Verifying the Measurement Calculus by Rewriting

Ross Duncan
Oxford University Computing Laboratory

Quantum States

Quantum computation is based on treating quantum mechanical systems as computational devices.

- States are unit vectors $|\psi\rangle, |\phi\rangle$ in some complex Hilbert space $\mathbb{C}^n$.

$$\text{Qubits:} \quad |0\rangle, |1\rangle \in \mathbb{C}^2 \qquad |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

- If two quantum systems with state spaces A and B are allowed to interact, the state space of the joint system is $A \otimes B$.

- **Consequence:** the joint system has states which cannot be decomposed into a product of its subsystems:

$$|00\rangle + |11\rangle \neq |\phi\rangle \otimes |\psi\rangle$$

  Such states are called *entangled*.

Quantum Circuits

Without external interactions, quantum systems evolve according to *unitary* dynamics. A model of quantum computation is called *universal* if it can perform any unitary map.

The quantum circuit model is based on some universal family of unitary gates, for example:

$$Z_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \wedge Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

By composing these 1- and 2-qubit operations, in sequence or parallel, any unitary map may be constructed.

Quantum Measurements

Quantum states are not freely accessible. *Measurements* are neither deterministic nor side-effect free.

Every basis $\{\mathbf{b}_i\}_{i=1}^n$ of a Hilbert space defines a **measurement** of that space

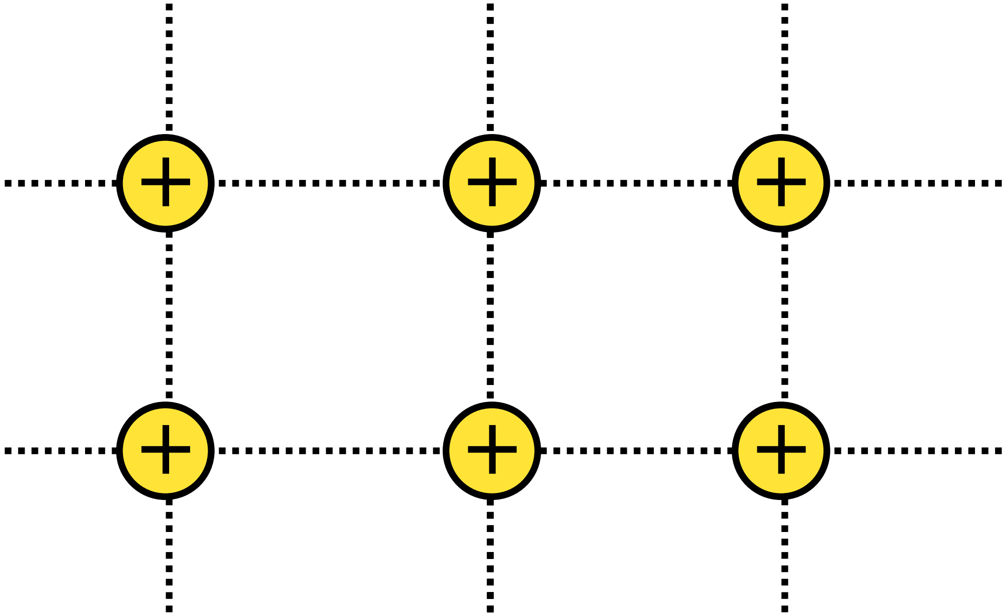
- The possible outcomes of the measurement are the individual basis vectors $\mathbf{b}_i$;
- The probability of the outcome $\mathbf{b}_i$ is $|\langle \mathbf{b}_i \mid \psi \rangle|^2$
- After the measurement the new state of the system is $\mathbf{b}_i$.

By measuring part of an entangled system we can alter the state of the entire system – this leads to *Measurement-Based Computing*.

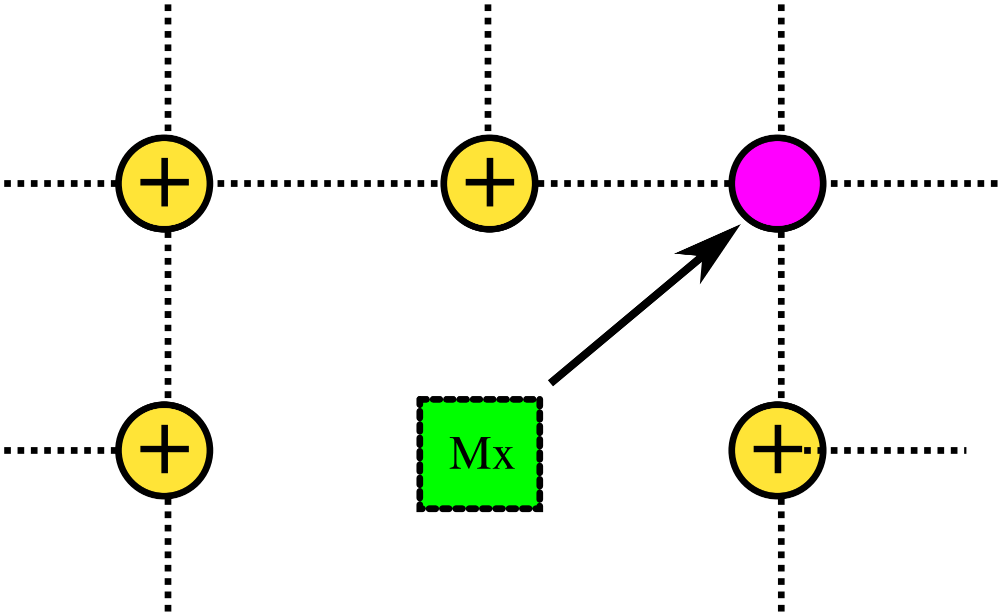
The One-Way Model

The One-way model was introduced by Raussendorf and Briegel; it is one of the most promising models of quantum computation with respect to implementations.

- Basic resource is a *cluster state*; a large multiply entangled state, generated by entangling operations between pairs of qubits.



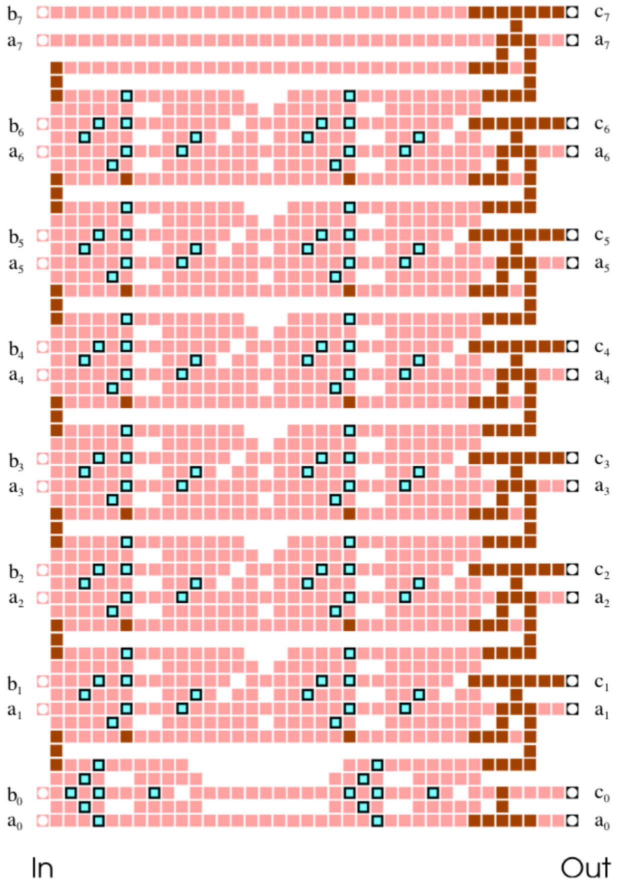
- Operations are single qubit measurements and single qubit unitaries.
- Operations can depend on the outcomes of earlier measurements.



- Measuring a qubit disentangles it, effectively removing it from the cluster, hence the name *one-way*.

Shown to be universal by simulating any quantum circuit.

1WQC Example



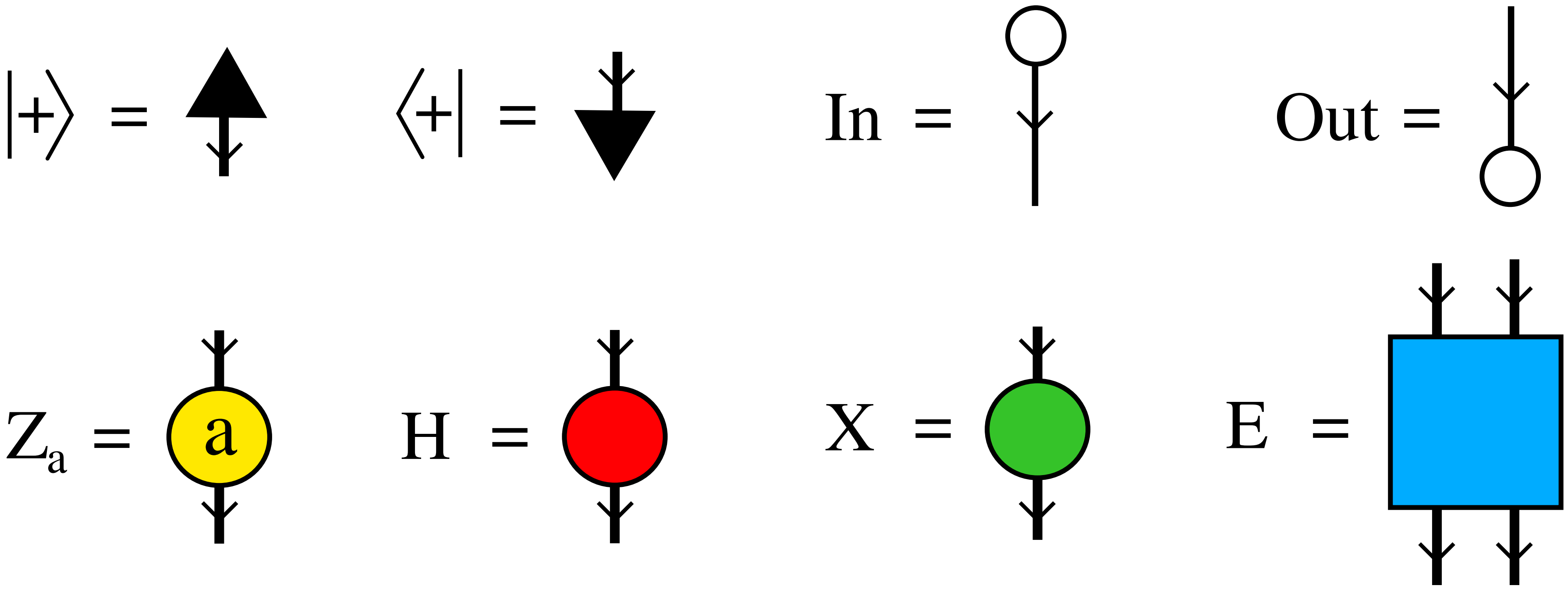
(diagram stolen from Raussendorf et al, PRA 68 (2003))

Entangled States

- The structure of an entangled state is essentially that of the computation which generated it;
- Can build a representation of such states as *diagrams* – graphs whose vertices are the basic interactions (gates)
- However such a representation will not generally be unique: need to consider a quotient of the free theory
- Do this by *rewriting on diagrams*

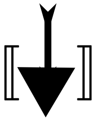
Formal Diagrams

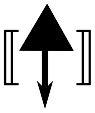
Definition 1. A formal *diagram* is a directed graph whose vertices are chosen from the following set:

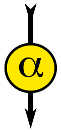


Semantics For Diagrams

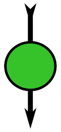
To each diagram D, with n inputs and m outputs, we assign a linear map $[\![D]\!] : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$.

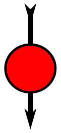
$[\![$  $]\!] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \end{pmatrix}$

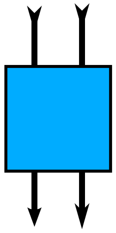
$[\![$  $]\!] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$[\![$ 

$]\!] = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$

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

$[\![$  $]\!] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$[\![$  $]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

Circuit-like Diagrams

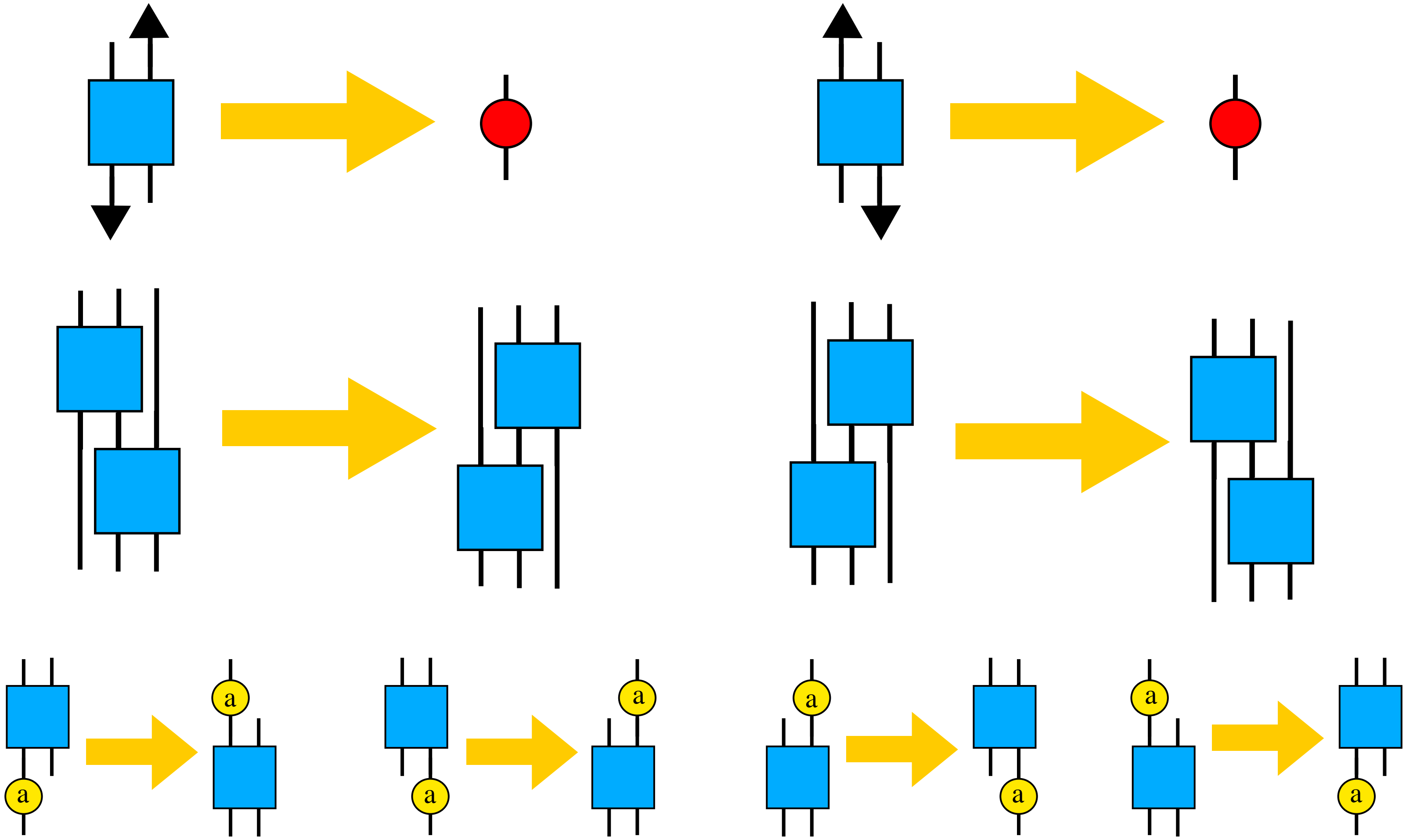
Definition 2. A diagram is called *circuit-like* if:

- It does not contain $\langle+|$; (i.e., no non-outputs), and
- It is acyclic.

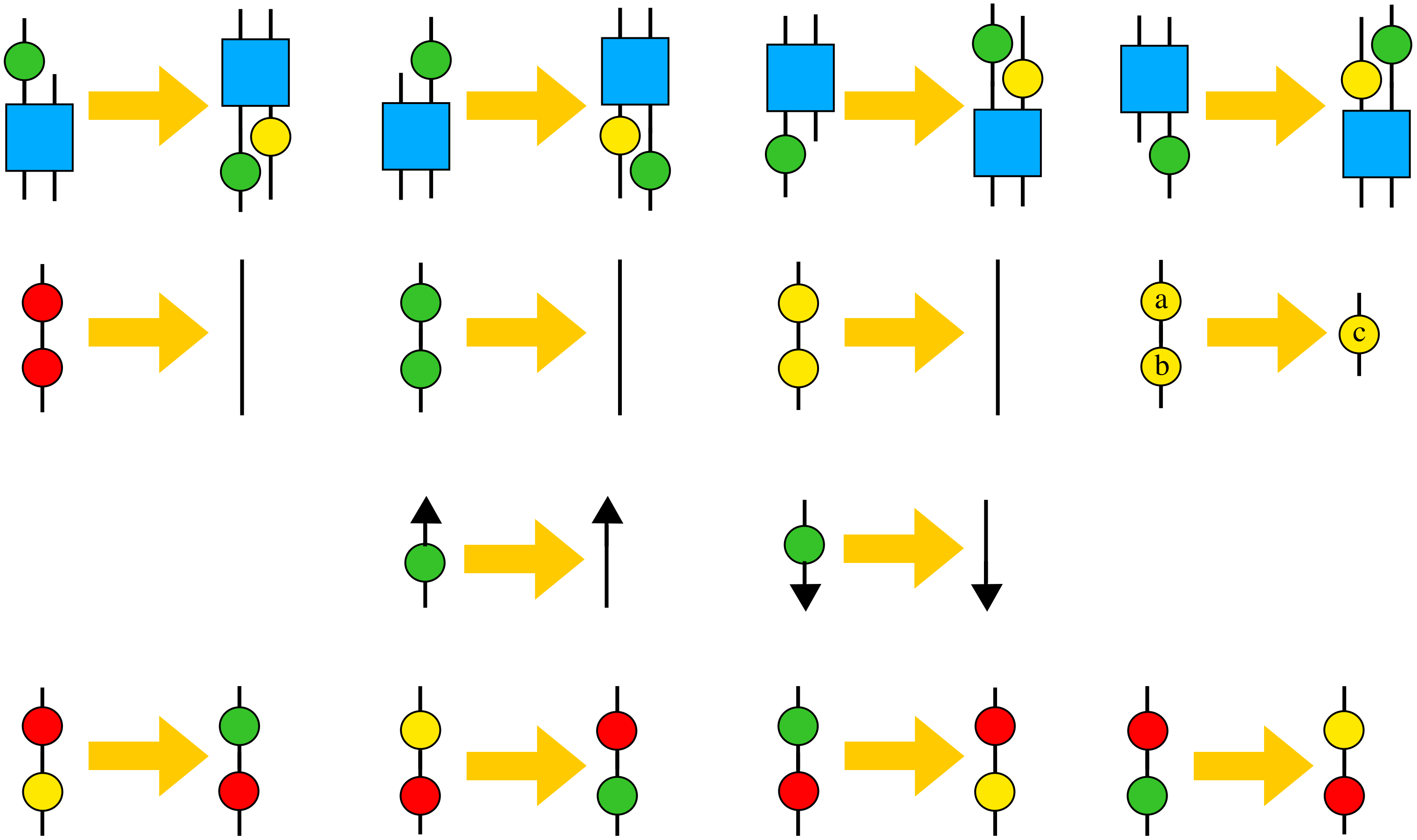
Since we have a universal set of unitaries, and sequential and parallel composition, it is clear that the image the circuit-like diagrams under $[\![\cdot]\!]$ contains all quantum circuits.

However $[\![\cdot]\!]$ is not faithful: there are infinitely many diagrams with the same denotation.

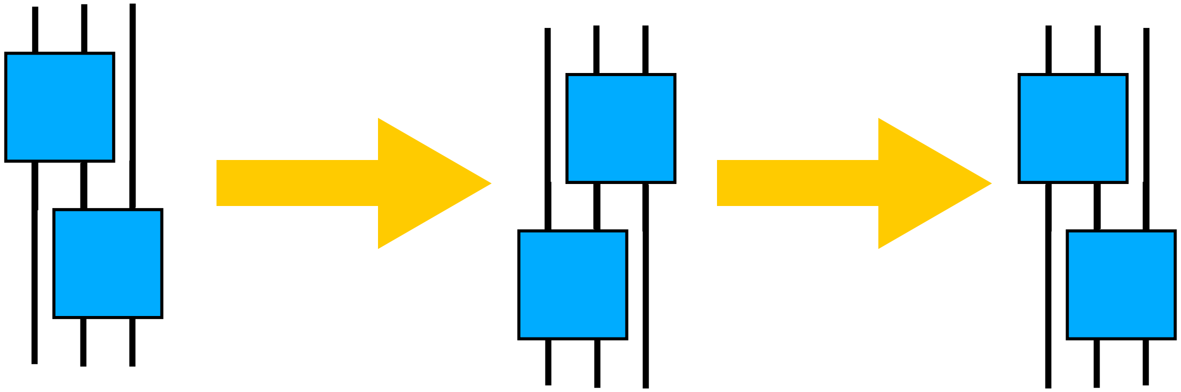
Rewrite System $\mathcal{R}$ (1)



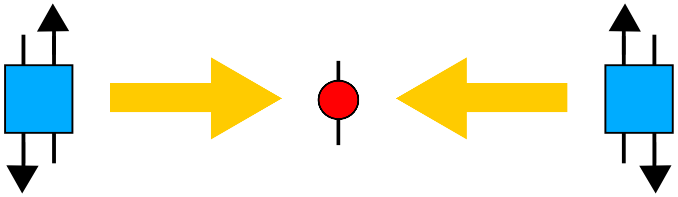
Rewrite System $\mathcal{R}$ (2)



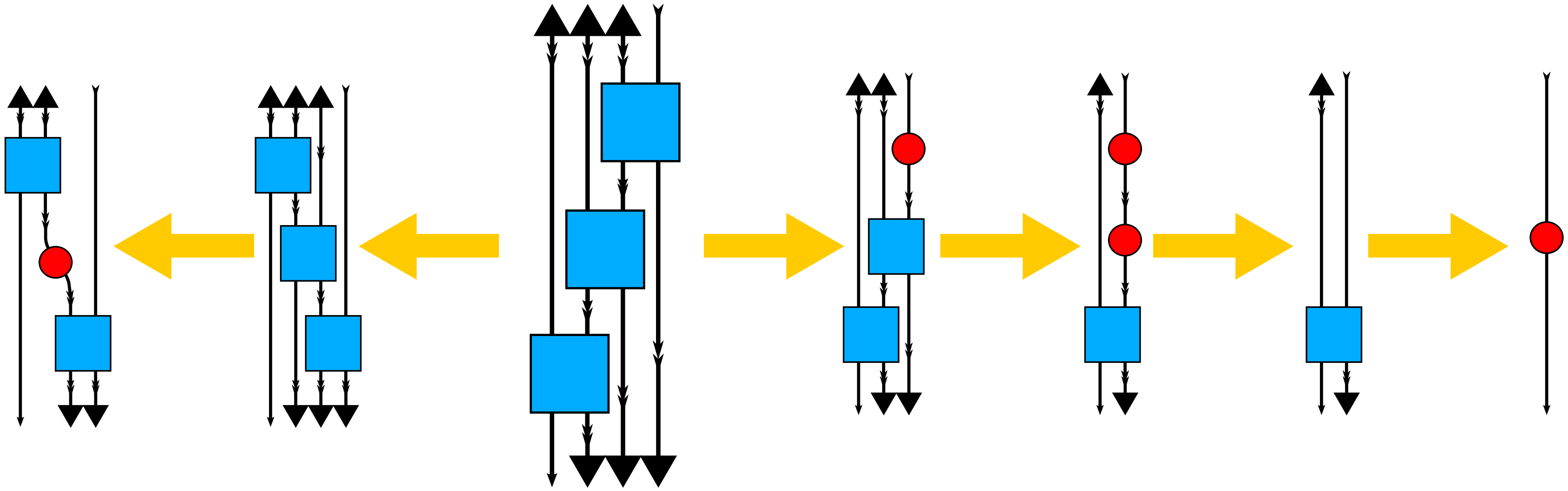
$\mathcal{R}$ is not terminating



Definition 3. Call a diagram D *irreducible* if no rewrite sequence starting from D contains the rules



$\mathcal{R}$ is not confluent



In this instance both end-point are terminal – no further rewrites are possible – but only the right hand one is circuit-like.

The Measurement Calculus

Introduced by Danos, Kashefi and Pananagden for the 1-way model

1. A set V of qubits, numbered $1, \ldots n$;
2. Subsets $I \subseteq V$, $O \subseteq V$ of inputs and outputs;
3. All $q \notin I$ initialised to $|+\rangle$;
4. All $q \notin O$ must eventually be measured and not reused.

Compute using *patterns* comprised of

$$\begin{aligned} N_i &= \text{Prepared qubit } |+\rangle \\ E_{ij} &= \wedge Z \\ X_i, Z_j &= \text{Pauli X,Z corrections} \\ M_i^{\alpha} &= \text{1-qubit measurement in basis } |0\rangle \pm e^{i\alpha} |1\rangle \end{aligned}$$

where i, j index over qubits.

Measurement Calculus (cont.)

Theorem. *Measurement patterns are universal with respect to unitaries.*

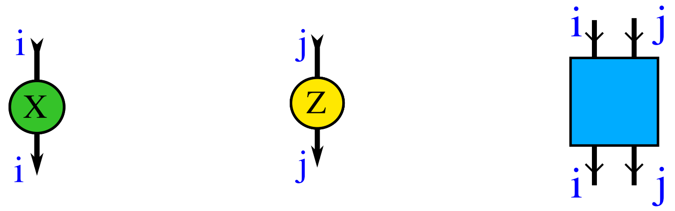
A slight variation with only X-Y measurements is approximately universal.

Theorem. *Every measurement pattern is equivalent to a pattern where all E_{ij} precede all M_i^α which precede all X_i, Y_j.*

Further there is an effective rewriting procedure to put any pattern into this (EMC)-normal form.

Labels and Conditionals

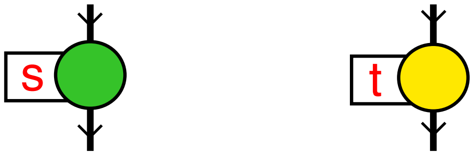
Definition 4. An A-*labelling* for diagram D is a map from the edge set of D to some set A; it is said to be *correct* when the edges incident at a Z_α, X and $\wedge Z$ vertices cohere as shown:



The rewrite rules must be modified to take the labels into account, but this is (mostly) easily done.

It is straightforward to show that the rewrites then preserve correctness of the labelling.

Definition 5. Let s,t be boolean variables, called signals; then operations conditional upon these variables take effect iff the associated boolean expression evaluates to true.

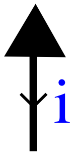


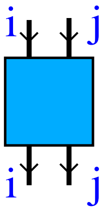
If a diagram contains conditional operations, its denotation is a set of linear maps, one for each possible valuation of the set of signals.

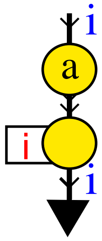
Again, minor modifications to the rewrites are required: conditional elements behave normally w.r.t. commuting rewrites; they cancel only with other conditional operations.

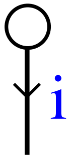
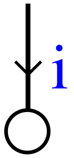
Translating the Measurement Calculus

Take a pattern $\mathfrak{P}$ to be in EMC form and define a diagram $D(\mathfrak{P})$, whose edges are labelled by the qubits of $\mathfrak{P}$, by translating $\mathfrak{P}$'s commands sequence:

$N_i \mapsto$ 

$E_{ij} \mapsto$ 

$M_i^a \mapsto$ 

If qubit i is not prepared or not measured then adjoin  or  as appropriate.

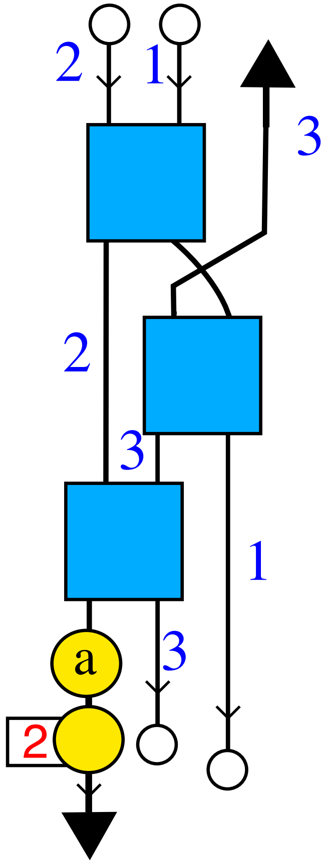
Small Example

Consider the 3-qubit measurement pattern

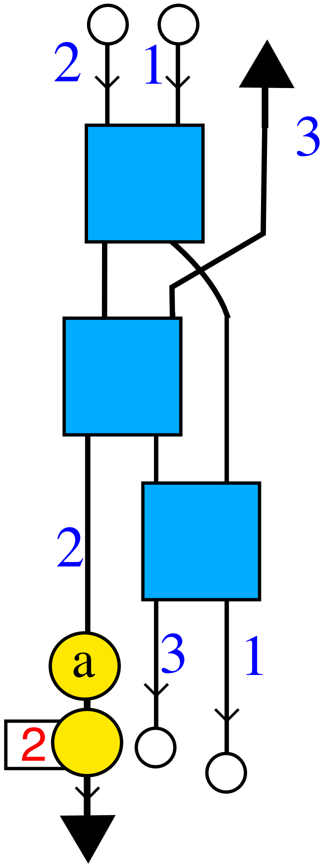
$$M_2^a E_{12} E_{13} E_{23} N_3$$

with $I = \{1, 2\}$ and $O = \{1, 3\}$.

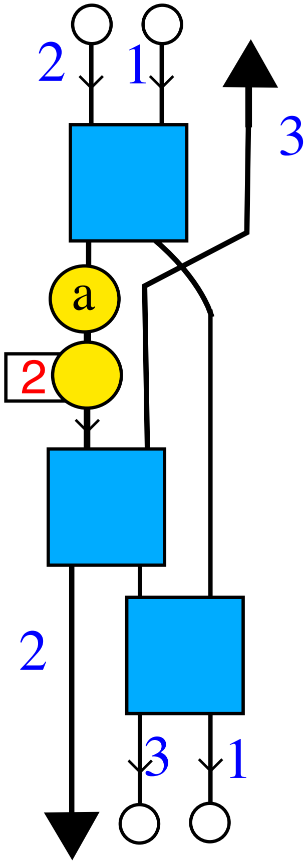
$M_2^a E_{12} E_{13} E_{23} N_3$



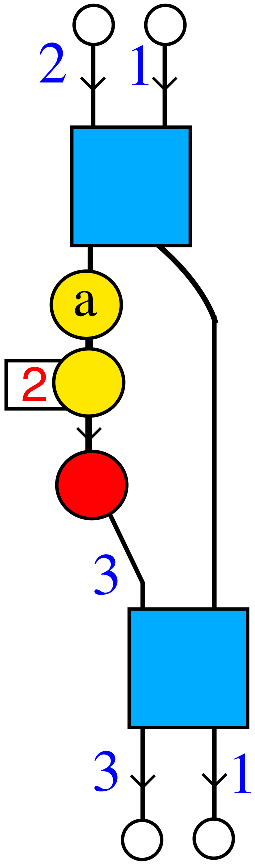
$M_2^a E_{12} E_{13} E_{23} N_3$



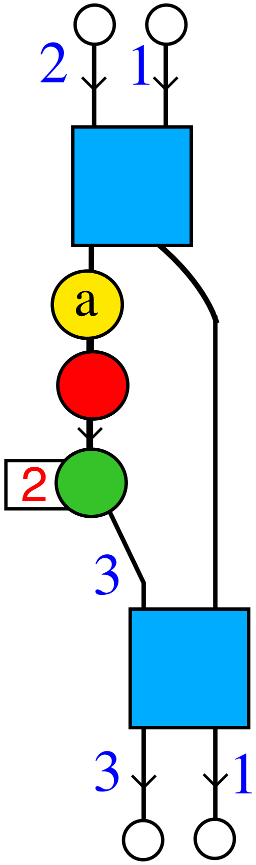
$M_2^a E_{12} E_{13} E_{23} N_3$



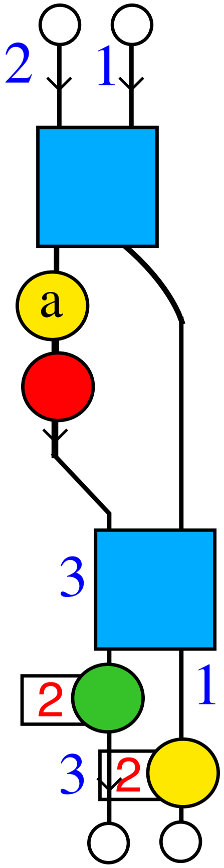
$M_2^a E_{12} E_{13} E_{23} N_3$



$M_2^a E_{12} E_{13} E_{23} N_3$



$M_2^a E_{12} E_{13} E_{23} N_3$



Flow

Definition 6. The entanglement graph of a pattern $(G_E(\mathfrak{P}), I, O)$ has *flow* if there exists a map $f : O^c \to I^c$ and a partial order $\leq$ on the vertices of G such that

- $f(i) \sim i$
- $i \leq f(i)$
- $j \sim f(i)$ implies $i \leq j$

Theorem (Danos-Kashefi). *If (G, I, O) has a flow $(f, \leq)$ then there is a pattern on G which is (strongly, uniformly) deterministic.*

The Main Theorem

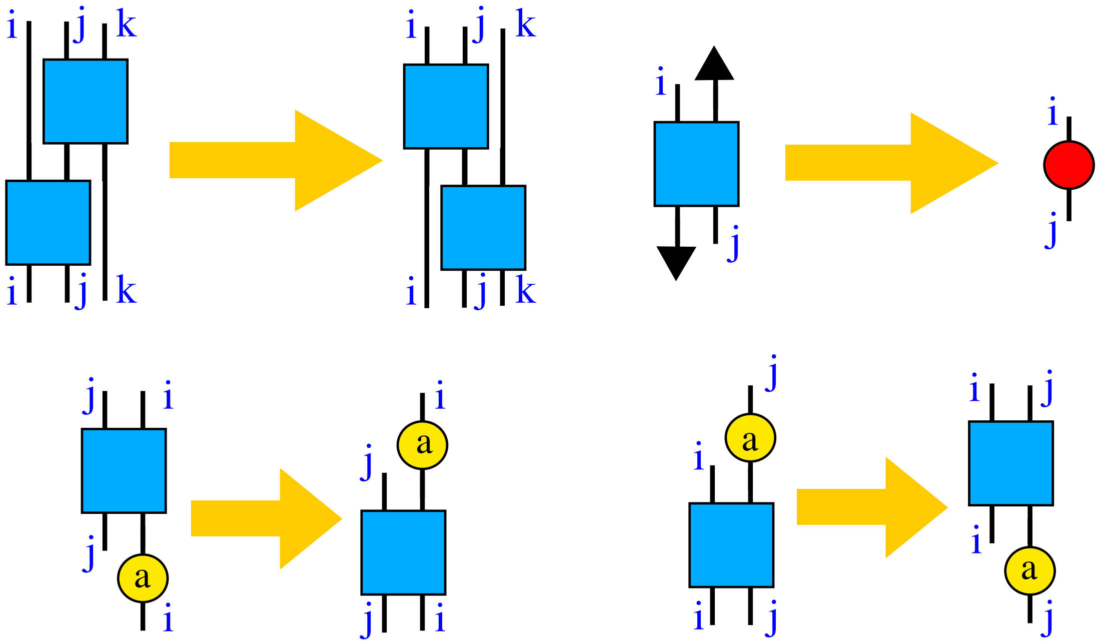
Theorem 7. *Let $\mathfrak{P}$ be a pattern with geometry (G, I, O), and let D be the diagram defined by $\mathfrak{P}$. (G, I, O) has a flow iff there exists a circuit-like irreducible diagram D' such that $D \xrightarrow{\mathcal{R}} D'$.*

From Flow to Circuits

Knowledge of a flow $(f, <)$ for a given pattern $\mathfrak{P}$ provides enough information to form a rewrite strategy to find a circuit-like reduct of $D(\mathfrak{P})$.

A Minimal Rewrite System $\mathcal{R}_f$

Suppose $\mathfrak{P}$ has a flow $(f, <)$. Let $\mathcal{R}_f$ be the transitive and reflexive closure of the following rewrite rules applied to the labelled diagram $D(\mathfrak{P})$:



Side Condition: these rules can be applied only when $f(i) = j$ or $f(j) = k$.

$\mathcal{R}_f$ is Strongly Normalising

Proposition 8. *$\mathcal{R}_f$ is both terminating and locally confluent.*

Proof. **Confluence**: check critical pairs; in each case the flow conditions prevent getting stuck off track.

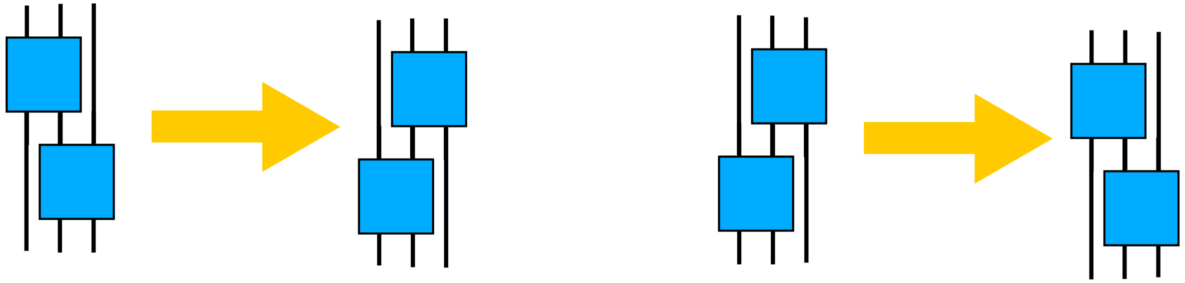
Termination: each rewrite has the effect of more closely aligning the temporal structure of the diagram with that of the flow, and since both are finite there can be no infinite reduction sequences. □

$\mathcal{R}_f$-Normal Forms are (almost) Circuit-like

Proposition 9. *Let D^* be the $\mathcal{R}_f$-normal form derived from $D(\mathfrak{P})$; then D^* contains no occurrence of $\langle +|$.*

Proof. Suppose that $\langle +|$ occurs in D^*; then it must also occur in $D(\mathfrak{P})$. It is possible to show that there is an $\mathcal{R}_f$-sequence beginning from $D(\mathfrak{P})$ such that the offending occurrence is eliminated. However $\mathcal{R}_f$ is confluent, so this is a contradiction. □

Proposition 10. *Let D^* be the $\mathcal{R}_f$-normal form derived from $D(\mathfrak{P})$; then there exists D^{**} such that $D^* \xrightarrow[\mathcal{R}]{} D^{**}$ and this rewrite sequence contains only the rules*



Proof. If D^* has a cycle, then necessarily it must traverse two consecutive $\wedge Z$ vertices – otherwise it forms an *influencing path*, contradicting the assumption that $\mathfrak{P}$ has a flow. Applying the rewrite to this pair of $\wedge Z$ vertices will break the cycle. □

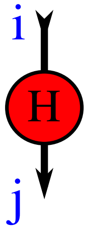
From Circuits to Flow

Since the translation from the measurement calculus syntax to diagrams added labels to $D(\mathfrak{P})$ corresponding to the physical qubits of the pattern $\mathfrak{P}$ there is enough information embedded in any circuit-like reduct of $D(\mathfrak{P})$ to reconstruct a flow for $\mathfrak{P}$.

Reconstructing the Flow

Let D^* be a circuit-like reduct of $D(\mathfrak{P})$.

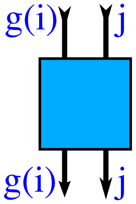
Definition 11. Let g be a partial function on V defined by

$g(i) = j$ iff  occurs in D^*.

Lemma 12. *The function g is a total injective function from O^c to I^c, such that $i \sim g(i)$.*

Reconstructing the Flow (cont.)

Now define a relation $<$ on V by the reflexive and transitive closure of

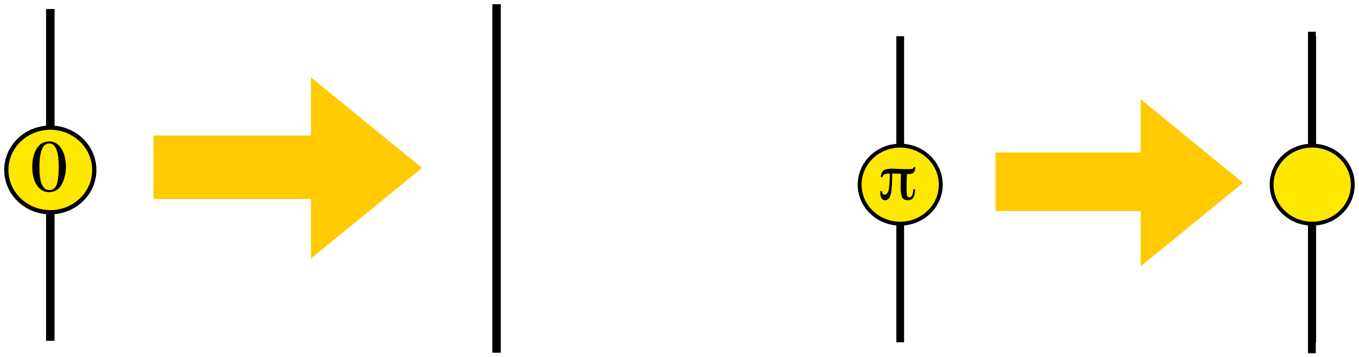
$\{i < g(i)\} \quad \cup \quad \Bigg\{ i < j \mid$  occurs in $D^* \Bigg\}$.

Proposition 13. *The pair* $(g, <)$ *defines a flow on* $\mathfrak{P}$.

Proof. By virtue of Lemma 12 and the definition of $<$, $(g, <)$ trivially satisfy the flow conditions. It remains to show that $<$ is a partial order, i.e. that it is anti-symmetric – this follows from the acyclicity of D^*. □

Uniformity

The statement of the flow theorem demonstrates *uniform* determinism. It is possible to augment $\mathcal{R}$ to find circuits for patterns which are not uniformly deterministic.



Remarks

- The equations of this rewriting system capture the notion the flow.
- Can use rewrites to find the corrections for a given pattern.
- However many true equations are not provable!
- Fails to capture *generalised flow* of Browne, Kashefi, Mhalla and Perdrix.
- Could make $\mathcal{R}$ well behaved at the cost of having normal forms which are not circuit-like – but is it possible to do better?
- There is a polytime flow finding algorithm [de Beaudrap] is it possible to build this in to the rewriting system?
- Is there a better set of primitives than the ones shown here?