Towards a quantum λ-calculus with quantum control

arXiv:1601.04294

Alejandro Díaz-Caro
Universidad Nacional de Quilmes

Joint work with
Gilles Dowek
Inria & ENS-Cachan

V Congreso Latinoamericano de Matemáticos
Logic and Computability Session
Barranquilla, Colombia, July 14, 2016

Goal

We want a **pure** functional extension of lambda calculus

i.e. we do not want clasical control / quantum data

Overview

Some quantum properties (with dead and alive cats)

- Projective measurement
- Destructive interference
- No-cloning
- Entanglement and separability

Expressing those properties in the lambda-calculus

- Superpositions, no-cloning and measurement

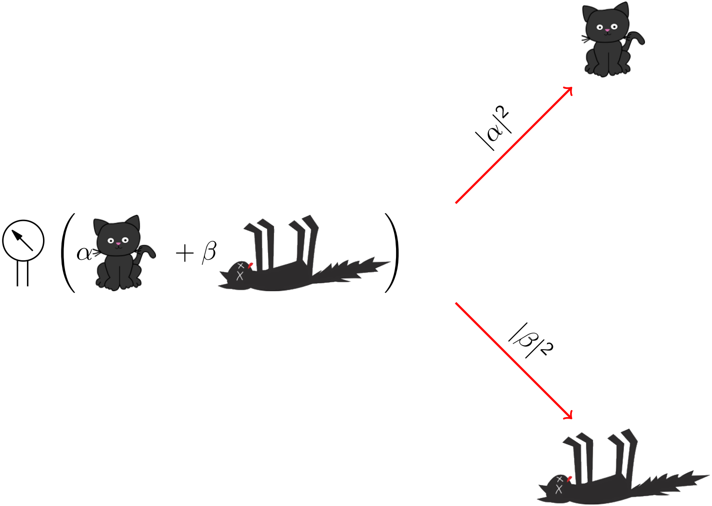
Examples

- Deutsch algorithm
- Teleportation algorithm

Projective measurement

$\Big(\alpha$  $+ \beta$  $\Big)$

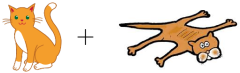
Projective measurement



Probabilistic vs. Quantum

Destructive interference

Probabilistic



Probabilistic vs. Quantum

Destructive interference

Probabilistic

a  $+\, b$ 

$$(a + b = 1)$$

Probabilistic vs. Quantum

Destructive interference

Probabilistic

a  $+\ b$ 

$(a + b = 1)$

Quantum

α  $+\ \beta$ 

$\left(|\alpha|^2 + |\beta|^2 = 1\right)$

Probabilistic vs. Quantum

Destructive interference

Probabilistic

a  $+\, b$ 

$$(a + b = 1)$$

Quantum

α  $-\,\beta$ 

$$\left(|\alpha|^2 + |-\beta|^2 = 1\right)$$

Probabilistic vs. Quantum

Destructive interference

Probabilistic

a  $+\, b$ 

$(a + b = 1)$

Quantum

α  $-\, \beta$ 

$\left(|\alpha|^2 + |-\beta|^2 = 1\right)$

$\frac{1}{2}\Big(\frac{1}{2}$  $+ \frac{1}{2}$  $\Big) + \frac{1}{2}\Big(\qquad\qquad\Big)$

Probabilistic vs. Quantum

Destructive interference

Probabilistic

a  $+\, b$ 

$(a + b = 1)$

Quantum

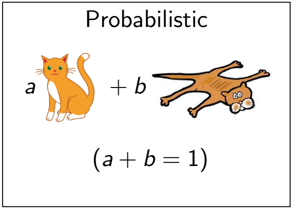
α  $-\, \beta$ 

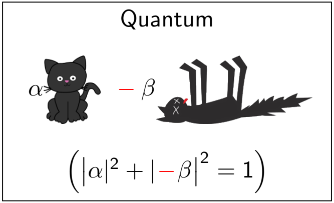
$\left(|\alpha|^2 + |-\beta|^2 = 1\right)$

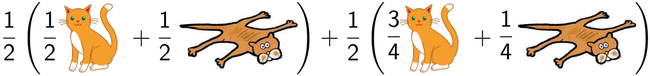
$\frac{1}{2}\Big(\frac{1}{2}$  $+ \frac{1}{2}$  $\Big) + \frac{1}{2}\Big(\alpha$  $+\, \beta$  $\Big)$

Probabilistic vs. Quantum

Destructive interference



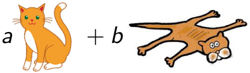




Probabilistic vs. Quantum

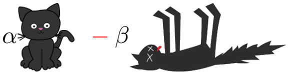
Destructive interference

Probabilistic

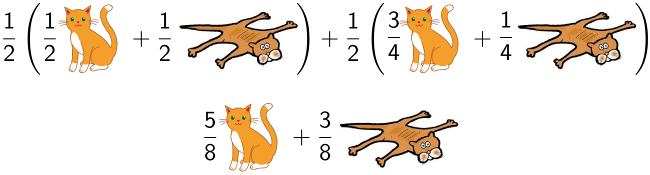


$(a + b = 1)$

Quantum

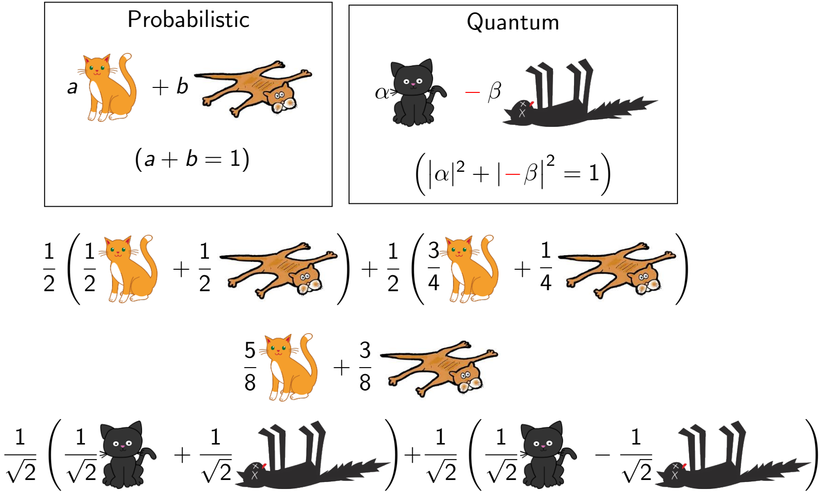


$\left(|\alpha|^2 + |-\beta|^2 = 1\right)$



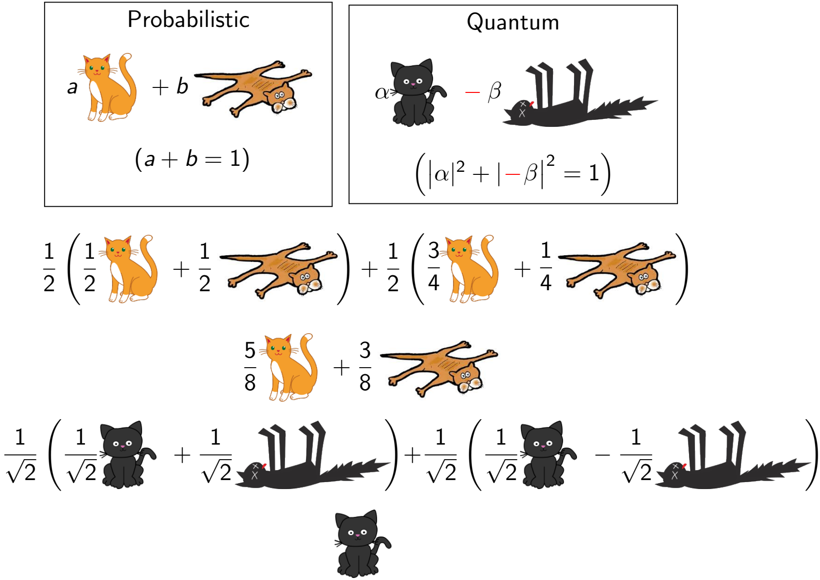
Probabilistic vs. Quantum

Destructive interference



Probabilistic vs. Quantum

Destructive interference



No-cloning

Superpositions vs. basis states

There is no universal cloning machine
for quantum states

No-cloning

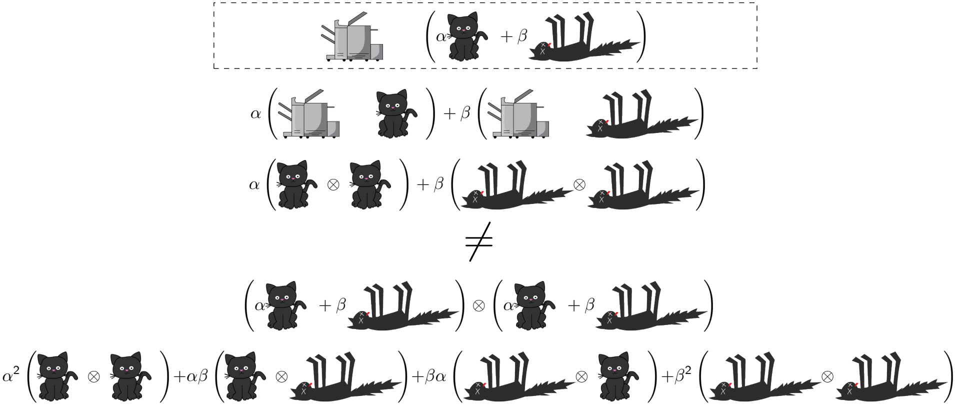
Superpositions vs. basis states

There is no universal cloning machine
for quantum states

No-cloning

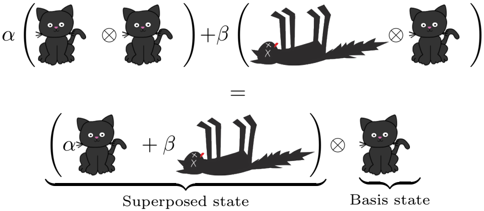
Superpositions vs. basis states

There is no universal cloning machine
for quantum states



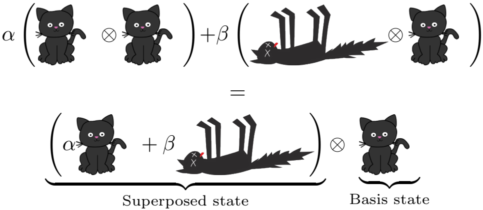
Entanglement and separability

Example 1

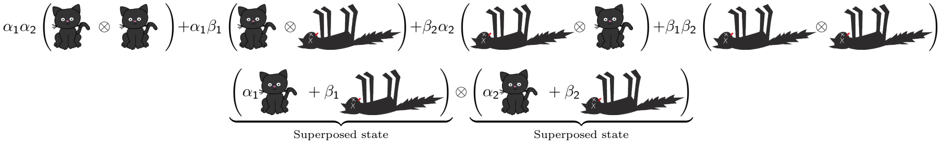


Entanglement and separability

Example 1

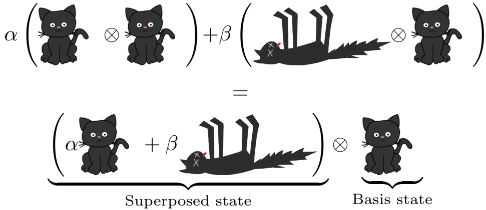


Example 2

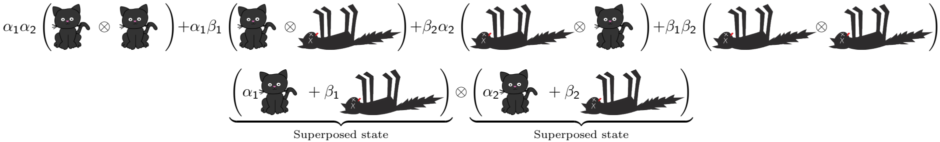


Entanglement and separability

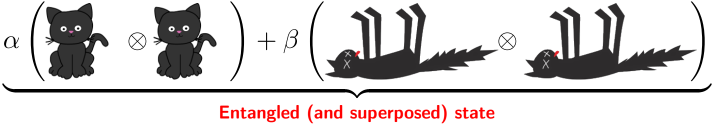
Example 1



Example 2



Example 3



Overview

- Some quantum properties (with dead and alive cats)
  - Projective measurement
  - Destructive interference
  - No-cloning
  - Entanglement and separability
- Expressing those properties in the lambda-calculus
  - Superpositions, no-cloning and measurement
- Examples
  - Deutsch algorithm
  - Teleportation algorithm

Logical linearity vs. algebraic linearity

No-cloning $\Longrightarrow$ logical-linear terms

e.g. $\lambda x.x \otimes x$ forbidden

Logical linearity vs. algebraic linearity

No-cloning $\implies$ logical-linear terms

e.g. $\lambda x.x \otimes x$ forbidden

Another way

No-cloning $\implies$ algebraic-linear operators

e.g. $M(\alpha.\left|0\right\rangle + \beta.\left|1\right\rangle) \to \alpha.M\left|0\right\rangle + \beta.M\left|1\right\rangle$

Logical linearity vs. algebraic linearity

No-cloning $\Longrightarrow$ logical-linear terms

e.g. $\lambda x.x \otimes x$ forbidden

Another way

No-cloning $\Longrightarrow$ algebraic-linear operators

e.g. $M(\alpha. |0\rangle + \beta. |1\rangle) \to \alpha.M |0\rangle + \beta.M |1\rangle$

What about measurement?

(Measurement operator)

$(\lambda x.\pi x) \quad (\alpha. |0\rangle + \beta. |1\rangle)$

$\alpha.(\lambda x.\pi x) |0\rangle + \beta.(\lambda x.\pi x) |1\rangle$ $\leftarrow$ **Wrong!**

Logical linearity vs. algebraic linearity

No-cloning $\Longrightarrow$ logical-linear terms

e.g. $\lambda x.x \otimes x$ forbidden

Another way

No-cloning $\Longrightarrow$ algebraic-linear operators

e.g. $M(\alpha.\left|0\right\rangle + \beta.\left|1\right\rangle) \to \alpha.M\left|0\right\rangle + \beta.M\left|1\right\rangle$

What about measurement?

(Measurement operator)

$$(\lambda x.\pi x) \quad (\alpha.\left|0\right\rangle + \beta.\left|1\right\rangle)$$

$$\alpha.(\lambda x.\pi x)\left|0\right\rangle + \beta.(\lambda x.\pi x)\left|1\right\rangle \qquad \leftarrow \textbf{Wrong!}$$

We can use a combination of both:

Logical-linear for abstractions taking superpositions

Algebraic-linear for abstractions taking basis states

Key point

We need to distinguish
superposed states
from
basis states

Basis states can be cloned
Superposed states cannot

Grammars

First version, without tensor

Types

$$\Psi := \mathbb{Q} \mid S(\Psi) \qquad \text{Qubit types}$$

$$A := \Psi \mid \Psi \Rightarrow A \mid S(A) \qquad \text{Types}$$

Terms

$$b := x \mid \lambda x^{\Psi}.t \mid |0\rangle \mid |1\rangle \qquad \text{Basis terms}$$

$$v := b \mid v + v \mid \alpha.v \mid \vec{0}_{S(A)} \qquad \text{Values}$$

$$t := v \mid tt \mid t + t \mid \alpha.t \mid \pi t \mid ?\cdot \qquad \text{Terms}$$

where $\alpha \in \mathbb{C}$

Two types of linearity

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{b}_{\mathbb{Q}} \quad \to \quad t[b/x] \qquad \text{call-by-base}$$

$$\underbrace{(\lambda x^{S(\Psi)}.t)}_{\text{linear abstraction}}\ \underbrace{u}_{S(\Psi)} \quad \to \quad t[u/x] \qquad \text{call-by-name}$$

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{(b_1 + b_2)}_{S(\mathbb{Q})} \quad \to \quad (\lambda x^{\mathbb{Q}}.t)\underbrace{b_1}_{\mathbb{Q}} + (\lambda x^{\mathbb{Q}}.t)\underbrace{b_2}_{\mathbb{Q}} \qquad \text{linear distribution}$$

Two types of linearity

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{b}_{\mathbb{Q}} \quad \to \quad t[b/x] \qquad \text{call-by-base}$$

$$\underbrace{(\lambda x^{S(\Psi)}.t)}_{\text{linear abstraction}} \underbrace{u}_{S(\Psi)} \quad \to \quad t[u/x] \qquad \text{call-by-name}$$

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{(b_1 + b_2)}_{S(\mathbb{Q})} \quad \to \quad (\lambda x^{\mathbb{Q}}.t)\underbrace{b_1}_{\mathbb{Q}} + (\lambda x^{\mathbb{Q}}.t)\underbrace{b_2}_{\mathbb{Q}} \qquad \text{linear distribution}$$

Problem?

$\lambda x^{\mathbb{Q}\Rightarrow\mathbb{Q}}.x(|0\rangle+|1\rangle) : (\mathbb{Q} \Rightarrow \mathbb{Q}) \Rightarrow \mathbb{Q}$ Non-linear! (not a superposition)

Two types of linearity

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{b}_{\mathbb{Q}} \quad \to \quad t[b/x] \qquad \text{call-by-base}$$

$$\underbrace{(\lambda x^{S(\Psi)}.t)}_{\text{linear abstraction}}\ \underbrace{u}_{S(\Psi)} \quad \to \quad t[u/x] \qquad \text{call-by-name}$$

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{(b_1 + b_2)}_{S(\mathbb{Q})} \quad \to \quad (\lambda x^{\mathbb{Q}}.t)\underbrace{b_1}_{\mathbb{Q}} + (\lambda x^{\mathbb{Q}}.t)\underbrace{b_2}_{\mathbb{Q}} \qquad \text{linear distribution}$$

Problem?

$\lambda x^{\mathbb{Q}\Rightarrow\mathbb{Q}}.x(|0\rangle + |1\rangle) : (\mathbb{Q} \Rightarrow \mathbb{Q}) \Rightarrow \mathbb{Q}$ Non-linear! (not a superposition)

No problem

It is a function which produces a superposition, *is not a superposition*
It can be cloned ✓

Two types of linearity

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{b}_{\mathbb{Q}} \quad \to \quad t[b/x] \qquad \text{call-by-base}$$

$$\underbrace{(\lambda x^{S(\Psi)}.t)}_{\text{linear abstraction}}\ \underbrace{u}_{S(\Psi)} \quad \to \quad t[u/x] \qquad \text{call-by-name}$$

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{(b_1 + b_2)}_{S(\mathbb{Q})} \quad \to \quad (\lambda x^{\mathbb{Q}}.t)\underbrace{b_1}_{\mathbb{Q}} + (\lambda x^{\mathbb{Q}}.t)\underbrace{b_2}_{\mathbb{Q}} \qquad \text{linear distribution}$$

Problem?

$\lambda x^{\mathbb{Q}\Rightarrow\mathbb{Q}}.x(|0\rangle+|1\rangle) : (\mathbb{Q} \Rightarrow \mathbb{Q}) \Rightarrow \mathbb{Q}$ Non-linear! (not a superposition)

No problem

It is a function which produces a superposition, *is not a superposition*
It can be cloned ✓

What about $\lambda y^{S(\mathbb{Q})}.\lambda x^{\mathbb{Q}}.xy$?

Two types of linearity

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{b}_{\mathbb{Q}} \quad\rightarrow\quad t[b/x] \qquad \text{call-by-base}$$

$$\underbrace{(\lambda x^{S(\Psi)}.t)}_{\text{linear abstraction}}\ \underbrace{u}_{S(\Psi)} \quad\rightarrow\quad t[u/x] \qquad \text{call-by-name}$$

$$(\lambda x^{\mathbb{Q}}.t)\underbrace{(b_1+b_2)}_{S(\mathbb{Q})} \quad\rightarrow\quad (\lambda x^{\mathbb{Q}}.t)\underbrace{b_1}_{\mathbb{Q}} + (\lambda x^{\mathbb{Q}}.t)\underbrace{b_2}_{\mathbb{Q}} \qquad \text{linear distribution}$$

Problem?

$\lambda x^{\mathbb{Q}\Rightarrow\mathbb{Q}}.x(|0\rangle+|1\rangle) : (\mathbb{Q}\Rightarrow\mathbb{Q})\Rightarrow\mathbb{Q}$ Non-linear! (not a superposition)

No problem

It is a function which produces a superposition, *is not a superposition*
It can be cloned ✓

What about $\lambda y^{S(\mathbb{Q})}.\lambda x^{\mathbb{Q}}.xy$?

Ok, let's stay in first order for now

Typing applications

$$\frac{\Gamma \vdash t : \Psi \Rightarrow A \quad \Delta \vdash u : \Psi}{\Gamma, \Delta \vdash tu : A} \Rightarrow_E$$

Typing applications

$$\frac{\Gamma \vdash t : \Psi \Rightarrow A \quad \Delta \vdash u : \Psi}{\Gamma, \Delta \vdash tu : A} \Rightarrow_E$$

What about $(\lambda x^{\mathbb{Q}}.t)\underbrace{(b_1 + b_2)}_{S(\mathbb{Q})}$?

Typing applications

$$\frac{\Gamma \vdash t : \Psi \Rightarrow A \quad \Delta \vdash u : \Psi}{\Gamma, \Delta \vdash tu : A} \Rightarrow_E$$

What about $(\lambda x^{\mathbb{Q}}.t)\underbrace{(b_1 + b_2)}_{S(\mathbb{Q})}$?

$$\frac{\Gamma \vdash t : \Psi \Rightarrow A \quad \Delta \vdash u : S(\Psi)}{\Gamma, \Delta \vdash tu : S(A)}$$

Typing applications

$$\frac{\Gamma \vdash t : \Psi \Rightarrow A \quad \Delta \vdash u : \Psi}{\Gamma, \Delta \vdash tu : A} \Rightarrow_E$$

What about $(\lambda x^{\mathbb{Q}}.t)\underbrace{(b_1 + b_2)}_{S(\mathbb{Q})}$?

$$\frac{\Gamma \vdash t : \Psi \Rightarrow A \quad \Delta \vdash u : S(\Psi)}{\Gamma, \Delta \vdash tu : S(A)}$$

What about $\underbrace{((\lambda x^{\mathbb{Q}}.t) + (\lambda y^{\mathbb{Q}}.u))}_{S(\mathbb{Q} \Rightarrow A)}\ v$?

Typing applications

$$\frac{\Gamma \vdash t : \Psi \Rightarrow A \quad \Delta \vdash u : \Psi}{\Gamma, \Delta \vdash tu : A} \Rightarrow_E$$

What about $(\lambda x^{\mathbb{Q}}.t)\underbrace{(b_1 + b_2)}_{S(\mathbb{Q})}$?

$$\frac{\Gamma \vdash t : \Psi \Rightarrow A \quad \Delta \vdash u : S(\Psi)}{\Gamma, \Delta \vdash tu : S(A)}$$

What about $\underbrace{((\lambda x^{\mathbb{Q}}.t) + (\lambda y^{\mathbb{Q}}.u))}_{S(\mathbb{Q} \Rightarrow A)}\ v$?

$$\frac{\Gamma \vdash t : S(\Psi \Rightarrow A) \quad \Delta \vdash u : S(\Psi)}{\Gamma, \Delta \vdash tu : S(A)} \Rightarrow_{ES}$$

Example

$$\dfrac{\dfrac{\vdash f : \mathbb{Q} \Rightarrow A \quad \vdash g : \mathbb{Q} \Rightarrow A}{\vdash f + g : S(\mathbb{Q} \Rightarrow A)}\, S_I^+ \qquad \dfrac{\dfrac{}{\vdash |0\rangle : \mathbb{Q}}\, Ax_{|0\rangle}}{\vdash |0\rangle : S(\mathbb{Q})}\, \preceq}{\vdash (f+g)\,|0\rangle : S(A)}\, \Rightarrow_{ES}$$

$$\Downarrow$$

$$\dfrac{\dfrac{\vdash f : \mathbb{Q} \Rightarrow A \quad \dfrac{}{\vdash |0\rangle : \mathbb{Q}}\, Ax_{|0\rangle}}{\vdash f\,|0\rangle : A}\, \Rightarrow_E \qquad \dfrac{\vdash g : \mathbb{Q} \Rightarrow A \quad \dfrac{}{\vdash |0\rangle : \mathbb{Q}}\, Ax_{|0\rangle}}{\vdash g\,|0\rangle : A}\, \Rightarrow_E}{\vdash f\,|0\rangle + g\,|0\rangle : S(A)}\, S_I^+$$

Measurement

$$\pi\left(\sum_{i=1}^{n}[\alpha_i.]b_i\right) \longrightarrow_{\left(\frac{|\alpha_k|^2}{\sum_{i=1}^{n}|\alpha_i|^2}\right)} b_k$$

- $\forall i,\ b_i = |0\rangle$ or $b_i = |1\rangle$.
- $\sum_{i=1}^{n}\alpha_i.b_i$ is normal (and hence $1 \leq n \leq 2$).
- $k \leq n$

Example

$$\pi(i.\,|0\rangle + 2.\,|1\rangle) \longrightarrow_{\left(\frac{1}{3}\right)} |0\rangle$$

$$\pi(i.\,|0\rangle + 2.\,|1\rangle) \longrightarrow_{\left(\frac{2}{3}\right)} |1\rangle$$

Adding tensor products

Intepretation of types

$$S(\mathbb{Q}) \quad \textbf{vs.} \quad \mathbb{Q}$$

$$\begin{aligned}
[\![\mathbb{Q}]\!] &= \{\left|0\right\rangle, \left|1\right\rangle\} \subseteq \mathbb{C}^2 \\
[\![A \otimes B]\!] &= [\![A]\!] \times [\![B]\!] \\
[\![S(A)]\!] &= \mathcal{G}[\![A]\!]
\end{aligned}$$

Adding tensor products

Intepretation of types

$$S(\mathbb{Q}) \quad \textbf{vs.} \quad \mathbb{Q}$$

$$\begin{aligned}
[\![\mathbb{Q}]\!] &= \{|0\rangle, |1\rangle\} \subseteq \mathbb{C}^2 \\
[\![A \otimes B]\!] &= [\![A]\!] \times [\![B]\!] \\
[\![S(A)]\!] &= \mathcal{G}[\![A]\!]
\end{aligned}$$

Examples

$$\begin{aligned}
({}^1/\sqrt{2}.\,|0\rangle + {}^1/\sqrt{2}.\,|1\rangle) \;\otimes\; |0\rangle &\in [\![S(\mathbb{Q}) \otimes \mathbb{Q}]\!] \\
&= \mathcal{G}(\{|0\rangle, |1\rangle\}) \times \{|0\rangle, |1\rangle\} \\
&= \mathbb{C}^2 \times \{|0\rangle, |1\rangle\}
\end{aligned}$$

$$\begin{aligned}
{}^1/\sqrt{2}.\,|0\rangle \otimes |0\rangle + {}^1/\sqrt{2}.\,|1\rangle \otimes |1\rangle &\in [\![S(\mathbb{Q} \otimes \mathbb{Q})]\!] \\
&= \mathcal{G}(\{|0\rangle, |1\rangle\} \times \{|0\rangle, |1\rangle\}) \\
&= \mathcal{G}(\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}) \\
&= \mathbb{C}^2 \otimes \mathbb{C}^2
\end{aligned}$$

Some information is lost on reduction

Subtyping

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \leq S(\mathbb{Q})$$

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{then} \quad S(S(\mathbb{Q})) \leq S(\mathbb{Q})$$

Some information is lost on reduction

Subtyping

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \leq S(\mathbb{Q})$$

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{then} \quad S(S(\mathbb{Q})) \leq S(\mathbb{Q})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \otimes \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \otimes S(\mathbb{Q}) \leq S(\mathbb{Q} \otimes \mathbb{Q})$$

Some information is lost on reduction

Subtyping

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \le S(\mathbb{Q})$$

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{then} \quad S(S(\mathbb{Q})) \le S(\mathbb{Q})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \otimes \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \otimes S(\mathbb{Q}) \le S(\mathbb{Q} \otimes \mathbb{Q})$$

$$|0\rangle \otimes (|0\rangle + |1\rangle) \quad : \quad \mathbb{Q} \otimes S(\mathbb{Q})$$

$$|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \quad : \quad S(\mathbb{Q} \otimes \mathbb{Q})$$

Some information is lost on reduction

Subtyping

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \leq S(\mathbb{Q})$$

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{then} \quad S(S(\mathbb{Q})) \leq S(\mathbb{Q})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \otimes \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \otimes S(\mathbb{Q}) \leq S(\mathbb{Q} \otimes \mathbb{Q})$$

$$|0\rangle \otimes (|0\rangle + |1\rangle) \quad : \quad \mathbb{Q} \otimes S(\mathbb{Q})$$

$$\hookrightarrow |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \quad : \quad S(\mathbb{Q} \otimes \mathbb{Q})$$

Some information is lost on reduction

Subtyping

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \leq S(\mathbb{Q})$$
$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{then} \quad S(S(\mathbb{Q})) \leq S(\mathbb{Q})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \otimes \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \otimes S(\mathbb{Q}) \leq S(\mathbb{Q} \otimes \mathbb{Q})$$

$$|0\rangle \otimes (|0\rangle + |1\rangle) \quad : \quad \mathbb{Q} \otimes S(\mathbb{Q})$$
$$|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \quad : \quad S(\mathbb{Q} \otimes \mathbb{Q})$$

Same happens in math!

$$(X-1)(X-2) \longrightarrow X^2 - 3X + 2$$

we lost the information that it was a product

Some information is lost on reduction

Subtyping

$$\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \leq S(\mathbb{Q})$$

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \quad \text{then} \quad S(S(\mathbb{Q})) \leq S(\mathbb{Q})$$

$$\{|0\rangle, |1\rangle\} \times \mathbb{C}^2 \subset \mathbb{C}^2 \otimes \mathbb{C}^2 \quad \text{then} \quad \mathbb{Q} \otimes S(\mathbb{Q}) \leq S(\mathbb{Q} \otimes \mathbb{Q})$$

$$|0\rangle \otimes (|0\rangle + |1\rangle) \quad : \quad \mathbb{Q} \otimes S(\mathbb{Q})$$

$$\hookrightarrow |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \quad : \quad S(\mathbb{Q} \otimes \mathbb{Q})$$

Same happens in math!

$$(X-1)(X-2) \longrightarrow X^2 - 3X + 2$$

we lost the information that it was a product

Solution: casting

$$|0\rangle \otimes (|0\rangle + |1\rangle) \not\rightarrow |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle$$

$$\Uparrow^{S(\mathbb{Q}\otimes\mathbb{Q})}_{\mathbb{Q}\otimes S(\mathbb{Q})} |0\rangle \otimes (|0\rangle + |1\rangle) \rightarrow |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle$$

Full grammars

Types

$Q := \mathbb{Q} \mid Q \otimes Q$	Basis qubit types
$\Psi := Q \mid S(\Psi) \mid \Psi \otimes \Psi$	Qubit types
$A := \Psi \mid \Psi \Rightarrow A \mid S(A) \mid A \otimes A$	Types

Terms

$b := x \mid \lambda x^{\Psi}.t \mid \lvert 0\rangle \mid \lvert 1\rangle \mid b \otimes b$	Basis terms
$v := b \mid v + v \mid \alpha.v \mid \vec{0}_{S(A)} \mid v \otimes v$	Values
$t := v \mid tt \mid t + t \mid \alpha.t \mid \pi_j t \mid ?\cdot$	Terms
$\mid t \otimes t \mid head\ t \mid tail\ t \mid \Uparrow^{S(B\otimes C)}_{S(A)} t$	

where $\alpha \in \mathbb{C}$

Measurement of the first j qubits

$$\pi_j\Big(\sum_{i=1}^{n}[\alpha_i.](b_{1i}\otimes\cdots\otimes b_{mi})\Big)$$

$$\longrightarrow \left(\sum_{i\in P}\left(\frac{|\alpha_i|^2}{\sum_{i=1}^{n}|\alpha_i|^2}\right)\right)$$

$$\bigotimes_{h=1}^{j} b_{hk}\otimes\sum_{i\in P}\left(\frac{\alpha_i}{\sqrt{\sum_{i\in P}|\alpha_i|^2}}\right).(b_{j+1,i}\otimes\cdots\otimes b_{mi})$$

$P\subseteq\mathbb{N}^{\leq n}$, such that $\forall i\in P$, $\forall h\leq j$, $b_{hi}=b_{hk}$.

Example

$$\pi_2(\ 2.(|0\rangle\otimes|1\rangle\otimes|1\rangle)\ +\ |0\rangle\otimes|1\rangle\otimes|0\rangle\ +\ 3.(|1\rangle\otimes|1\rangle\otimes|1\rangle)\ )$$

$$|0\rangle\otimes|1\rangle\otimes(\tfrac{2}{\sqrt{5}}.\,|1\rangle+\tfrac{1}{\sqrt{5}}.\,|0\rangle)$$

$$|1\rangle\otimes|1\rangle\otimes(1.\,|1\rangle)$$

Overview

Some quantum properties (with dead and alive cats)
- Projective measurement
- Destructive interference
- No-cloning
- Entanglement and separability

Expressing those properties in the lambda-calculus
- Superpositions, no-cloning and measurement

Examples
- Deutsch algorithm
- Teleportation algorithm

Deutsch algorithm

Preliminaries

Hadamard

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle \qquad H\left|1\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle$$

Deutsch algorithm

Preliminaries

Hadamard

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle \qquad H\left|1\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle$$

$$H = \lambda x^{\mathbb{Q}}.{}^{1}/\sqrt{2}.(\left|0\right\rangle + x?{-\left|1\right\rangle}\cdot\left|1\right\rangle)$$

Deutsch algorithm

Preliminaries

Hadamard

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

$$H = \lambda x^{\mathbb{Q}}.{}^{1}/_{\sqrt{2}}.(|0\rangle + x?{-|1\rangle}\cdot|1\rangle)$$

Oracle

A "black box" implementing a function $f : \{0,1\} \to \{0,1\}$

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$$

Deutsch algorithm

Preliminaries

Hadamard

$$H\,|0\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \qquad H\,|1\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$$

$$H = \lambda x^{\mathbb{Q}}.{}^{1}\!/\!\sqrt{2}.(|0\rangle + x?{-}|1\rangle{\cdot}|1\rangle)$$

Oracle

A "black box" implementing a function $f : \{0,1\} \to \{0,1\}$

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$$

$$not = \lambda x^{\mathbb{Q}}.x?|0\rangle{\cdot}|1\rangle$$

Deutsch algorithm

Preliminaries

Hadamard

$$H\,|0\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \qquad H\,|1\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$$

$$H = \lambda x^{\mathbb{Q}}.{}^{1}/_{\sqrt{2}}.(|0\rangle + x?{-}|1\rangle{\cdot}|1\rangle)$$

Oracle

A "black box" implementing a function $f : \{0,1\} \to \{0,1\}$

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$$

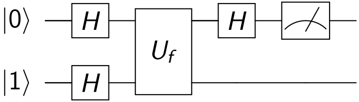
$$\begin{aligned} not &= \lambda x^{\mathbb{Q}}.x?|0\rangle{\cdot}|1\rangle \\ U_f &= \lambda x^{\mathbb{Q}\otimes\mathbb{Q}}.(head\ x) \otimes ((tail\ x)?not(f(head\ x)){\cdot}f(head\ x)) \end{aligned}$$

Deutsch algorithm

Goal:
Given an oracle U_f **determine whether f is constant or not**

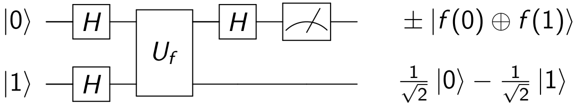
Deutsch algorithm

Goal:
Given an oracle U_f **determine whether f is constant or not**



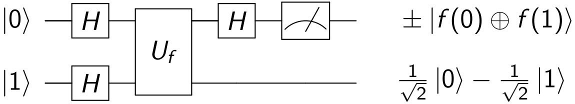
Deutsch algorithm

Goal:
Given an oracle U_f **determine whether f is constant or not**



Deutsch algorithm

Goal:
Given an oracle U_f **determine whether f is constant or not**



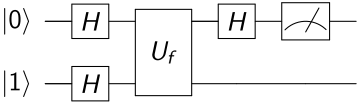
If f constant, $f(0) \oplus f(1) = 0$

$$\pm |0\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right)$$

If f not constant, $f(0) \oplus f(1) = 1$

$$\pm |1\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right)$$

Deutsch in λ



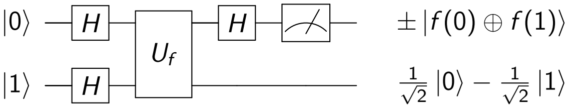
$$\pm |f(0) \oplus f(1)\rangle$$

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

$$\begin{aligned}
not &= \lambda x^{\mathbb{Q}}.x?|0\rangle{\cdot}|1\rangle \\
H &= \lambda x^{\mathbb{Q}}.{}^{1}\!/\!{}_{\sqrt{2}}.(|0\rangle + x?{-}|1\rangle{\cdot}|1\rangle) \\
H_{both} &= \lambda x^{\mathbb{Q}\otimes\mathbb{Q}}.(H(head\ x)) \otimes (H(tail\ x)) \\
U_f &= \lambda x^{\mathbb{Q}\otimes\mathbb{Q}}.(head\ x) \otimes ((tail\ x)?not(f(head\ x)){\cdot}f(head\ x)) \\
H_1 &= \lambda x^{\mathbb{Q}\otimes\mathbb{Q}}.(H(head\ x)) \otimes (tail\ x)
\end{aligned}$$

$$Deutsch_f = \pi_1(\Uparrow^{S(\mathbb{Q}\otimes\mathbb{Q})}_{S(S(\mathbb{Q})\otimes\mathbb{Q})} H_1(U_f \Uparrow^{S(\mathbb{Q}\otimes\mathbb{Q})}_{S(\mathbb{Q}\otimes S(\mathbb{Q}))} \Uparrow^{S(\mathbb{Q}\otimes S(\mathbb{Q}))}_{S(S(\mathbb{Q})\otimes S(\mathbb{Q}))} H_{both}(|0\rangle \otimes |1\rangle))$$

Deutsch in λ



$$
\begin{aligned}
not &= \lambda x^{\mathbb{Q}}.x?|0\rangle{\cdot}|1\rangle \\
H &= \lambda x^{\mathbb{Q}}.{}^1\!/\!\sqrt{2}.(|0\rangle + x?{-}|1\rangle{\cdot}|1\rangle) \\
H_{both} &= \lambda x^{\mathbb{Q}\otimes\mathbb{Q}}.(H(head\ x)) \otimes (H(tail\ x)) \\
U_f &= \lambda x^{\mathbb{Q}\otimes\mathbb{Q}}.(head\ x) \otimes ((tail\ x)?not(f(head\ x)){\cdot}f(head\ x)) \\
H_1 &= \lambda x^{\mathbb{Q}\otimes\mathbb{Q}}.(H(head\ x)) \otimes (tail\ x)
\end{aligned}
$$

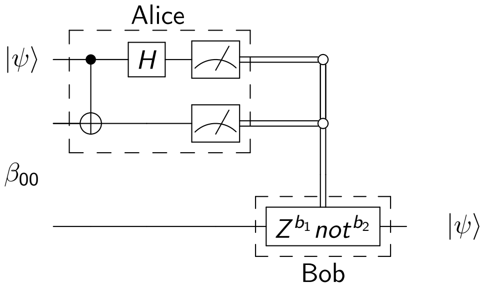
$$
Deutsch_f = \pi_1(\Uparrow^{S(\mathbb{Q}\otimes\mathbb{Q})}_{S(S(\mathbb{Q})\otimes\mathbb{Q})} H_1(U_f \Uparrow^{S(\mathbb{Q}\otimes\mathbb{Q})}_{S(\mathbb{Q}\otimes S(\mathbb{Q}))} \Uparrow^{S(\mathbb{Q}\otimes S(\mathbb{Q}))}_{S(S(\mathbb{Q})\otimes S(\mathbb{Q}))} H_{both}(|0\rangle \otimes |1\rangle)
$$

$$
\vdash Deutsch_f : \mathbb{Q} \otimes \mathbb{Q} \Rightarrow \mathbb{Q} \otimes S(\mathbb{Q})
$$

$$
\begin{aligned}
Deutsch_{id} &\longrightarrow^{*}_{(1)} \pi_1({}^1\!/\!\sqrt{2}.\,|1\rangle \otimes |0\rangle - {}^1\!/\!\sqrt{2}.\,|1\rangle \otimes |1\rangle) \\
&\longrightarrow_{(1)} |1\rangle \otimes ({}^1\!/\!\sqrt{2}.\,|0\rangle - {}^1\!/\!\sqrt{2}.\,|1\rangle)
\end{aligned}
$$

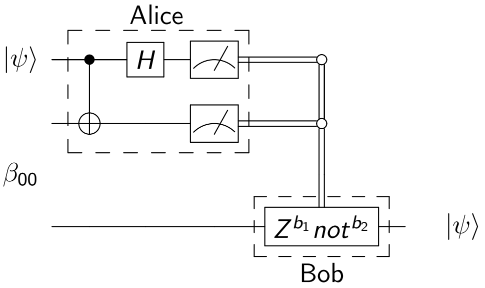
Teleportation

Goal:
To send a qubit, using an *entangled* pair, by sending only two bits of information



where $\beta_{00} = \frac{1}{\sqrt{2}} |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \otimes |1\rangle$

Teleportation in λ



$$\vdash Teleportation : S(\mathbb{Q}) \Rightarrow S(\mathbb{Q})$$

$$Teleportation\ q \longrightarrow_{(1)} q$$

$$Alice =$$

$$\lambda x^{S(\mathbb{Q})\otimes S(\mathbb{Q}\otimes\mathbb{Q})}.\pi_2(\Uparrow^{S(\mathbb{Q}\otimes\mathbb{Q}\otimes\mathbb{Q})}_{S(S(\mathbb{Q})\otimes\mathbb{Q}\otimes\mathbb{Q})} H^3_1(cnot^3_{12} \Uparrow^{S(\mathbb{Q}\otimes\mathbb{Q}\otimes\mathbb{Q})}_{S(\mathbb{Q}\otimes S(\mathbb{Q}\otimes\mathbb{Q}))} \Uparrow^{S(\mathbb{Q}\otimes S(\mathbb{Q}\otimes\mathbb{Q}))}_{S(S(\mathbb{Q})\otimes S(\mathbb{Q}\otimes\mathbb{Q}))} x))$$

$$U^b = \lambda b^{\mathbb{Q}}.\lambda x^{\mathbb{Q}}.b?Ux{\cdot}x$$

$$Bob = \lambda x^{\mathbb{Q}\otimes\mathbb{Q}\otimes\mathbb{Q}}.Z^{head\ x} not^{head\ tail\ x}.(tail\ tail\ x)$$

$$\beta_{00} = {}^1/\sqrt{2}.\ |0\rangle \otimes |0\rangle + {}^1/\sqrt{2}.\ |1\rangle \otimes |1\rangle$$

$$Teleportation = \lambda q^{S(\mathbb{Q})}.Bob\ (\Uparrow^{S(\mathbb{Q}\otimes\mathbb{Q}\otimes\mathbb{Q})}_{S(\mathbb{Q}\otimes\mathbb{Q}\otimes S(\mathbb{Q}))} Alice\ x \otimes \beta_{00})$$

Summarising

- Extension of (pure) first-order lambda-calculus for quantum computing
- Logical-linearity and algebraic-linearity both used for no-cloning
- Denotational semantics:

  Types: sets of vectors or vector spaces

  Terms: vectors

If $\Gamma \vdash t : A$ then $[\![t]\!]_{\phi_\Gamma} \subseteq [\![A]\!]$