Geometry of abstraction
in quantum computation

Dusko Pavlovic

Kestrel Institute
and
Oxford University

Oxford, August 2008

Outline

Introduction
Quantum programming
\(\lambda\)-abstraction

Graphical notation

Geometry of abstraction
Abstraction with pictures
Consequences

Geometry of \(\|\)-abstraction
\(\|\)-monoidal categories
Quantum objects
Abstraction in \(\|\)-monoidal categories
Classical objects
Base

Category of measurements
Future work

Introduction

What do quantum programmers do?

\[ \begin{array}{c}
\text{x} \\
\text{f(x)} \\
\text{y} \\
\end{array} \]

Outline

Introduction
Quantum programming
\(\lambda\)-abstraction

Graphical notation

Geometry of abstraction
Abstraction with pictures
Consequences

Geometry of \(\|\)-abstraction
\(\|\)-monoidal categories
Quantum objects
Abstraction in \(\|\)-monoidal categories
Classical objects
Base

Category of measurements
Future work

Introduction

What do quantum programmers do?

\[ \begin{array}{c}
\text{x} \\
\text{f(x)} \\
\text{y} \\
\end{array} \]

\[ U_f \]

<table>
<thead>
<tr>
<th>x ∈ (\mathbb{Z}_m^2)</th>
<th>f(x) ∈ (\mathbb{Z}_n^2)</th>
</tr>
</thead>
</table>

Introduction

What do quantum programmers do?

\[ \begin{array}{c}
\text{x} \\
\text{f(x)} \\
\text{y} \\
\end{array} \]

\[ U_f \]

<table>
<thead>
<tr>
<th>x ∈ (\mathbb{Z}_m^2)</th>
<th>f(x) ∈ (\mathbb{Z}_n^2)</th>
</tr>
</thead>
</table>
**Introduction**

What do quantum programmers do?

**Simon’s algorithm**

\[
\begin{align*}
\ f : \mathbb{Z}_2^n &\to \mathbb{Z}_2^n : x \mapsto \mathbf{f}(x) \\
\ f' : \mathbb{Z}_2^{m+n} &\to \mathbb{Z}_2^{m+n} : x, y \mapsto x, \mathbf{f}(x) \oplus y \\
\ U_r : \mathbb{C}^{2^m} &\to \mathbb{C}^{2^m} : |x, y\rangle \mapsto |x, \mathbf{f}(x) \oplus y\rangle \\
\end{align*}
\]

Simon = \((H^m \otimes \text{id})U_r(H^m \otimes \text{id})\vert 0, 0\rangle = \sum_{x, z \in \mathbb{Z}_2^n} (-1)^{x \cdot z} |z, \mathbf{f}(x)\rangle

...to find a hidden subgroup

measurement \(\rightarrow\) find \(c\) such that \(\mathbf{f}(x + c) = \mathbf{f}(x)\)

**Shor’s algorithm**

\[
\begin{align*}
\ f : \mathbb{Z}_2^n &\to \mathbb{Z}_2^n : x \mapsto \hat{a}^x \mod q \\
\ f' : \mathbb{Z}_2^{m+n} &\to \mathbb{Z}_2^{m+n} : x, y \mapsto x, \hat{a}^x + y \mod q \\
\ U_r : \mathbb{C}^{2^m} &\to \mathbb{C}^{2^m} : |x, y\rangle \mapsto |x, \hat{a}^x + y \mod q\rangle \\
\end{align*}
\]

Shor = \((FT_m \otimes \text{id})U_r(FT_m \otimes \text{id})\vert 0, 0\rangle = \sum_{x, z \in \mathbb{Z}_2^n} (-1)^{x \cdot z} |z, \mathbf{f}(x)\rangle

...to find a hidden subgroup

measurement \(\rightarrow\) find \(c\) such that \(\hat{a}^{x+c} = \hat{a}^x \mod q\)

**Hallgren’s algorithm**

\[
\begin{align*}
\ h : \mathbb{Z}_2^n &\to \mathbb{Z}_2^n : x \mapsto \mathbf{l}_x \text{ (fraction ideal)} \\
\ h' : \mathbb{Z}_2^{m+n} &\to \mathbb{Z}_2^{m+n} : x, y \mapsto x, y - h(x) \\
\ U_h : \mathbb{C}^{2^m} &\to \mathbb{C}^{2^m} : |x, y\rangle \mapsto |x, y - h(x)\rangle \\
\end{align*}
\]

Hallgren = \((FT_m \otimes \text{id})U_h(FT_m \otimes \text{id})\vert d, d\rangle = \sum_{x, z \in \mathbb{Z}_2^n} (-1)^{x \cdot z} |z, h(x)\rangle

...to find a hidden subgroup

measurement \(\rightarrow\) find \(R\) such that \(h(x + R) = h(x)\)
Introduction
Quantum prog. = functional prog. + superposition + entanglement

λ-abstraction

\[ \lambda x. p(x) : B^a \text{ in } \mathcal{S} \]

\[ p(x) : B \text{ in } \mathcal{S}[x : X] \]

\[ \mathcal{S} \]

\[ F \]

\[ \mathcal{C} \]

\[ 1 \xrightarrow{a} FX \]

\[ Z \]

\[ \langle \rangle \]

\[ S \]

\[ F_a \]

\[ X \]

\[ S[x] \]

\[ x \]

\[ t \]

\[ a \]

\[ f_a \]

\[ Z[x] \]

\[ \text{ad}_a \]
Theorem (Lambek, Adv. in Math. 79)

Let $S$ be a cartesian closed category, and $S[x]$ the free cartesian closed category generated by $S$ and $x : 1 \to X$.

Then the inclusion $\lambda x \cdot S \to S[x]$ has a right adjoint $\lambda x \cdot S[x] \to S : A \to A^X$ and the transpositions

\[
\begin{align*}
A^X 
\xrightarrow{S[x](\lambda x \cdot A, B)}
S[1] 
\xrightarrow{\lambda x \cdot S[x](\lambda x \cdot A, B)}
A^X
\end{align*}
\]

model $\lambda$-abstraction and application.

$S[x]$ is isomorphic with the Kleisli category for the power monad $(-)^X$. 

---

Theorem (Lambek, Adv. in Math. 79)

Let $S$ be a cartesian closed category, and $S[x]$ the free cartesian closed category generated by $S$ and $x : 1 \to X$.

Then the inclusion $\lambda x \cdot S \to S[x]$ has a left adjoint $\lambda x \cdot S[x] \to S : A \to A^X$ and the transpositions

\[
\begin{align*}
A \xrightarrow{\lambda x \cdot S[x](\lambda x \cdot A, B)}
S[1] 
\xleftarrow{\lambda x \cdot S[x](\lambda x \cdot A, B)}
A
\end{align*}
\]

model $\lambda$-abstraction and application.

$S[x]$ is isomorphic with the Kleisli category for the product comonad $X \times (-)$. 

---

**Future work**

Measurements

‡

abstraction

Geometry of

notation

Graphical

Introduction
**Theorem (DP, MSCS 95)**

Let \( C \) be a monoidal category, and \( C[x] \) the free monoidal category generated by \( C \) and \( x : 1 \to X \).

Then the strong adjunctions \( \text{ab}_x, \text{ad}_x : C \to C[x] \) are in one-to-one correspondence with the internal comonoid structures on \( X \). The transpositions

\[
\begin{array}{c}
\lambda : X \otimes A \otimes B \\
\downarrow \\
\eta : A \otimes A \otimes B
\end{array}
\]

model action abstraction and application. \( C[x] \) is isomorphic with the Kleisli category for the comonad \( X \otimes (\_ \to \_) \), induced by any of the comonoid structures.
Given $ab_x, \vdash ad_x: C \to C[x]$, conditions 1-3. imply:

1. $ab_x(A) \vdash X \otimes A$
2. $\eta(A) \vdash X \otimes A$
3. $\eta_x = x$

Therefore the correspondence

$\mathcal{C}(ab_x(A), B) \leftrightarrow \mathcal{C}[x](A, ad_x(B))$
Proof (\(\star\))

...is actually

\[
C(X \otimes A, B) \xrightarrow{\kappa X} C[x](A, B)
\]

Proof (\(\star\))

...with

\[
C(X \otimes A, B) \xrightarrow{\kappa X} C[x](A, B)
\]

Proof (\(\star\))

...and

\[
C(X \otimes A, B) \xrightarrow{\kappa X} C[x](A, B)
\]

Proof (\(\star\))

The bijection corresponds to the conversion:

\[
C(X \otimes A, B) \xrightarrow{\kappa X} C[x](A, B)
\]

\[
(\kappa x \cdot \varphi(x)) \circ (x \otimes A) = \varphi(x) \quad (\iota\text{-rule})
\]

\[
\kappa x : (f \circ (x \otimes A)) = f \quad (\eta\text{-rule})
\]

The comonoid structure \((X, \Delta, \top)\) is

\[
\begin{align*}
\Delta & = \kappa X \\
\top & = \kappa X \id
\end{align*}
\]

Proof (\(\star\))

The conversion rules imply the comonoid laws

\[
\begin{align*}
\Delta & = \\
\top & = \\
\end{align*}
\]
Proof (1)

Given \((X, \Delta, \mathbb{T})\), use its copying and deleting power, and the symmetries, to normalize every \(c[x]\)-arrow:

\[
\varphi(x) = \mathbb{T} \circ (x \otimes A)
\]

Remark

\(c[x] \cong c_X\) and \(c[x, y] \cong c_{X \otimes Y} \cong \mathcal{L}(X \otimes Y \otimes),\) reduce the finite polynomials to the Kleisli morphisms.

Remark

\(c[x] \cong c_X\) and \(c[x, y] \cong c_{X \otimes Y} \cong \mathcal{L}(X \otimes Y \otimes),\) reduce the finite polynomials to the Kleisli morphisms.

Remark

\(c[x] \cong c_X\) and \(c[x, y] \cong c_{X \otimes Y} \cong \mathcal{L}(X \otimes Y \otimes),\) reduce the finite polynomials to the Kleisli morphisms.

Interpretation

But the extensions \(c'[x]\), where \(x'\) is large are also of interest.

\(\text{Cf. } \text{N}[\text{N}], \text{Set}[\text{Set}], \text{and } \text{CPM}(C).\)
Geometry of quantum abstraction
Dusko Pavlovic

Introduction
Graphical notation
Geometry of abstraction
Abstraction with pictures
Consequences
Geometry of ‡-abstraction
Measurements
Future work

Interpretation

Upshot
In symmetric monoidal categories, abstraction applies just to copiable and deletable data.

Definition

A vector \( \varphi \in C(I, X) \) is a base vector (or a set-like element) with respect to the abstraction operation \( \kappa x \) if it can be copied and deleted in \( C[x] \):

\[
(\kappa x \varphi \otimes x) \circ \varphi = \varphi \otimes \varphi \\
(\kappa x \text{id}_I) \circ \varphi = \text{id}_I
\]

Proposition

\( \varphi \in C(I, X) \) is a base vector with respect to \( \kappa x \) if and only if it is a homomorphism for the comonoid structure

\[
X \otimes X \xrightarrow{\Delta} X \xrightarrow{\kappa} I
\]
corresponding to \( \kappa x \).

Corollary

The substitution functors \( C[x] \rightarrow C \) are in one-to-one correspondence with the base vectors of type \( X \).

Interpretation

Upshot
In other words, only the base vectors can be substituted for variables.

Definition

Substitution is a structure preserving ioof \( C[x] \rightarrow C \).

Corollary

The substitution functors \( C[x] \rightarrow C \) are in one-to-one correspondence with the base vectors of type \( X \).
Definitions

A $\dagger$-category $\mathcal{C}$ is given with an involutive ioof $\dagger: \mathcal{C}^{\text{op}} \to \mathcal{C}$.

A morphism $f$ in a $\dagger$-category $\mathcal{C}$ is called unitary if $f^\dagger = f^{-1}$.

A (symmetric) monoidal category $\mathcal{C}$ is $\dagger$-monoidal if its monoidal isomorphisms are unitary.
\(\vdash\)-monoidal categories

Using the monoidal notations for:
- vectors: \(C(A) = C(I,A)\)
- scalars: \(I = C(I, I)\)

in every \(\vdash\)-monoidal category we can define

1. **abstract inner product**
   \[
   (\dashv -)_A : C(A) \times C(A) \rightarrow I \\
   (\varphi, \psi : I \rightarrow A) \mapsto (I \otimes_A \varphi{\downarrow \psi})
   \]

2. **partial inner product**
   \[
   (\dashv -)_{\otimes A} : C(A \otimes B) \times C(A) \rightarrow C(B) \\
   (\varphi : I \rightarrow A \otimes B, \psi : I \rightarrow A) \mapsto (I \otimes_A \varphi{\downarrow \psi})
   \]

\(\vdash\)-monoidal categories

Using the monoidal notations for:
- vectors: \(C(A) = C(I,A)\)
- scalars: \(I = C(I, I)\)

in every \(\vdash\)-monoidal category we can define

1. **abstract inner product**
   \[
   (\dashv -)_A : C(A) \times C(A) \rightarrow I \\
   (\varphi, \psi : I \rightarrow A) \mapsto (I \otimes_A \varphi{\downarrow \psi})
   \]

2. **partial inner product**
   \[
   (\dashv -)_{\otimes A} : C(A \otimes B) \times C(A) \rightarrow C(B) \\
   (\varphi : I \rightarrow A \otimes B, \psi : I \rightarrow A) \mapsto (I \otimes_A \varphi{\downarrow \psi})
   \]

**entangled vectors** \(\eta \in C(A \otimes A)\), such that \(\forall \varphi \in C(A)\)

\[
\langle \eta | \varphi \rangle_A = \psi
\]

\(\vdash\)-monoidal categories

Using entangled vectors \(\eta_A : I \rightarrow A \otimes A\) and,
\(\eta_B : I \rightarrow B \otimes B\)
their adjoints \(\varepsilon_A = \eta_A^\dagger : A \otimes A \rightarrow I\) and
\(\varepsilon_B = \eta_B^\dagger : B \otimes B \rightarrow I\)

we can define for every \(f : A \rightarrow B\)

1. **the dual** \(f^\dagger : B \rightarrow A\)
   \[
   f^\dagger = B \overset{\eta_B}{\rightarrow} BAA \overset{\eta_A^\dagger}{\rightarrow} BAA \overset{\varepsilon_A}{\rightarrow} A
   \]

2. **the conjugate** \(f^\ast : A \rightarrow B\)
   \[
   f^\ast = f^{\dagger \ast} = f^\dagger
   \]

**Proposition**

For every object \(A\) in a \(\vdash\)-monoidal category \(\mathcal{C}\) holds
\[(a) \iff (b) \iff (c).\]
\[ \eta \in \mathcal{C}(A \otimes A) \text{ is entangled} \]

\[ \varepsilon \circ (\psi \otimes \varphi) = \langle \varphi | \psi \rangle \]

\[ A \Rightarrow A \otimes A \Rightarrow A \Rightarrow A \]

The three conditions are equivalent if \( \varepsilon \) generates \( \mathcal{C} \).
Abstraction in ∇-monoidal categories

Theorem
Let $C$ be a ∇-monoidal category, and $X \otimes X \xrightarrow{\Delta} X \xrightarrow{\iota} I$ a comonoid that induces $ab_x \dashv ad_x : C \to C[x]$. Then the following conditions are equivalent:

(a) $ad_x : C \to C[x]$ creates $\triangledown : [x]^{op} \to C[x]$ such that $(x(x)) = x^1 \circ x = id_x$.

(b) $\eta = \Delta \circ \bot$ and $\epsilon = \eta^\sharp = \triangledown \circ \top$ realize $X \to X$.

(c) $(X \otimes \triangledown) \circ (\Delta \otimes X) = \Delta \circ \triangledown = (\triangledown \otimes X) \circ (X \otimes \Delta)$

where $X \otimes X \xrightarrow{\gamma} X \xrightarrow{\iota} I$ is the induced monoid $\triangledown = \Delta \uparrow$ and $\bot = \top^\uparrow$.
Abstraction in \(\&\)-monoidal categories

Theorem in pictures

(b) \[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = X = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

Proof of (b) \(\implies\) (c)

Lemma 1

If (b) holds then

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \Delta = \Delta \]

Proof of Lemma 1

Lemma 2

If \[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = X = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

then

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = X = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

Proof of Lemma 1

Using Lemma 2, and the fact that (b) implies \(\nabla = \Delta^\dagger = \Delta^*\), we get

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

Proof of (b) \(\implies\) (c)

Then (c) also holds because

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

Proof of (b) \(\implies\) (c)

Then (c) also holds because

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

Proof of (b) \(\implies\) (c)

Then (c) also holds because

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

Proof of (b) \(\implies\) (c)

Then (c) also holds because

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]

\[\begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array} = \begin{array}{c}
\Delta \\
\end{array}\begin{array}{c}
\Delta \\
\end{array}\]
There is more to categories than just diagram chasing.

There is also picture chasing.

**Definition**

A *classical object* in a $\otimes$-monoidal category $\mathcal{C}$ is a comonoid $X \otimes X \xrightarrow{\Delta} X \xrightarrow{\top} I$ satisfying the equivalent conditions from the preceding theorem.

Let $\mathcal{C}_{cl}$ be the category of classical objects and comonoid homomorphisms in $\mathcal{C}$.

**Question:** What is classical about classical objects?
Consequences

Upshot

The Frobenius condition (c) assures the preservation of the abstraction operation under $\otimes$.

This leads to entanglement.

Consequences

Proposition

The vectors $\mathcal{C}(X)$ of any classical object $X$ form a $\otimes$-algebra.
Proposition

The vectors $\mathcal{C}(X)$ of any classical object $X$ form a $\dagger$-algebra.

\[
\varphi \cdot \psi = \nabla^\circ (\varphi \otimes \psi) \\
\epsilon = \perp \\
\varphi^* = \varphi^{\dagger} = \varphi^{-1}
\]

Definition

Two vectors $\varphi, \psi \in \mathcal{C}(A)$ in a $\dagger$-monoidal category are orthonormal if their inner product is idempotent:

\[
\langle \varphi \mid \psi \rangle = (\langle \varphi \mid \psi \rangle)^2
\]

Proposition

Any two base vectors are orthonormal.
In particular, any two variables in a polynomial category are orthonormal.

Definition

A classical object $X$ is standard if it is (regularly) generated by its base vectors

\[
\mathcal{B}(X) = \{ \varphi \in \mathcal{C}(X) \mid (s_X \cdot x \otimes x)\varphi = \varphi \otimes \varphi \\
\wedge (s_X \cdot \text{id}_X)\varphi = \text{id}_X \}
\]

in the sense

\[
\forall f, g \in \mathcal{C}(X, Y). (\forall \varphi \in \mathcal{B}(X). f\varphi = g\varphi) \Rightarrow f = g
\]

A base is regular if $\mathcal{C}(X, Y) \rightarrow \mathcal{C}(Y)^{\mathcal{B}(X)}$ splits.
The classical structure is induced by a base

**Proposition 1.**
All standard classical structures, that an object $X \in C$ may carry, induce the bases with the same number of elements.

**Proposition 2.**
Let $X \in C$ be a classical object with a regular base. Then the equipotent regular bases on any $Y \in C$ are in one-to-one correspondence with the unitaries $X \to Y$.

**Definition**
A qubit type in an arbitrary $\mathcal{C}$-monoidal category $\mathcal{C}$ is a classical object $\mathbb{B}$ with a unitary $H$ of order 2. The induced bases are usually denoted by $|0\rangle, |1\rangle$, and $|+\rangle, |-\rangle$.

**Computing with qubits**
A $\mathcal{C}$-monoidal category with $\mathbb{B}$ suffices for the basic quantum algorithms.

Moreover,
$$\mathcal{F}\text{Hilb}_\Delta \cong \mathcal{F}\text{Set}$$
Proof

A $\star$-algebra in $\text{FHilb}$ is a $C^*$-algebra.

Thus for a classical $X \in \text{FHilb}$,

$$\nabla : \text{FHilb}(X) \to \text{FHilb}(X, X)$$

$$(I \to X) \mapsto (X \otimes^A X \otimes^\nabla X)$$

is a representation of a commutative $C^*$-algebra.

Working through the Gelfand-Naimark duality, we get

$$X \cong C^n$$

— because the spectrum of a commutative finitely dimensional $C^*$-algebra is a discrete set of minimal central projections, while the representing spaces are the full matrix algebras $\mathbb{C}(1)$
Claim: Simple quantum algorithms have simple categorical semantics.

Task: Implement and analyze quantum algorithms in nonstandard models: network computation, data mining.