What Can be Observed Locally?

Round-based Models of Quantum Distributed Computing

Cyril Gavoille
Adrian Kosowski
LaBRI - University of Bordeaux

Marcin Markiewicz
Institute of Theoretical Physics and Astrophysics
University of Gdańsk

Florence, October 2010
Outline

• What does quantum mean?
  • Some intuition
  • Some definitions

• How does Quantum Information help?
  • Quantum Computing – centralised models
  • Quantum Communication Complexity

• Where does locality come into play?
  • Locality in Computer Science vs. Locality in Physics
  • Quantum extensions of Linial’s LOCAL model
  • Proving lower bounds on the round complexity of problems
A quantization of the *LOCAL* model:

Creating a quantum model which:

- when restricted to classical states is precisely the *LOCAL* model
- captures the same principles of locality.
1. The observables

- What do we assume about the structure of the data?
  Let’s say we know that the data is a pair of bits \((b_1, b_0) \in \mathcal{Y} = \{00, 01, 10, 11\}\).

- What characteristics of the data are measurable?
  Let’s say we can measure the value of bits \(b_1\) and \(b_0\) directly.

2. Measurement of the state

- What does the (randomized) algorithm in the black box produce?
  **Identification:** run an experiment many times independently, measuring \(A = 2b_1 + b_0\) each time, obtain a probability distribution of values...
Describing a physical system

- **Let’s say the box flips a coin and outputs 01 or 10.** We have the state $\mu$:
  $\mu(00) = \mu(11) = 0$, $\mu(01) = \mu(10) = \frac{1}{2}$

- **Observables:** random variables $=>$ a commutative matrix algebra over complex numbers

\[
B_0 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad B_1 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad A = 2B_1 + B_0 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 2/1 & 2/1 & 0 & 0 \end{bmatrix}
\]

- **Permissable probabilistic measures are described by linear functionals over the defined algebra of observables**

\[
E_\mu A = \sum_{x \in \Xi} [A(x) \ast \mu(x)] \quad \Rightarrow \quad E_\mu A = \text{Tr} (A \mu)
\]

(the trace is the sum of elements on the diagonal)
What is a measurement?

- Recall that we were measuring an observable $A$ in state $\mu$

$$A = 2B_1 + B_0 = \begin{bmatrix} 0 & 01 & 10 & 11 \\ 0 & 1 & 2 & 3 \end{bmatrix} \quad \mu = \begin{bmatrix} 0 & 01 & 10 & 11 \\ 0 & 1/2 & 1/2 & 0 \end{bmatrix}$$

- The expected result of the measurement was given as: $\text{Tr} (A \mu) = 1.5$
- The possible outcomes are $\{0, 1, 2, 3\}$ with probabilities $\{0, 1/2, 1/2, 0\}$, resp.
  - The outcomes are the eigenvalues $\lambda_i$ of the matrix $A$... ($A = \sum \lambda_i P_i$)
  - The probability of obtaining outcome $\lambda_i$ is exactly $\text{Tr} (P_i \mu)$

- **What changes in the quantum case?**
  We allow $A$ to be any complex-valued matrix with positive (real) eigenvalues.
The Quantum Framework

- As computer scientists, we will find the following intuition useful:

> The quantum framework is a generalization of classical probability

- quantum algorithms are more powerful than randomized algorithms
- quantum information can be manipulated in ways in which classical information cannot
The problem with our universe...

• It is possible to perform a physical experiment in which we look at 4 characteristics of a simple system, and obtain marginal distributions for which there does not exist a joint distribution, in any probabilistic space.
  • So called “violation of Bell’s Theorem”, first verified by Aspect (1982).
• Quantum Mechanics has to rely on an extension of the classical framework
What properties must a quantum state fulfill?

- Must be a density matrix (positive spectrum, trace normalised to 1)
- Two examples of valid states (density matrices):

\[
\begin{bmatrix}
0 & 1/2 & 1/2 & 0 \\
1/2 & 1/2 & 0 & 0
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 1/2 & 1/2 & 0 \\
1/2 & 1/2 & 0 & 0
\end{bmatrix}
\]

- Do \(\mu_1\) and \(\mu_2\) describe the same state? [Recall that: \(E_\mu A = \text{Tr} (A \mu)\)]
  - Depends on what characteristics of the system are observable...
    - For the classical example with diagonal observables only – same state
    - For a richer class of quantum observables – these are distinct states...
      - The state \(\mu_2\) has no good classical interpretation!
Describing a physical system

Dirac’s bra-ket notation for pure states

- A state $\mu$ is called projective if $\mu = \psi^+ \psi$ for some row vector $\psi$.
- The cross ($^+$) denotes Hermitian transpose – transpose & conjugate.
- Projective states are equivalent to so-called pure states in this context.

\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1/2 & 1/2 & 0 \\
0 & 1/2 & 1/2 & 0 \\
0 & 0 & 0 & 0 \\
\end{bmatrix}
\begin{bmatrix}
0 \\
1/\sqrt{2} \\
1/\sqrt{2} \\
0 \\
\end{bmatrix} =

\frac{1}{\sqrt{2}}
\begin{bmatrix}
0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} & 11 \\
0 & 1/\sqrt{2} & 1/\sqrt{2} & 0 \\
\end{bmatrix}
\]

- It is often more convenient to work on such vectors $\psi$, especially when using tensor products. A basis vector is usually written as a $|\text{ket}\rangle$:

\[
\psi =
\begin{bmatrix}
0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} & 11 \\
0 & 1/\sqrt{2} & 1/\sqrt{2} & 0 \\
\end{bmatrix}
= 1/\sqrt{2} |01\rangle + 1/\sqrt{2} |10\rangle
\]
What is a quantum bit?

- A classical bit: 0 or 1
- A probabilistic classical bit: \((p_0, p_1)\)
- A quantum bit (or qubit):

\[
\alpha \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \beta \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle
\]

... where \(\alpha, \beta\) are complex numbers

- State of a quantum system \(\psi\) is denoted by \(|\psi\rangle\) (bra/ket notation)
  (a 1-qubit or a \(n\)-qubit register)
Quantum Operators

- Operators on $n$-qubit system are represented by $2^n \times 2^n$ complex-valued matrices.
- There are restrictions on the possible operators, usually: unitary matrix.
- In particular, there is no operator $M$ such that $M|\psi0\rangle = |\psi\psi\rangle$.
  
  => No Cloning Property.
- Classical operator (NOT, AND ...) can be converted into algebraic operators (by adding extra wires).
- Like classical $n$-bit operations, quantum operators can be decomposed as combinations (products and tensor products) of 1-qubit operators (gates).
  
  => Quantum Universal Turing Machine.
Quantum circuits: the set-up

- Goal: transform a $k$-bit input vector into an $n$-bit output vector
- Encoding classical input the quantum way
- $U$ – transforming the quantum information (quantum operations)
- $M$ – performing a measurement to obtain classical output
A centralised quantum computer

Transforming the data: what is feasible?

- Any unitary matrix can be built up from single-input gates, and the two-input controlled-not (CNOT) gate

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

(a) The Hadamard gate

- Certain operations cannot be performed, e.g. “qubit copying”.

\[
\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}
\]
Transforming the data: what’s the complexity of operation $U$?

- Building up the system from elementary bricks.

For both types of combinations, the complexity measure is subadditive:

$$C(U) \leq C(U_1) + C(U_2)$$

- Elementary gates acting on spaces of size $O(1)$ are assumed to have complexity $O(1)$. 

$$U = U_1 \otimes U_2$$

$$U = U_2 U_1$$
Quantum Distributed Computing
Why should quantum information help?

• **Negative evidence**: even when Alice and Bob share entanglement, they cannot do any magic
  
  (E.g. no way to exchange information without sending messages)

• **Negative evidence**: Holevo’s theorem – the usable information content (entropy) of an $n$-qubit state is not greater than that of an $n$-bit string.
  
  • so, does it make sense to send qubits at all?

• **But**: it turns out that

  *Quantum information sometimes reduces communication complexity*

  • One possible explanation: Information is no longer encoded at specific locations. *The state is a global property of the system.*

• **First examples:**
  
  • Grover’s $O(\sqrt{n})$-time search algorithm, 1997
  
  • Cleve & Buhrman, 1997 – simple 3-party proof-of-concept example
Problem definition

- Three parties, Alice, Bob, and Carol, are given an \( n \)-bit input string, each (strings \( a, b, c \), respectively).
- It is known that for all \( n \) indices, the bits fulfill the condition: \( a_i \oplus b_i \oplus c_i = 1 \)
- Goal: Alice is to compute the value of \( a_1 b_1 c_1 \oplus a_2 b_2 c_2 \oplus ... \oplus a_n b_n c_n \)

Theorem. Any classical protocol requires communication of at least 3 bits.

Quantum solution

- We do not change the communication capabilities of the system – classical messages (classical bits) only.
- We allow Alice, Bob and Carol to preshare an entangled state: \( \frac{1}{2} ( |001\rangle + |010\rangle + |100\rangle - |111\rangle ) \) // repeated \( n \) times
- Now, the problem can be solved using 2 communicated bits in total (Bob sends Alice 1 bit, Carol sends Alice 1 bit.)
Example (Cleve & Buhrman, 1997)

Details

- Each party $p$ transforms its $i$-th qubit ($q_i$) depending on the values of the $i$-th input bit ($x_i$).

\[
\text{for each } i \in \{1, \ldots, n\} \text{ do} \\
\text{if } x_i^p = 0 \text{ then apply } H \text{ to } q_i^p \\
\text{measure } q_i^p \text{ yielding bit } s_i^p \\
\]

\[
s^p \leftarrow s_1^p + \cdots + s_n^p
\]

- Each party other than Alice transmits its bit $s$ to Alice.
- Alice returns $s^A \oplus s^B \oplus s^C$ as output.
The Question of Locality
The classical **LOCAL** model

**Assumptions of the **LOCAL** model**

- The distributed system consists of a set of processors $V$, $|V|=n$
- The system operates in synchronous rounds
- No faults are present
- The system input is encoded as a *labeled* graph:
  - edge set $E$; $G=(V,E)$
  - node labels $x(v)$, for $v \in V$
- The result of computations is given through local variables $y(v)$, for $v \in V$
- *Messages exchanged in each round may have unbounded size*
- *The computational capabilities of each node are unbounded*
- As a rule, we will assume that nodes have unique identifiers
Quantum extensions

- **System initialization** *(before the input is set)*
  - by default: all the processors have an identical starting state
  - +S: the algorithm may redefine any global separable (=classical) state as a starting state of the system
  - +E: the algorithm may redefine any global entangled (=quantum) state as a starting state of the system

- **Communication capabilities**
  - by default: the processors communicate by exchanging classical messages (bits)
  - +Q: in each round, the processors can communicate by exchanging quantum information (qubits)
The **LOCAL+E** model

How much does the +E extension help?

- **+E**: Entangled initial state
  - allows us to take full advantage of quantum capabilities of the system
- Proof-of-concept "Mod 4" problem showing that +E does help:

  Variant of famous Greenberger-Horne-Zeilinger (GHZ) experiment

  - $V$ consists of 3 nodes $\{v_1, v_2, v_3\}$, whereas $E$ is empty
  - Each node has an input label $x_i \in \{0,1\}$ provided $(x_1 + x_2 + x_3) \in \{0,2\}$
  - **Goal**: output labels $y_i \in \{0,1\}$ must be such that:
    
    $$2(y_1 + y_2 + y_3) \equiv (x_1 + x_2 + x_3) \mod 4$$

  - cannot be solved with $Pr > \frac{3}{4}$ in (classical) LOCAL+S model, in any time
  - can be solved deterministically in 0 rounds with the +E extension
    (pre-shared GHZ state $|000> + |111>$)
Mod 4 problem – a conceptual look
Mod 4 problem – a conceptual look

The \textit{LOCAL+E} model
Mod 4 problem – a conceptual look

The $\text{LOCAL}+\text{E}$ model

$V_1 \ x_1 = 1$

$V_2 \ x_2 = 0$

$V_3 \ x_3 = 1$
The \textit{LOCAL}+\textit{E} model

Mod 4 problem – a conceptual look

\begin{align*}
\nu_1 & \quad x_1 = 1 \\
\nu_2 & \quad x_2 = 0 \\
\nu_3 & \quad x_3 = 1
\end{align*}

\begin{align*}
y_1 & = 1 \\
y_2 & = 0 \\
y_3 & = 0
\end{align*}
The \textit{LOCAL+E} model

Mod 4 problem – a conceptual look
### The $\text{LOCAL}+E$ model

#### Outcome of a quantum algorithm for the "Mod 4" problem

<table>
<thead>
<tr>
<th>Input $(x_1, x_2, x_3)$</th>
<th>Probability $p^i$</th>
<th>Output $(y_1^i, y_2^i, y_3^i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(0, 0, 0)$</td>
<td>1/4</td>
<td>$(0, 0, 0)$</td>
</tr>
<tr>
<td></td>
<td>1/4</td>
<td>$(0, 1, 1)$</td>
</tr>
<tr>
<td></td>
<td>1/4</td>
<td>$(1, 0, 1)$</td>
</tr>
<tr>
<td></td>
<td>1/4</td>
<td>$(1, 1, 0)$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Input $(x_1, x_2, x_3)$</th>
<th>Probability $p^i$</th>
<th>Output $(y_1^i, y_2^i, y_3^i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(0, 1, 1)$</td>
<td>1/4</td>
<td>$(1, 1, 1)$</td>
</tr>
<tr>
<td>or $(1, 0, 1)$</td>
<td>1/4</td>
<td>$(1, 0, 0)$</td>
</tr>
<tr>
<td>or $(1, 1, 0)$</td>
<td>1/4</td>
<td>$(0, 1, 0)$</td>
</tr>
</tbody>
</table>

$$2(y_1 + y_2 + y_3) \equiv (x_1 + x_2 + x_3) \mod 4$$
A comparison of the computational power of quantum models

The quantum models are more powerful than the classical ones.

Do they have any natural limits (lower time bounds)?
A comparison of the computational power of quantum models

The quantum models are more powerful than the classical ones.

Do they have any natural limits (lower time bounds)?
**Understanding of locality in the **LOCAL** model**

- each node builds up its view during the execution of the algorithm
  - after $t$ rounds, $\text{VIEW}_t(Gx, v)$ describes the distance-$t$ neighbourhood of $v$ in the labeled input graph $Gx$
- when considering deterministic algorithms, an output vector $y$ can be reached in $t$ rounds if and only if there exists a function $f$ such that:
  $y(v) = f(\text{VIEW}_t(Gx, v))$, for all $v \in V$
- this intuition can be extended to allow for randomized algorithms.
- no similar complete characterization is known for quantum approaches
  - doing it precisely would give a nice result on the capabilities of quantum operations (completely positive maps)
- **However**: we know of a weaker, but still view-based, bound on the computational power of any quantum algorithm.
The meaning of locality

Physical locality: the $\varphi$-$\text{LOCAL}$ model

- **Thesis.** Locality is violated if and only if, based on the available output data, we can conclusively verify that after $t$ rounds: some subset $S$ of processors was affected by input data initially localized outside its view, which is $\text{VIEW}_t(Gx, S) := \bigcup_{v \in S} \text{VIEW}_t(Gx, v)$.

- The preservation of locality should be interpreted in a probabilistic way:
  - consider the outcome of an algorithm after $t$ rounds; for the subset $S$, we look at the probability $p$ of obtaining any given output vector $y[S]$
  - if two inputs differ only by edges/label located outside $\text{VIEW}_t(Gx^{(i)}, S)$, then this probability $p$ must necessarily be the same for both inputs
  - (otherwise, we would be able to detect this remote difference in the input by performing many parallel executions of our algorithm)

- $\varphi$-$\text{LOCAL}$ is provably not less powerful than the quantum models
The meaning of locality

Example: why is the "Mod 4" problem in $\varphi$-LOCAL?

<table>
<thead>
<tr>
<th>Input $(x_1, x_2, x_3)$</th>
<th>Probability $p^i$</th>
<th>Output $(y_1^i, y_2^i, y_3^i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0, 0)</td>
<td>1/4</td>
<td>(0, 0, 0)</td>
</tr>
<tr>
<td></td>
<td>1/4</td>
<td>(0, 1, 1)</td>
</tr>
<tr>
<td></td>
<td>1/4</td>
<td>(1, 0, 1)</td>
</tr>
<tr>
<td></td>
<td>1/4</td>
<td>(1, 1, 0)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Input $(x_1, x_2, x_3)$</th>
<th>Probability $p^i$</th>
<th>Output $(y_1^i, y_2^i, y_3^i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 1, 1)</td>
<td>1/4</td>
<td>(1, 1, 1)</td>
</tr>
<tr>
<td>or (1, 0, 1)</td>
<td>1/4</td>
<td>(1, 0, 0)</td>
</tr>
<tr>
<td>or (1, 1, 0)</td>
<td>1/4</td>
<td>(0, 1, 0)</td>
</tr>
<tr>
<td></td>
<td>1/4</td>
<td>(0, 0, 1)</td>
</tr>
</tbody>
</table>

• we consider the above solution (obtained by the quantum algorithm), and one by one all possible sets $S$.
• for example, let $S=\{v_1\}$; since the graph is empty, $\text{VIEW}_t(Gx, S) = \{v_1\}$
• what are the probabilities of particular outputs?
  • in this case, regardless of $Gx$: $\Pr[y_1=0] = \frac{1}{2}$ and $\Pr[y_1=1] = \frac{1}{2}$
• so, these probabilities are not affected by the values of $x_2, x_3$, and the $\varphi$-LOCAL condition is not violated.
Lower time bounds in quantum models

So, what lower bounds can be proved in $\varphi$-$\text{LOCAL}$?

- Most proofs of lower time bounds which rely on view-based arguments will hold in $\varphi$-$\text{LOCAL}$ (and hence also all the quantum models)
  
  - The problem of finding a maximal independent set in the system graph requires $\Omega(\sqrt{(\log n / \log \log n)})$ rounds to solve [Kuhn, Moscibroda, Wattenhofer, 2004]

  - The problem of finding a locally minimal (greedy) coloring of the system graph requires $\Omega(\log n / \log \log n)$ rounds to solve [G., Klasing, K., Navarra, Kuszner, 2009]

  - The problem of finding a spanner with $O(n^{1+1/k})$ edges requires $\Omega(k)$ rounds to solve [Elkin 2007; Derbel et al. 2008]

- What about Linial’s famous $\Omega(\log^* n)$ bound on $(\Delta+1)$-coloring?
  
  - The neighbourhood-graph technique does not work in $\varphi$-$\Lambda\text{LOCAL}$...
Lower time bounds in quantum models

Example: time required to 2-color the even ring

- In the **LOCAL** model, \( \frac{n}{2} - 1 \) rounds are required and sufficient
  - simpler version of the same neighbourhood graph technique
- In \( \varphi-\text{LOCAL} \), \( \left\lceil \frac{n-2}{4} \right\rceil \) rounds are required and sufficient
- Sketch of lower bound
  - let \( t < \left\lceil \frac{n-2}{4} \right\rceil \), there will be at least two nodes \( u \) and \( v \) of the ring whose views are still disjoint
  - let \( S = \{u,v\} \);
  - the color values of \( u \) and \( v \) are necessarily the same if these vertices are at an even distance, and odd otherwise
    - there exist corresponding input graphs \( G_x^{(1)} \) and \( G_x^{(2)} \) with odd and even distance between \( u \) and \( v \), respectively
    - but the difference cannot be detected based on the local views of \( u \) and \( v \).
Is it possible to design a real quantum routine for 2-coloring $C_6$ in 1 round?

In the $\text{LOCAL}$ model, 2 rounds are required and sufficient.

In the $\varphi$-$\text{LOCAL}$ model, 1 round is required and sufficient.
Some open problems:

• Can quantum distributed algorithms be designed for any combinatorial problems of significance to practice or theory?

• How many rounds are required to 3-color the ring in the studied quantum models and in $\varphi$-LOCAL?

• What is the lower time bound on the $(\Delta+1)$-coloring problem in quantum models? (Currently all we know is that we need at least one round...)

• Is it possible to design a real quantum routine for 2-coloring $C_6$ in 1 round? (In the $\varphi$-LOCAL model 1 round is required and sufficient)

• Does $LOCAL+E = \varphi$-LOCAL?
Thank You!