Towards Quantamorphisms

Some thoughts on (constructive) reversibility

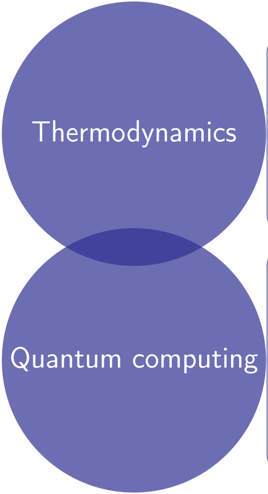
A. Neri   J.N. Oliveira   R.S. Barbosa

INESC TEC & University of Minho

ARCA meeting, 28 Feb 2018

Context

Thermodynamics & Quantum computing



Landauer's principle — any logically **irreversible** manipulation of information is followed by an increase in entropy, which in this case there is **energy consumption**;

- Quantum logic gates are represented by **unitary** matrices;
- A **unitary transformation** is an isomorphism between two Hilbert spaces, in other words: **bijective transformation**.

The Goal

Ut facient opus signa

- Use correct by construction methods to achieve reversible/quantum programming.
- *[...] by the aid of symbolism, we can make transitions in reasoning almost mechanically by the eye*
  [...] Civilisation advances by extending the number of important operations which can be performed without thinking about them."

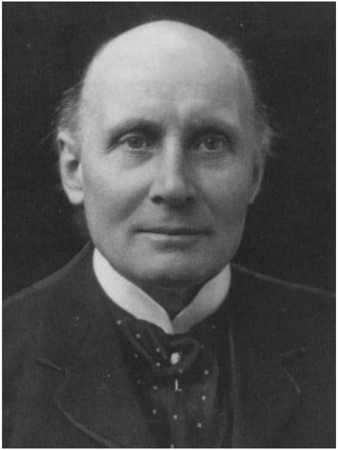


Figure: Alfred Whitehead (1911)

Generalise $y = f\ x$ to $y\ R\ x$ (or $(y, x) \in R$).

Both denoted by the arrows: $X \xrightarrow{f} Y$ and $X \xrightarrow{R} Y$.

$y\ R\ x$ is read as "it is true that y is related to x by R".

In addiction to the operators of categories (target, source, composition and identity), an *allegory* has:

- partial order;
- converse;
- intersection.

Converse

The relation: *John loves Mary*.
May be written as:

- *Mary is loved by John* or
- *Mary loves*$^\circ$ *John*.

The passive voice is the converse operation - $yRx \Leftrightarrow xR^\circ y$:

✓ $(R \cdot S)^\circ = S^\circ \cdot R^\circ$

✓ $id^\circ = id$

Partial Order

Relations are ordered:
$R \subseteq S \Leftrightarrow \langle \forall y, x :: yRx \Rightarrow ySx \rangle$
Functions are the only relation f, g to hold **shunting rules**:

✓ $f \cdot R \subseteq S \Leftrightarrow R \subseteq f^\circ \cdot S$

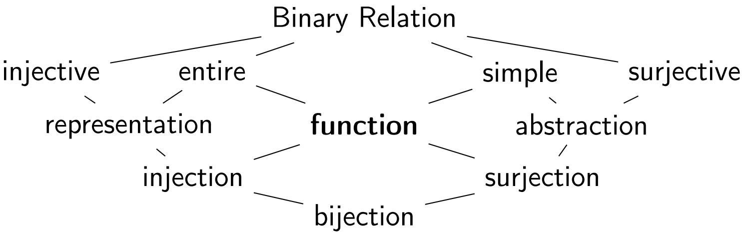
✓ $R \cdot f^\circ \subseteq S \Leftrightarrow R \subseteq S \cdot f$

A consequence of the shunting rules is the equality:

✓ $f \subseteq g \Leftrightarrow f = g \Leftrightarrow g \subseteq f$

Relations & Allegories

Relation bestiary



$R : A \leftarrow B$ is simple if $\underbrace{R \cdot R^\circ}_{img\ R} \subseteq id_A$

R simple $\Leftrightarrow$ R° injective

$R : A \leftarrow B$ is entire if $id_B \subseteq \underbrace{R^\circ \cdot R}_{ker\ R}$

R surjective $\Leftrightarrow$ R° entire

f **function**
$\Leftrightarrow \ img\ f \subseteq id \wedge id \subseteq ker\ f$
f **bijection** $\Leftrightarrow$ f° **function**
$\Leftrightarrow img\ f = id \wedge id = ker\ f$

Increasing Injectivity

We want achieve a **refinement** ordering to increase **injectivity** computation (towards **reversibility**).
To do that, we exploit the **injectivity preorder**:

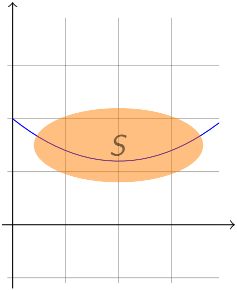
$$R \leqslant S \Leftrightarrow \ker S \subseteq \ker R$$

This ordering is rich in properties, e.g. it is upper-bounded:

$$R \triangledown S \leqslant X \Leftrightarrow R \leqslant X \wedge S \leqslant X \quad (1)$$

Using this property, we have that **pairing always increases injectivity**:

$$R \leqslant R \triangledown S \text{ and } S \leqslant R \triangledown S$$



Increasing Injectivity

The previous information shows: $\ker(R \triangledown S) \subseteq (\ker R) \cap (\ker S)$ is the equality:

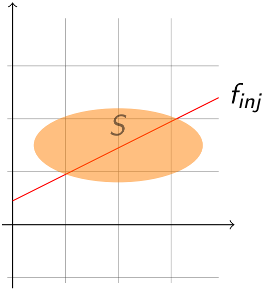
$$\ker(R \triangledown S) = (\ker R) \cap (\ker S) \tag{2}$$

In general :

$(R \triangledown S)^\circ \cdot (Q \triangledown P) = (R^\circ \cdot Q) \cap (S^\circ \cdot P)$

Injectivity shunting rule:

$R \cdot g \leqslant S \Leftrightarrow R \leqslant S \cdot g^\circ$



Ordering function by Injectivity

Restricted to functions:

$$! \leqslant f \leqslant id$$

A function is injective iff:

$$id \leqslant f$$

$f \triangledown id$ is always injective
f and g are **complementary** iff:

$$id \leqslant (f \triangledown g)$$

e.g. *fst* and *snd* are complementary.

Minimal Complements

Definition

g is the minimal complement of f iff:

1. $id \leqslant f \triangledown g$
2. $id \leqslant f \triangledown h$ and $h \leqslant g$ then $g \leqslant h$

Minimal complements (not unique in general) characterise "what is missing" in the original function for **injectivity** to hold.

exclusive-or

$$(\dot\vee) = \begin{array}{c|cccc} & 0 & 0 & 1 & 1 \\ & 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{array}$$

This function is surjective but not injective.
Its minimal complement is:

$$fst = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Minimal Complements

Example Analyse

$$\ker \dot{\vee} = \ker \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$\ker g$ has to cancel all 1's that fall outside the diagonal.

The identity would work but it is not minimal.

Other possibility is add 1s where $\ker(\dot{\vee})$ has 0s:

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Kernels of functions are equivalence relations: **reflexive**, **symmetric** and **transitive**.

A symmetric+reflexive relation is an equivalence iff it is difunctional.

> A relation is difunctional iff
> $R \cdot R^{\circ} \cdot R \subseteq R$

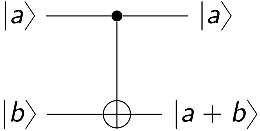
Result
CNOT

To ensure difunctionality we cancel zeros symmetrically, outside the diagonal:

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} = \ker \mathit{fst} \text{ or } \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} = \ker \mathit{snd}$$

fst and snd are minimal complements of $\dot{\vee}$. Complementing $\dot{\vee}$ with fst :

$$2 \times 2 \xrightarrow{\mathit{fst} \triangledown \dot{\vee}} 2 \times 2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



CNOT quantum gate

Going General

In the example the functions of type $A \times B \xrightarrow{fst} A$ and $A \times B \rightarrow B$ are paired, making room for the **bijection** $A \times B \rightarrow A \times B$
We want to offer arbitraty $f : A \rightarrow B$ in a bijective envelope of the type:
$A \times B \rightarrow A \times B$

Supposing f is a recursive function, e.g. $f = \textbf{foldr}\, g\ b$.
To construct the envelope we start to define: $\llparenthesis f \rrparenthesis(x, b) = \textbf{foldr}\, \overline{f}\ b\ x$
where $\overline{f}\ a\ b = f(a, b)$

$$\llparenthesis f \rrparenthesis([], b) = b$$
$$\llparenthesis f \rrparenthesis(a : x, b) = f(a, \llparenthesis f \rrparenthesis(x, b))$$

$$\begin{tikzcd}
{[A] \times B} \arrow[d, "\llparenthesis f \rrparenthesis"'] & B + A \times ([A] \times B) \arrow[l, "\alpha"'] \arrow[d, "id + id \times \llparenthesis f \rrparenthesis"] \\
B & B + A \times B \arrow[l, "{[id, f]}"]
\end{tikzcd}$$

$$Functor : F\ X = B + A \times X$$

Going General

Natural ($\mathbb{N}_0$)

Starting from a simple fold, over natural numbers ($\textbf{for}\ f\ i\ n = f^n\ i$):

$$\textbf{for}\ f\ i\ 0 = i$$
$$\textbf{for}\ f\ i(n+1) = f(\textbf{for}\ f\ i\ n)$$

$$\begin{tikzcd}
\mathbb{N}_0 \times B \arrow[d, "(\!| f |\!)"'] & B + \mathbb{N}_0 \times B \arrow[l, "\alpha"'] \arrow[d, "id + (\!| f |\!)"] \\
C & B + C \arrow[l, "f"]
\end{tikzcd}$$

$$Functor : F\ X = B + X$$

$$\alpha = [\underline{0} \triangledown id, succ \times id] = [\underline{0}, succ \cdot fst] \triangledown [id, snd]$$

The complementation fst with f:

$$(\!| [\underline{0}, succ] |\!) \triangledown (\!| [id, f] |\!) :: \mathbb{N}_0 \times B \leftarrow \mathbb{N}_0 \times B \quad (3)$$

General Case

$\Psi\ f$

The complementation in (3) is reminds us of the banana-split rule:

banana-split

$$(\!| f |\!) \triangledown (\!| g |\!) = (\!| (f \cdot (id + fst)) \triangledown (g \cdot (id + snd)) |\!)$$

Defining: $\mathbb{N}_0 \times B \xleftarrow{\Psi f} \mathbb{N}_0 \times B = fst \triangledown (\!| [id, f] |\!)$, where $f : B \rightarrow B$
That is, $\Psi f(n, b) = (n, f^n b)$ is a for-loop that keeps its input.

Using the banana-split rule: $\Psi f = (\!| [\underline{0} \triangledown id, succ \times f] |\!)$

$$\begin{cases} \Psi f(\underline{0} \triangledown id) = \underline{0} \triangledown id \\ \Psi f \cdot (succ \times id) = (succ \times f) \cdot \Psi f \end{cases} \tag{4}$$

General Case

Ψ preserves injectivity

$$[\underline{0} \triangledown id, succ \times f] \text{ is } \textbf{injective} \text{ iff } f \text{ is injective}$$

By the rule:

[R,S] injective iff both R, S injective and $R^{\circ} \cdot S \subseteq \perp$

Note that $\underline{0}^{\circ} \cdot succ \subseteq \perp$ since there is no $n \in \mathbb{N}_0$ such that $succ\ n = 0$.

To prove that Ψ preserves injectivity it is enough to prove that $(\!|\ \_\ |\!)$ does so:

$$f \text{ injective} \Rightarrow (\!| f |\!) \text{ injective} \qquad (5)$$

Towards Quantamorphim

Matrices

matrices as arrows

- $M : B \leftarrow A$ is a matrices with #A columns and #B rows.
- M is defined in a field, e.g. complex numbers.
- If the domain A or the codomain B are 1 then M is a column vector or a row vector.
- the composition $M \cdot N$ is matrix multiplication
  $b(M \cdot N)c = \langle \Sigma a :: (bMa) \times (aNc) \rangle$

Towards Quantamorphisms

Bijections → unitary transformations

Relations and Functions can be seen as boolean matrices. e.g. negation function ($\neg$). But as matrix it became divisible:

$$\neg = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = (\sqrt{\neg}) \cdot (\sqrt{\neg}) = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} \cdot \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$$

The matrix ($\sqrt{\neg}$) is unitary - refined notion of reversible:

A matrix $A \xleftarrow{M} A$ is unitary iff

$$M^\dagger \cdot M = id = M \cdot M^\dagger$$

where $M^\dagger = \overline{M}^\circ$ is the conjugate transpose of M and

$$\overline{x + y\ i} = x - y\ i \qquad \overline{\begin{bmatrix} M & N \\ P & Q \end{bmatrix}} = \begin{bmatrix} \overline{M} & \overline{N} \\ \overline{P} & \overline{Q} \end{bmatrix}$$

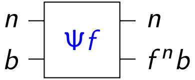
Quantum mechanical processes governed by unitary matrices are the building blocks of Quantum Programming.

Towards Quantamorphisms

Reversible → Unitary

Recall:

$$\Psi f \cdot \alpha = [\underline{0} \triangledown id, succ \times f] \cdot (id + \Psi f)$$



We need to extend pairing $(\_ \triangledown \_)$ and junction $[\_, \_]$ to arbitrary matrices.

$(\_ \triangledown \_)$ gives rise to Khatri-Rao product:

$(x, y)(M \triangledown N)a = (xMa)(yNa)$

$R \cup S$ become $b(M + N)a$

$R \cap S$ become $b(M \times N)a$

Linearity is the essence:

$Q \cdot (M + N) = Q \cdot M + Q \cdot N$

$(M + N) \cdot Q = M \cdot Q + N \cdot Q$

The Khatri-Rao leads to the Kronecker tensor (or product):

$$\begin{array}{c} A \\ M \downarrow \\ C \end{array} \qquad \begin{array}{c} B \\ N \downarrow \\ D \end{array} \qquad \begin{array}{c} A \times B \\ \downarrow M \otimes N \\ C \times D \end{array}$$

by $M \otimes N = (M \cdot fst) \triangledown (N \cdot snd)$

$[R, S]$ corresponds to $[M|N]$ which collates matrices horizontally

Towards Quantamorphisms

The property of relations: $[R, S] \cdot [P, Q]^\circ = R \cdot P^\circ \cup S \cdot Q^\circ$
holds for matrices: $[M|N] \cdot [P|Q]^\circ = M \cdot P^\circ + N \cdot Q^\circ$
Then

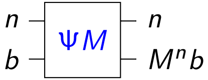
$$\Psi M = [\underline{0} \triangledown id, (succ \otimes M) \cdot \Psi M] \cdot^\circ$$

$$\Leftrightarrow \Psi M = ([\underline{0} \triangledown id) \cdot ([\underline{0} \triangledown id)^\circ + (succ \otimes M) \cdot \Psi M \cdot (succ^\circ \otimes id)$$

Thus we obtain a recursive matrix definition whose least fixpoint is:

$$\Psi M = \mu X.(B + (succ \otimes M) \cdot X \cdot (succ^\circ \otimes id)$$

where $B = (\underline{0} \triangledown id) \cdot (\underline{0} \triangledown id)^\circ$



The quantamorphism implementing the quantum for gate which iterates M over the second input controlled by the first one.

Quantamorphism ΨM in Matlab

matlab — vi quanta.m — 54×30

```
function R = quanta(n,M)

%   n * b <---- alpha ------ b + n * b
%       |                        |
%       |                        |
%       X                     id + X
%       |                        |
%       |                        |
%       v                        V
%   n * b <---- [ A B ]----- b + n * b

   [b,a] = size(M);
   if ~(b==a)
       error('M must be square');
   else
       R0=zeros(n*b,n*b); id=eye(b);
       A=kr(const(b,n,1),id);
       alpha=[A kron(succ(n),id)];
       B=kron(succ(n),M);
       C=[A B];
       R = fix(b,R0,C,alpha);
   end
end

function R = fix(b,X,C,alpha)
   id=eye(b);
   Y= C*(oplus(id,X))*alpha';
   if (Y==X) R = X; else R = fix(b,Y,C,alpha); end
end
```

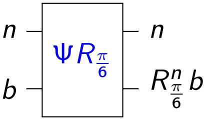
Towards Quantamorphisms

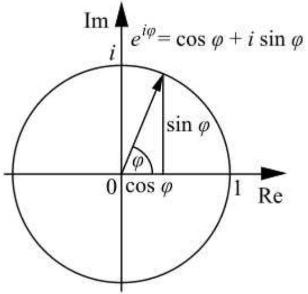
Iterating a phase-shift gate

Consider the so-called phase shift gate defined by $R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$

To the specific case of:

$$R_{\frac{\pi}{6}} = \begin{bmatrix} 1 & 0 \\ 0 & 0.867 + 0.5i \end{bmatrix}$$





Towards Quantamorphisms

Iterating a phase-shift gate

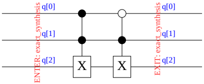
f_4 is unitary:

$$
\left[\begin{array}{cc|cc|cc|cc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0.867+0.5i & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0.5+0.867i & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & i
\end{array}\right]
$$

Note the effect of complementation $(fst \triangledown \_)$ shifting the corresponding iteration of gate $R_{\frac{\pi}{6}}$ along the diagonal.

Towards Quantamorphisms

Quipper



This is the quantum circuit for **for** $(\neg)(i, q)$ where $i = 0..3$:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Conclusions & Future work

- Build upon previous work on stochastic folds in LAoP;
- Towards correct by construction quantum programs;
- Quantamorphisms have the advantage over other quantum strategies of dispensing with measurements;
- The (linear) algebra of (unitary) quantamorphims is the topic of my MSc project (grantee INESC TEC);
- It would be interesting see in a Picturing Quantum Process approach, and the quipper implementation.

References I

- F. Bancilhon and N. Spyratos. Update semantics of relational views. ACM TDS, 6(4):557–575, December 1981.
- R. Bird and O. de Moor. Algebra of Programming. Series in Computer Science. Prentice-Hall, 1997.
- J.N. Foster, M.B. Greenwald, J.T. Moore, B.C. Pierce, and A. Schmitt. Combinators for bidirectional tree transformations: A linguistic approach to the view-update problem. ACM Trans. Program. Lang. Syst., 29(3):17, 2007. ISSN 0164-0925.
- P.J. Freyd and A. Scedrov. Categories, Allegories, volume 39 of Mathematical Library. North-Holland, 1990.
- Ralf Hinze. Adjoint folds and unfolds — an extended study. Science of Computer Programming, 78(11):2108–2159, 2013. ISSN 0167-6423.
- Hsiang-Shang Ko and Zhenjiang Hu. An axiomatic basis for bidirectional programming. PACMPL, 2(POPL):41:1–41:29, 2018. doi: 10.1145/3158129. URL http://doi.acm.org/10.1145/3158129.

References II

- K. Matsuda, Z. Hu, K. Nakano, M. Hamana, and M. Takeichi. Bidirectionalization transformation based on automatic derivation of view complement functions, 2007. 12th ACM SIGPLAN International Conference on Functional Programming (ICFP 2007), Freiburg, Germany, October 1-3.
- C. Morgan. Programming from Specification. Series in Computer Science. Prentice-Hall International, 1990. C.A.R. Hoare, series editor.
- S-C. Mu, Z. Hu, and M. Takeichi. An injective language for reversible computation. In MPC 2004, pages 289–313, 2004. doi: 10.1007/978-3-540-27764-4 16.
- D. Murta and J.N. Oliveira. A study of risk-aware program transformation. SCP, 110:51–77, 2015.
- J.N. Oliveira. A relation-algebraic approach to the "Hoare logic" of functional dependencies. JLAP, 83(2):249–262, 2014.

References III

- N.S. Yanofsky and M.A. Mannucci. Quantum Computing for Computer Scientists. Cambridge University Press, 2008. doi:10.1017/CBO9780511813887.