Title: Higher-Order Quantum Computations

Date: Jun 02, 2009 10:15 AM

URL: http://pirsa.org/09060016

Abstract: TBA

Higher order types in quantum information

Observation. When interesting phenomena occur in quantum information theory, this usually happens at *higher order types*.

In quantum information theory, we usually distinguish *systems* (such as qubits, electrons) from *processes* (such as quantum circuits, experiments).

However, the distinction is sometimes blurred. A unknown process can sometimes be regarded as a system to interact with, in which case it is often called a *blackbox*.

Higher order types in quantum information

Observation. When interesting phenomena occur in quantum information theory, this usually happens at *higher order types*.

In quantum information theory, we usually distinguish *systems* (such as qubits, electrons) from *processes* (such as quantum circuits, experiments).

However, the distinction is sometimes blurred. A unknown process can sometimes be regarded as a system to interact with, in which case it is often called a *blackbox*.

Higher order types in quantum information

Observation. When interesting phenomena occur in quantum information theory, this usually happens at *higher order types*.

In quantum information theory, we usually distinguish *systems* (such as qubits, electrons) from *processes* (such as quantum circuits, experiments).

However, the distinction is sometimes blurred. A unknown process can sometimes be regarded as a system to interact with, in which case it is often called a *blackbox*.

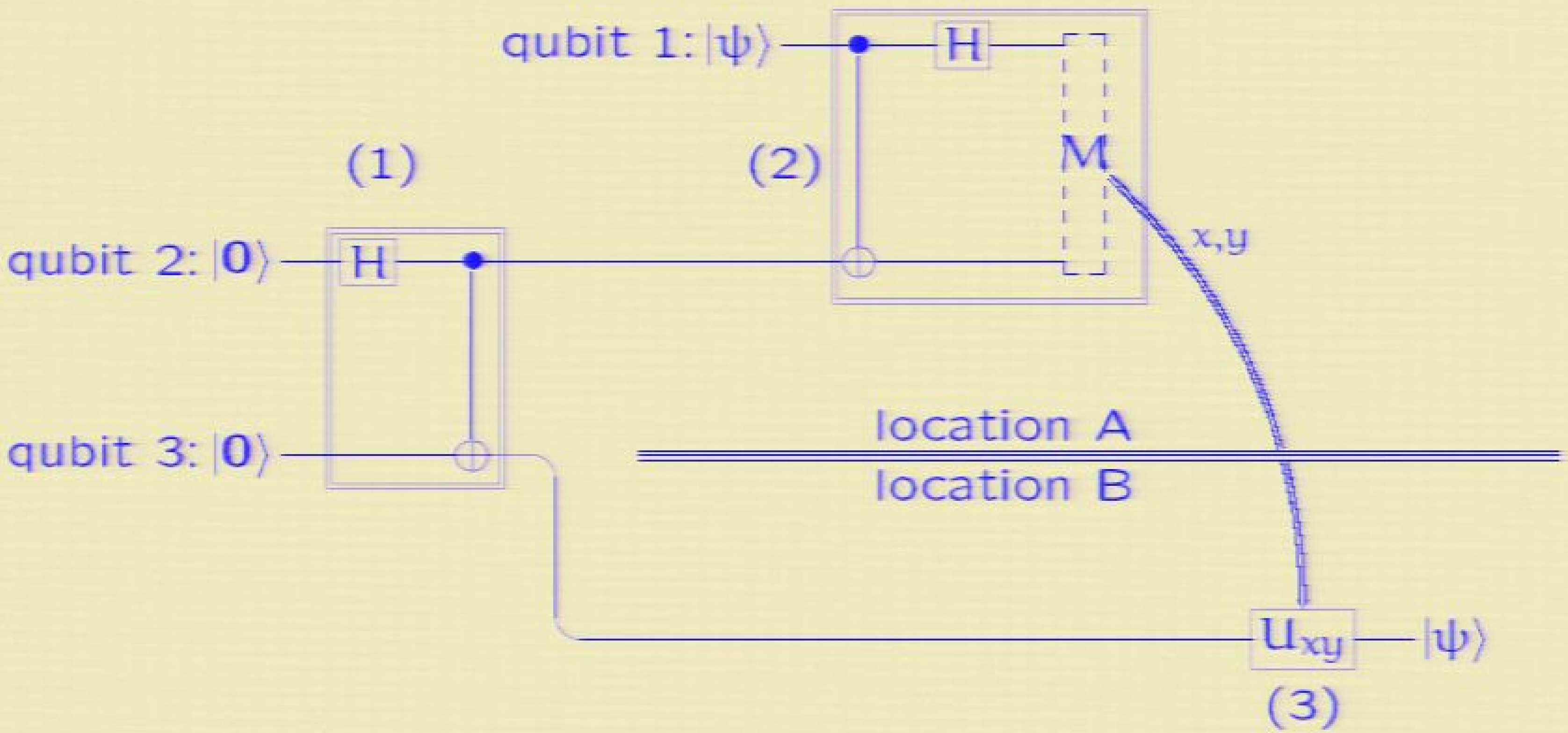
Higher order types

A *type* is a description of an interface to a system or process. Examples: **qbit**, **qbit** $\otimes$ **qbit**, **bit** $\oplus$ **qbit**, **qbit** $\multimap$ **bit**.

By a *higher order type*, we mean a type where a function space occurs in a nested way, for example:

- as an input to a function (blackbox): $(A \multimap B) \multimap C$,
- as an output to a function: $A \multimap (B \multimap C)$,
- as a component of a pair: $(A \multimap B) \otimes (C \multimap D)$.

Example 1: Quantum teleportation:



f_1 : $I \multimap \mathbf{qbit} \otimes \mathbf{qbit}$
f_2 : $\mathbf{qbit} \otimes \mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit}$
f_3 : $\mathbf{qbit} \otimes \mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit}$

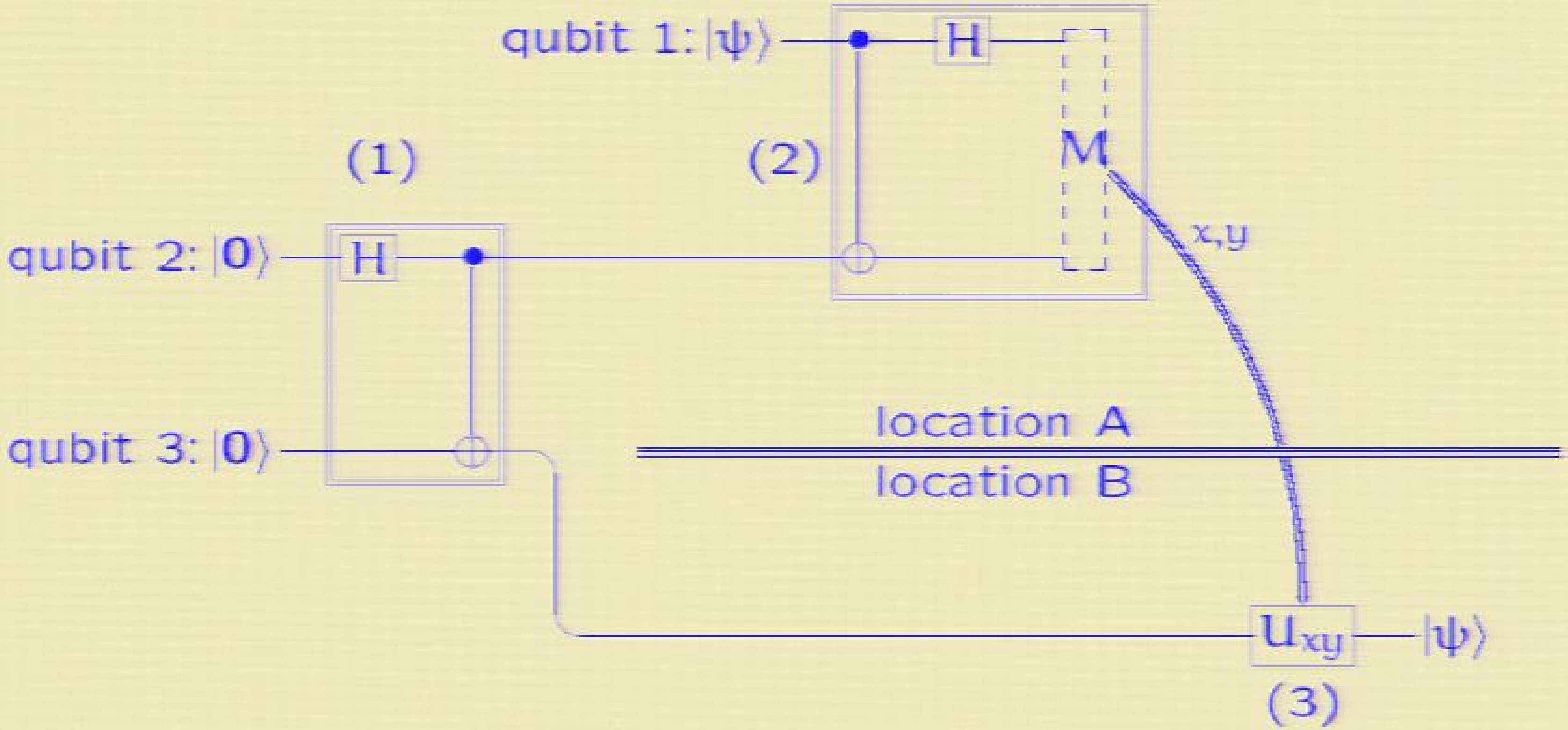
Higher order types

A *type* is a description of an interface to a system or process. Examples: **qbit**, **qbit** $\otimes$ **qbit**, **bit** $\oplus$ **qbit**, **qbit** $\multimap$ **bit**.

By a *higher order type*, we mean a type where a function space occurs in a nested way, for example:

- as an input to a function (blackbox): $(A \multimap B) \multimap C$,
- as an output to a function: $A \multimap (B \multimap C)$,
- as a component of a pair: $(A \multimap B) \otimes (C \multimap D)$.

Example 1: Quantum teleportation:



$f_1 : \; I \multimap \mathbf{qbit} \otimes \mathbf{qbit}$
$f_2 : \; \mathbf{qbit} \otimes \mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit}$
$f_3 : \; \mathbf{qbit} \otimes \mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit}$

Teleportation, continued:

$$\begin{aligned} f_1 &: \ I \multimap \mathbf{qbit} \otimes \mathbf{qbit} \\ f_2 &: \ \mathbf{qbit} \otimes \mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit} \\ f_3 &: \ \mathbf{qbit} \otimes \mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit} \end{aligned}$$

Curry f_2 and f_3:

$$\begin{aligned} f_1 &: \ I \multimap \mathbf{qbit} \otimes \mathbf{qbit} \\ \tilde{f}_2 &: \ \mathbf{qbit} \multimap (\mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit}) \\ \tilde{f}_3 &: \ \mathbf{qbit} \multimap (\mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit}) \end{aligned}$$

Combine all three functions:

$$F = f_1; (\tilde{f}_2 \otimes \tilde{f}_3) : I \multimap (\mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit}) \otimes (\mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit})$$

This is a thunk. Letting $(g, h) = F(*)$ yields a pair of *entangled functions* $g : \mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit}$ and $h : \mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit}$.

Moreover, $h \circ g = \mathrm{id}$ (teleportation) and $g \circ h = \mathrm{id}$ (dense coding). Are they inverses? No, because single use only!

Entangled functions

- *Entangled functions* are a central concept in higher-order quantum information theory.
- They can have unexpected and novel properties. There is no classical analog.
- A possibly-entangled function can be understood as a "quantum state with an interface".
- Is there a mathematical description?

Teleportation, continued:

$$\begin{aligned} f_1 &: \ I \multimap \mathbf{qbit} \otimes \mathbf{qbit} \\ f_2 &: \ \mathbf{qbit} \otimes \mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit} \\ f_3 &: \ \mathbf{qbit} \otimes \mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit} \end{aligned}$$

Curry f_2 and f_3:

$$\begin{aligned} f_1 &: \ I \multimap \mathbf{qbit} \otimes \mathbf{qbit} \\ \tilde{f}_2 &: \ \mathbf{qbit} \multimap (\mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit}) \\ \tilde{f}_3 &: \ \mathbf{qbit} \multimap (\mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit}) \end{aligned}$$

Combine all three functions:

$$F = f_1; (\tilde{f}_2 \otimes \tilde{f}_3) : I \multimap (\mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit}) \otimes (\mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit})$$

This is a thunk. Letting $(g, h) = F(*)$ yields a pair of *entangled functions* $g : \mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit}$ and $h : \mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit}$.

Moreover, $h \circ g = \mathrm{id}$ (teleportation) and $g \circ h = \mathrm{id}$ (dense coding). Are they inverses? No, because single use only!

Entangled functions

- *Entangled functions* are a central concept in higher-order quantum information theory.
- They can have unexpected and novel properties. There is no classical analog.
- A possibly-entangled function can be understood as a "quantum state with an interface".
- Is there a mathematical description?

Example 2: Bell inequalities

In the previous example, we had a pair of entangled functions $g : \mathbf{qbit} \multimap \mathbf{bit} \otimes \mathbf{bit}$ and $h : \mathbf{bit} \otimes \mathbf{bit} \multimap \mathbf{qbit}$.

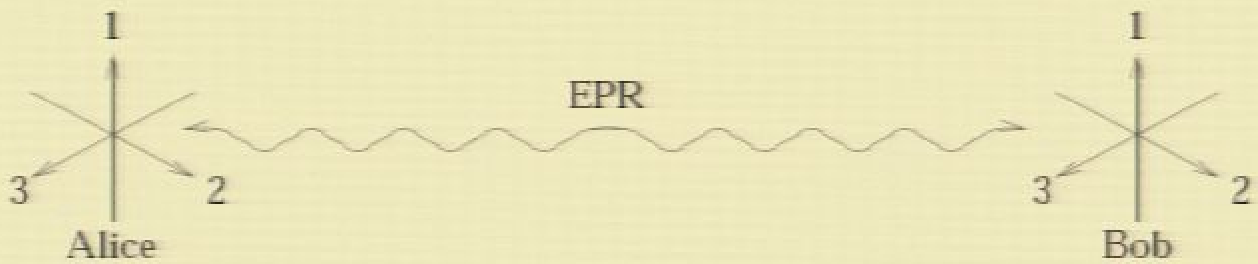
The next example involves a pair of entangled functions whose type is purely classical.

$$g : 3 \to \mathbf{bit}, \quad h : 3 \to \mathbf{bit}.$$

Here, $3 = \mathrm{I} + \mathrm{I} + \mathrm{I}$ (a 3-element set) and $\mathbf{bit} = \mathrm{I} + \mathrm{I}$ (a 2-element set).

Bell's experiment

Alice and Bob each receive one component of an entangled pair, at a distance.



Each of Alice and Bob performs an experiment that depends on an *additional input*, namely, a choice of axis 1, 2, 3 to measure in. They choose this input independently. The probabilities that Alice and Bob observe the same value are:

	1	2	3
1	1	$\frac{1}{4}$	$\frac{1}{4}$
2	$\frac{1}{4}$	1	$\frac{1}{4}$
3	$\frac{1}{4}$	$\frac{1}{4}$	1

Bell's experiment, continued

The *Bell inequalities* state that in any local hidden variable theory,

$$P_{\mathbf{1},\mathbf{2}}(\text{equal}) + P_{\mathbf{2},\mathbf{3}}(\text{equal}) + P_{\mathbf{1},\mathbf{3}}(\text{equal}) \geq 1$$

However,

$$P_{\mathbf{1},\mathbf{2}}(\text{equal}) + P_{\mathbf{2},\mathbf{3}}(\text{equal}) + P_{\mathbf{1},\mathbf{3}}(\text{equal}) = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}$$

So the predictions of quantum theory are *incompatible* with "local hidden variable theories".

Bell's experiment, stated with entangled functions

There exists a pair of entangled functions $g, h : \{1, 2, 3\} \to \mathbf{bit}$, such that for all $x, y \in \{1, 2, 3\}$:

$$P\left(g(x) = h(y)\right) = \begin{cases} 1 & \text{if } x = y, \\ 1/4 & \text{if } x \neq y. \end{cases}$$

Bell's argument shows that if g, h were merely *probabilistic* functions (or even if the pair (g, h) were sampled from a *probability distribution* of such pairs), then

$$P\left(g(x) = h(x)\right) = 1 \quad \text{for all } x$$

implies

$$P\left(g(1) = h(2)\right) + P\left(g(2) = h(3)\right) + P\left(g(1) = h(3)\right) \geq 1.$$

This is easy to check using semantics.

Discussion of Bell's experiment

- Logicians would say: "Quantum computation is not *conservative* over probabilistic computation".
- Category theorists would say: "The embedding of probabilistic computation in quantum computation is not *full*".
- Physicists say: "There is no *local hidden variable theory* for quantum mechanics".

Example 3: PR boxes (Popescu and Rohrlich)

Consider the following problem:

- Alice and Bob are given the task of creating a pair of Boolean functions of one argument,

  $$g, h : \mathbf{bit} \multimap \mathbf{bit}.$$

  Alice keeps g and Bob keeps h. They go to different rooms.

- Alice is given a random bit x and Bob is given a random bit y (x and y are independent and uniformly distributed).

- The functions g and h are supposed to satisfy:

  $$g(x) \oplus h(y) = x \vee y,$$

  where $\oplus$ denotes "exclusive or", and $\vee$ denotes "or".

PR boxes, best probabilistic solution

$$g(0) \oplus h(0) = 0$$
$$g(0) \oplus h(1) = 1$$
$$g(1) \oplus h(0) = 1$$
$$g(1) \oplus h(1) = 1$$

What is Alice and Bob's probability of success?

It is easily seen that with classical (even probabilistic) functions, the best Alice and Bob can hope for is to win 75% of the time.

One possible solution is: let g and h be the constant 1 function. Or let g be the constant 0 function and h the identity function.

One cannot do better.

PR boxes, best probabilistic solution

$$g(0) \oplus h(0) = 0$$
$$g(0) \oplus h(1) = 1$$
$$g(1) \oplus h(0) = 1$$
$$g(1) \oplus h(1) = 1$$

What is Alice and Bob's probability of success?

It is easily seen that with classical (even probabilistic) functions, the best Alice and Bob can hope for is to win 75% of the time.

One possible solution is: let g and h be the constant 1 function. Or let g be the constant 0 function and h the identity function.

One cannot do better.

The probabilities of agreement are:

	1	2
1	1	$\frac{1}{4}$
3	$\frac{1}{4}$	$\frac{1}{4}$

In other words,

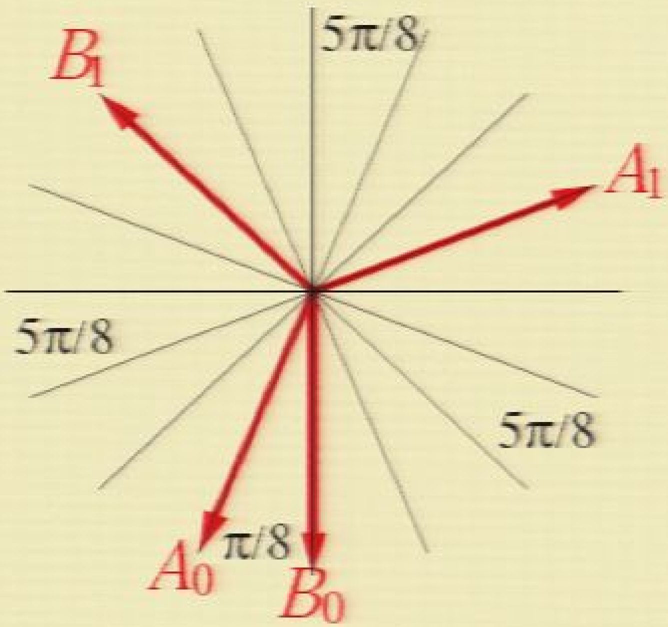
$$P\left(g(0) \oplus h(0) = 0\right) = 1$$
$$P\left(g(0) \oplus h(1) = 1\right) = \frac{3}{4}$$
$$P\left(g(1) \oplus h(0) = 1\right) = \frac{3}{4}$$
$$P\left(g(1) \oplus h(1) = 1\right) = \frac{3}{4}$$

Therefore, the combined chance of success (on uniformly distributed input) is $\frac{1+.75+.75+.75}{4} = 0.8125$.

PR boxes, best quantum solution

Actually, the optimal success rate Alice and Bob can achieve is $\sin(\pi/8) \equiv 85.36\%$. It is done as follows:

If $x = 0$, Alice measures in basis A_0, else in basis A_1. If $y = 0$, Bob measures in basis B_0, else in basis B_1.



$$P\left(g(0) \oplus h(0) = 0\right) = \cos^2(\tfrac{\pi}{8}) = .8536$$
$$P\left(g(0) \oplus h(1) = 1\right) = \sin^2(\tfrac{5\pi}{8}) = .8536$$
$$P\left(g(1) \oplus h(0) = 1\right) = \sin^2(\tfrac{5\pi}{8}) = .8536$$
$$P\left(g(1) \oplus h(1) = 1\right) = \sin^2(\tfrac{5\pi}{8}) = .8536$$

Discussion of PR Box example

- The conclusion is similar to that of Bell's experiment. Quantum computation is not conservative over probabilistic computation at the type $(\mathbf{bit} \multimap \mathbf{bit}) \otimes (\mathbf{bit} \multimap \mathbf{bit})$.

- The fact that this is a higher-order type is essential. Indeed, one can show that *quantum computation is conservative over probabilistic computation for first-order types*.

- These examples beg for a denotational semantics, to answer such question as:
  - What exactly are the quantum definable functions at higher-order types?
  - Do there exist Bell-like situation at *all* higher-order types?
  - Are there any new phenomena as the complexity of types increases?

Semantics of higher-order quantum computation

An important open problem: to find a *fully complete* semantics of higher-order quantum computation.

This means: at each higher-order type, characterize exactly which quantum operations are information-theoretically possible.

In other words: find sets of *generalized Bell inequalities*, at each higher-order type, which jointly characterize precisely the quantum definable elements.

Semantics of higher-order quantum computation

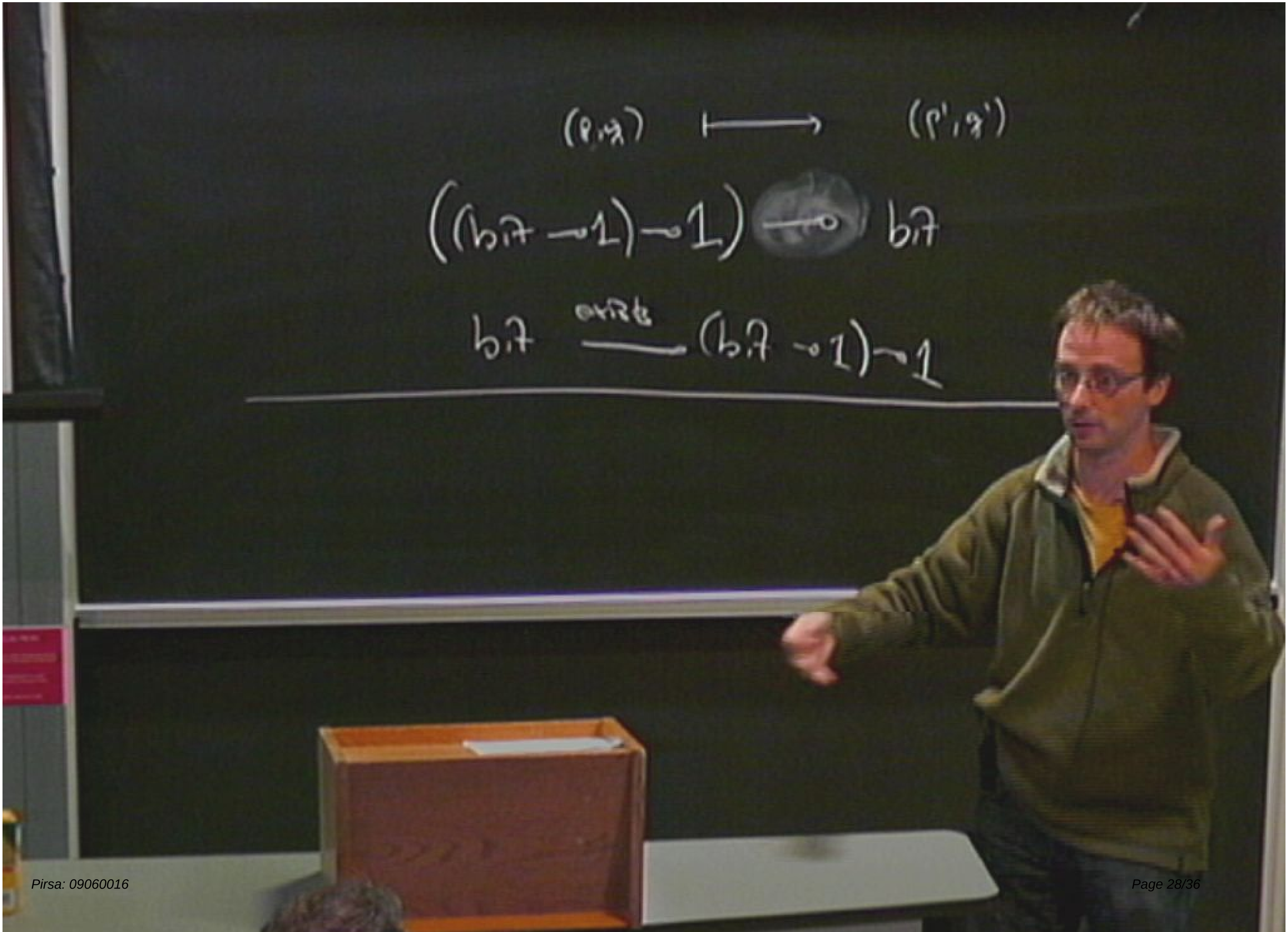
An important open problem: to find a *fully complete* semantics of higher-order quantum computation.

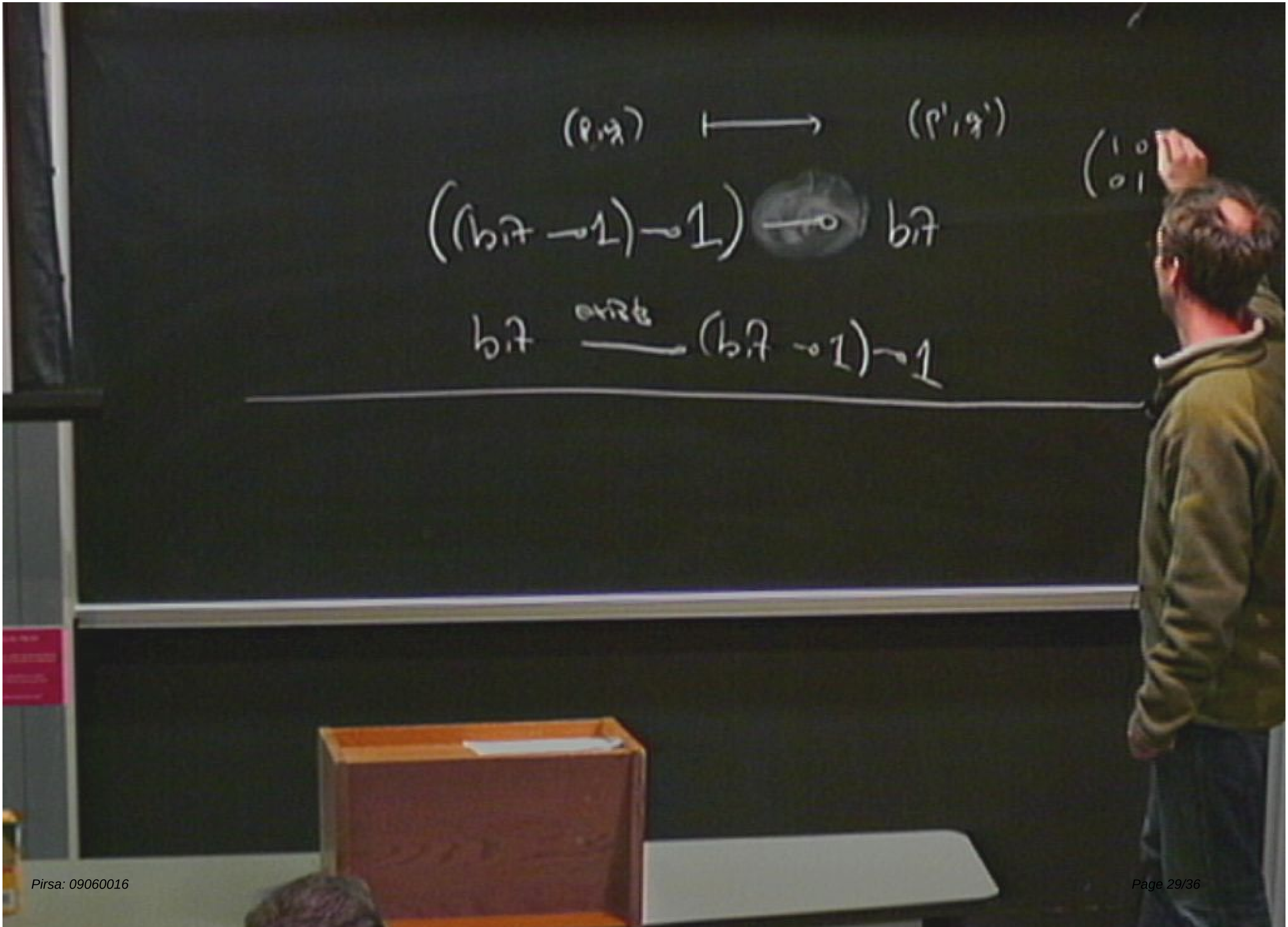
This means: at each higher-order type, characterize exactly which quantum operations are information-theoretically possible.

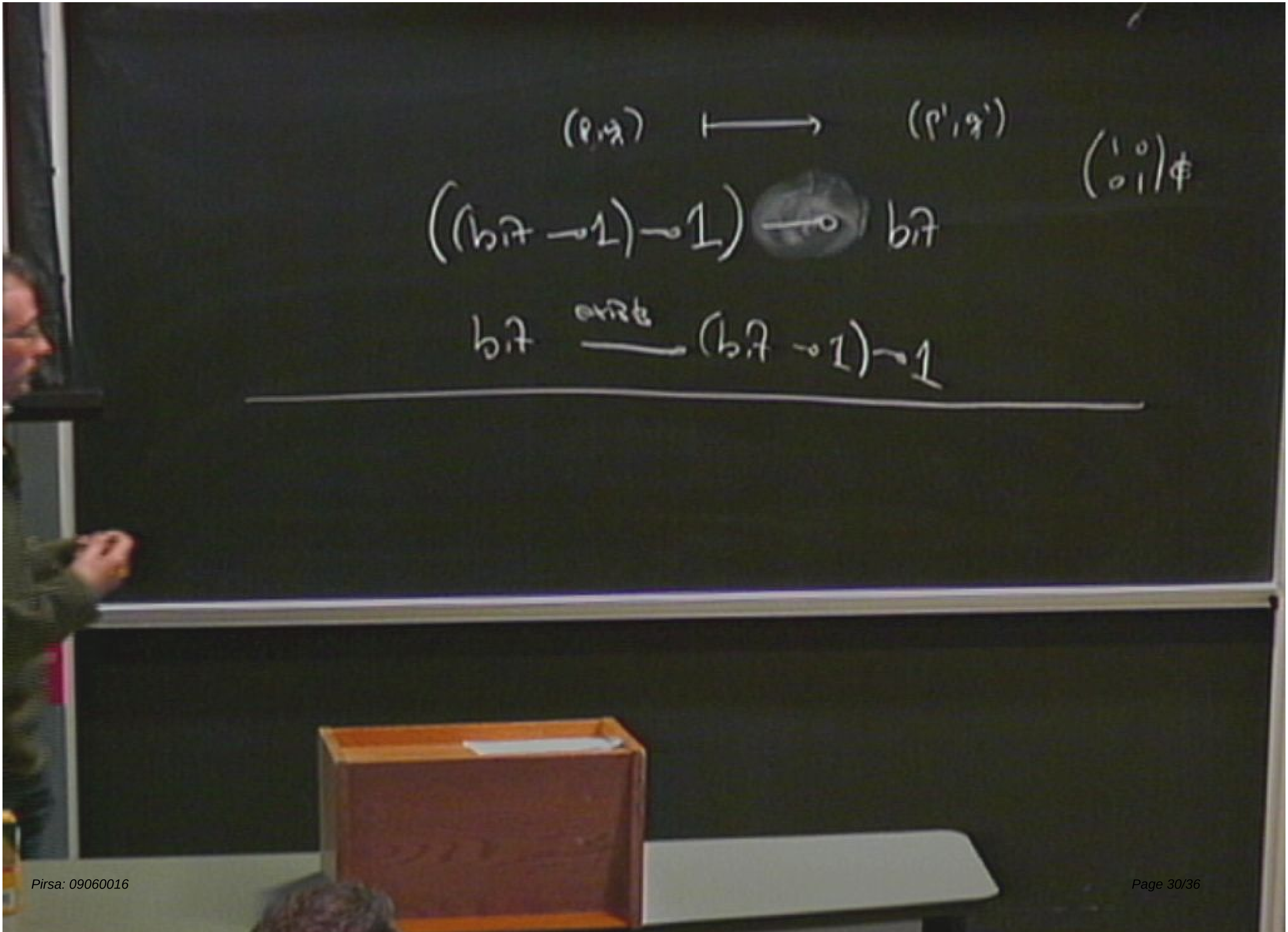
In other words: find sets of *generalized Bell inequalities*, at each higher-order type, which jointly characterize precisely the quantum definable elements.

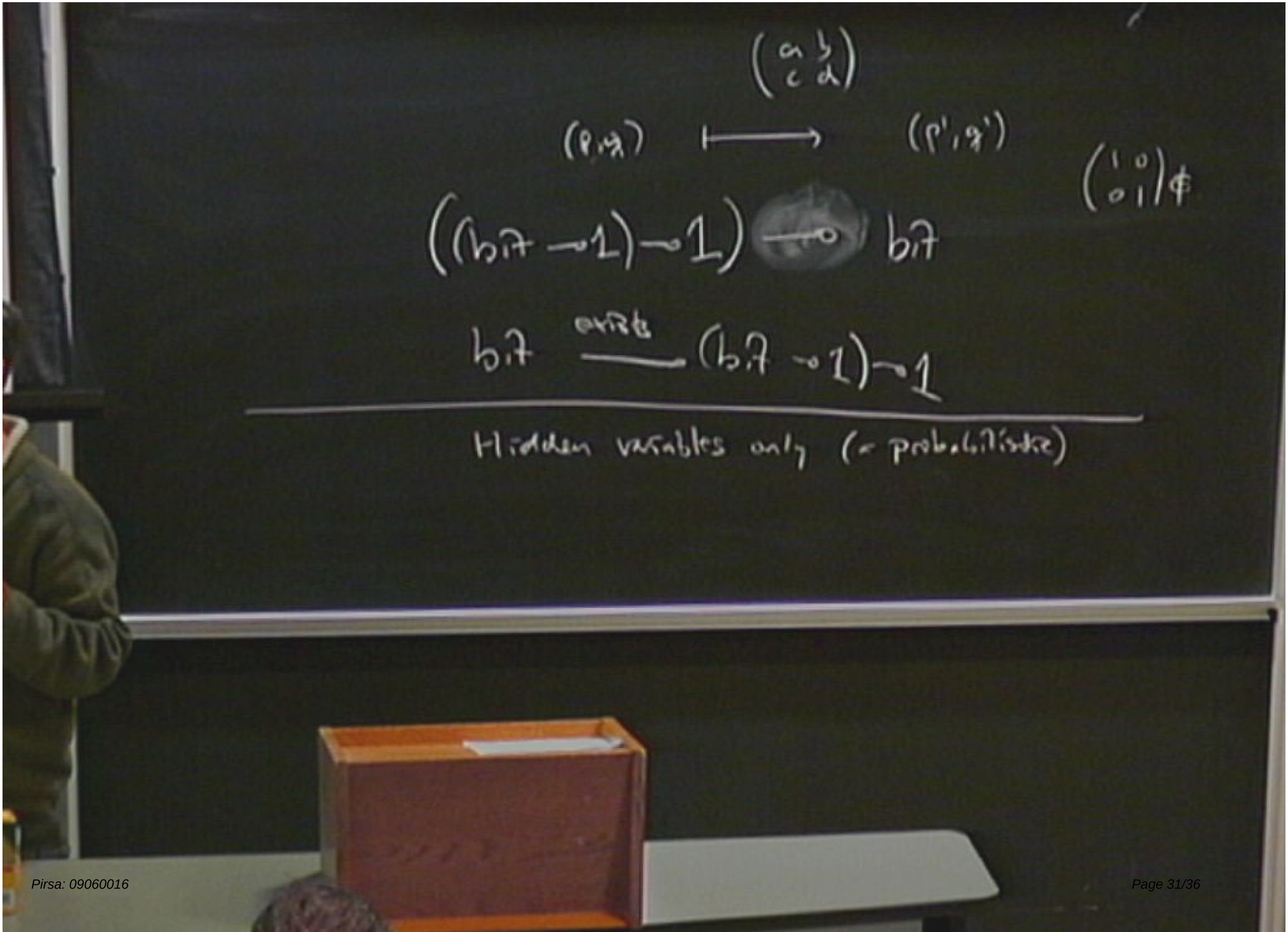
$$(\mathrm{bit} \multimap 1) \multimap 1 \xrightarrow{\times} \mathrm{bit}$$

$$\mathrm{bit} \xrightarrow{\mathrm{eval}} (\mathrm{bit} \multimap 1) \multimap 1$$


(p,q) ⟼ (p',q')
((bit ⊸ 1) ⊸ 1) ⊸ bit
bit ⟶ (bit ⊸ 1) ⊸ 1


(p,q) ⟼ (p',q')
((bit ⊸ 1) ⊸ 1) ⊸ bit
bit ⟶ (bit ⊸ 1) ⊸ 1


(p, q) ⟼ (p', q')
((bit ⊸ 1) ⊸ 1) ⊸ bit
bit → (bit ⊸ 1) ⊸ 1


(a b / c d)
(p,q) ⟼ (p',q')
((bit ⊸ 1) ⊸ 1) ⊸ bit
bit exists (bit ⊸ 1) ⊸ 1
Hidden variables only (≠ probabilistic)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$(p, q) \longmapsto (p', q')$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin$$

$$((\text{bit} \multimap 1) \multimap 1) \multimap \text{bit}$$

$$\text{bit} \xrightarrow{\text{exists}} (\text{bit} \multimap 1) \multimap 1$$

Hidden variables only (= probabilistic)

The state of the art

- At first-order types $A \multimap B$, where A, B are ground types, the quantum realizable functions are precisely the superoperators, so the full abstraction problem is solved.

- [Acín, Navascués, Pironio 2008] gave an (infinite) hierarchy of *necessary conditions* for types of the form

$$(n_1 \multimap m_1) \otimes (n_2 \multimap m_2),$$

where n_1, m_1, n_2, m_2 are of the form $I \oplus \ldots \oplus I$. The conditions use *semidefinite programming*. They are conjectured to be jointly complete.

The state of the art

- At first-order types $A \multimap B$, where A, B are ground types, the quantum realizable functions are precisely the superoperators, so the full abstraction problem is solved.

- [Acín, Navascués, Pironio 2008] gave an (infinite) hierarchy of *necessary conditions* for types of the form

$$(n_1 \multimap m_1) \otimes (n_2 \multimap m_2),$$

where n_1, m_1, n_2, m_2 are of the form $I \oplus \ldots \oplus I$. The conditions use *semidefinite programming*. They are conjectured to be jointly complete.

The state of the art, continued

- [Selinger, Valiron 2004–2009] defined a lambda calculus for higher-order quantum computation, and an operational semantics. We also gave categorical axioms for what it means to be a *denotational model* of this calculus.

- [Malherbe, Selinger 2009] recently found an example of such a model, using presheaves. However, it is probably not fully complete at higher-order types.

- [Valiron 2008] defined a notion of *Kripke normed spaces*, similar to Kripke logical relations in lambda calculus. It is fully complete at higher types, but only works for *probabilistic computation* at the moment.

The End