

Determinism and Computational Power of Real Measurement-based Quantum Computation

Simon Perdrix, Luc Sanselme

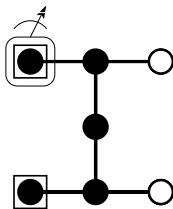
CNRS, Inria Project team CARTE, LORIA
simon.perdrix@loria.fr

FCT'17 – Bordeaux



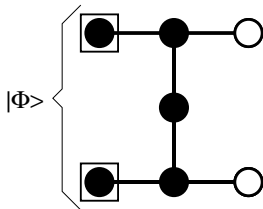
Introduction - Context

MBQC: Measurement-based Quantum Computation [Briegel, Raussendorf'01]



- Universal model of quantum computation.
- Conceptual and technological breakthrough
- Decreasing depth of quantum computations [Browne, Kashefi, Perdrix'10]
- Blind QC [Broadbent, Fitzsimon, Kashefi'09]
- Interactive Proofs [McKague]

Resource: Graph state

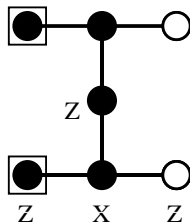


Property. Given a graph G , and $u \in V(G) \setminus I$,

$$X_u Z_{N(u)} |G\rangle = |G\rangle$$

where $X = \begin{matrix} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{matrix}$ and $Z = \begin{matrix} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{matrix}$

Resource: Graph state

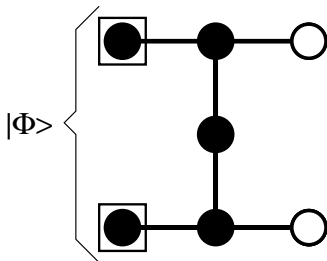


Property. Given a graph G , and $u \in V(G) \setminus I$,

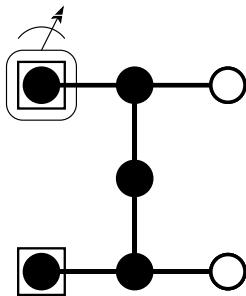
$$X_u Z_{N(u)} |G\rangle = |G\rangle$$

where $X = \begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \mapsto \begin{matrix} |1\rangle \\ |0\rangle \end{matrix}$ and $Z = \begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \mapsto \begin{matrix} |0\rangle \\ -|1\rangle \end{matrix}$

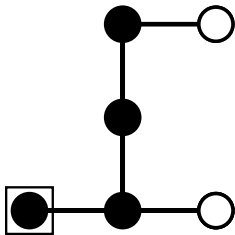
The tool: measurements



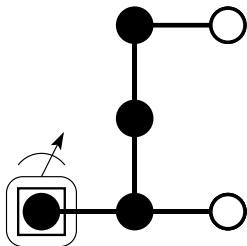
The tool: measurements



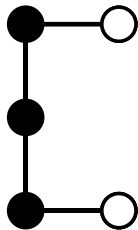
The tool: measurements



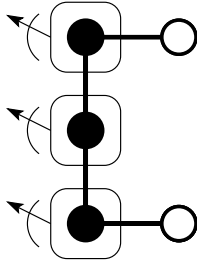
The tool: measurements



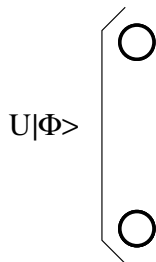
The tool: measurements



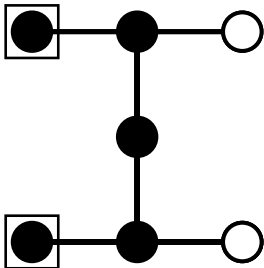
The tool: measurements



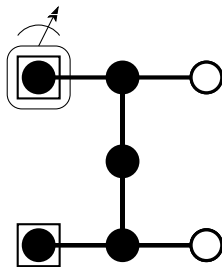
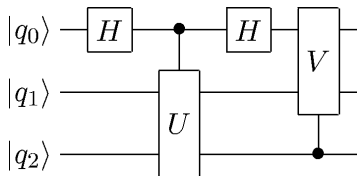
The tool: measurements



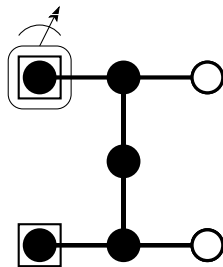
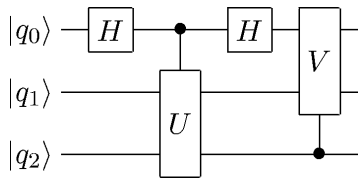
The tool: measurements



Circuits vs MBQC

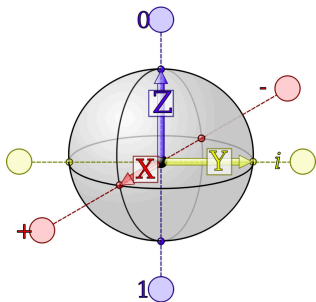


Circuits vs MBQC



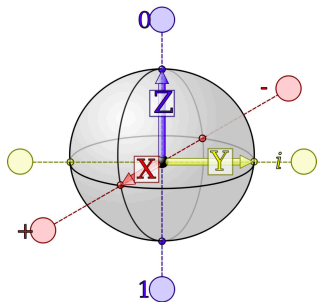
The tool: measurements (ctd)

1-qubit measurements are parametrised by a point of the Bloch sphere.



The tool: measurements (ctd)

1-qubit measurements are parametrised by a point of the Bloch sphere.



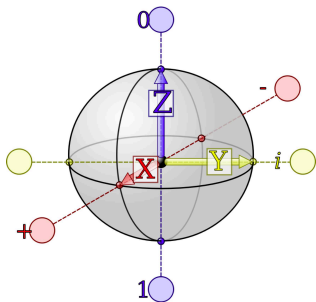
In MBQC, measurements are in the:

- (X,Y)-plane



The tool: measurements (ctd)

1-qubit measurements are parametrised by a point of the Bloch sphere.



In MBQC, measurements are in the:

- (X,Y)-plane

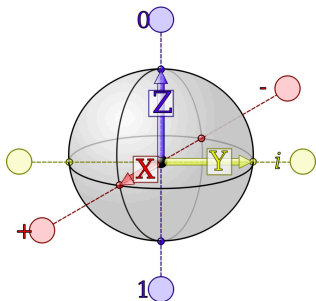


- (X,Z)-plane



The tool: measurements (ctd)

1-qubit measurements are parametrised by a point of the Bloch sphere.



In MBQC, measurements are in the:

- (X,Y)-plane



- (X,Z)-plane

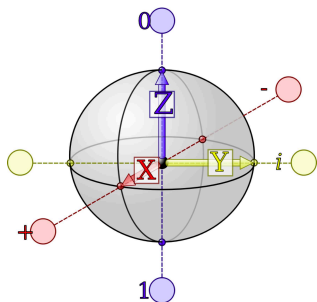


- (Z,Y)-plane



The tool: measurements (ctd)

1-qubit measurements are parametrised by a point of the Bloch sphere.



In MBQC, measurements are in the:

- (X,Y)-plane



- (X,Z)-plane



- (Z,Y)-plane



- according to X

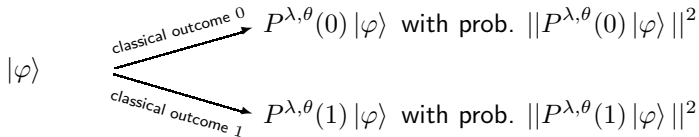
- according to Y

- according to Z

Each measurement is parameterised by $\lambda \in \{X, Y, Z, (X, Y), (X, Z), (Z, Y)\}$ and an angle θ when λ is a plane.

Irreversibility and Non determinism

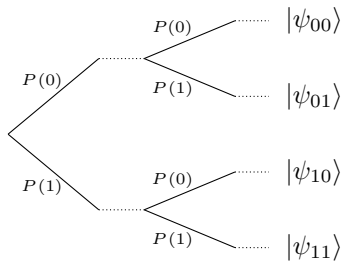
Each measurement $M^{\lambda,\theta}$ (plane λ , angle θ) is characterised by two projections $\{P^{\lambda,\theta}(0), P^{\lambda,\theta}(1)\}$.



Towards Reversibility



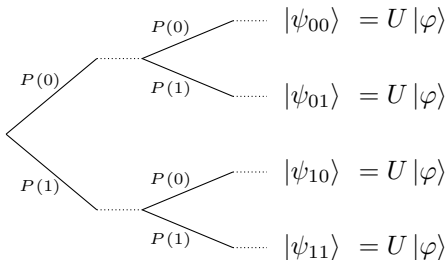
$$|\varphi\rangle \mapsto E_G |\varphi\rangle$$



Towards Reversibility



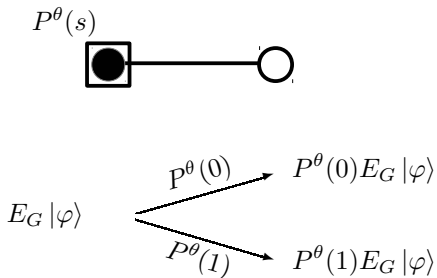
$$|\varphi\rangle \mapsto E_G |\varphi\rangle$$



Robust determinism:

- Deterministic: all branches produce the same quantum state.
- Uniformity: independent of the angles.
- Strongness: every branch has a non zero probability.
- Stepwise.

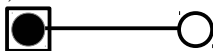
Towards Reversibility



When measurement in the (X, Y) -plane, $P^\theta(1)Z = P^\theta(0)$

Towards Reversibility

$$P^\theta(s) \circ Z^s$$



$$E_G |\varphi\rangle \begin{cases} \xrightarrow{P^\theta(0)} P^\theta(0) E_G |\varphi\rangle \\ \xrightarrow{P^\theta(1)Z = P^\theta(0)} P^\theta(0) E_G |\varphi\rangle \end{cases}$$

When measurement in the (X, Y) -plane, $P^\theta(1)Z = P^\theta(0)$

Deterministic

Towards Reversibility

$$P^\theta(s) \circ Z^s$$



$$E_G |\varphi\rangle \begin{cases} \xrightarrow{P^\theta(0)} P^\theta(0) E_G |\varphi\rangle \\ \xrightarrow{P^\theta(1)Z = P^\theta(0)} P^\theta(0) E_G |\varphi\rangle \end{cases}$$

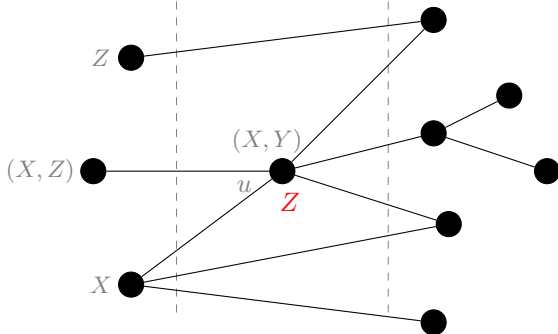
When measurement in the (X, Y) -plane, $P^\theta(1)Z = P^\theta(0)$

Deterministicbut **acausal**

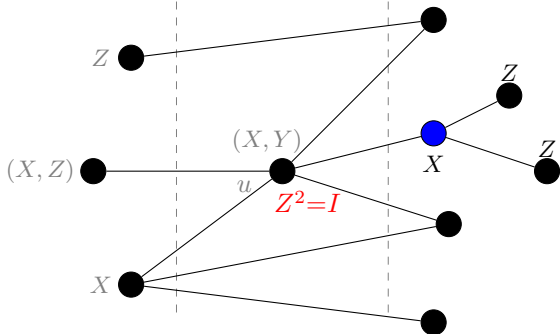
already meas.

to be corrected

not yet measured



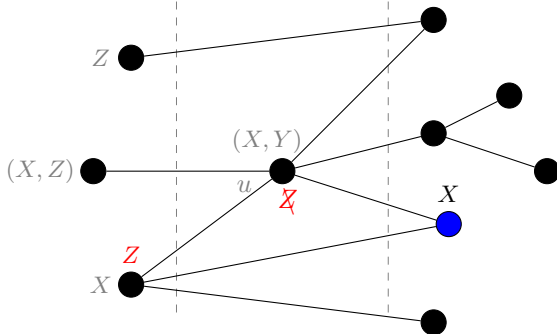
already meas. to be corrected not yet measured



- $p(u) > u$
- $u \in N(p(u))$
- $\forall v \in N(p(u)) \setminus \{u\}, v > u.$

Causal Flow [DK'04]

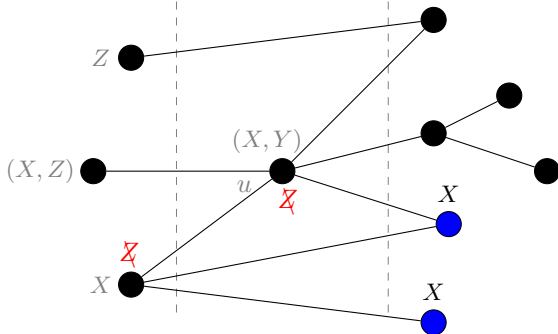
already meas. to be corrected not yet measured



- $p(u) > u$
- $u \in N(p(u))$
- $\forall v \in N(p(u)) \setminus \{u\}, v > u.$

Causal Flow [DK'04]

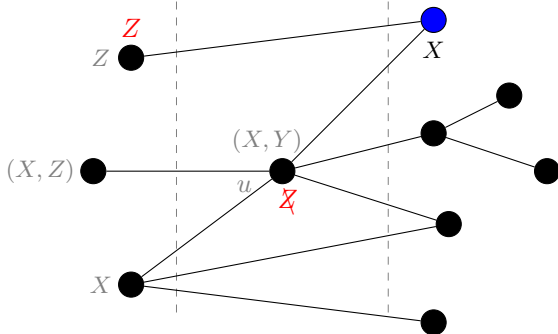
already meas. to be corrected not yet measured



- $\forall v \in p(u), v > u$
- $u \in \text{Odd}(p(u))$, where $\text{Odd}(D) := \{v \in V : |N(v) \cap D| = 1 \pmod{2}\}$.
- $\forall v \in \text{Odd}(p(u)) \setminus \{u\}, v > u$.

GFlow [BKMP'07]

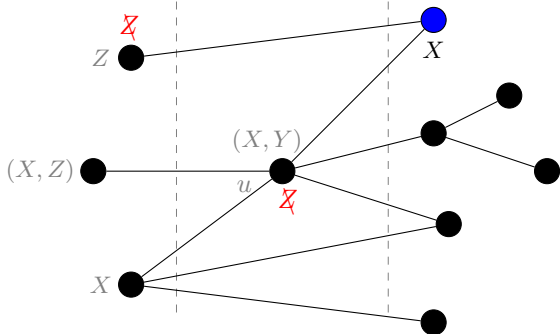
already meas. to be corrected not yet measured



- $\forall v \in p(u), v > u$
- $u \in \text{Odd}(p(u))$, where $\text{Odd}(D) := \{v \in V : |N(v) \cap D| = 1 \pmod{2}\}$.
- $\forall v \in \text{Odd}(p(u)) \setminus \{u\}, v > u$.

GFlow [BKMP'07]

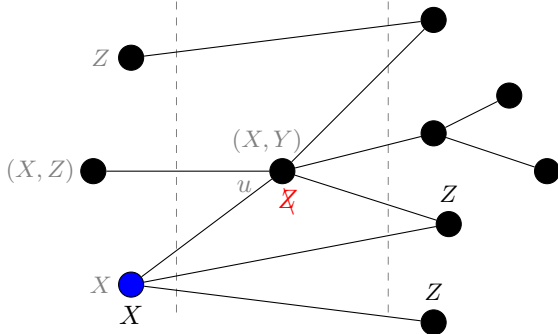
already meas. to be corrected not yet measured



- $\forall v \in p(u), v > u$
- $u \in \text{Odd}(p(u))$, where $\text{Odd}(D) := \{v \in V : |N(v) \cap D| = 1 \pmod{2}\}$.
- $\forall v \in \text{Odd}(p(u)) \setminus \{u\}, v > u$ or $\lambda_v = \{Z\}$.

Pauli Flow [BKMP'07]

already meas. to be corrected not yet measured



- $\forall v \in p(u), v > u$ or $\lambda_v = \{X\}$.
- $u \in \text{Odd}(p(u))$, where $\text{Odd}(D) := \{v \in V : |N(v) \cap D| = 1 \pmod{2}\}$.
- $\forall v \in \text{Odd}(p(u)) \setminus \{u\}, v > u$ or $\lambda_v = \{Z\}$.

Pauli Flow [BKMP'07]

Pauli Flow

- Definition.** An open graph state (G, I, O, λ) has **Pauli flow** if there exist a map $p : O^c \rightarrow 2^{I^c}$ and a strict partial order $<$ over O^c such that $\forall u, v \in O^c$,
- (P1) if $v \in p(u)$, $u \neq v$, and $\lambda_v \notin \{\{X\}, \{Y\}\}$ then $u < v$,
 - (P2) if $v \leq u$, $u \neq v$, and $\lambda_v \notin \{\{Y\}, \{Z\}\}$ then $v \notin \text{Odd}p(u)$,
 - (P3) if $v \leq u$, $u \neq v$, and $\lambda_v = \{Y\}$ then $v \in p(u) \Leftrightarrow v \in \text{Odd}p(u)$,
 - (P4) if $\lambda_u = \{X, Y\}$ then $u \notin p(u)$ and $u \in \text{Odd}p(u)$,
 - (P5) if $\lambda_u = \{X, Z\}$ then $u \in p(u)$ and $u \in \text{Odd}p(u)$,
 - (P6) if $\lambda_u = \{Y, Z\}$ then $u \in p(u)$ and $u \notin \text{Odd}p(u)$,
 - (P7) if $\lambda_u = \{X\}$ then $u \in \text{Odd}p(u)$,
 - (P8) if $\lambda_u = \{Z\}$ then $u \in p(u)$,
 - (P9) if $\lambda_u = \{Y\}$ then either: $u \notin p(u) \ \& \ u \in \text{Odd}p(u)$ or $u \in p(u) \ \& \ u \notin \text{Odd}p(u)$.

Theorem [Browne, Kashefi, Mhalla, Perdrix 07]

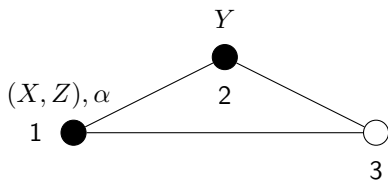
Pauli flow is a sufficient condition for robust determinism.

Theorem [Browne, Kashefi, Mhalla, Perdrix 07]

Pauli Flow is necessary for robust determinism when $\forall u, |\lambda_u| = 2$.

Is Pauli Flow necessary for robust determinism ?

Counter Example

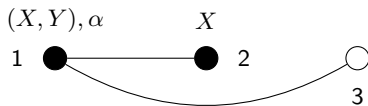


No Pauli flow but robust determinism.

Restrictions

- $\{X, Y\}$ -MBQC: $\forall u, \lambda_u \in \{\{X\}, \{Y\}, \{X, Y\}\}$.
- Universal model of quantum computation

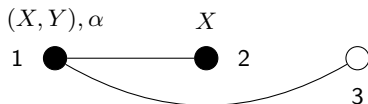
Robustly deterministic
but no Pauli flow:



Restrictions

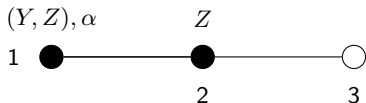
- $\{X, Y\}$ -MBQC: $\forall u, \lambda_u \in \{\{X\}, \{Y\}, \{X, Y\}\}$.
 - Universal model of quantum computation

Robustly deterministic
but no Pauli flow:



- $\{Y, Z\}$ -MBQC: $\forall u, \lambda_u \in \{\{Y\}, \{Z\}, \{Y, Z\}\}$.
 - Universal model of quantum computation

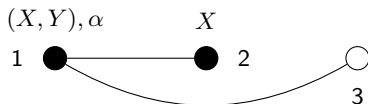
Robustly deterministic
but no Pauli flow:



Restrictions

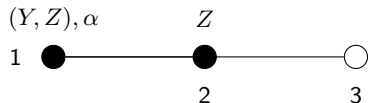
- $\{X, Y\}$ -MBQC: $\forall u, \lambda_u \in \{\{X\}, \{Y\}, \{X, Y\}\}$.
 - Universal model of quantum computation

Robustly deterministic
but no Pauli flow:



- $\{Y, Z\}$ -MBQC: $\forall u, \lambda_u \in \{\{Y\}, \{Z\}, \{Y, Z\}\}$.
 - Universal model of quantum computation

Robustly deterministic
but no Pauli flow:

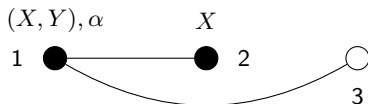


- $\{X, Z\}$ -MBQC: $\forall u, \lambda_u \in \{\{X\}, \{Z\}, \{X, Z\}\}$.
 - **Real** MBQC
 - Universal model of quantum computation.

Restrictions

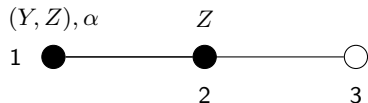
- $\{X, Y\}$ -MBQC: $\forall u, \lambda_u \in \{\{X\}, \{Y\}, \{X, Y\}\}$.
 - Universal model of quantum computation

Robustly deterministic
but no Pauli flow:



- $\{Y, Z\}$ -MBQC: $\forall u, \lambda_u \in \{\{Y\}, \{Z\}, \{Y, Z\}\}$.
 - Universal model of quantum computation

Robustly deterministic
but no Pauli flow:



- $\{X, Z\}$ -MBQC: $\forall u, \lambda_u \in \{\{X\}, \{Z\}, \{X, Z\}\}$.
 - **Real** MBQC
 - Universal model of quantum computation.

Theorem. Pauli flow is necessary and sufficient for real (i.e. $\{X, Z\}$ -MBQC) robust determinism.

Application: Interactive Proofs

McKague's interactive proofs protocol based on real MBQC:

- A classical verifier
- Polynomial number of quantum provers.
- real MBQC is crucial: no way for the verifier to distinguish a state and its conjugate.

McKague's open question: Protocol with 2 provers only.

Application: Interactive Proofs

McKague's interactive proofs protocol based on real MBQC:

- A classical verifier
- Polynomial number of quantum provers.
- real MBQC is crucial: no way for the verifier to distinguish a state and its conjugate.

McKague's open question: Protocol with 2 provers only.
⇔ Universal real MBQC on bipartite graphs.

Application: Interactive Proofs

McKague's interactive proofs protocol based on real MBQC:

- A classical verifier
- Polynomial number of quantum provers.
- real MBQC is crucial: no way for the verifier to distinguish a state and its conjugate.

McKague's open question: Protocol with 2 provers only.
⇔ Universal real MBQC on bipartite graphs.

Theorem. All measurements of a robustly deterministic real bipartite MBQC can be performed in parallel.

Corollary. McKague's protocol does not work with 2 provers.

Conclusion and future work

- Pauli flow characterises robust determinism for real-MBQC.
- Efficient algorithm for Pauli flow?
(efficient algorithm exists for GFlow [Mhalla, Perdrix'08])
- Counter examples for $\{X, Y\}$ and $\{Y, Z\}$ planes.
- Extension of Pauli flow?
- Weak power of real bipartite MBQC.
- Equivalent to commuting quantum circuits?