The Search for Structure in Quantum Computation

Prakash Panangaden
on sabbatical at:
Oxford University,
on leave from:
McGill University.

Outline

Outline

What are basic themes in Computer Science?

Outline

What are basic themes in Computer Science?

What makes quantum mechanics so strange?

Outline

What are basic themes in Computer Science?

What makes quantum mechanics so strange?

Why shouldn't we leave it to physicists?

Outline

What are basic themes in Computer Science?

What makes quantum mechanics so strange?

Why shouldn't we leave it to physicists?

What does *our* expertise buy us?

Outline

What are basic themes in Computer Science?

What makes quantum mechanics so strange?

Why shouldn't we leave it to physicists?

What does *our* expertise buy us?

What challenges are open to us?

Some basic themes

Some basic themes

Understanding structure: *the* fundamental theme.

Some basic themes

Understanding structure: *the* fundamental theme.

- How are systems structured?

Some basic themes

Understanding structure: *the* fundamental theme.

- How are systems structured?
- How is behaviour described?

Some basic themes

Understanding structure: *the* fundamental theme.

- How are systems structured?
- How is behaviour described?
- How do behavioural descriptions *compose*?

Some basic themes

Understanding structure: *the* fundamental theme.

- How are systems structured?
- How is behaviour described?
- How do behavioural descriptions *compose*?
- How do we *verify* systems?

Some basic themes

Understanding structure: *the* fundamental theme.

- How are systems structured?
- How is behaviour described?
- How do behavioural descriptions *compose*?
- How do we *verify* systems?
- How do we design systems?

In the 1960s and 1970s it was understood that programs should be structured: control flow structures, block structure, type systems, modules etc.

In the 1960s and 1970s it was understood that programs should be structured: control flow structures, block structure, type systems, modules etc.

After a struggle it was understood that sequential deterministic programs denoted functions

In the 1960s and 1970s it was understood that programs should be structured: control flow structures, block structure, type systems, modules etc.

After a struggle it was understood that sequential deterministic programs denoted functions

and that when programs are combined, the functions denoting their meanings are combined

In the 1960s and 1970s it was understood that programs should be structured: control flow structures, block structure, type systems, modules etc.

After a struggle it was understood that sequential deterministic programs denoted functions

and that when programs are combined, the functions denoting their meanings are combined

according to ordinary function composition.

In the 1960s and 1970s it was understood that programs should be structured: control flow structures, block structure, type systems, modules etc.

After a struggle it was understood that sequential deterministic programs denoted functions

and that when programs are combined, the functions denoting their meanings are combined

according to ordinary function composition.

Soon after it was realized that concurrent programs could not be modelled by functions *or even by relations*.

The theory of processes was born to make sense of systems featuring concurrency and nondeterminism.

The theory of processes was born to make sense of systems featuring concurrency and nondeterminism.

It expanded to include real-time systems and probabilistic systems and even continuous dynamics.

The theory of processes was born to make sense of systems featuring concurrency and nondeterminism.

It expanded to include real-time systems and probabilistic systems and even continuous dynamics.

It is still active and is reaching a high level of abstraction and internal mathematical beauty: coalgebras, monads, presheaf models etc.

The theory of processes was born to make sense of systems featuring concurrency and nondeterminism.

It expanded to include real-time systems and probabilistic systems and even continuous dynamics.

It is still active and is reaching a high level of abstraction and internal mathematical beauty: coalgebras, monads, presheaf models etc.

But quantum computation poses entirely new challenges!

Quantum Statistics

Quantum Statistics

- You have two boxes, A and B, and two particles that can each be in either box with equal probability. What is the probability that there is one particle in each box?

Quantum Statistics

- You have two boxes, A and B, and two particles that can each be in either box with equal probability. What is the probability that there is one particle in each box?
- If you answered 1/2 you are correct classically, but this is not what happens in quantum mechanics!

Quantum Statistics

- You have two boxes, A and B, and two particles that can each be in either box with equal probability. What is the probability that there is one particle in each box?
- If you answered 1/2 you are correct classically, but this is not what happens in quantum mechanics!
- Depending on the type of particle the answer could be 1/3 (bosons) or 1 (fermions).

At lunch yesterday:

At lunch yesterday:

Holger: Quantum systems are just continuous-time Markov chains!

At lunch yesterday:

Holger: Quantum systems are just continuous-time Markov chains!

Quantum systems do indeed have probabilistic features but

At lunch yesterday:

Holger: Quantum systems are just continuous-time Markov chains!

Quantum systems do indeed have probabilistic features but there are entire new aspects.

At lunch yesterday:

Holger: Quantum systems are just continuous-time Markov chains!

Quantum systems do indeed have probabilistic features but

there are entire new aspects.

Indeed the probabilistic aspects are not what makes quantum mechanics tricky.

At lunch yesterday:

Holger: Quantum systems are just continuous-time Markov chains!

Quantum systems do indeed have probabilistic features but

there are entire new aspects.

Indeed the probabilistic aspects are not what makes quantum mechanics tricky.

There are complex numbers and interference which blatantly violate basic commonsense rules of logic.

The Setting

There are two distinct scenarios:

The Setting

There are two distinct scenarios:

(1) using the power of quantum computation to achieve algorithmic speed-ups and

The Setting

There are two distinct scenarios:

(1) using the power of quantum computation to achieve algorithmic speed-ups and

(2) using the laws of quantum mechanics to guarantee privacy in communication.

The Setting

There are two distinct scenarios:

(1) using the power of quantum computation to achieve algorithmic speed-ups and

(2) using the laws of quantum mechanics to guarantee privacy in communication.

I would like to add a third: using the *non-local* nature of quantum computation to achieve distributed computing tasks.

Whether we can build a quantum "computer" is not important!!

Whether we can build a quantum “computer”
is not important!!

Can we reason about quantum communication protocols?

Whether we can build a quantum "computer"
is not important!!

Can we reason about quantum communication protocols?

Can we reason about security in the quantum setting?

Whether we can build a quantum "computer" is not important!!

Can we reason about quantum communication protocols?

Can we reason about security in the quantum setting?

Quantum devices are "out there" and communication protocols have been implemented over tens of kilometers.

Whether we can build a quantum "computer"
is not important!!

Can we reason about quantum communication protocols?

Can we reason about security in the quantum setting?

Quantum devices are "out there" and communication protocols have been implemented over tens of kilometers.

We need to get engaged in this enterprise because:

Whether we can build a quantum "computer"
is not important!!

Can we reason about quantum communication protocols?

Can we reason about security in the quantum setting?

Quantum devices are "out there" and communication protocols have been implemented over tens of kilometers.

We need to get engaged in this enterprise because:

(a) it is of fundamental interest and *we* can contribute,

Whether we can build a quantum "computer" is not important!!

Can we reason about quantum communication protocols?

Can we reason about security in the quantum setting?

Quantum devices are "out there" and communication protocols have been implemented over tens of kilometers.

We need to get engaged in this enterprise because:

(a) it is of fundamental interest and *we* can contribute,

(b) if we don't physics will take all the money and run!

The first surprise: superposition.

The first surprise: superposition.

Quantum systems can be in two "states" at the same time!

The first surprise: superposition.

Quantum systems can be in two “states” at the same time!

This is *not* the same as being in a probabilistic mixture.

The first surprise: superposition.

Quantum systems can be in two “states” at the same time!

This is *not* the same as being in a probabilistic mixture.

Consider photons, they can be polarized in various ways: vertically, horizontally *and in linear combinations of these*.

The first surprise: superposition.

Quantum systems can be in two "states" at the same time!

This is *not* the same as being in a probabilistic mixture.

Consider photons, they can be polarized in various ways: vertically, horizontally *and in linear combinations of these*.

I write $|\updownarrow\rangle$ to denote a vertically polarized photon and $|\leftrightarrow\rangle$ for a horizontally polarized photon.

The first surprise: superposition.

Quantum systems can be in two "states" at the same time!

This is *not* the same as being in a probabilistic mixture.

Consider photons, they can be polarized in various ways: vertically, horizontally *and in linear combinations of these*.

I write $|\updownarrow\rangle$ to denote a vertically polarized photon and $|\leftrightarrow\rangle$ for a horizontally polarized photon.

There are polarizing filters that **only** let through photons that are polarized the same way as the filters.

The first surprise: superposition.

Quantum systems can be in two "states" at the same time!

This is *not* the same as being in a probabilistic mixture.

Consider photons, they can be polarized in various ways: vertically, horizontally *and in linear combinations of these*.

I write $|\updownarrow\rangle$ to denote a vertically polarized photon and $|\leftrightarrow\rangle$ for a horizontally polarized photon.

There are polarizing filters that **only** let through photons that are polarized the same way as the filters.

More precisely if the filter makes an angle θ with the photon polarization then the photon gets through with probability $\cos^2\theta$.

In the lab we can prepare photons that are in a superposed state of horizontal and vertical polarization:

In the lab we can prepare photons that are in a superposed state of horizontal and vertical polarization:

$$|\swarrow\!\!\!\!\nearrow\rangle = \frac{1}{\sqrt{2}}[|\updownarrow\rangle + |\leftrightarrow\rangle].$$

In the lab we can prepare photons that are in a superposed state of horizontal and vertical polarization:

$$|\swarrow\!\!\nearrow\rangle = \frac{1}{\sqrt{2}}[|\updownarrow\rangle + |\leftrightarrow\rangle].$$

We can also prepare a $\frac{1}{2}$, $\frac{1}{2}$ *mixture* of $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ photons.

In the lab we can prepare photons that are in a superposed state of horizontal and vertical polarization:

$$|\nearrow\!\!\!\!\swarrow\rangle = \frac{1}{\sqrt{2}}[|\updownarrow\rangle + |\leftrightarrow\rangle].$$

We can also prepare a $\frac{1}{2}$, $\frac{1}{2}$ *mixture* of $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ photons.

Is there a difference?

In the lab we can prepare photons that are in a superposed state of horizontal and vertical polarization:

$$|\swarrow\!\!\!\nearrow\rangle = \frac{1}{\sqrt{2}}[|\updownarrow\rangle + |\leftrightarrow\rangle].$$

We can also prepare a $\frac{1}{2}$, $\frac{1}{2}$ *mixture* of $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ photons.

Is there a difference?

Yes! A filter aligned at 45° will let all the superposed photons through, but only half of the mixture.

In the lab we can prepare photons that are in a superposed state of horizontal and vertical polarization:

$$|\nearrow\!\!\!\!\swarrow\rangle = \frac{1}{\sqrt{2}}[|\updownarrow\rangle + |\leftrightarrow\rangle].$$

We can also prepare a $\frac{1}{2}$, $\frac{1}{2}$ *mixture* of $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ photons.

Is there a difference?

Yes! A filter aligned at $45°$ will let all the superposed photons through, but only half of the mixture.

Superposition is observably different from a mixture.

In the lab we can prepare photons that are in a superposed state of horizontal and vertical polarization:

$$|\swarrow\!\!\!\nearrow\rangle = \frac{1}{\sqrt{2}}[|\updownarrow\rangle + |\leftrightarrow\rangle].$$

We can also prepare a $\frac{1}{2}$, $\frac{1}{2}$ *mixture* of $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ photons.

Is there a difference?

Yes! A filter aligned at $45°$ will let all the superposed photons through, but only half of the mixture.

Superposition is observably different from a mixture.

Quantum systems are not "just" probabilistic.

Non-locality and Entanglement

A key idea due to Einstein, Podolsky and Rosen (1935) which was intended as an attack on quantum mechanics. Turned out to be revolutionary and led to the notion of non-locality and entanglement.

EPR - Bohm's version

Two-state quantum particle: $|\uparrow\rangle$ for spin up and $|\downarrow\rangle$ for spin down.

Two-particle basis states written: $|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle$ and $|\downarrow\downarrow\rangle$.

EPR - Bohm's version

Two-state quantum particle: $|\uparrow\rangle$ for spin up and $|\downarrow\rangle$ for spin down.

Two-particle basis states written: $|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle$ and $|\downarrow\downarrow\rangle$.

Consider the state: $\frac{1}{\sqrt{2}}[|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle]$. This state can be *prepared in a laboratory*. Measuring the spin of one particle "makes" the other one have the opposite spin.

Information is *nonlocal*, a quantum mechanical state is nonlocal. We can substitute entanglement for communication.

- The probabilistic behaviour of quantum mechanics is inherent.

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

- 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

- 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,

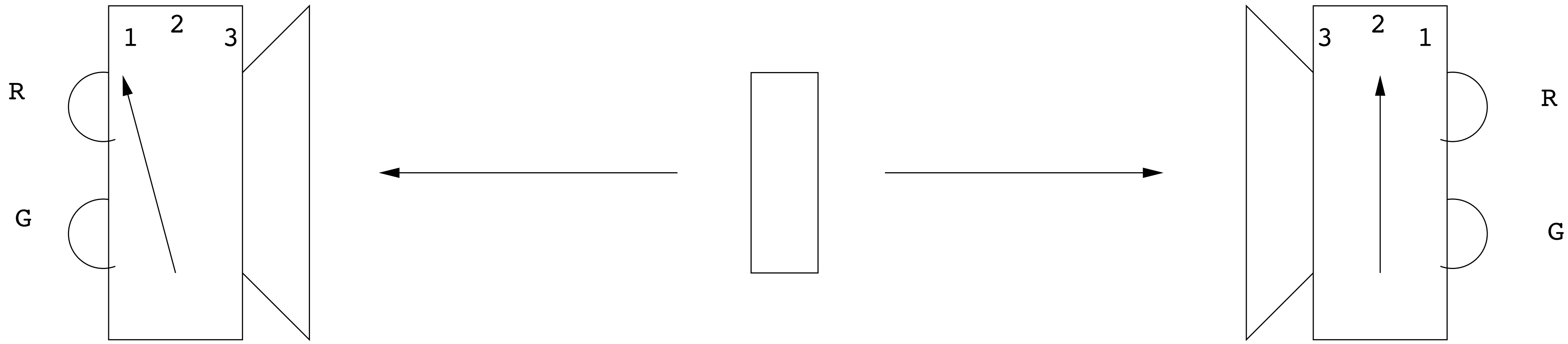
- The probabilistic behaviour of quantum mechanics is inherent.
- It is not possible to explain the probabilities as an abstraction of some hidden deterministic behaviour.
- More precisely: there is no theory that is
  - local,
  - causal,

- 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.

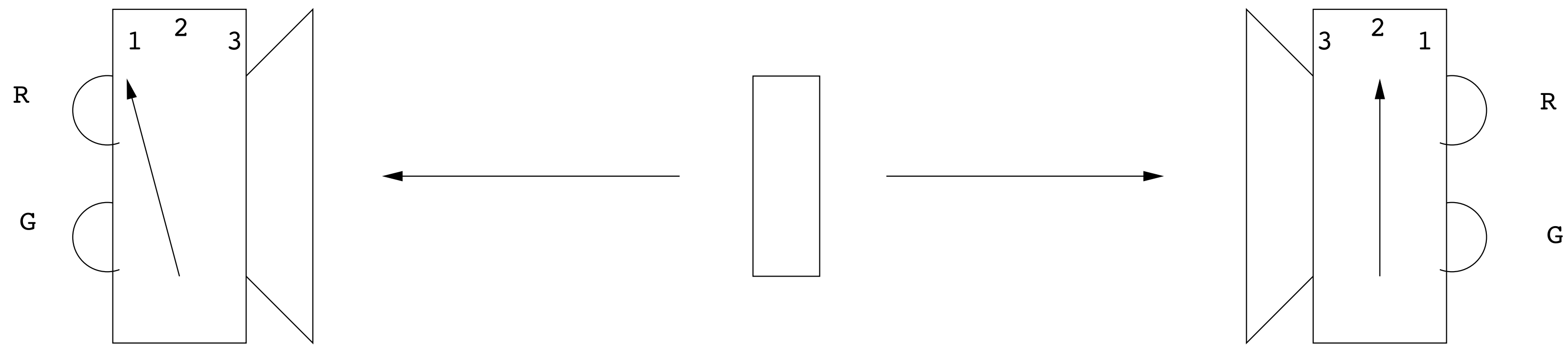
A simple version of Bell's inequality that can be understood easily.



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.



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!

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

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.*

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.*

We write GGR for a typical particle type: it means that for the detector settings 1,2 and 3 respectively the light flashes green, green and red respectively.

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

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.

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: $RRG, RGR, GRR, GGR, GRG, RGG$.

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.

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 experiment can be realized in the lab.

The data do not support the reasoning above: when the settings are different the lights match only a $\frac{1}{4}$ of the time!

What is wrong with the reasoning?

Why did we assume that there was something that fixed the outcome *deterministically*?

Why did we assume that there was something that fixed the outcome *deterministically*?

Because otherwise we cannot explain why the lights *always* agree when the settings are the same when we assume that what happens at each detector is independent of what happens at the other.

Why did we assume that there was something that fixed the outcome *deterministically*?

Because otherwise we cannot explain why the lights *always* agree when the settings are the same when we assume that what happens at each detector is independent of what happens at the other.

Something non-local is going on.

Why did we assume that there was something that fixed the outcome *deterministically*?

Because otherwise we cannot explain why the lights *always* agree when the settings are the same when we assume that what happens at each detector is independent of what happens at the other.

Something non-local is going on.

What kinds of transition systems are these?
We have studied all kinds of transition systems,
we should analyze *from the perspective of transition system theory* the kinds of systems that arise in quantum mechanics.

Measurement

Measurement

- Measurement is an **interaction** between system and apparatus.

Measurement

- Measurement is an **interaction** between system and apparatus.

- Measurements do not uncover some pre-existing physical property of a system. There is no **objective property** being measured.

Measurement

- Measurement is an **interaction** between system and apparatus.

- Measurements do not uncover some pre-existing physical property of a system. There is no **objective property** being measured.

- The **record** or **result** of a measurement is an objective property.

The Stern-Gerlach Experiment

- Send neutral atoms through a varying magnetic field.
- Observe two peaks - the beam is split into an "up" and a "down."
- Rotate the apparatus and still observe the beam split in two.

No Objective Values?

No Objective Values?

The Stern-Gerlach experiment measures a component of the magnetic moment: a vector quantity.

No Objective Values?

The Stern-Gerlach experiment measures a component of the magnetic moment: a vector quantity.

Along *any axis* the value is $+1$ or -1 (in some units).

No Objective Values?

The Stern-Gerlach experiment measures a component of the magnetic moment: a vector quantity.

Along *any axis* the value is $+1$ or -1 (in some units).

What if we measured it along three axes, $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ at $120°$ to each other?

No Objective Values?

The Stern-Gerlach experiment measures a component of the magnetic moment: a vector quantity.

Along *any axis* the value is $+1$ or -1 (in some units).

What if we measured it along three axes, $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ at $120°$ to each other?

Note that $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 = 0$. So the sum of the measured components must add up to zero.

No Objective Values?

The Stern-Gerlach experiment measures a component of the magnetic moment: a vector quantity.

Along *any axis* the value is $+1$ or -1 (in some units).

What if we measured it along three axes, $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ at 120° to each other?

Note that $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 = 0$. So the sum of the measured components must add up to zero.

But 3 number chosen from the set $\{+1, -1\}$ cannot add up to zero!

Contextuality

Contextuality

Some measurements interfere with each other.

Contextuality

Some measurements interfere with each other.

Thus certain sets of measurements are compatible, while others are not.

Contextuality

Some measurements interfere with each other.

Thus certain sets of measurements are compatible, while others are not.

We have seen such ideas in computer science: e.g. when we talk about *conflict* in event structures.

Contextuality

Some measurements interfere with each other.

Thus certain sets of measurements are compatible, while others are not.

We have seen such ideas in computer science: e.g. when we talk about *conflict* in event structures.

The sets of possible compatible measurements in which a given measurement can appear are the **contexts** for the given measurement.

Contextuality

Some measurements interfere with each other.

Thus certain sets of measurements are compatible, while others are not.

We have seen such ideas in computer science: e.g. when we talk about *conflict* in event structures.

The sets of possible compatible measurements in which a given measurement can appear are the **contexts** for the given measurement.

One would hope that the *possible* measurement outcomes would not depend on what else one *chooses* to measure.

Contextuality

Some measurements interfere with each other.

Thus certain sets of measurements are compatible, while others are not.

We have seen such ideas in computer science: e.g. when we talk about *conflict* in event structures.

The sets of possible compatible measurements in which a given measurement can appear are the **contexts** for the given measurement.

One would hope that the *possible* measurement outcomes would not depend on what else one *chooses* to measure.

This is called **non-contextuality**.

Kochen-Specker Theorem

Quantum mechanics is not non-contextual
or, quantum mechanics is contextual.

There is a compatible family M of quantum measurements such that the following statements contradict each other:

If A, B, C are in M and $C = A + B$
then $val(C) = val(A) + val(B)$
and similarly for products,

all the members of M have definite values.

Beautiful analysis due to Samson Abramsky

Beautiful analysis due to Samson Abramsky

Let $\mathcal{S}$ be a family of subsets of a finite set X. We say that $\mathcal{S}$ is a *KS family* if $\mathrm{card}(\mathcal{S})$ is odd, and for each $x \in X$, $c(x)$ is even, where:

$$c(x) = \mathrm{card}\{S \in \mathcal{S} | x \in S\}.$$

Beautiful analysis due to Samson Abramsky

Let $\mathcal{S}$ be a family of subsets of a finite set X. We say that $\mathcal{S}$ is a *KS family* if $\mathrm{card}(\mathcal{S})$ is odd, and for each $x \in X$, $c(x)$ is even, where:

$$c(x) = \mathrm{card}\{S \in \mathcal{S} | x \in S\}.$$

Let $\mathcal{S}$ be a KS family on X.
There is no function $\phi : X \to \{0, 1\}$ such that, for all $S \in \mathcal{S}$:

$$\sum_{x \in S} \phi(x) = 1.$$

Beautiful analysis due to Samson Abramsky

Let $\mathcal{S}$ be a family of subsets of a finite set X. We say that $\mathcal{S}$ is a *KS family* if $\mathrm{card}(\mathcal{S})$ is odd, and for each $x \in X$, $c(x)$ is even, where:

$$c(x) = \mathrm{card}\{S \in \mathcal{S} | x \in S\}.$$

Let $\mathcal{S}$ be a KS family on X.
There is no function $\phi : X \to \{0,1\}$ such that, for all $S \in \mathcal{S}$:

$$\sum_{x \in S} \phi(x) = 1.$$

Define $v = \sum_{S \in \mathcal{S}} \sum_{x \in S} \phi(x)$. This is clearly odd.

Beautiful analysis due to Samson Abramsky

Let $\mathcal{S}$ be a family of subsets of a finite set X. We say that $\mathcal{S}$ is a *KS family* if $\mathrm{card}(\mathcal{S})$ is odd, and for each $x \in X$, $c(x)$ is even, where:

$$c(x) = \mathrm{card}\{S \in \mathcal{S} | x \in S\}.$$

Let $\mathcal{S}$ be a KS family on X.
There is no function $\phi : X \to \{0, 1\}$ such that, for all $S \in \mathcal{S}$:

$$\sum_{x \in S} \phi(x) = 1.$$

Define $v = \sum_{S \in \mathcal{S}} \sum_{x \in S} \phi(x)$. This is clearly odd. However,

Beautiful analysis due to Samson Abramsky

Let $\mathcal{S}$ be a family of subsets of a finite set X. We say that $\mathcal{S}$ is a *KS family* if $\mathrm{card}(\mathcal{S})$ is odd, and for each $x \in X$, $c(x)$ is even, where:

$$c(x) = \mathrm{card}\{S \in \mathcal{S} | x \in S\}.$$

Let $\mathcal{S}$ be a KS family on X.
There is no function $\phi : X \to \{0, 1\}$ such that, for all $S \in \mathcal{S}$:

$$\sum_{x \in S} \phi(x) = 1.$$

Define $v = \sum_{S \in \mathcal{S}} \sum_{x \in S} \phi(x)$. This is clearly odd. However,

$$v = \sum_{x \in X} c(x)\phi(x)$$

Beautiful analysis due to Samson Abramsky

Let $\mathcal{S}$ be a family of subsets of a finite set X. We say that $\mathcal{S}$ is a *KS family* if $\mathrm{card}(\mathcal{S})$ is odd, and for each $x \in X$, $c(x)$ is even, where:

$$c(x) = \mathrm{card}\{S \in \mathcal{S} | x \in S\}.$$

Let $\mathcal{S}$ be a KS family on X.
There is no function $\phi : X \to \{0, 1\}$ such that, for all $S \in \mathcal{S}$:

$$\sum_{x \in S} \phi(x) = 1.$$

Define $v = \sum_{S \in \mathcal{S}} \sum_{x \in S} \phi(x)$. This is clearly odd. However,

$$v = \sum_{x \in X} c(x)\phi(x)$$ which is clearly even!

The usual proofs of Kochen-Specker are essentially clever constructions of KS sets satisfying the conditions of the proposition.

The usual proofs of Kochen-Specker are essentially clever constructions of KS sets satisfying the conditions of the proposition.

Why does say anything of interest?

The usual proofs of Kochen-Specker are essentially clever constructions of KS sets satisfying the conditions of the proposition.

Why does say anything of interest?

The state space of a common quantum system is the set of directions in 3-space.

The usual proofs of Kochen-Specker are essentially clever constructions of KS sets satisfying the conditions of the proposition.

Why does say anything of interest?

The state space of a common quantum system is the set of directions in 3-space.

If we measure it along three orthogonal directions we should get a 1 for one direction and 0 for the other two.

The usual proofs of Kochen-Specker are essentially clever constructions of KS sets satisfying the conditions of the proposition.

Why does say anything of interest?

The state space of a common quantum system is the set of directions in 3-space.

If we measure it along three orthogonal directions we should get a 1 for one direction and 0 for the other two.

In short we want the kind of ϕ mentioned in the proposition.

The usual proofs of Kochen-Specker are essentially clever constructions of KS sets satisfying the conditions of the proposition.

Why does say anything of interest?

The state space of a common quantum system is the set of directions in 3-space.

If we measure it along three orthogonal directions we should get a 1 for one direction and 0 for the other two.

In short we want the kind of ϕ mentioned in the proposition.

But people have constructed KS sets of triples of orthogonal directions!

There is no consistent assignment of the values of a property.

There is no consistent assignment of the values of a property.

The outcome is created by the measurement process, there is no “value” that can be assigned before the system is measured!

Composing Systems

A fundamental difference between quantum systems and classical systems is how we put subsystems together.

Composing Systems

A fundamental difference between quantum systems and classical systems is how we put subsystems together.

We combine systems by taking **tensor products** of the state spaces: $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$.

Composing Systems

A fundamental difference between quantum systems and classical systems is how we put subsystems together.

We combine systems by taking **tensor products** of the state spaces: $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$.

To describe the state of n bits I have to specify n boolean values.

Composing Systems

A fundamental difference between quantum systems and classical systems is how we put subsystems together.

We combine systems by taking **tensor products** of the state spaces: $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$.

To describe the state of n bits I have to specify n boolean values.

To describe the state of n qubits I have to specify 2^n complex numbers.

If V and W are vector spaces with bases $\{v_i\}$ and $\{w_j\}$ respectively then the tensor product is the vectors space with basis $\{v_i \otimes w_j\}$.

If V and W are vector spaces with bases $\{v_i\}$ and $\{w_j\}$ respectively then the tensor product is the vectors space with basis $\{v_i \otimes w_j\}$.

Note that there are vectors in the tensor product space that cannot be decomposed into products.

If V and W are vector spaces with bases $\{v_i\}$ and $\{w_j\}$ respectively then the tensor product is the vectors space with basis $\{v_i \otimes w_j\}$.

Note that there are vectors in the tensor product space that cannot be decomposed into products.

For example $v_1 \otimes w_1 + v_2 \otimes w_2$.

If V and W are vector spaces with bases $\{v_i\}$ and $\{w_j\}$ respectively then the tensor product is the vectors space with basis $\{v_i \otimes w_j\}$.

Note that there are vectors in the tensor product space that cannot be decomposed into products.

For example $v_1 \otimes w_1 + v_2 \otimes w_2$. This is entanglement!

If V and W are vector spaces with bases $\{v_i\}$ and $\{w_j\}$ respectively then the tensor product is the vectors space with basis $\{v_i \otimes w_j\}$.

Note that there are vectors in the tensor product space that cannot be decomposed into products.

For example $v_1 \otimes w_1 + v_2 \otimes w_2$. This is entanglement!

It gives quantum computation its power and is also the key ingredient of phenomena like teleportation.

If V and W are vector spaces with bases $\{v_i\}$ and $\{w_j\}$ respectively then the tensor product is the vectors space with basis $\{v_i \otimes w_j\}$.

Note that there are vectors in the tensor product space that cannot be decomposed into products.

For example $v_1 \otimes w_1 + v_2 \otimes w_2$. This is entanglement!

It gives quantum computation its power and is also the key ingredient of phenomena like teleportation.

There are *provably impossible* classical distributed computing tasks that can be done with suitable entangled states.

Categorical Quantum Mechanics

Abramsky, Coecke, Selinger, Landsman, Jacobs and others...

Categorical Quantum Mechanics

Abramsky, Coecke, Selinger, Landsman, Jacobs and others...

Axiomatize quantum mechanics in terms of dagger-compact categories:

Categorical Quantum Mechanics

Abramsky, Coecke, Selinger, Landsman, Jacobs and others...

Axiomatize quantum mechanics in terms of dagger-compact categories:

basic algebraic aspects of tensor product and reversibility and duality.

Categorical Quantum Mechanics

Abramsky, Coecke, Selinger, Landsman, Jacobs and others...

Axiomatize quantum mechanics in terms of dagger-compact categories:

basic algebraic aspects of tensor product and reversibility and duality.

Captures "abstract" quantum mechanics, one can explore "toy" quantum mechanics and ask what is the minimal structure needed to reveal key aspects of quantum mechanics.

A number of significant results have appeared in this field in the last couple of years:

A number of significant results have appeared in this field in the last couple of years:

A powerful diagrammatic notation for quantum computation: Selinger, Coecke, Paquette, Duncan, Kissinger.

A number of significant results have appeared in this field in the last couple of years:

A powerful diagrammatic notation for quantum computation: Selinger, Coecke, Paquette, Duncan, Kissinger.

A theory of complementary observables: Coecke, Duncan.

A number of significant results have appeared in this field in the last couple of years:

A powerful diagrammatic notation for quantum computation: Selinger, Coecke, Paquette, Duncan, Kissinger.

A theory of complementary observables: Coecke, Duncan.

A theory of classical structures: Coecke, Pavlovic, Vicary.

A number of significant results have appeared in this field in the last couple of years:

A powerful diagrammatic notation for quantum computation: Selinger, Coecke, Paquette, Duncan, Kissinger.

A theory of complementary observables: Coecke, Duncan.

A theory of classical structures: Coecke, Pavlovic, Vicary.

Quantum logic in dagger categories: Jacobs, Heunen.

A number of significant results have appeared in this field in the last couple of years:

A powerful diagrammatic notation for quantum computation: Selinger, Coecke, Paquette, Duncan, Kissinger.

A theory of complementary observables: Coecke, Duncan.

A theory of classical structures: Coecke, Pavlovic, Vicary.

Quantum logic in dagger categories: Jacobs, Heunen.

A categorical view of topological quantum computation: Paquette, P.

A number of significant results have appeared in this field in the last couple of years:

A powerful diagrammatic notation for quantum computation: Selinger, Coecke, Paquette, Duncan, Kissinger.

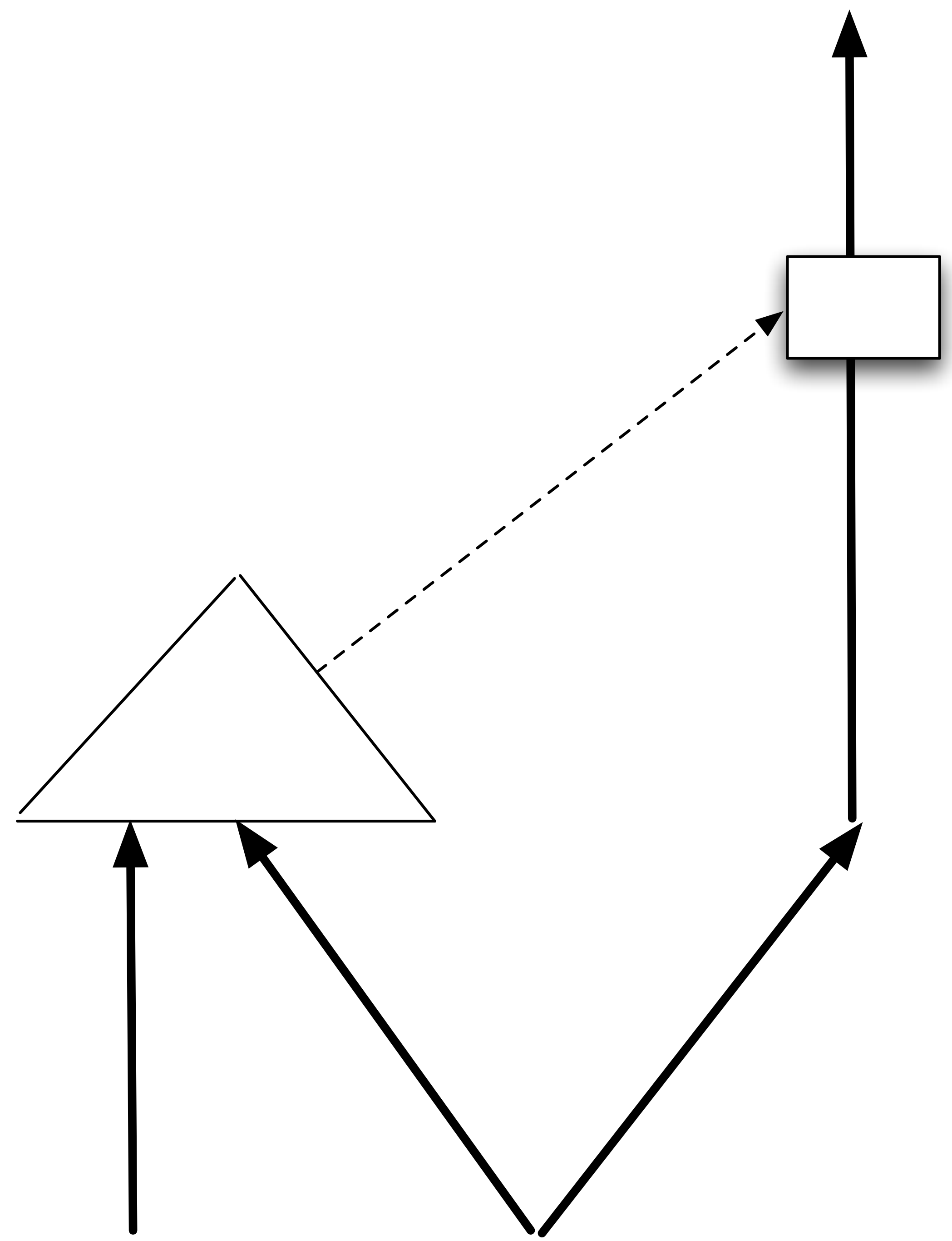
A theory of complementary observables: Coecke, Duncan.

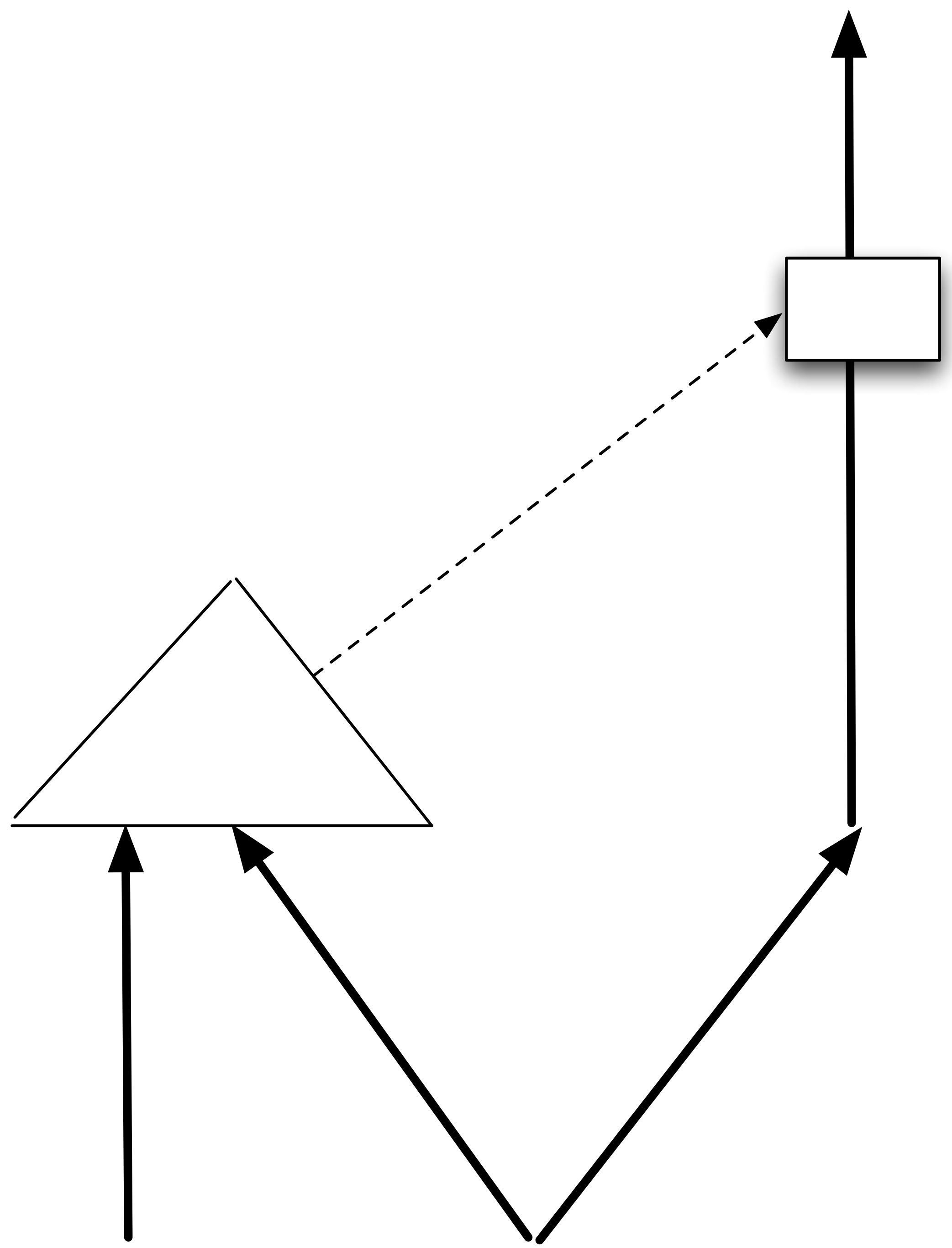
A theory of classical structures: Coecke, Pavlovic, Vicary.

Quantum logic in dagger categories: Jacobs, Heunen.

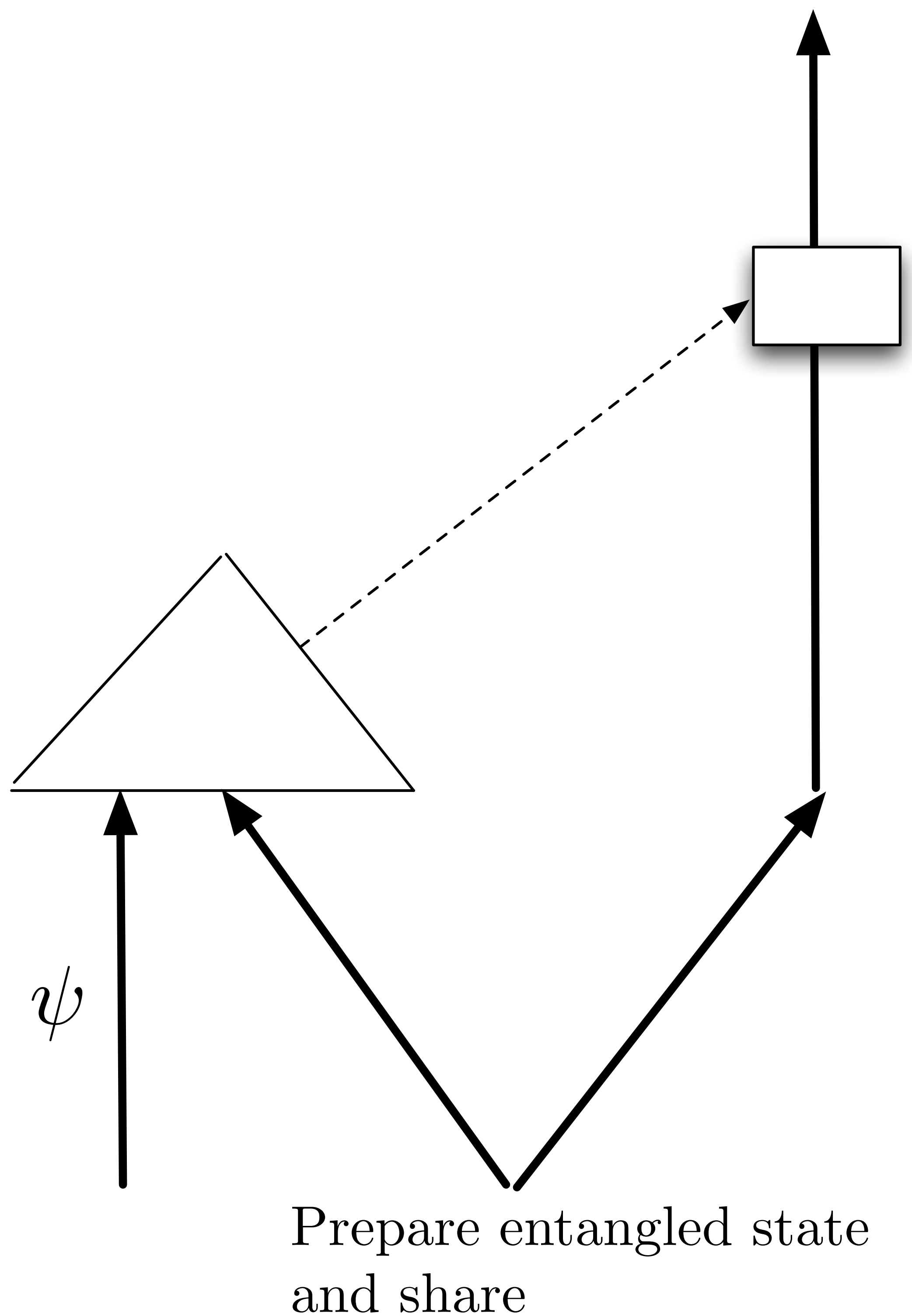
A categorical view of topological quantum computation: Paquette, P.

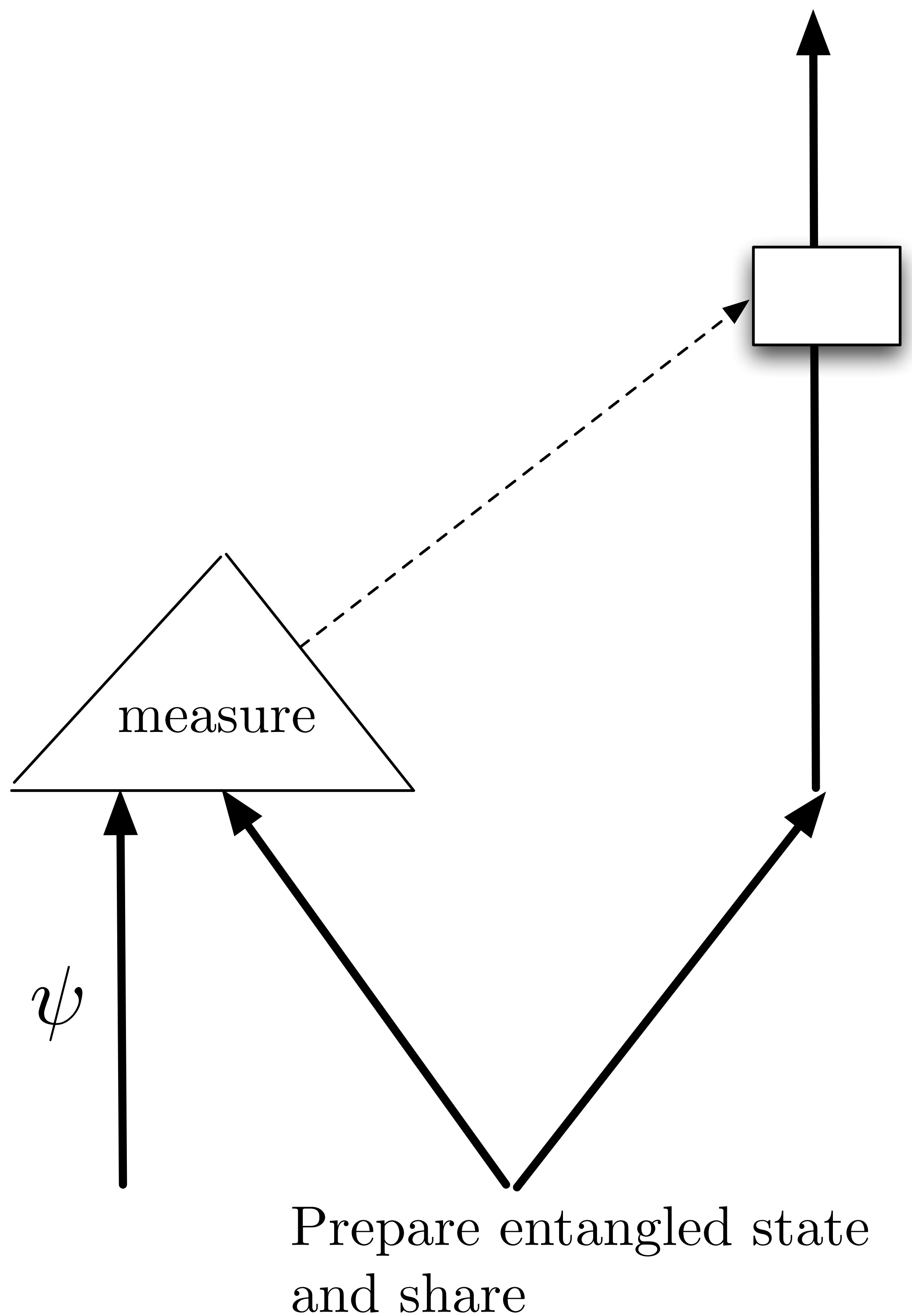
and more!

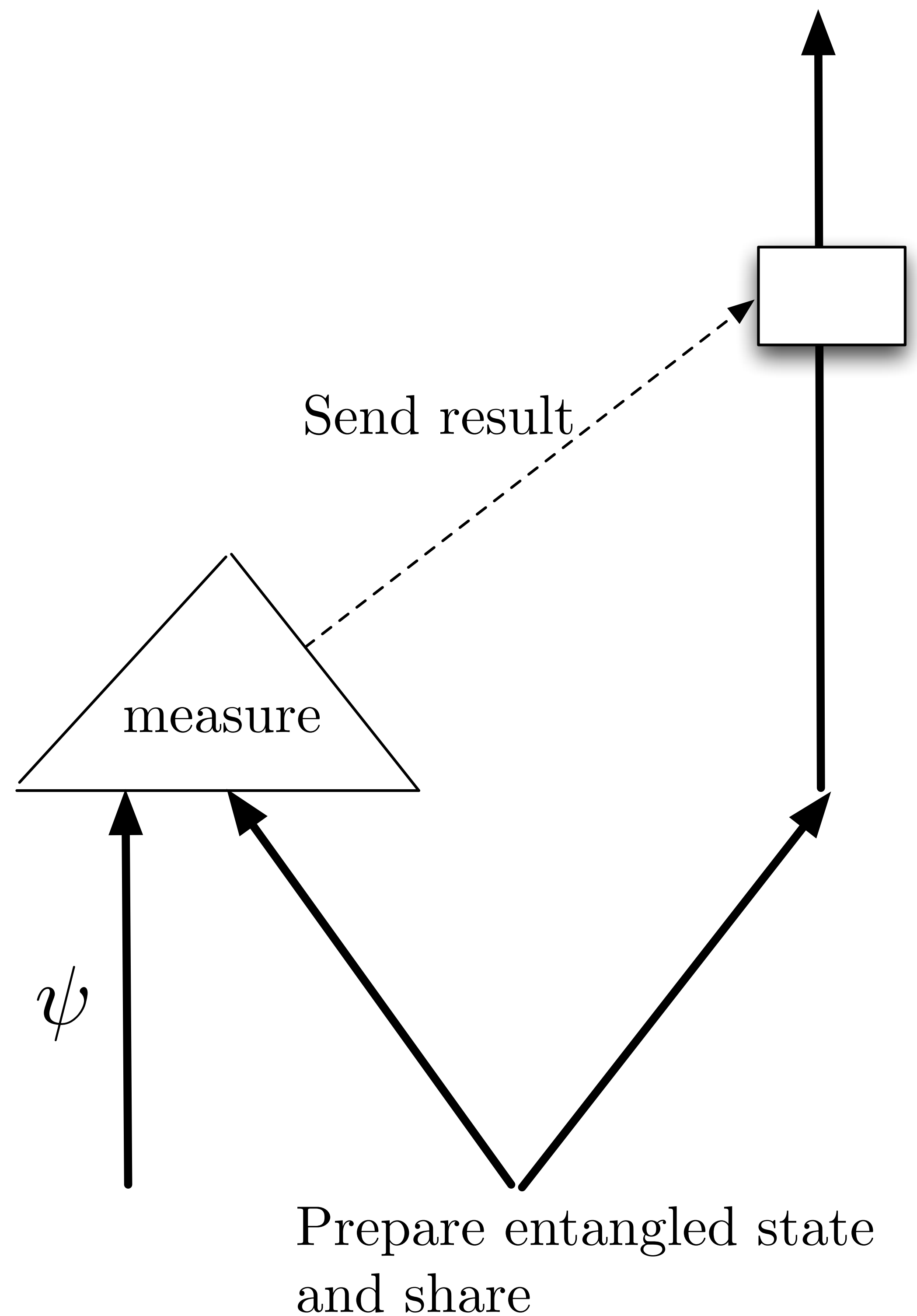


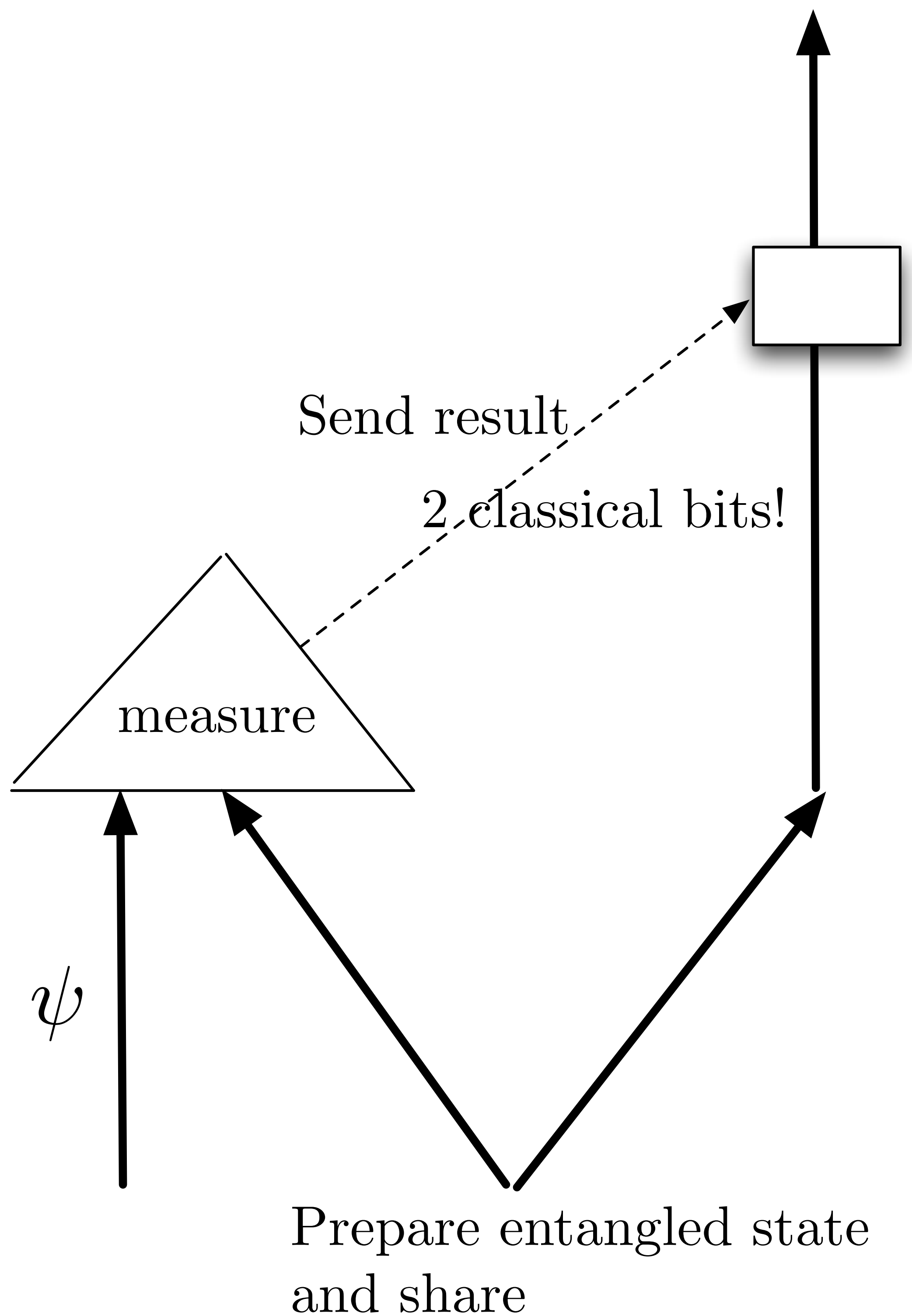


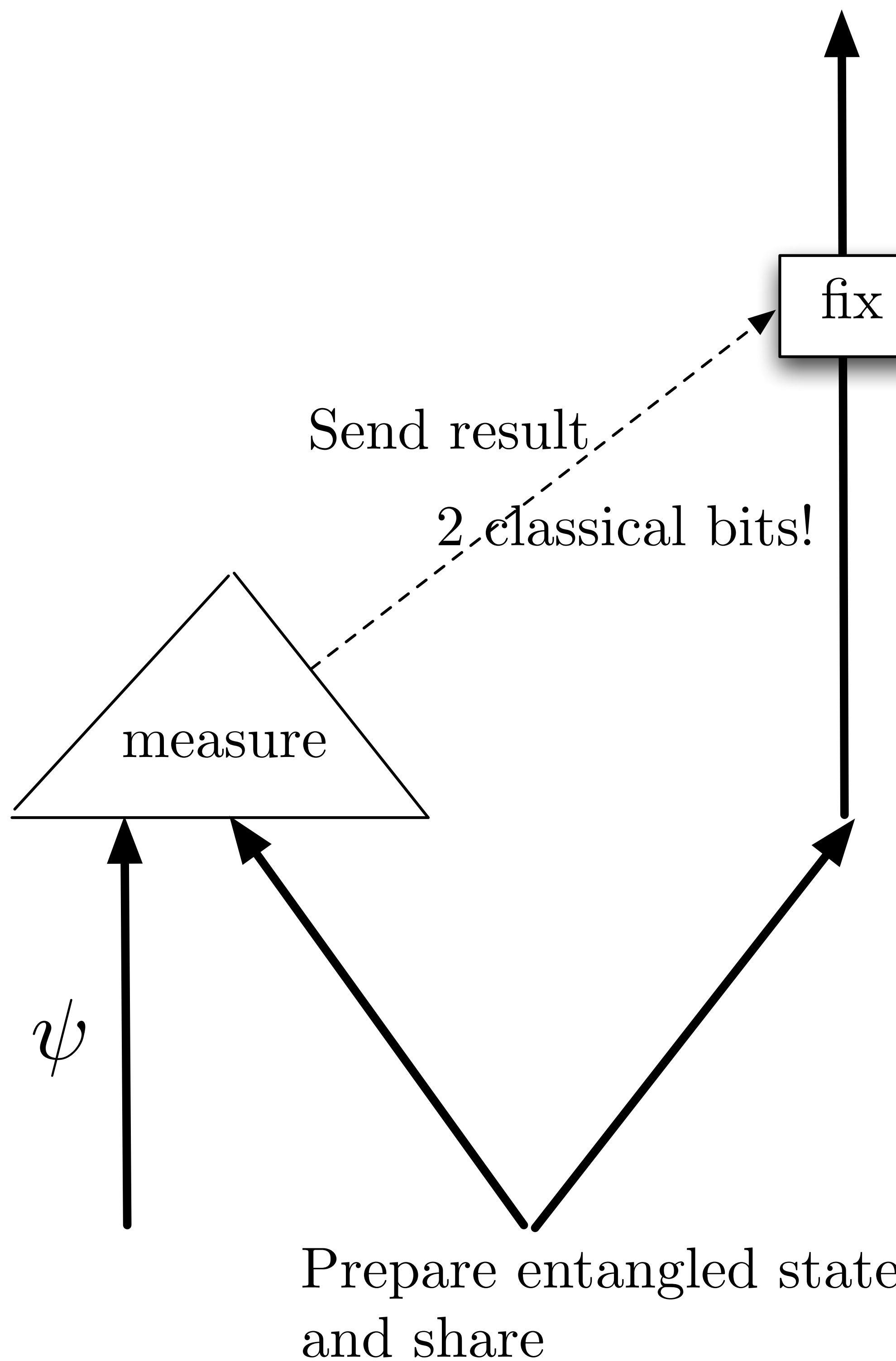
Prepare entangled state
and share

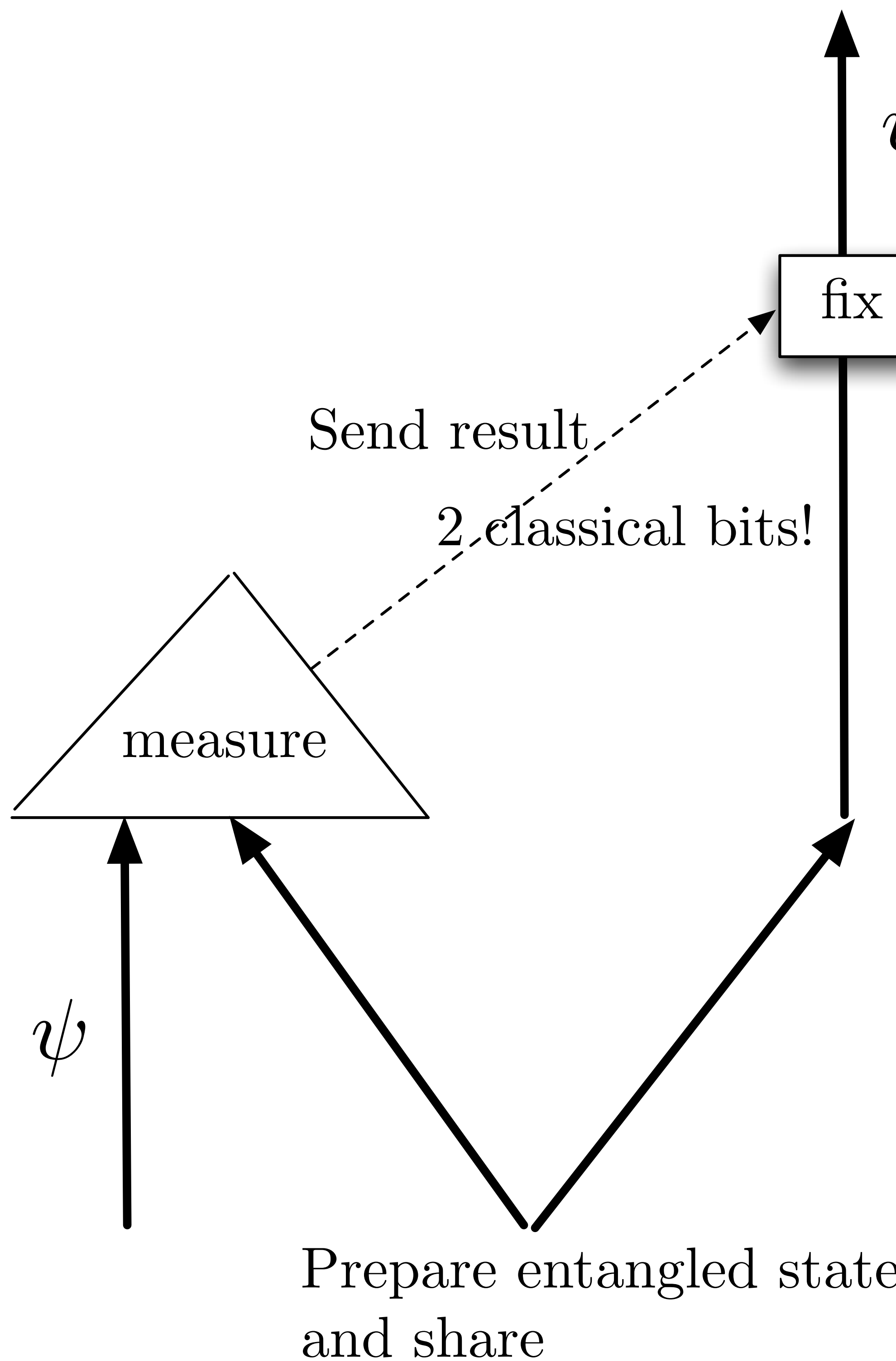

ψ
Prepare entangled state
and share


measure
ψ
Prepare entangled state
and share


Send result
measure
ψ
Prepare entangled state
and share


Send result
2 classical bits!
measure
ψ
Prepare entangled state and share


fix
Send result
2 classical bits!
measure
ψ
Prepare entangled state
and share



ψ
fix
Send result
2 classical bits!
measure
ψ
Prepare entangled state
and share

The Point of Teleportation

The result of a measurement tells you what fix 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?

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

The magic is that only one-qubit measurements and corrections are needed

The magic is that only one-qubit measurements and corrections are needed provided that one has the right type of entanglement.

The magic is that only one-qubit measurements and corrections are needed provided that one has the right type of entanglement.

Programs for computing in this model are called patterns.

The magic is that only one-qubit measurements and corrections are needed provided that one has the right type of entanglement.

Programs for computing in this model are called patterns.

Physicists described these patterns in terms of explicit layout of qubits on a grid. Extremely painful to follow.

The magic is that only one-qubit measurements and corrections are needed provided that one has the right type of entanglement.

Programs for computing in this model are called patterns.

Physicists described these patterns in terms of explicit layout of qubits on a grid. Extremely painful to follow.

Extremely hard to prove general results based on example patterns. The physicists intuitions are so good that they (almost) never make mistakes.

The magic is that only one-qubit measurements and corrections are needed provided that one has the right type of entanglement.

Programs for computing in this model are called patterns.

Physicists described these patterns in terms of explicit layout of qubits on a grid. Extremely painful to follow.

Extremely hard to prove general results based on example patterns. The physicists intuitions are so good that they (almost) never make mistakes.

But their proofs tend to be example demonstrations.

There was no *systematic* understanding of how patterns could be *composed*.

There was no *systematic* understanding of how patterns could be *composed*.

The Measurement Calculus [Danos, Kashefi, P. – JACM 2007]

A success story for the ideas from this community.

There was no *systematic* understanding of how patterns could be *composed*.

The Measurement Calculus [Danos, Kashefi, P. – JACM 2007]

A success story for the ideas from this community.

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

There was no *systematic* understanding of how patterns could be *composed*.

The Measurement Calculus [Danos, Kashefi, P. – JACM 2007]

A success story for the ideas from this community.

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 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.

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.

This allows one to program compositionally but in the end the composed program is rewritten to a normal form so that one never has to do on-the-fly entanglement.

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.

This allows one to program compositionally but in the end the composed program is rewritten to a normal form so that one never has to do on-the-fly entanglement.

A lot of work has been done since 2007 by Elham Kashefi and her many collaborators using this framework.

Things that this community can do for quantum computer science.

Things that this community can do for quantum computer science.

Verification of quantum protocols.

Things that this community can do for quantum computer science.

Verification of quantum protocols.

Yes, these are probabilistic systems, but a huge amount of manual preprocessing has to be done to extract some probabilistic model that can be checked using existing tools.

Things that this community can do for quantum computer science.

Verification of quantum protocols.

Yes, these are probabilistic systems, but a huge amount of manual preprocessing has to be done to extract some probabilistic model that can be checked using existing tools.

A good concept of weak bisimulation for quantum systems was only achieved *this year* [POPL 2011] by Yuan Feng, Runyao Duan and Mingsheng Ying.

Things that this community can do for quantum computer science.

Verification of quantum protocols.

Yes, these are probabilistic systems, but a huge amount of manual preprocessing has to be done to extract some probabilistic model that can be checked using existing tools.

A good concept of weak bisimulation for quantum systems was only achieved *this year* [POPL 2011] by Yuan Feng, Runyao Duan and Mingsheng Ying.

We have no clue what is the right modal logic for quantum systems in the spirit of van Benthem-Hennessy-Milner.

How do we even write specifications?

How do we even write specifications?

Simply using probabilistic logics misses the point.

How do we even write specifications?

Simply using probabilistic logics misses the point.

For example, how do you say in PCTL*
that entanglement is preserved?

How do we even write specifications?

Simply using probabilistic logics misses the point.

For example, how do you say in PCTL*
that entanglement is preserved?

In 2005 a weakest precondition semantics for quantum programming was developed [D'Hondt and P.] with a radically different notion of what is meant by a proposition.

How do we even write specifications?

Simply using probabilistic logics misses the point.

For example, how do you say in PCTL*
that entanglement is preserved?

In 2005 a weakest precondition semantics for quantum programming was developed [D'Hondt and P.] with a radically different notion of what is meant by a proposition.

Is this the right way to proceed?

What is quantum knowledge?

What is quantum knowledge?

We can write epistemic logics like the ones used in distributed systems [Halpern, Moses etc.]

What is quantum knowledge?

We can write epistemic logics like the ones used in distributed systems [Halpern, Moses etc.]

but strange things happen.

What is quantum knowledge?

We can write epistemic logics like the ones used in distributed systems [Halpern, Moses etc.]

but strange things happen.

For example, in teleportation, Alice “knows” ψ before she teleports it to Bob

What is quantum knowledge?

We can write epistemic logics like the ones used in distributed systems [Halpern, Moses etc.]

but strange things happen.

For example, in teleportation, Alice "knows" ψ before she teleports it to Bob

but after teleporting it she no longer knows it

What is quantum knowledge?

We can write epistemic logics like the ones used in distributed systems [Halpern, Moses etc.]

but strange things happen.

For example, in teleportation, Alice "knows" ψ before she teleports it to Bob

but after teleporting it she no longer knows it

not even in the time-stamped sense, "before I teleported I know I used to have ψ."

What is quantum knowledge?

We can write epistemic logics like the ones used in distributed systems [Halpern, Moses etc.]

but strange things happen.

For example, in teleportation, Alice "knows" ψ before she teleports it to Bob

but after teleporting it she no longer knows it

not even in the time-stamped sense, "before I teleported I know I used to have ψ."

She cannot "write it down"; that would violate the no-cloning theorem.

Topological Quantum Computing

Quantum systems are extremely unstable, how do we manipulate them with the exquisite precision needed while maintaining entanglement?

Many ideas in the physics community (each more expensive than the last).

One brilliant idea (due to Kitaev): use topological configurations like knots and braids that do not come apart easily.

Beautiful and interesting mathemtics and many opportunities for us to formalize the appropriate methods for reasoning about such systems. See tutorial slides on my web page.

Nobody can drive us out of the paradise that Heisenberg has created for us!

with apologies to David Hilbert.


RBS
TAYLORS
31 ST GILES

OSC
OXFORD
SUPERCOMPUTING
CENTRE
MFPS XXV

Thanks!

and thanks again,

and a final thank you!