Introduction to quantum computation and simulability

Ernesto F. Galvão
Instituto de Física, Universidade Federal Fluminense
(Niterói, Brazil)

\[ u = \sqrt{1 - \varepsilon} |0\rangle + \sqrt{\varepsilon} |1\rangle \]

\[ q = \varepsilon p \]

ICTP-SAIFR – IFT/UNESP, October 15th-19th, 2018
Introduction to quantum computation and simulability

Lecture 8: Measurement-based QC (MBQC) II

Outline:

• Applications of MBQC:
  • models for quantum spacetime
  • blind quantum computation

• Time-ordering in MBQC

• MBQC without adaptativity:
  • Clifford circuits
  • IQP circuits

• Introduction to quantum contextuality

• Contextuality as a computational resource
  • in magic state distillation
  • in MBQC

• For slides and links to related material, see
Application: blind quantum computation

- Classical/quantum separation in MBQC allow for implementation of novel protocols – such as blind quantum computation
- Here, client has limited quantum capabilities, and uses a server to do computation for her.
- Blind = server doesn’t know what’s being computed.

Broadbent, Fitzsimons, Kashefi, arxiv:0807.4154 [quant-ph]
Application: model for quantum spacetime

- MBQC can serve as a discrete toy model for quantum spacetime:

<table>
<thead>
<tr>
<th>quantum space-time</th>
<th>MBQC</th>
</tr>
</thead>
<tbody>
<tr>
<td>quantum substrate</td>
<td>graph states</td>
</tr>
<tr>
<td>events</td>
<td>measurements</td>
</tr>
<tr>
<td>principle establishing global</td>
<td>determinism requirement for computations</td>
</tr>
<tr>
<td>space-time structure</td>
<td></td>
</tr>
</tbody>
</table>

[Raussendorf et al., arxiv:1108.5774]

- Even closed timelike curves (= time travel) have analogues in MBQC!

[Dias da Silva, Kashefi, Galvão PRA 83, 012316 (2011)]
Time-ordering in MBQC

Note that some measurements are not adaptive, but in fixed bases. These can be performed at once at beginning of computation.

Parts of protocol corresponding to Clifford gates are non-adaptive.

MBQC neatly separates Clifford (non-adaptive) from non-Clifford (adaptive) parts of the computation.

Back-and-forth translations between models reveal possible circuit optimizations.
Circuit optimization: example

- We’ve seen that MBQC allows for implementation of Clifford operations in constant time. Back-translating to the circuit model we obtain circuits which implement all the Clifford part in constant time:

- No adaptativity in Clifford MBQC -> no adaptativity in circuit.
- Depth is 4 (3 CZs and 1 single-qubit unitary for measurement)

- **Trade-off**: depth becomes constant, at cost of increasing number of qubits
- For non-Clifford circuits, depth increases by the number of layers of non-Clifford gates
The complexity class IQP was initially studied by Shepherd, Bremner, and Jozsa.

Initialization and measurement in computational basis, but only commuting gates (in X basis).
- Temporal order of gates irrelevant; strong restriction on computational power.

IQP circuits in MBQC

- IQP circuits can be implemented in the MBQC model – the translation is curious.

\[ \text{Commuting gates in } X \text{ basis} \]

\[ \text{IQP circuits in MBQC} \]

- Translation:

\[ \text{non-adaptive MBQC} \]

\[ \text{IQP* hardness of simulation} \]

- Hamiltonian:

\[ \text{Hardness of simulating non-adaptive MBQC} \]

- Now: prior to measurement, decohere each qubit in its measurement eigenbasis. This doesn’t change statistics, but results in states which are separable and discord-free.

\[ \text{this “Classical” MBQC is hard to simulate exactly} \]

Where’s the quantum ingredient there?
Which resource gives MBQC its power?

- Clearly, the correlations in the resource state.

- Analysis of MBQC protocols in terms of Bell inequalities:
  - Anders/Browne PRL 102, 050502 (2009)

- …but measurements are usually not space-like separated:
  quantum contextuality

- Raussendorf, PRA 88, 022322 (2013)
Quantum contextuality

- Context of an observable $A = $ set of commuting observables measured together with $A$
- Non-contextuality hypothesis: outcomes of observables are context-independent
- Violated by quantum mechanics!


<table>
<thead>
<tr>
<th>1 $\otimes \sigma_z$</th>
<th>$\sigma_z \otimes 1$</th>
<th>$\sigma_z \otimes \sigma_z$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma_x \otimes 1$</td>
<td>1 $\otimes \sigma_x$</td>
<td>$\sigma_x \otimes \sigma_x$</td>
</tr>
<tr>
<td>$\sigma_x \otimes \sigma_z$</td>
<td>$\sigma_z \otimes \sigma_x$</td>
<td>$\sigma_y \otimes \sigma_y$</td>
</tr>
</tbody>
</table>

- Operators in each row and column commute; Moreover, they are the product of the other two in same row/column
- EXCEPTION: third column:
  \[
  \sigma_y \otimes \sigma_y = -\sigma_z \otimes \sigma_z \cdot \sigma_x \otimes \sigma_x
  \]
- So it's impossible to assign +1 or -1 values to each observable in a context-independent way.
  QM is contextual.
Proof by Peres (1991) – Kochen and Specker flavour

- Consider 57 states in 3-dimensional Hilbert space, real amplitudes.
  - Orthogonal triads must be colored black, white, white.
  - Some of the triads above have vectors in common.
  - One can show that there’s no possible coloring satisfying the orthogonality relations.
Contextuality is necessary for magic state distillation

- The Mermin square proof of quantum contextuality is state-independent – any state violates the non-contextuality hypothesis.
- For Hilbert space dimension $d>2$, all contextuality proofs are state-dependent.
- So what’s special about states revealing contextuality?

- Howard et al. (2014) looked at that problem in the QC model of Clifford computer + magic states:

\[
|A\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\pi/4} |1\rangle)
\]

- Result: any state out of $\mathcal{P}_{\text{SIM}}$ violates a state-dependent non-contextuality inequality, using stabilizer measurements. States in $\mathcal{P}_{\text{SIM}}$ are non-contextual.

\[
\mathcal{Q} = \text{general quantum states}
\]

\[
\mathcal{P}_{\text{SIM}} = \text{simulable under stabilizer measurements}
\]

\[
\mathcal{P}_{\text{STAB}} = \text{stabilizer states}
\]

\[
\text{contextuality is necessary for magic-state computation}
\]
Contextuality in MBQC: evaluating non-linear Boolean functions
Computation using correlations

- Measurement-based quantum computation (MBQC) computes with correlations
  - what properties of the correlations enable computation in MBQC?

- Anders and Browne modelled MBQC with:
  - $N$ boxes, 1-bit inputs, 1-bit outputs
  - auxiliary pre- and post-computation restricted to sums modulo-2

- Popescu-Rohrlich correlations:
  deterministic evaluation of $i_1$ AND $i_2$
  
  \[
  p(o_1, o_2 \mid i_1, i_2) = \frac{1}{2} \delta_{o_1 \oplus o_2, i_1 AND i_2}
  \]

- Quantum correlations result in input-independent error
  \[
  e = \sin^2(\pi / 8) \cong 0.15
  \]
- Non-contextual correlations necessarily result in larger error
  \[
  e_{NC}^{NC} \geq 1 / 4
  \]
  (Tsirelson bound)
Deterministic OR from 3-qubit GHZ correlations

- Stabilizers of 3-qubit GHZ state enable deterministic evaluation of AND gate:

\[ i_3 = i_1 \oplus i_2 \]

\[
\begin{align*}
    \{ & i_j = 0 \Rightarrow \text{Measure X} \\
    & i_j = 1 \Rightarrow \text{Measure Y} \\
\end{align*}
\]

\[ |GHZ\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) \]

- GHZ stabilizers:

\[
\{ X_1 X_2 X_3, -X_1 Y_2 Y_3, -Y_1 X_2 Y_3, -Y_1 Y_2 X_3 \} \]

\[ \Rightarrow O_1 \oplus O_2 \oplus O_3 = i_1 \text{ OR } i_2 \]

- NOT is free and NOR is universal, so this is sufficient for universal classical computation

- Motivation: is GHZ non-contextuality required for classical computation? Is the quantum AND gate with e=0.15 useless?
Thm. 1: Non-linear Boolean functions require strong contextuality for deterministic MBQC evaluation.

Thm. 2: MBQC evaluation of arbitrary, $k$-bit Boolean function $f$ using non-contextual resources results in average error

$$e_f^{NC} \geq \frac{\nu_f}{2^k}$$

$$\nu_f = \text{non-linearity of } f = \min_{\text{linear } g} \left[ \text{no. outputs s.t. } g(i) \neq f(i) \right]$$

Example: $i_1 \text{ AND } i_2 = i_1i_2$ is nonlinear. Its closest linear approximation is e.g. the constant function 0:
2 Theorems by Raussendorf

• Thm. 1: Non-linear Boolean functions require strong contextuality for deterministic MBQC evaluation.

• Thm. 2: MBQC evaluation of arbitrary, $k$-bit Boolean function $f$ using non-contextual resources results in average error

$$e_f^{NC} \geq \frac{\nu_f}{2^k}$$

How much contextuality is sufficient for bounded bias evaluation of any Boolean function? [Oestereich, E.F.G., PRA 96, 062305 (2017)]

• Arbitrarily small violation of non-contextuality inequality $e_f^{NC} \geq \frac{\nu_f}{2^k}$ is sufficient.
Restricted models of quantum computation

- |ψ⟩
- I/2
- |0⟩
- |0⟩
- H
- H
- H
- H
- H

Diagonal in \(Z\) basis

- pure qubit
- \(n\) maximally mixed qubits
Restricted models of quantum computation

• Restrictions allow us to:

  • Identify regimes in which **quantum computers are simulable**
    Clifford circuits
    matchgates
    MBQC on a 1D chain

  • Find new intermediate models which may be **useful**, even if not universal
    DQC1 or “one-clean-qubit” model by Knill/Laflamme
    Permutational quantum computation (Jordan)

  • Eliminate or **minimize resource use**, with a view to feasible experiments
    Boson Sampling – Aaronson and Arkhipov
    Non-adaptive MBQC

• Translations between models is particularly interesting, as resource trade-offs are possible