EITQ

Circuit and Quantum Complexity

Renaud Vilmart

Quantum Complexity??

- Quantum Turing Machines
  - 1st versions : Assume any small-sized unitary $\implies$ uncomputable
  - How do we "read" information from the quantum tape?
  - More natural to use circuits
- How do we define complexity classes with circuits?
- Is there a quantum version of **P** or **BPP**?
- Is there a quantum version of **NP**?
- Can we compare classical and quantum complexity classes?
- What if we allow “exotic” physics?

Presentation Plan

(Quantum) Complexity via Circuits

Exotic Physics

Classical Complexity of Quantum Problems

Circuit Complexity for “Easy” Problems

A Probabilistic Version of **NP**

- Interactive proof system: verifier (us with reasonable computational power) interacts with a prover (some oracle with infinite power)

A Probabilistic Version of **NP**

- Interactive proof system: verifier (us with reasonable computational power) interacts with a prover (some oracle with infinite power)
  - If w accepted and prover is honest, verifier can be convinced
  - If w rejected, any prover can only convince with very small probability

A Probabilistic Version of **NP**

- Interactive proof system: verifier (us with reasonable computational power) interacts with a prover (some oracle with infinite power)
  - If w accepted and prover is honest, verifier can be convinced
  - If w rejected, any prover can only convince with very small probability
- **NP**: verifier is a poly-time deterministic TM, with just one message from the prover (who has access to the input)

A Probabilistic Version of **NP**

- Interactive proof system: verifier (us with reasonable computational power) interacts with a prover (some oracle with infinite power)
  - If w accepted and prover is honest, verifier can be convinced
  - If w rejected, any prover can only convince with very small probability
- **NP**: verifier is a poly-time deterministic TM, with just one message from the prover (who has access to the input)
- Arthur-Merlin protocol: verifier (poly-time PTM) is called Arthur, and the prover is called Merlin.

A Probabilistic Version of **NP**

- Interactive proof system: verifier (us with reasonable computational power) interacts with a prover (some oracle with infinite power)
  - If w accepted and prover is honest, verifier can be convinced
  - If w rejected, any prover can only convince with very small probability
- **NP**: verifier is a poly-time deterministic TM, with just one message from the prover (who has access to the input)
- Arthur-Merlin protocol: verifier (poly-time PTM) is called Arthur, and the prover is called Merlin.
- **MA**: Languages recognised by an Arthur-Merlin protocol with a single message (from Merlin to Arthur), and with error probability $\frac{1}{3}$

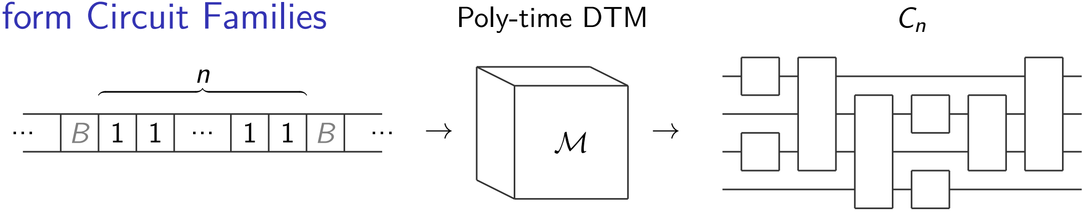
A Probabilistic Version of **NP**

- Interactive proof system: verifier (us with reasonable computational power) interacts with a prover (some oracle with infinite power)
  - If w accepted and prover is honest, verifier can be convinced
  - If w rejected, any prover can only convince with very small probability
- **NP**: verifier is a poly-time deterministic TM, with just one message from the prover (who has access to the input)
- Arthur-Merlin protocol: verifier (poly-time PTM) is called Arthur, and the prover is called Merlin.
- **MA**: Languages recognised by an Arthur-Merlin protocol with a single message (from Merlin to Arthur), and with error probability $\frac{1}{3}$
- $\mathbf{NP} \subseteq \mathbf{MA}$, and $\mathbf{BPP} \subseteq \mathbf{MA}$

A Probabilistic Version of **NP**

- Interactive proof system: verifier (us with reasonable computational power) interacts with a prover (some oracle with infinite power)
  - If w accepted and prover is honest, verifier can be convinced
  - If w rejected, any prover can only convince with very small probability
- **NP**: verifier is a poly-time deterministic TM, with just one message from the prover (who has access to the input)
- Arthur-Merlin protocol: verifier (poly-time PTM) is called Arthur, and the prover is called Merlin.
- **MA**: Languages recognised by an Arthur-Merlin protocol with a single message (from Merlin to Arthur), and with error probability $\frac{1}{3}$
- $\mathbf{NP} \subseteq \mathbf{MA}$, and $\mathbf{BPP} \subseteq \mathbf{MA}$
- $\mathbf{P} = \mathbf{BPP} \implies \mathbf{NP} = \mathbf{MA}$

Uniform Circuit Families



Definition (Uniform Family of Circuits)

- A gate of the form $g : n \to m$ with $n, m \in \mathbb{N}$ has name g, has n inputs and m outputs. Let $\mathcal{G}$ be a set of gates.
- $\mathcal{V}_n := \{x_i : 0 \to 1 \mid 0 < i \leq n\}$ is a set of k variables
- $\mathcal{O} := \{o_i : 1 \to 0\}$ a set of "outputs"
- A circuit is a directed (edge-ordered) acyclic graph $G = (V, E)$ and a labelling function $V \to \mathcal{G} \cup \mathcal{V} \cup \mathcal{O}$, such that if $v \mapsto g : n \to m$, then v has n incoming edges and m outgoing edges
- $(C_n)_{n \in \mathbb{N}}$ is a poly-time uniform family of circuits if there exists a poly-time Turing machine $\mathcal{M}$ that produces C_n on word $1 \overset{n}{\cdots} 1$.

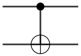
A Circuit-Based Definition of **P** and **NP**

Definition (Reversible Circuit)

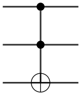
A reversible circuit is a boolean circuit composed of the logic gates:

$|0\rangle$

$: |x\rangle \mapsto |x \oplus 1\rangle$



$: |x, y\rangle \mapsto |x, y \oplus x\rangle$



$: |x, y, z\rangle \mapsto |x, y, z \oplus xy\rangle$

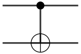
A Circuit-Based Definition of **P** and **NP**

Definition (Reversible Circuit)

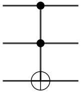
A reversible circuit is a boolean circuit composed of the logic gates:

$|0\rangle$ —

$: |x\rangle \mapsto |x \oplus 1\rangle$



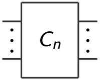
$: |x, y\rangle \mapsto |x, y \oplus x\rangle$

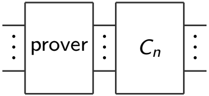


$: |x, y, z\rangle \mapsto |x, y, z \oplus xy\rangle$

$L \in \mathbf{P}$:	$L \in \mathbf{NP}$:

$\exists (C_n)_{n\in\mathbb{N}}$ a poly-sized uniform family of reversible boolean circuits, such that in:





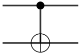
A Circuit-Based Definition of **P** and **NP**

Definition (Reversible Circuit)

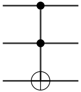
A reversible circuit is a boolean circuit composed of the logic gates:

$|0\rangle$

$: |x\rangle \mapsto |x \oplus 1\rangle$



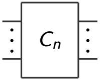
$: |x, y\rangle \mapsto |x, y \oplus x\rangle$

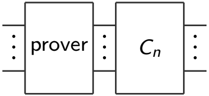


$: |x, y, z\rangle \mapsto |x, y, z \oplus xy\rangle$

$L \in \mathbf{P}$:	$L \in \mathbf{NP}$:

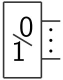
$\exists (C_n)_{n \in \mathbb{N}}$ a poly-sized uniform family of reversible boolean circuits, such that in:



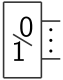


- If input $\in L$ and prover honest, first output is $|1\rangle$
- If input $\notin L$, first output is $|0\rangle$

A Circuit-Based Definition of **BPP** and **MA**

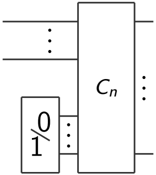
We denote  a (uniform) random bitstring generator.

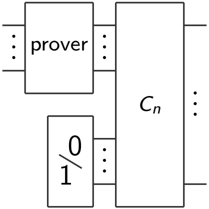
A Circuit-Based Definition of **BPP** and **MA**

We denote  a (uniform) random bitstring generator.

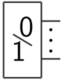
$L \in$ **BPP**:	$L \in$ **MA**:

$\exists (C_n)_{n \in \mathbb{N}}$ a poly-sized uniform family of reversible boolean circuits, such that in:





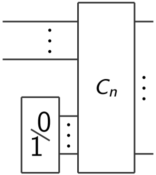
A Circuit-Based Definition of **BPP** and **MA**

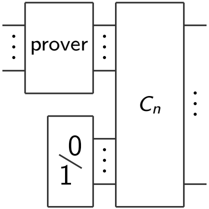
We denote 

a (uniform) random bitstring generator.

$L \in$ **BPP**: | $L \in$ **MA**:

$\exists (C_n)_{n\in\mathbb{N}}$ a poly-sized uniform family of reversible boolean circuits, such that in:





- If input $\in L$ and prover honest, $\Pr[\text{first output is } |1\rangle] \geq \frac{2}{3}$
- If input $\notin L$, $\Pr[\text{first output is } |1\rangle] \leq \frac{1}{3}$

Bounded-error Quantum Polynomial (**BQP**) and Quantum Merlin Arthur **QMA**

Definition (Quantum Circuit)

A quantum circuit is a reversible circuit augmented with 1-qubit (computable) unitaries and Z-measurements:

$-\boxed{U}- \quad : |x\rangle \mapsto U|x\rangle$

Bounded-error Quantum Polynomial (**BQP**) and Quantum Merlin Arthur **QMA**

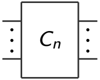
Definition (Quantum Circuit)

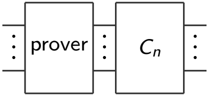
A quantum circuit is a reversible circuit augmented with 1-qubit (computable) unitaries and Z-measurements:

$-\boxed{U}- \quad : |x\rangle \mapsto U|x\rangle$ 

$L \in \mathbf{BQP}$:	$L \in \mathbf{QMA}$:

$\exists (C_n)_{n\in\mathbb{N}}$ a poly-sized uniform family of quantum circuits, such that in:





Bounded-error Quantum Polynomial (**BQP**) and Quantum Merlin Arthur **QMA**

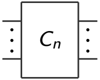
Definition (Quantum Circuit)

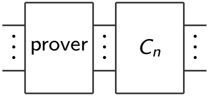
A quantum circuit is a reversible circuit augmented with 1-qubit (computable) unitaries and Z-measurements:

$: |x\rangle \mapsto U|x\rangle$

$L \in \mathbf{BQP}$:	$L \in \mathbf{QMA}$:

$\exists(C_n)_{n\in\mathbb{N}}$ a poly-sized uniform family of quantum circuits, such that in:





- If input $\in L$ and prover honest, $\Pr[\text{first output is } |1\rangle] \geq \frac{2}{3}$
- If input $\notin L$, $\Pr[\text{first output is } |1\rangle] \leq \frac{1}{3}$

Some **BQP** and **QMA** Problems

BQP:

- Prime factorisation
- Evaluation of Jones polynomials at k'th root of unity
- Sampling from the solution of a linear system $Ax = b$

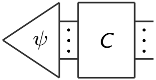
Some **BQP** and **QMA** Problems

BQP:

- Prime factorisation
- Evaluation of Jones polynomials at k'th root of unity
- Sampling from the solution of a linear system $Ax = b$

QMA:

- Quantum circuit SAT:
  Given C a quantum circuit, $p \in [0, 1]$ a probability, does there exist $|\psi\rangle$ such that:

  has probability $\geq p$ of measuring $|1\rangle$ on 1st qubit?
- Checking if quantum circuit is not identity
- Local Hamiltonian minimal eigenvalue
- Detecting insecure quantum encryption

Presentation Plan

(Quantum) Complexity via Circuits

Exotic Physics

Classical Complexity of Quantum Problems

Circuit Complexity for "Easy" Problems

Exotic Physics: Postselection

Definition (Postselection)

Postselection (or postselected measurement) is a measurement of which we choose the outcome (provided it does not have probability 0): $—\langle 0|$.

Exotic Physics: Postselection

Definition (Postselection)

Postselection (or postselected measurement) is a measurement of which we choose the outcome (provided it does not have probability 0): $—\langle 0|$.

PostBQP: **BQP** with postselection

Exotic Physics: Postselection

Definition (Postselection)

Postselection (or postselected measurement) is a measurement of which we choose the outcome (provided it does not have probability 0): $-\!\!\!-\langle 0|$.
PostBQP: **BQP** with postselection

Theorem (Aaronson)

$\boldsymbol{PostBQP} = \boldsymbol{PP}$

Exotic Physics: Postselection

Definition (Postselection)

Postselection (or postselected measurement) is a measurement of which we choose the outcome (provided it does not have probability 0): $—\langle 0|$.

PostBQP: **BQP** with postselection

Theorem (Aaronson)

PostBQP $=$ ***PP***

The order of application of postselected measurement w.r.t. usual measurement is important.
E.g., with $|EPR\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$:

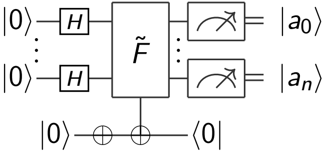
$\mathtt{Meas}_1 \circ \langle 0|_2 \, |EPR\rangle = |0\rangle$ but $\langle 0|_2 \circ \mathtt{Meas}_1 \, |EPR\rangle$ is not always defined.

SAT $\in$ **PostBQP**

$F(p_1, ..., p_n)$ SAT formula. Check if $F(True, ..., True) = True$. If yes, F is satisfiable. Otherwise, define $\tilde{F} := F \vee (p_1 \wedge ... \wedge p_n)$. Notice that $\tilde{F}$ is satisfiable and has exactly one more solution than F.

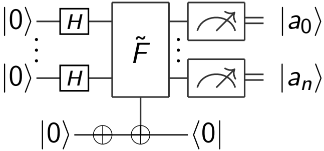
SAT $\in$ **PostBQP**

$F(p_1, ..., p_n)$ SAT formula. Check if $F(True, ..., True) = True$. If yes, F is satisfiable. Otherwise, define $\tilde{F} := F \vee (p_1 \wedge ... \wedge p_n)$. Notice that $\tilde{F}$ is satisfiable and has exactly one more solution than F. Compute:



SAT $\in$ **PostBQP**

$F(p_1, ..., p_n)$ SAT formula. Check if $F(True, ..., True) = True$. If yes, F is satisfiable. Otherwise, define $\tilde{F} := F \vee (p_1 \wedge ... \wedge p_n)$. Notice that $\tilde{F}$ is satisfiable and has exactly one more solution than F. Compute:

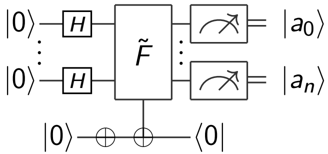


Check if $(a_0, ..., a_n) = (True, ..., True)$. Do the computation twice.

- If $(a_0, ..., a_n) = (True, ..., True)$ both times, reject
- If $(a_0, ..., a_n) \neq (True, ..., True)$, accept (and $(a_0, ..., a_n)$ is a solution)

SAT $\in$ **PostBQP**

$F(p_1, ..., p_n)$ SAT formula. Check if $F(True, ..., True) = True$. If yes, F is satisfiable. Otherwise, define $\tilde{F} := F \vee (p_1 \wedge ... \wedge p_n)$. Notice that $\tilde{F}$ is satisfiable and has exactly one more solution than F. Compute:



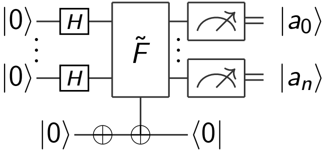
Check if $(a_0, ..., a_n) = (True, ..., True)$. Do the computation twice.

- If $(a_0, ..., a_n) = (True, ..., True)$ both times, reject
- If $(a_0, ..., a_n) \neq (True, ..., True)$, accept (and $(a_0, ..., a_n)$ is a solution)

If F unsat., $(a_0, ..., a_n)$ will be $(True, ..., True)$ everytime, so we reject with proba 1.

SAT $\in$ **PostBQP**

$F(p_1, ..., p_n)$ SAT formula. Check if $F(True, ..., True) = True$. If yes, F is satisfiable. Otherwise, define $\tilde{F} := F \vee (p_1 \wedge ... \wedge p_n)$. Notice that $\tilde{F}$ is satisfiable and has exactly one more solution than F. Compute:



Check if $(a_0, ..., a_n) = (True, ..., True)$. Do the computation twice.

- If $(a_0, ..., a_n) = (True, ..., True)$ both times, reject
- If $(a_0, ..., a_n) \neq (True, ..., True)$, accept (and $(a_0, ..., a_n)$ is a solution)

If F unsat., $(a_0, ..., a_n)$ will be $(True, ..., True)$ everytime, so we reject with proba 1. If F is sat., $(a_0, ..., a_n)$ has $\leq \frac{1}{4}$ proba of being $(True, ..., True)$ both times, so the probability we accept is $\geq \frac{3}{4} > \frac{2}{3}$.

Exotic Physics: Non-linearity

Theorem (Gisin)

Introducing non-linear corrections into quantum mechanics allows for supraliminal communications.

Theorem (Abrams, Lloyd)

Nonlinear quantum mechanics implies polynomial-time solution for ***NP-complete*** *and* ***#P-complete*** *problems.*

Proof sketch:

- create state $\frac{(2^n - s)|0\rangle + s|1\rangle}{N}$
- use non-linearity to separate cases $s = 0$ and $s \neq 0$ exponentially fast

Presentation Plan

(Quantum) Complexity via Circuits

Exotic Physics

Classical Complexity of Quantum Problems

Circuit Complexity for “Easy” Problems

Oracles, Classical Simulation

Definition ($\mathbf{P}^{\#\mathbf{P}}$)

Class of problems solvable by a poly-time deterministc Turing machine with access to a $\#\mathbf{P}$ oracle (i.e. where we are allowed to solve a $\#\mathbf{P}$ problem in time $\mathcal{O}(1)$).

Postselected measurements can be represented in the perfect-matching-counting framework, hence:

$\mathbf{BQP} \subseteq \mathbf{PostBQP} = \mathbf{PP} \subseteq \mathbf{P}^{\#\mathbf{P}}$

- Planar matchgate quantum circuits (with postselections) $\to$ **P**
- Clifford circuits (with postselections) $\to$ **P**

Unitarity Checking

- Setup:
  - Quantum circuit C with postselections
- Question:

Does C implement a unitary operator?

Theorem

*Unitarity checking is **coNP-hard**.*

Postselection Removal

- Setup:
  - Quantum circuit C with postselections
  - Promise that C implements a unitary operator U
- Output:

  A circuit C' without postselection that implements U

Theorem (de Beaudrap, Kissinger, van de Wetering)

*Postselection removal is **#P-hard**.*

Hermiticity Checking

- Setup:
  - Quantum circuit C with postselections
- Question:

Does C implement a Hermitian operator?

Theorem

Hermiticity checking is ***coNP-hard****.*

Presentation Plan

(Quantum) Complexity via Circuits

Exotic Physics

Classical Complexity of Quantum Problems

Circuit Complexity for “Easy” Problems

Bounded Fanin Circuits

Definition (**NC**)

A problem is in $\mathbf{NC}^i$ if there exists a family of boolean circuits:

- composed of gates with fanin ≤ 2
- of polynomial size
- of depth $\mathcal{O}(\log^i(n))$

that solve it.

$$\mathbf{NC} := \bigcup_i \mathbf{NC}^i.$$

For these classes and the following, adding **u** as a suffix means we ask that the family of circuits be uniform (e.g. $\mathbf{uNC}^i$).

E.g.: Computing the parity of 1s in a bitstring is in $\mathbf{NC}^1$.

Unbounded Fanin Circuits

Definition (**AC**)

A problem is in $\mathbf{AC}^i$ if there exists a family of boolean circuits:

- where AND and OR gates have unbounded fanin
- of polynomial size
- of depth $\mathcal{O}(\log^i(n))$

that solve it.

$$\mathbf{AC} := \bigcup_i \mathbf{AC}^i.$$

E.g.: Deciding if all symbols in a bitstring are 1 is in $\mathbf{AC}^0$.

Remark: rather sensitive to the chosen gate set.

$$\mathbf{NC}^i \subseteq \mathbf{AC}^i \subseteq \mathbf{NC}^{i+1}$$

Quantum Circuits with Unbounded Fanin

Definition (QAC)

A family of unitaries $(U_n)_{n\in\mathbb{N}}$ acting on n qubits is in $\mathbf{QAC}^i$ if there exists a family of quantum circuits:

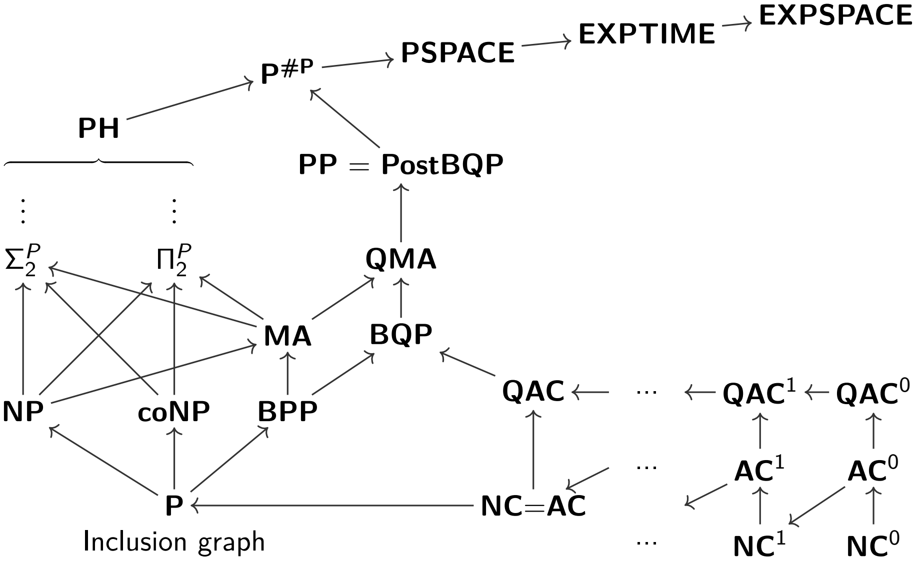
- composed of 1-qubit gates and unbounded fanin Toffoli gates
- of depth $\mathcal{O}(\log^i(n))$

that implements it.

$$\mathbf{QAC} := \bigcup_i \mathbf{QAC}^i.$$

Well studied, but not well understood.
Open problem: is $|x_1, \ldots, x_n, b\rangle \mapsto |x_1, \ldots, x_n, b \oplus x_1 \oplus \ldots \oplus x_n\rangle$ in $\mathbf{QAC}^0$?

Overview of Complexity Classes



Inclusion graph