacent pair is entangled: cluster states.
- A measurement is applied to each qubit: this may be along the axes or at some angle to it.

Basic Ideas

- There is a “cluster” of qubits arranged in a grid; each adjacent pair is entangled: cluster states.
- A measurement is applied to each qubit: this may be along the axes or at some angle to it.
- The angle along which a measurement is made may depend on the result of a previous measurement.

Basic Ideas

- There is a “cluster” of qubits arranged in a grid; each adjacent pair is entangled: cluster states.
- A measurement is applied to each qubit: this may be along the axes or at some angle to it.
- The angle along which a measurement is made may depend on the result of a previous measurement.
- Once a qubit is measured it is never used again.

The CNOT Pattern

control	X	Y	Y	Y	Y	Y	O
				Y			
target	X	X	X	Y	X	X	O

Each square is a qubit; X means measure the observable σ_x. Later it was realized that one can do this with fewer qubits.

The Need for Structure

- Understanding the previous pattern is painful if you are not a physicist: too low level.

The Need for Structure

- Understanding the previous pattern is painful if you are not a physicist: too low level.
- Very hard to prove general results based on example patterns. The physicists' intuitions are so good that they rarely make wrong statements but their "proofs" tend to be demonstrations by example.

The Need for Structure

- Understanding the previous pattern is painful if you are not a physicist: too low level.
- Very hard to prove general results based on example patterns. The physicists' intuitions are so good that they rarely make wrong statements but their "proofs" tend to be demonstrations by example.
- No *systematic* understanding of how patterns can be composed.

Benefits of Formalization

- We give a precise textual syntax for patterns. We do not worry about the geometrical layout but refer to qubits by name.

Benefits of Formalization

- We give a precise textual syntax for patterns. We do not worry about the geometrical layout but refer to qubits by name.
- The language comes with a natural compositional structure: inductive definition of possible patterns.

Benefits of Formalization

- We give a precise textual syntax for patterns. We do not worry about the geometrical layout but refer to qubits by name.
- The language comes with a natural compositional structure: inductive definition of possible patterns.
- We give a precise operational semantics and denotational semantics for the patterns.

Benefits of Formalization

- We give a precise textual syntax for patterns. We do not worry about the geometrical layout but refer to qubits by name.
- The language comes with a natural compositional structure: inductive definition of possible patterns.
- We give a precise operational semantics and denotational semantics for the patterns.
- We develop a *calculus* of patterns and using rewriting theory arguments show that all patterns can be put in a normal form.

The Syntax of Patterns

- Type: (V, I, O), $I \cap O$ need not be empty.

The Syntax of Patterns

- Type: (V, I, O), $I \cap O$ need not be empty.
- E_{ij} entangle i and j; this is a controlled-Z.

The Syntax of Patterns

- Type: (V, I, O), $I \cap O$ need not be empty.
- E_{ij} entangle i and j; this is a controlled-Z.
- M_i^α measure qubit i in a basis rotated by angle α.

The Syntax of Patterns

- Type: (V, I, O), $I \cap O$ need not be empty.
- E_{ij} entangle i and j; this is a controlled-Z.
- M_i^α measure qubit i in a basis rotated by angle α.
- X_i, Z_i apply σ_x or σ_z to qubit i.

The Syntax of Patterns

- Type: (V, I, O), $I \cap O$ need not be empty.
- E_{ij} entangle i and j; this is a controlled-Z.
- M_i^α measure qubit i in a basis rotated by angle α.
- X_i, Z_i apply σ_x or σ_z to qubit i.
- Programs are just sequences of commands read from right to left.

Dependency Propagation

- Both corrections and measurements may depend on measurement outcomes: signals.

Dependency Propagation

- Both corrections and measurements may depend on measurement outcomes: signals.
- Signal expressions are $0, 1, s_i, s_i + s_j$. Here s_i is the result of the measurement on qubit i.

Dependency Propagation

- Both corrections and measurements may depend on measurement outcomes: signals.
- Signal expressions are $0, 1, s_i, s_i + s_j$. Here s_i is the result of the measurement on qubit i.
- We write ${}^t[M_i^\alpha]^s$ for measurement $[M_i^\alpha]$ modified by signals s and t.

Dependency Propagation

- Both corrections and measurements may depend on measurement outcomes: signals.
- Signal expressions are $0, 1, s_i, s_i + s_j$. Here s_i is the result of the measurement on qubit i.
- We write ${}^t[M_i^\alpha]^s$ for measurement $[M_i^\alpha]$ modified by signals s and t.
- X_i^s, Z_i^s: dependent corrections.

Restrictions on Patterns

(D0) no command depends on an outcome not yet measured;

Restrictions on Patterns

(D0) no command depends on an outcome not yet measured;

(D1) no command acts on a qubit already measured;

Restrictions on Patterns

(D0) no command depends on an outcome not yet measured;

(D1) no command acts on a qubit already measured;

(D2) no command acts on a qubit not yet prepared, unless it is an input qubit;

Restrictions on Patterns

(D0) no command depends on an outcome not yet measured;

(D1) no command acts on a qubit already measured;

(D2) no command acts on a qubit not yet prepared, unless it is an input qubit;

(D3) a qubit i is measured if and only if i is not an output.

The Execution of Patterns

Entangle according to the E commands, then measure the qubits as indicated by the M commands and finally apply the corrections.

An Example Pattern

$$\mathcal{H} = (\{1,2\},\{1\},\{2\},X_2^{s_1}M_1^0E_{12}).$$

If the input is $\alpha|0\rangle + \beta|1\rangle$ then after E we get

$$\frac{1}{\sqrt{2}}[\alpha(|00\rangle + |01\rangle) + \beta(|10\rangle - |11\rangle).$$

After the measurement there are two possible outcomes:

$$\frac{1}{2}[(\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle] \text{ or } \frac{1}{2}[(\alpha-\beta)|0\rangle + (\alpha+\beta)|1\rangle].$$

The correction only kicks in for the second branch and it makes the two outcomes identical.

This pattern implements Hadamard.

Semantics

- Operational semantics is given as a probabilistic transition system.

Semantics

- Operational semantics is given as a probabilistic transition system.
- The denotational semantics associates to each pattern a certain type of operator (a completely positive map, for those who know and care).

Semantics

- Operational semantics is given as a probabilistic transition system.
- The denotational semantics associates to each pattern a certain type of operator (a completely positive map, for those who know and care).
- The proof that the two semantics agree is easy.

Composing Patterns 1

Two patterns $\mathcal{P}_1$ and $\mathcal{P}_2$ may be composed if $V_1 \cap V_2 = O_1 = I_2$.

The composite pattern $\mathcal{P}_2\mathcal{P}_1$ is defined as:

— $V := V_1 \cup V_2$, $I = I_1$, $O = O_2$,

— commands are concatenated.

Composing Patterns 2

Two patterns $\mathcal{P}_1$ and $\mathcal{P}_2$ may be tensored if $V_1 \cap V_2 = \emptyset$. The tensor pattern $\mathcal{P}_1 \otimes \mathcal{P}_2$ is defined as:

— $V = V_1 \cup V_2$, $I = I_1 \cup I_2$, and $O = O_1 \cup O_2$,

— commands are concatenated.

Some Benefits

- Composing patterns makes it easy to put together known patterns.

Some Benefits

- Composing patterns makes it easy to put together known patterns.
- We use the semantics to show that our pattern language is universal.

Some Benefits

- Composing patterns makes it easy to put together known patterns.
- We use the semantics to show that our pattern language is universal.
- We came up with a striking new implementation of controlled unitary; only 14 qubits instead of $40+$ known before.

Some Benefits

- Composing patterns makes it easy to put together known patterns.
- We use the semantics to show that our pattern language is universal.
- We came up with a striking new implementation of controlled unitary; only 14 qubits instead of $40+$ known before.
- We came up with a new - very simple - set of generators for unitaries as part of our proof of universality. [DKP Phys. Rev. A. Dec 2005]

A Huge Problem

Composing patterns ruins the nice EMC form of the patterns.

This form is very important if we want to avoid generating new entanglements on the fly.

Rewriting Rules

Using the algebra of the Pauli operators and qubits we showed how to define a rewrite system for patterns. These rules allow one to flip the order of certain commands. Example

$$E_{ij} X_i^s = X_i^s Z_j^s E_{ij}$$

which we orient as a rewrite rule

$$E_{ij} X_i^s \Rightarrow X_i^s Z_j^s E_{ij}.$$

Operators on disjoint qubits commute.

Standardization

- The rewriting process terminates and results in a pattern which is in the EMC form.

Standardization

- The rewriting process terminates and results in a pattern which is in the EMC form.
- Thus we can freely combine patterns and run it through the standardization engine to ensure that it is in EMC form.

Distributed computation in the 1W model

- One can group collections of qubits into locations to give a **distributed** model [DDKP 05].

Distributed computation in the 1W model

- One can group collections of qubits into locations to give a **distributed** model [DDKP 05].
- One can analyze classical distributed computation problems in the quantum setting, e.g. leader election [DP 06]

Distributed computation in the 1W model

- One can group collections of qubits into locations to give a **distributed** model [DDKP 05].
- One can analyze classical distributed computation problems in the quantum setting, e.g. leader election [DP 06]
- One can discuss epistemic concepts in a quantum setting and analyze knowledge flow in e.g. teleportation [DP05]

Using entanglement for Leader Election

- Suppose that two agents want to choose one of themselves as a leader and they share a Bell pair or, if there are three agents, they share $W_3 = |001\rangle + |010\rangle + |100\rangle$.

Using entanglement for Leader Election

- Suppose that two agents want to choose one of themselves as a leader and they share a Bell pair or, if there are three agents, they share $W_3 = |001\rangle + |010\rangle + |100\rangle$.
- They can each measure in the basis $|0\rangle, |1\rangle$; the one who gets $|1\rangle$ is the leader.

Using entanglement for Leader Election

- Suppose that two agents want to choose one of themselves as a leader and they share a Bell pair or, if there are three agents, they share $W_3 = |001\rangle + |010\rangle + |100\rangle$.
- They can each measure in the basis $|0\rangle, |1\rangle$; the one who gets $|1\rangle$ is the leader.
- Each agent has the same chance of getting elected, the process is guaranteed to terminate in one step. Exactly what is classically impossible!

Conclusions

- The one-way model is based on primitive fundamental concepts and has some attractions from the point of view of physical implementation.

Conclusions

- The one-way model is based on primitive fundamental concepts and has some attractions from the point of view of physical implementation.
- We have benefited from the formalization of measurement-based computation: EMC form, composing patterns, succinct representations.

Conclusions

- The one-way model is based on primitive fundamental concepts and has some attractions from the point of view of physical implementation.
- We have benefited from the formalization of measurement-based computation: EMC form, composing patterns, succinct representations.
- In fact there are several measurement calculi and translations between them which show how the models are related.

Conclusions

- The one-way model is based on primitive fundamental concepts and has some attractions from the point of view of physical implementation.
- We have benefited from the formalization of measurement-based computation: EMC form, composing patterns, succinct representations.
- In fact there are several measurement calculi and translations between them which show how the models are related.
- The one-way quantum computer plays a central role in relating these models.

What is to be done

- We need to show how higher-level models (e.g. Selinger's Quantum Programming Language) can be translated into the 1WQC.

What is to be done

- We need to show how higher-level models (e.g. Selinger's Quantum Programming Language) can be translated into the 1WQC.
- Understand quantum analogues of process algebras and equivalences. Good test: is teleportation "equivalent" to sending a qubit?

What is to be done

- We need to show how higher-level models (e.g. Selinger's Quantum Programming Language) can be translated into the 1WQC.
- Understand quantum analogues of process algebras and equivalences. Good test: is teleportation "equivalent" to sending a qubit?
- Understand resource inequalities: Igor Devetak, Aram Harrow and Andreas Winter have written a very interesting paper that should stimulate process algebraists.

What is to be done

- We need to show how higher-level models (e.g. Selinger's Quantum Programming Language) can be translated into the 1WQC.
- Understand quantum analogues of process algebras and equivalences. Good test: is teleportation "equivalent" to sending a qubit?
- Understand resource inequalities: Igor Devetak, Aram Harrow and Andreas Winter have written a very interesting paper that should stimulate process algebraists.