Measurement-based Quantum Computation

Elham Kashefi

University of Edinburgh
Measurement-based QC

Measurements play a central role.

Scalable implementation

Clear separation between classical and quantum parts of computation

Entanglement

Clear separation between creation and consumption of resources
**Basic Commands**

- **New qubits**, to prepare the auxiliary qubits:  $N$
- **Entanglements**, to build the quantum channel:  $E$
- **Measurements**, to propagate(manipulate) qubits:  $M$
- ** Corrections**, to make the computation deterministic:  $C$
2-state System $\mathbb{C}^2$

The canonical basis, $(1,0)$, $(0,1)$, also called the computational basis, is usually denoted $|0\rangle$, $|1\rangle$. It is orthonormal by definition of $\langle x, y \rangle_{\mathbb{C}^2}$.

$|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

$|\pm_\alpha\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle)$

The preparation map $N^\alpha_i$ is defined to be:

$|\pm_\alpha\rangle \otimes \_ : \mathcal{H}_n \rightarrow \mathbb{C}^2 \otimes \mathcal{H}_n$
Maps over $\mathbb{C}^2$

Pauli Spin Matrices

\[ X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \]

Other Single qubit gates

\[ H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad P(\alpha) := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \]

\[ P(\alpha)^* = P(-\alpha) \]
The two qubit state $\mathbb{C}^2 \otimes \mathbb{C}^2$

Canonical basis

$\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$

Bases need not be made of decomposable elements, they can consist of entangled states.

Graph basis

\[
\begin{align*}
\mathcal{G}_{00} &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \\
\mathcal{G}_{01} &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle) \\
\mathcal{G}_{10} &= \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle) \\
\mathcal{G}_{11} &= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)
\end{align*}
\]
Maps on $\mathbb{C}^2 \otimes \mathbb{C}^2$

- In general if $f: A \to B$ and $g: A' \to B'$, one defines $f \otimes g: A \otimes A' \to B \otimes B'$: $\psi \otimes \phi \mapsto f(\psi) \otimes g(\phi)$.

- Or given $f: \mathbb{C}^2 \to \mathbb{C}^2$, one defines $\wedge f$ (read controlled-$f$) a new map on $\mathbb{C}^2 \otimes \mathbb{C}^2$:

\[
\begin{align*}
\wedge f |0\rangle |\psi\rangle & := |0\rangle |\psi\rangle \\
\wedge f |1\rangle |\psi\rangle & := |1\rangle f(|\psi\rangle)
\end{align*}
\]

Entangling Map

$\wedge Z(|+\rangle \otimes |+\rangle) = G_{00}$
Pauli and Clifford

Define the **Pauli group** over $A$ as the closure of $\{X_i, Z_i \mid 1 \leq i \leq n\}$ under composition and $\otimes$. These are all local maps (corrections).

Define the **Clifford group** over $A$ as the normalizer of the Pauli group, that is to say the set of unitaries $f$ over $A$ such that for all $g$ in the Pauli group, $fgf^{-1}$ is also in the Pauli group.

**Entangling Map is in Clifford**

\[
\wedge Z_{ij} X_i = X_i Z_j \wedge Z_{ij} \\
\wedge Z_{ij} Z_i = Z_i \wedge Z_{ij}
\]
Projective Measurement on $\mathcal{H}_n$

A complete measurement is given by an orthonormal basis

$$\mathcal{B} = \{\psi_a\}$$

which defines a decomposition into orthogonal 1-dimensional subspaces

$$\mathcal{H}_n = \bigoplus_a E_a$$

Define $|\psi_a\rangle\langle\psi_a| : \mathcal{H}_n \to E_a$ to be projection to $E_a$
Destructive Measurement

Given a complete measurement over $A$, as $A = \{\psi_a\}$, one can extend it to an incomplete measurement on $A \otimes B$, with components given by $|\psi_a\rangle\langle\psi_a| : A \otimes B \rightarrow B$.

$1$-qubit destructive measurement

$M^\alpha$ associated to $\{|+\alpha\rangle\}$
Unitary Action

If $U$ maps orthonormal basis $B$ to $A$ then

$$M^A = UM^BU^\dagger$$

- **$X$-action:**

  $$X|+\alpha\rangle = |+_{-\alpha}\rangle$$
  $$X|-\alpha\rangle = -|_{-\alpha}\rangle$$

- **$Z$-action:**

  $$Z|+\alpha\rangle = |_{+\alpha+\pi}\rangle$$
  $$Z|-\alpha\rangle = |_{-\alpha+\pi}\rangle$$
Quantum Pacman
Quantum Pacman
Quantum Pacman
Quantum Pacman
A formal language

- $N_i$ prepares qubit in $|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

- $M_i^{\alpha}$ projects qubit onto basis states $|\pm \alpha\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm e^{i\alpha}|1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm e^{i\alpha} \end{pmatrix}$

- $E_{i,j}$ creates entanglement $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

- Local Pauli corrections $X_i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z_i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- **Feed forward**: measurements and corrections commands are allowed to depend on previous measurements outcomes.

$$C_i^s \quad [M_i^{\alpha}]^s = M_i^{(-1)^s \alpha} \quad s[M_i^{\alpha}] = M_i^{\alpha + s\pi}$$
Dependent Commands

The measurement outcome $s_i \in \mathbb{Z}_2$:

- 0 refers to the $\langle + \alpha \rangle$ projection,
- 1 refers to the $\langle - \alpha \rangle$ projection.

measurements and corrections may be parameterised by signal $\sum_i s_i$

- $[M_i^\alpha]^s = M_i^{(-1)^s\alpha} = M_i^\alpha X_i^s$
- $t[M_i^\alpha] = M_i^{t\pi + \alpha} = M_i^\alpha Z_i^s$

with $X^0 = Z^0 = I$, $X^1 = X$, $Z^1 = Z$.

\[ t[M_i^\alpha]^s = M_i^{t\pi + (-1)^s\alpha} \]
Patterns of Computation

\[(V, I, O, A_n \ldots A_1)\]

\[\mathcal{H} := (\{1, 2\}, \{1\}, \{2\}, X_2^{s_1} M_1^0 E_{12} N_2^0)\]

Sequential or Parallel Composition

\[X_3^{s_2} M_2^0 E_{23} \quad X_2^{s_1} M_1^0 E_{12}\]
Definiteness Conditions

no command depends on outcomes not yet measured
no command acts on a qubit already measured
a qubit $i$ is measured if and only if $i$ is not an output
Example

\[ \mathcal{H} := (\{1, 2\}, \{1\}, \{2\}, X_2^{s_1} M_1^0 E_{12} N_2^0) \]

Starting with the input state \( (a|0\rangle + b|1\rangle)|+\rangle \)

\[
(a|0\rangle + b|1\rangle)|+\rangle \xrightarrow{E_{12}} \frac{1}{\sqrt{2}} (a|00\rangle + a|01\rangle + b|10\rangle - b|11\rangle)
\]

\[
H \xrightarrow{M_1^0} \begin{cases}
\frac{1}{2}((a + b)|0\rangle + (a - b)|1\rangle) & s_1 = 0 \\
\frac{1}{2}((a - b)|0\rangle + (a + b)|1\rangle) & s_1 = 1
\end{cases}
\]

\[
X_2^{s_1} \xrightarrow{H} \frac{1}{2}((a + b)|0\rangle + (a - b)|1\rangle)
\]
State Space

\[ S := \bigcup_{V,W} \mathcal{H}_V \times \mathbb{Z}_2^W \]

In other words a computation state is a pair \( q, \Gamma \), where \( q \) is a quantum state and \( \Gamma \) is a map from some \( W \) to the outcome space \( \mathbb{Z}_2 \). We call this classical component \( \Gamma \) an outcome map and denote by \( \varnothing \) the unique map in \( \mathbb{Z}_2^\varnothing \).
Operational Semantics

\[
\begin{align*}
q, \Gamma & \xrightarrow{N_i^\alpha} q \otimes |+\alpha\rangle_i, \Gamma \\
q, \Gamma & \xrightarrow{E_{ij}} \wedge Z_{ij} q, \Gamma \\
q, \Gamma & \xrightarrow{X_i^s} X_i^{s\Gamma} q, \Gamma \\
q, \Gamma & \xrightarrow{Z_i^s} Z_i^{s\Gamma} q, \Gamma \\
q, \Gamma & \xrightarrow{t[M_i^\alpha]^s} \langle +\alpha \Gamma|_i q, \Gamma[0/i] \\
q, \Gamma & \xrightarrow{t[M_i^\alpha]^s} \langle -\alpha \Gamma|_i q, \Gamma[1/i]
\end{align*}
\]

where \( \alpha_\Gamma = (-1)^{s\Gamma} \alpha + t_{\Gamma} \pi \).
Denotational Semantics

Let $A_s = C_s \Pi_s U$ be a branch map, the pattern realises the cptp-map

$$T(\rho) := \sum_s A_s \rho A_s^\dagger$$

Density operator: A probability distribution over quantum states
A pattern is strongly deterministic if all the branch maps are equal.

**Theorem.** A strongly deterministic pattern realises a unitary embedding.
Universal Gates

\[ \wedge Z \ := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \]

\[ J(\alpha) \ := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix} \]

\[ U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta) \]

\[ P(\alpha) = J(0) J(\alpha) \]

\[ H = J(0) \]

\[ H^i = J(\frac{\pi}{2}) \]
Generating Patterns

\[ \wedge Z := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \]

\[ \wedge \mathfrak{z} := E_{12} \]

\[ J(\alpha) := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix} \]

\[ \hat{J}(\alpha) := X^s_2 M_1^{-\alpha} E_{12} \]
Example (ctrl-U)

\[ U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta) \]

\[ \wedge U_{12} = J_1^0 J_1^{\alpha'} J_2^0 J_2^{\beta+\pi} J_2^{-\frac{\gamma}{2}} J_2^{-\frac{\pi}{2}} J_2^0 \wedge Z_{12} J_2^2 J_2^0 \wedge Z_1 J_2^2 J_2^0 \wedge \mathbb{Z}_{12} J_2 \]

\[ \alpha' = \alpha + \frac{\beta+\gamma+\delta}{2} \]
Example (ctrl-U)

Wild Pattern

\[
X^s_B M^0_B E_{BC} X^s_A M^0_A - \alpha' E_{AB} X^s_j M^0_j E_{jk} X^s_i M^0_i - \beta - \pi E_{ij}
\]
\[
X^s_i M^2_h E_{hi} X^s_h M^2_g E_{gh} X^s_g M^0_f E_{fg} X^s_f M^0_e E_{ef} X^s_e M^2_e - \pi E_{ef}
\]
\[
X^s_c M^2_d E_{de} X^s_d M^2_c E_{cd} X^s_c M^0_b E_{bc} E_{Ab} X^s_a M^2_a - \beta - \delta + \pi E_{ab}
\]

Standard Pattern

\[
Z^s_i + s_g + s_e + s_c + s_a X^s_j + s_h + s_f + s_d + s_b X^s_B Z^s_A + s_e + s_c
\]
\[
M^0_B M^0_A - \alpha' M^0_j [M^\beta - \pi i] s_h + s_f + s_d + s_b [M^\gamma e h] s_g + s_e + s_c + s_a [M^\pi f g] s_f + s_d + s_b
\]
\[
M^0_f [M^\pi c d] s_d + s_b [M^\beta e f g] s_c + s_a [M^\pi e c d] s_b M^0_b M^0_a - \beta + \delta + \pi
\]
\[
E_{BC} E_{AB} E_{i j} E_{e f} E_{de} E_{cd} E_{bc} E_{ab} E_{Ab}
\]
**Measurement Calculus**

Pushing entanglement to the beginning

\[
\begin{align*}
E_{ij} X^s_i &= X^s_i Z_j^s E_{ij} \\
E_{ij} X^s_j &= X^s_j Z^s_i E_{ij} \\
E_{ij} Z^s_i &= Z^s_i E_{ij} \\
E_{ij} Z^s_j &= Z^s_j E_{ij}
\end{align*}
\]

Pushing correction to the end

\[
\begin{align*}
t[M_i^\alpha]^s X^r_i &= t[M_i^\alpha]^s+r \\
t[M_i^\alpha]^s Z^r_i &= t+r[M_i^\alpha]^s
\end{align*}
\]

**Theorem.** The re-writing system is confluent and terminating.

**Theorem.** An MQC model admits a standardisation procedure iff the \( E \) operator is normaliser of all the \( C \) operators.
Algorithm

\[ U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta) \]

\[ \tilde{J}(0)(4, 5) \tilde{J}(\alpha)(3, 4) \tilde{J}(\beta)(2, 3) \tilde{J}(\gamma)(1, 2) = \]

\[ X_5^{s_4} M_4^0 E_45 X_4^{s_3} M_3^\alpha E_34 X_3^{s_2} M_2^\beta E_23 X_2^{s_1} M_1^{\gamma} E_12 \Rightarrow EX \]
\[ X_5^{s_4} M_4^0 E_45 X_4^{s_3} M_3^\alpha E_34 X_3^{s_2} M_2^\beta X_2^{s_1} Z_3^{s_1} M_1^{\gamma} E_123 \Rightarrow MX \]
\[ X_5^{s_4} M_4^0 E_45 X_4^{s_3} M_3^\alpha E_34 X_3^{s_2} Z_3^{s_1} [M_2^\beta]^{s_1} M_1^{\gamma} E_123 \Rightarrow EXZ \]
\[ X_5^{s_4} M_4^0 E_45 X_4^{s_3} M_3^\alpha X_3^{s_2} Z_3^{s_1} Z_4^{s_2} [M_2^\beta]^{s_1} M_1^{\gamma} E_1234 \Rightarrow MXZ \]
\[ X_5^{s_4} M_4^0 E_45 X_4^{s_3} Z_4^{s_2} s_1 [M_3^\alpha]^{s_2} [M_2^\beta]^{s_1} M_1^{\gamma} E_1234 \Rightarrow EXZ \]
\[ X_5^{s_4} M_4^0 X_4^{s_3} Z_4^{s_2} Z_5^{s_3} s_1 [M_3^\alpha]^{s_2} [M_2^\beta]^{s_1} M_1^{\gamma} E_12345 \Rightarrow MXZ \]

Worst Case Complexity: \( O(N^5) \) where \( N \) is the number of qubits in the given pattern
The Key Feature of MBQC

A clean separation between Classical and Quantum Control

Entanglement Graph

Execution Graph
Parallelisation

Signal Shifting

\[
\begin{align*}
t[M_i^\alpha]^s & \Rightarrow S_i^t [M_i^\alpha]^s \\
X_j^s S_i^t & \Rightarrow S_i^t X_j^s[t+s_i/s_i] \\
Z_j^s S_i^t & \Rightarrow S_i^t Z_j^s[t+s_i/s_i] \\
t[M_j^\alpha]^s S_i^r & \Rightarrow S_i^r t[r+s_i/s_i] [M_j^\alpha]^s[r+s_i/s_i] \\
S_i^s S_j^t & \Rightarrow S_j^t S_i^s[t+s_j/s_j]
\end{align*}
\]
Reducing Depth

Depth of a pattern is the length of the longest feed-forward chain

Standardisation and Signal Shifting reduce depth.

\[ Z_g Z_{g_f} Z_{g_e} X_{e_f} X_{e_e} [M_d^\delta s_b] [M_c^\gamma s_a] M_b^\beta M_a^\alpha E_G \]
Depth Complexity

All the models for QC are equivalent in computational power.

**Theorem.** There exists a logarithmic separation in depth complexity between MBQC and circuit model.

**Parity function:** MQC needs 1 quantum layer and $O(\log n)$ classical layers whereas in the circuit model the quantum depth is $\Omega(\log n)$. 

A. Broadbent and E. Kashefi, MBQC07
Automated Parallelising Scheme

**Theorem.** Forward and backward translation between circuit model and MQC can only decrease the depth.
**Characterisation**

**Theorem.** A pattern has depth $d + 2$ if and only if on any influencing path we obtain $P^* N^{i \leq d} P^*$ after applying the following rewriting rule:

$$N P_1^* \alpha_1 \beta_1 P_2^* \alpha_2 \beta_2 \cdots P_k^* N \begin{cases} N N & \text{if} \quad \forall P_i^* \neq X(XY)^* \\ N & \text{otherwise} \end{cases}$$
The Magical Clifford Sequence

\[(H)^{odd}(H^{i}(H)^{odd})^{*}\]
Can be parallelised to a pattern with depth 2
A pattern is deterministic if all the branches are the same.

How to obtain global determinism via local controls

A necessary and sufficient condition for determinism based on geometry of entanglement
Graph State as Stabiliser States

Graph Stabilisers:

\[ K_i := X_i \left( \prod_{j \in N_G(i)} Z_j \right) \]

\[ K_i E_G N_{Ic} = E_G N_{Ic} \]
Graph Stabilisers:

\[ K_i := X_i \left( \prod_{j \in NG(i)} Z_j \right) \]

\[ K_i E_G N_{I_c} = E_G N_{I_c} \]
Graph State as Stabiliser States

Graph Stabilisers:

\[ K_i := X_i(\prod_{j \in N_G(i)} Z_j) \]

\[ K_i E_G N_{Ic} = E_G N_{Ic} \]
Graph State as Stabiliser States

Graph Stabilisers:

\[ K_i := X_i \prod_{j \in N_G(i)} Z_j \]

\[ K_i E_G N_{Ic} = E_G N_{Ic} \]
**Flow**

**Definition.** An entanglement graph \((G, I, O)\) has flow if there exists a map \(f : O^c \rightarrow I^c\) and a partial order \(\leq\) over qubits

- (i) \(x \sim f(x)\)
- (ii) \(x \preceq f(x)\)
- (iii) for all \(y \sim f(x)\), we have \(x \preceq y\)
Flow

Find

- a qubits to qubits assignment
- a matching partial order
Flow

Find

- a qubits to qubits assignment
- a matching partial order
Theorem. A pattern is uniformly and step-wise deterministic iff its graph has a flow.
No dependency Theorems

**Theorem.** A unitary map is in Clifford iff \( \exists \) a pattern implementing it with measurement angles 0 and \( \frac{\pi}{2} \).

**Theorem.** If pattern \( P \) with no dependent commands implements unitary \( U \), then \( U \) is in Clifford.

Pauli Measurements
Gottesman Knill Theorem

If the states of computation are restricted to the stabiliser states and the operation over them to the Clifford group then the corresponding quantum computation can be efficiently simulated using Classical Computing.

Efficient representation in terms of Pauli Operators

Preserves the efficient representation
Corollary. Any MBQC pattern with only Pauli measurements can be efficiently simulated using Classical Computing.

Quantum Pattern


Classical Pattern

Model checking for a class of quantum protocols using PRISM

S. J. Gay, R. Nagarajan and N. Papanikolaou.