Categorical Quantum Computing: the necessity of Euler decomposition

Simon Perdrix

CNRS, Laboratoire d’Informatique de Grenoble

Joint work with Ross Duncan (U. Oxford)

Categorical Computer Science’09, Grenoble
Context and Motivations
Categorical axiomatisation of QIP

- †-compact closed categories [Abramsky, Coecke, LiCS’04], categorical axiomatisation of the teleportation underlying the information flow.

- Basis structure [Pavlovic, Coecke, 06], categorical semantics of State transfer [Coecke, Paquette, Perdrix, MFPS’08]

- Unbiased basis [Coecke, Duncan, ICALP’08], proof of Shor algorithm.

Diagram: [See image for diagram representation]
Categorical axiomatisation of QIP

- $\dagger$-compact closed categories [Abramsky, Coecke, LiCS’04], categorical axiomatisation of the teleportation underlying the information flow.

- Basis structure [Pavlovic, Coecke, 06], categorical semantics of State transfer [Coecke, Paquette, Perdrix, MFPS’08]

- Unbiased basis [Coecke, Duncan, ICALP’08], proof of Shor algorithm.
Categorical axiomatisation of QIP

- †-compact closed categories [Abramsky, Coecke, LiCS’04], categorical axiomatisation of the teleportation underlying the information flow.

- Basis structure [Pavlovic, Coecke, 06], categorical semantics of State transfer [Coecke, Paquette, Perdrix, MFPS’08]

- Unbiased basis [Coecke, Duncan, ICALP’08], proof of Shor algorithm.
An Example Computation

The heart of Shor’s algorithm for factorisation is the Quantum Fourier Transform.

\[ |1\rangle \quad \pi \quad \text{H} \quad \text{H} \quad = \quad \text{H} \quad \pi \quad \text{H} \]

\[ |0\rangle \quad \text{H} \quad \text{H} \quad \text{H} \quad \pi/4 \quad -\pi/4 \quad \pi/4 \]

... an example computation with inputs symbolically by rewriting...

Lucas Dixon (U. Edinburgh) (photo by Dan Oi, U. Strathclyde at QUISCO Inaugural Meeting)
Towards a categorical axiomatisation of entanglement

**Graph states:**

- Representation of entanglement
- Applications: One-way QC [Raussendorf, Briegel 00], Quantum secret sharing [Markham, Sanders 08].

**This talk:** Abstract proof of the fundamental properties of graph states.

**Objectives:**

- Reveal the structures of entanglement.
- Refine the graphical language.
Diagrammatic language
Diagrammatic language

Definition
A diagram is a finite undirected open graph generated by the family of vertices:

where \( \alpha \in [0, 2\pi) \).
• Composition ($\circ$)

![Composition Diagram]

• Tensor ($\otimes$)

![Tensor Diagram]

• Dagger ($\dagger$)

![Dagger Diagram]
Diagrams form a †-compact closed category with basis structures.
Diagrams form a $†$-compact closed category with basis structures.
\[ \begin{bmatrix} H \\ H \end{bmatrix} = \begin{bmatrix} H \end{bmatrix} \]
Hadamard
Complementary basis

Copying

Bialgebra

$\pi$-Commutation
Interpretation in FdHilb

\[
\begin{bmatrix}
\end{bmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix}
1 \\
1
\end{pmatrix}
\]

\[
\begin{bmatrix}
\end{bmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix}
1 & 1
\end{pmatrix}
\]

\[
\begin{bmatrix}
\end{bmatrix} = \begin{pmatrix}
1 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 1
\end{pmatrix}
\]

\[
\begin{bmatrix}
\end{bmatrix} = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
\]

\[
\begin{bmatrix}
\end{bmatrix} = R_z(\alpha) = \begin{pmatrix}
1 & 0 \\
0 & e^{i\alpha}
\end{pmatrix}
\]

\[
\begin{bmatrix}
\end{bmatrix} = H = \frac{1}{\sqrt{2}} \begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix}
\]

\[
\begin{bmatrix}
\end{bmatrix} = R_x(\alpha)
\]

\[
\begin{bmatrix}
\end{bmatrix} = \Lambda Z = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1
\end{pmatrix}
\]
Interpretation in FdHilb

\[ \begin{bmatrix} 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \]

\[ \begin{bmatrix} 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \end{pmatrix} \]

\[ \begin{bmatrix} \alpha \end{bmatrix} = R_z(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \]

\[ \begin{bmatrix} H \end{bmatrix} = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \]

\[ \begin{bmatrix} \alpha \end{bmatrix} = R_x(\alpha) \]

\[ \begin{bmatrix} \alpha \end{bmatrix} = \Lambda Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \]
Abstract Graph states
Abstract Graph states

Definition
An abstract graph state is a diagram composed of green dots and $H$ only such that:
– every green dot is connected to exactly one input or output
– every $H$ is connecting two green dots
– there is no connection between two green dots

\[
\left[ \begin{array}{c} H \\ \hline \end{array} \right] = |G_{\text{triangle}}\rangle:
\]
Abstract Graph states

Definition
An **abstract graph state** is a diagram composed of green dots and $H$ only such that:
- every green dot is connected to exactly one input or output
- every $H$ is connecting two green dots
- there is no connection between two green dots

\[ \begin{bmatrix} H & H \\ H & \end{bmatrix} = |G_{\text{triangle}}\rangle : \]
Property (Fixpoint)

Given a graph $G$ and a vertex $u \in V(G)$,

$$R_{x \pi}^{(u)} R_{z \pi}^{(\mathcal{N}_G(u))} |G\rangle = |G\rangle$$
Proof fixpoint
Theorem (Van den Nest)

Given a graph $G$ and a vertex $u \in V(G)$,

$$R_x(\pi/2)^{(u)} R_z(-\pi/2)^{(NG(u))} |G\rangle = |G * u\rangle .$$

where $G * u = G \Delta K_{NG(u)}$ is the graph obtained by applying a local complementation on $u$ in $G$ [Bouchet85].

Two locally equivalent graphs represent the same entanglement
Theorem (Van den Nest)

Given a graph $G$ and a vertex $u \in V(G)$,

$$R_x(\frac{\pi}{2})^{(u)} R_z(-\frac{\pi}{2})^{(NG(u))} |G\rangle = |G \ast u\rangle .$$

where $G \ast u = G \Delta K_{NG(u)}$ is the graph obtained by applying a local complementation on $u$ in $G$ [Bouchet85].

Two locally equivalent graphs represent the same entanglement.
Euler decomposition

\[ H = -\pi/2 - \pi/2 - \pi/2 \]
Lemma

The $H$-decomposition into $\pi/2$ rotations is not unique:

$$H = -\pi/2 - \pi/2 - \pi/2 = \Rightarrow H = -\pi/2 - \pi/2 - \pi/2$$

Proof:

$$H = \pi/2 = H = \pi/2 = \pi/2 = \pi/2 = \pi/2$$
Lemma

Each colour of $\pi/2$ rotation may be expressed in terms of the other colour.

Proof:
Lemma

\[ H = -\frac{\pi}{2} - \frac{\pi}{2} - \frac{\pi}{2} \Rightarrow \frac{\pi}{2} \]

\[ H \quad H \quad H = \]

\[ \begin{array}{c}
\text{Lemma}
\end{array} \]
Proof

\[ H \square H = H - \pi / 2 - \pi / 2 - \pi / 2 = H - \pi / 2 - \pi / 2 - \pi / 2 = -\pi / 2 H - \pi / 2 - \pi / 2 = \pi / 2 \]
Lemma

Local complementation implies the $H$-decomposition:

$$
\begin{align*}
H &\xrightleftharpoons{\pi/2} H - \pi/2 - \pi/2 = H
\end{align*}
$$
\[
\begin{align*}
H & = -\frac{\pi}{2} \\
H & = \frac{\pi}{2} \\
H & = -\frac{\pi}{2} \\
H & = \frac{\pi}{2} \\
H & = H
\end{align*}
\]
Theorem
Van den Nest’s theorem holds if and only if $H$ has a Euler decomposition:
H-decomposition is a new rule

Let $\llbracket \cdot \rrbracket^b$ be exactly as $\llbracket \cdot \rrbracket$ with the following change:

$$\llbracket \alpha \rrbracket^b = R_z(2\alpha)$$

This functor preserves all the axioms of the language, but

$$\llbracket H \rrbracket^b \neq \llbracket \pi/2 \rrbracket^b \circ \llbracket \pi/2 \rrbracket^b \circ \llbracket \pi/2 \rrbracket^b$$

hence the Euler decomposition is not derivable from the axioms of the theory.


- Abstract proof of Van den Nest theorem.
- Euler decomposition as a sufficient and necessary condition for Van den Nest theorem.
- Refine the diagrammatic language and point out a structure of entanglement.

Van den Nest Theorem: Locally equivalent graphs represent the same entanglement.
There exist graphs which are representing the same entanglement but which are not locally equivalent [Ji, Chen, Wei, Ying’08].

- Refine the language for capturing the previous case.
- Apply to states that cannot be represented by graphs.
Conclusion

• Abstract proof of Van den Nest theorem.

• \( H \) Euler decomposition as a sufficient and necessary condition for Van den Nest theorem.

• Refine the diagrammatic language and point out a structure of entanglement.

Van den Nest Theorem: Locally equivalent graphs represent the same entanglement.
There exist graphs which are representing the same entanglement but which are not locally equivalent [Ji,Chen,Wei,Ying’08].

• Refine the language for capturing the previous case.

• Apply to states that cannot be represented by graphs.
Lucas Dixon & Ross Duncan & Aleks Kissinger

http://dream.inf.ed.ac.uk/projects/quantomatic