Typing quantum superpositions and measurement

Alejandro Díaz-Caro
Universidad Nacional de Quilmes & CONICET
Buenos Aires, **Argentina**

Gilles Dowek
Inria, LSV, ENS Paris-Saclay
Cachan, **France**

TPNC 2017

December 18-20, 2017, Prague, Czech Republic

Motivation

We are interested in the most natural way of **forbidding dupplication** in **quantum programming languages** and **formal logics**

Outline

Quantum mechanics, in two slides

Simply typed lambda calculus, in two slides

Motivation, better explained

Our work: A quantum lambda calculus

Quantum mechanics, in two slides

(I) The postulates 1 and 2

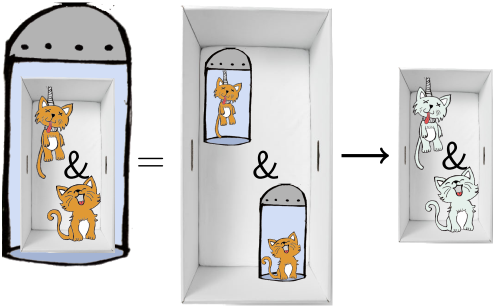
Postulate 1: Quantum states

(A bit) more precisely:
Normalized vectors $\in \mathbb{C}^{2^n}$

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha\left|0\right\rangle + \beta\left|1\right\rangle \in \mathbb{C}^2$$

$$\begin{pmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{pmatrix} = \begin{array}{l}\alpha(\left|0\right\rangle \otimes \left|0\right\rangle) + \beta(\left|0\right\rangle \otimes \left|1\right\rangle)\\ +\gamma(\left|1\right\rangle \otimes \left|0\right\rangle) + \delta(\left|1\right\rangle \otimes \left|1\right\rangle)\\ \in \mathbb{C}^4\end{array}$$

Postulate 2: Evolution



(A bit) more precisely:
Unitary transformation (matrix)

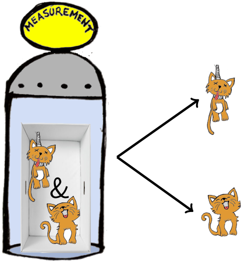
$$U\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = U(\alpha\left|0\right\rangle + \beta\left|1\right\rangle)$$

$$= \delta\left|0\right\rangle + \gamma\left|1\right\rangle = \begin{pmatrix}\delta\\ \gamma\end{pmatrix}$$

Quantum computing, in two slides

(II) The postulates 3 and 4

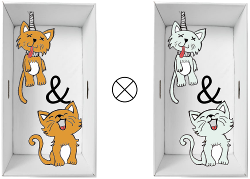
Postulate 3: Measurement



(A bit) more precisely:

$\sum_{i=0}^{2^n} \alpha_i \left|i\right\rangle$ **collapses** to $\left|k\right\rangle$
with probability $|\alpha_k|^2$

Postulate 4: Composition

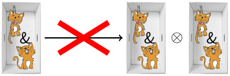


More precisely: Tensor product

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \otimes \begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \begin{pmatrix}\alpha\gamma\\ \alpha\delta\\ \beta\gamma\\ \beta\delta\end{pmatrix} \in \mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$$

Consequence: No cloning

A superposed state cannot be cloned



Simply typed lambda calculus, in two slides

(I) History, definitions, and intuitions

Introduced in 1936 by Alonzo Church

Motivation: Studying the *foundations of mathematics*
(in particular, the concept of recursion)

Why we still use it?

- Simplest model to study properties of programming languages (base of functional programming)
- Connection with logics (Curry-Howard isomorphism)

Grammar

$$t := x \mid \lambda x.t \mid tt$$

Rewrite rule

$$(\lambda x.t)\ r \to t[r/x]$$

Example: Let x^2+1 be a λ-term (with some codification)

$f(x) = x^2 + 1$ would be written $\lambda x.x^2 + 1$

$f(t)$ is written $(\lambda x.x^2+1)\ t$ and reduces to

$$(x^2+1)[t/x] \quad = \quad t^2+1$$

Simply typed lambda calculus, in two slides

(II) Types and logic

$$\begin{array}{lrcl} \textbf{Terms} & t & := & x \mid \lambda x^A.t \mid tt \\ \textbf{Types} & A & := & \tau \mid A \Rightarrow A \end{array}$$

- τ is a *basic type*
- $A \Rightarrow B$ is the function type

Context: A set of typed variables: $\Gamma = x_1^{A_1}, \dots, x_n^{A_n}$

Typing rules | Derivation rules

$$\frac{}{\Gamma, x^A \vdash x : A} \qquad \frac{\Gamma, x^A \vdash t : B}{\Gamma \vdash \lambda x^A.t : A \Rightarrow B} \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash r : A}{\Gamma \vdash tr : B}$$

Example of type derivation

$$\frac{\dfrac{\dfrac{}{y^{A\Rightarrow A} \vdash y : A \Rightarrow A}}{\vdash \lambda y^{A\Rightarrow A}.y : (A \Rightarrow A) \Rightarrow (A \Rightarrow A)} \quad \dfrac{\dfrac{}{x^A \vdash x : A}}{\vdash \lambda x^A.x : A \Rightarrow A}}{\vdash (\lambda y^{A\Rightarrow A}.y)\ (\lambda x^A.x) : A \Rightarrow A}$$

Verification: $(\lambda y^{A\Rightarrow A}.y)\ (\lambda x^A.x)$ rewrites to $\lambda x^A.x$ (of type $A \Rightarrow A$)

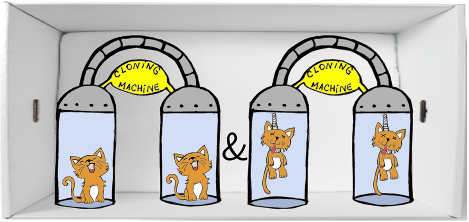
Motivation

Two approaches in the literature to deal with no cloning

Linear-logic approach

e.g. $\lambda x.(x \otimes x)$ is forbidden

Linear-algebra approach



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

Motivation

Measurement

The linear-algebra approach does not make sense here…

…but the linear-logic one, does

---

e.g.

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

Wrong!

(Measurement operator)

Key point

We need to distinguish superposed states from basis states using types

Basis states can be cloned
Superposed states cannot

Functions receiving superposed states, cannot clone its argument

Grammars

First version, without tensor

Types

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

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

Terms

$$t := \underbrace{x \mid \lambda x^{\Psi}.t \mid \ |0\rangle\ \mid\ |1\rangle}_{\text{basis terms}} \mid tt \mid \pi t \mid ?\cdot \mid \underbrace{t + t \mid \alpha.t \mid \vec{0}_{S(A)}}_{\text{linear combinations}}$$

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

Typing applications

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

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

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

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

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

Measurement

$$\pi(\alpha_1.b_1 + \alpha_2.b_2) \longrightarrow_{\left(\frac{|\alpha_k|^2}{|\alpha_1|^2+|\alpha_2|^2}\right)} b_k$$

- For $i = 1, 2$, $b_i = |0\rangle$ or $b_i = |1\rangle$.
- $k = 1, 2$

Example

$$\begin{tikzcd}
 & {|0\rangle} \\
\pi(i.\,|0\rangle + 2.\,|1\rangle) \arrow[ur, "\left(\frac{1}{5}\right)"'] \arrow[dr, "\left(\frac{4}{5}\right)"'] & \\
 & {|1\rangle}
\end{tikzcd}$$

Adding tensor products

Intepretation of types

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

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

Examples

$$\underbrace{|0\rangle}_{\mathbb{B}} \otimes \underbrace{(1/\sqrt{2}.\, |0\rangle + 1/\sqrt{2}.\, |1\rangle)}_{S(\mathbb{B})} \in \{|0\rangle, |1\rangle\} \times \mathbb{C}^2$$

$$\underbrace{1/\sqrt{2}.(|0\rangle \otimes |0\rangle) + 1/\sqrt{2}.(|0\rangle \otimes |1\rangle)}_{S(\mathbb{B}\otimes\mathbb{B})} \in \mathbb{C}^2 \otimes \mathbb{C}^2$$

Some information is lost on reduction

Subtyping

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

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \qquad \text{then} \qquad S(S(\mathbb{B})) \leq S(\mathbb{B})$$

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

Some information is lost on reduction

Subtyping

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

$$\mathcal{G}(\mathcal{G}A) = \mathcal{G}A \qquad \text{then} \qquad S(S(\mathbb{B})) \leq S(\mathbb{B})$$

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

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

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

Some information is lost on reduction

Subtyping

$$\begin{array}{rcl} \{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 & \text{then} & \mathbb{B} \leq S(\mathbb{B}) \\ \mathcal{G}(\mathcal{G}A) = \mathcal{G}A & \text{then} & S(S(\mathbb{B})) \leq S(\mathbb{B}) \end{array}$$

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

$$\begin{tikzcd} |0\rangle \otimes (|0\rangle + |1\rangle) \quad : \quad \mathbb{B} \otimes S(\mathbb{B}) \arrow[d, bend right] \\ |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \quad : \quad S(\mathbb{B} \otimes \mathbb{B}) \end{tikzcd}$$

Some information is lost on reduction

Subtyping

$$\begin{array}{rcl} \{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 & \text{then} & \mathbb{B} \leq S(\mathbb{B}) \\ \mathcal{G}(\mathcal{G}A) = \mathcal{G}A & \text{then} & S(S(\mathbb{B})) \leq S(\mathbb{B}) \end{array}$$

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

$$\begin{tikzcd} |0\rangle \otimes (|0\rangle + |1\rangle) \arrow[d, bend right] & : & \mathbb{B} \otimes S(\mathbb{B}) \\ |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle & : & S(\mathbb{B} \otimes \mathbb{B}) \end{tikzcd}$$

Same happens in math!

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

we lost the information that it was a product

Some information is lost on reduction

Subtyping

$$\begin{array}{rcl} \{|0\rangle, |1\rangle\} \subset \mathbb{C}^2 & \text{then} & \mathbb{B} \leq S(\mathbb{B}) \\ \mathcal{G}(\mathcal{G}A) = \mathcal{G}A & \text{then} & S(S(\mathbb{B})) \leq S(\mathbb{B}) \end{array}$$

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

$$\begin{tikzcd} |0\rangle \otimes (|0\rangle + |1\rangle) \arrow[d, bend right] & : & \mathbb{B} \otimes S(\mathbb{B}) \\ |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle & : & S(\mathbb{B} \otimes \mathbb{B}) \end{tikzcd}$$

Same happens in math!

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

we lost the information that it was a product

Solution: casting

$$\begin{array}{rcl} |0\rangle \otimes (|0\rangle + |1\rangle) & \not\to & |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \\ \Uparrow^{S(\mathbb{B}\otimes\mathbb{B})}_{\mathbb{B}\otimes S(\mathbb{B})} |0\rangle \otimes (|0\rangle + |1\rangle) & \to & |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \end{array}$$

Full grammars

Types

$$Q := \mathbb{B} \mid Q \otimes Q \qquad \text{Basis qubit types}$$

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

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

Terms

$$t := x \mid \lambda x^{\Psi}.t \mid |0\rangle \mid |1\rangle \mid tt \mid \pi_j t \mid ?\cdot \mid t + t \mid \alpha.t \mid \vec{0}_{S(A)}$$

$$\mid t \otimes t \mid head\ t \mid tail\ t \mid \Uparrow_{S(A)}^{S(B\otimes C)} t$$

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

Measurement of the first j qubits

Example

$$\begin{tikzcd}
 & \pi_2\big(\, 2.(|\mathbf{0}\rangle \otimes |\mathbf{1}\rangle \otimes |1\rangle) \;+\; |\mathbf{0}\rangle \otimes |\mathbf{1}\rangle \otimes |0\rangle \;+\; 3.(|\mathbf{1}\rangle \otimes |\mathbf{1}\rangle \otimes |1\rangle)\,\big) \arrow[dl, "(\frac{5}{14})"'] \arrow[dr, "(\frac{9}{14})"] & \\
|\mathbf{0}\rangle \otimes |\mathbf{1}\rangle \otimes (\frac{2}{\sqrt{5}}.\,|1\rangle + \frac{1}{\sqrt{5}}.\,|0\rangle) & & |\mathbf{1}\rangle \otimes |\mathbf{1}\rangle \otimes (1.\,|1\rangle)
\end{tikzcd}$$

The full type system

$Q := \mathbb{B} \mid Q \otimes Q$	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

$$\frac{}{x : \Psi \vdash x : \Psi}\ \mathsf{ax} \qquad \frac{}{\vdash \vec{0}_{S(A)} : S(A)}\ \mathsf{ax}_{\vec{0}} \qquad \frac{}{\vdash |0\rangle : \mathbb{B}}\ \mathsf{ax}_{|0\rangle} \qquad \frac{}{\vdash |1\rangle : \mathbb{B}}\ \mathsf{ax}_{|1\rangle}$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \alpha.t : S(A)}\ S_I^{\alpha} \qquad \frac{\Gamma \vdash t : A \quad \Delta \vdash u : A}{\Gamma, \Delta \vdash t + u : S(A)}\ S_I^{+} \qquad \frac{\Gamma \vdash t : Q_n^S}{\Gamma \vdash \pi_j t : Q_n^{S \setminus \{1,\dots,j\}}}\ S_E$$

$$\frac{\Gamma \vdash t : A \ {\scriptstyle (A \preceq B)}}{\Gamma \vdash t : B}\ \preceq \qquad \frac{}{\vdash ?\cdot : \mathbb{B} \Rightarrow \mathbb{B} \Rightarrow \mathbb{B} \Rightarrow \mathbb{B}}\ \mathsf{if} \qquad \frac{\Gamma, x : \Psi \vdash t : A}{\Gamma \vdash \lambda x : \Psi\ t : \Psi \Rightarrow A}\ \Rightarrow_I$$

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

$$\frac{\Gamma \vdash t : A}{\Gamma, x : Q \vdash t : A}\ W \qquad \frac{\Gamma, x : Q, y : Q \vdash t : A}{\Gamma, x : Q \vdash (x/y)t : A}\ C$$

$$\frac{\Gamma \vdash t : A \quad \Delta \vdash u : B}{\Gamma, \Delta \vdash t \otimes u : A \otimes B}\ \otimes_I \qquad \frac{\Gamma \vdash t : \mathbb{B} \otimes Q}{\Gamma \vdash \mathit{head}\ t : \mathbb{B}}\ \otimes_{Er} \qquad \frac{\Gamma \vdash t : \mathbb{B} \otimes Q}{\Gamma \vdash \mathit{tail}\ t : Q}\ \otimes_{El}$$

$$\frac{\Gamma \vdash t : S(S(A) \otimes B)}{\Gamma \vdash\Uparrow_{S(S(A)\otimes B)}^{S(A\otimes B)} t : S(A \otimes B)}\ \Uparrow_r \qquad \frac{\Gamma \vdash t : S(A \otimes S(B))}{\Gamma \vdash\Uparrow_{S(A\otimes S(B))}^{S(A\otimes B)} t : S(A \otimes B)}\ \Uparrow_l \qquad \frac{\Gamma \vdash\Uparrow_{S(B)}^{S(A)} t : S(A)}{\Gamma \vdash\Uparrow_{S(B)}^{S(A)} \alpha.t : S(A)}\ \Uparrow^{\alpha} \qquad \frac{\Gamma \vdash\Uparrow_{S(B)}^{S(A)} t : S(A) \quad \Delta \vdash\Uparrow_{S(B)}^{S(A)} r : S(A)}{\Gamma, \Delta \vdash\Uparrow_{S(B)}^{S(A)} t + r : S(A)}\ \Uparrow^{+}$$

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

Works in progress

- Strong normalisation and confluence proof (with J. P. Rinaldi)
- Categorical model (with O. Malherbe)
- Haskell implementation (with I. Grimma and P. E. Martínez López)

Backup slides

Why first order

$$\mathsf{CM} = \lambda y^{S(\mathbb{B})}.((\lambda x^{\mathbb{B}\Rightarrow S(\mathbb{B})}.(x\,|0\rangle)\otimes(x\,|0\rangle))\ (\lambda z^{\mathbb{B}}.y))$$

$$\begin{aligned}
&\mathsf{CM}\ (\alpha.\,|0\rangle+\beta.\,|1\rangle)\\
&\to(\lambda x^{\mathbb{B}\Rightarrow S(\mathbb{B})}.(x\,|0\rangle)\otimes(x\,|0\rangle))\ (\lambda z^{\mathbb{B}}.(\alpha.\,|0\rangle+\beta.\,|1\rangle))\\
&\to((\lambda z^{\mathbb{B}}.(\alpha.\,|0\rangle+\beta.\,|1\rangle))\,|0\rangle)\otimes((\lambda z^{\mathbb{B}}.(\alpha.\,|0\rangle+\beta.\,|1\rangle))\,|0\rangle)\\
&\to^{2}(\alpha.\,|0\rangle+\beta.\,|1\rangle)\otimes(\alpha.\,|0\rangle+\beta.\,|1\rangle)
\end{aligned}$$

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

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

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

Deutsch algorithm

Preliminaries

Hadamard

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

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

Oracle

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

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

Deutsch algorithm

Preliminaries

Hadamard

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

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

Oracle

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

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

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

Deutsch algorithm

Preliminaries

Hadamard

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

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

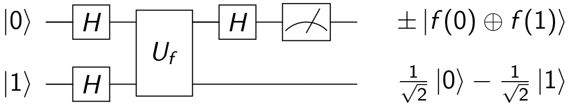
Oracle

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

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

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

Deutsch in λ



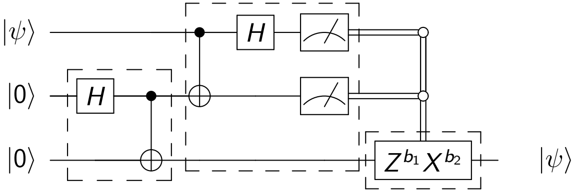
$$\begin{aligned}
not &= \lambda x^{\mathbb{B}}.x?|0\rangle{\cdot}|1\rangle \\
H &= \lambda x^{\mathbb{B}}.{}^{1}\!/\!\sqrt{2}.(|0\rangle + x?{-}|1\rangle{\cdot}|1\rangle) \\
H^{\otimes 2} &= \lambda x^{\mathbb{B}\otimes\mathbb{B}}.(H(head\ x))\otimes(H(tail\ x)) \\
U_f &= \lambda x^{\mathbb{B}\otimes\mathbb{B}}.(head\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

$$Deutsch_f = \pi_1(\Uparrow^{S(\mathbb{B}\otimes\mathbb{B})}_{S(S(\mathbb{B})\otimes\mathbb{B})} H_1(U_f \Uparrow^{S(\mathbb{B}\otimes\mathbb{B})}_{S(\mathbb{B}\otimes S(\mathbb{B}))} \Uparrow^{S(\mathbb{B}\otimes S(\mathbb{B}))}_{S(S(\mathbb{B})\otimes S(\mathbb{B}))} H^{\otimes 2}(|0\rangle \otimes |1\rangle))$$

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

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

Teleportation in λ



$$\mathrm{epr} = \lambda x^{\mathbb{B}\otimes\mathbb{B}}.\mathrm{cnot}(H_1\ x)$$

alice =

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

$$U^b = (\lambda b^{\mathbb{B}}.\lambda x^{\mathbb{B}}.b?Ux{\cdot}x)\ b$$
$$\mathrm{bob} = \lambda x^{\mathbb{B}\otimes\mathbb{B}\otimes\mathbb{B}}.Z^{head\ x}not^{head\ (tail\ x)}.(tail\ (tail\ x))$$
$$Teleportation = \lambda q^{S(\mathbb{B})}.\mathrm{bob}\ (\Uparrow^{S(\mathbb{B}\otimes\mathbb{B}\otimes\mathbb{B})}_{S(\mathbb{B}\otimes\mathbb{B}\otimes S(\mathbb{B}))}\ \mathrm{alice}\ (q\otimes(\mathrm{epr}\ \ |0\rangle\otimes|0\rangle)))$$

$$\vdash Teleportation : S(\mathbb{B}) \Rightarrow S(\mathbb{B})$$
$$Teleportation\ q \longrightarrow_{(1)} q$$