Quantum state synthesis complexity classes

The quantum equivalent of functional classes

Hugo Delavenne

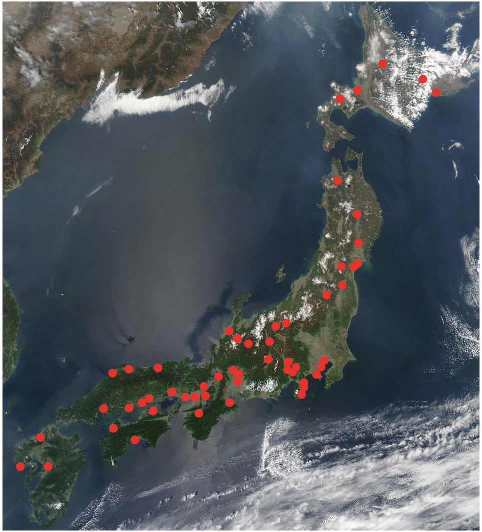
Quantum Algorithms and Complexity Group, Nagoya University, Japan

Under the supervision of François Le Gall

October 2022 – June 2023

Motosuko (Yamanashi)

Research internship in Japan



General idea

(Quantum) Complexity theory studies decision problems: binary outputs.

Physicists want quantum problems: quantum outputs.
(Also some computer science interest.)

Very recent approach [Aar16, RY21].

[Aar16] Scott Aaronson. The complexity of quantum states and transformations: from quantum money to black holes. **arXiv preprint arXiv:1607.05256, 2016**

[RY21] Gregory Rosenthal and Henry Yuen. Interactive proofs for synthesizing quantum states and unitaries. **arXiv preprint arXiv:2108.07192, 2021**

Summary

1. Classical functional complexity classes

2. The same but quantum
   - Quantum information
   - Quantum decision classes
   - State synthesis complexity classes

3. Results

4. Conclusion

Matsumoto-jo (Nagano)

Classical functional complexity classes

Miyajima (Hiroshima)

Decision classes are sets of languages $L \subseteq \Sigma^*$.

Definition P (Polynomial)

$L \in \mathbf{P}$ iff $\exists$ a PTTM M s.t. $\forall x \in \Sigma^*, x \in L \iff M(x)$ accepts.

Definition NP (Nondeterministic Polynomial)

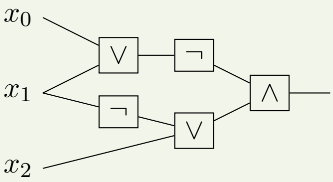
$L \in \mathbf{NP}$ iff $\exists$ a PTTM M s.t.

- $\forall x \in L, \exists w \in \Sigma^*, M(x, w)$ accepts.
- $\forall x \notin L, \forall w \in \Sigma^*, M(x, w)$ rejects.

CircuitSAT is the language of satisfiable boolean circuits.

Example CircuitSAT **circuit**

The following circuit is in CircuitSAT



CircuitSAT $\in \mathbf{NP}$ by running the circuit on a given valuation.
CircuitSAT $\in \mathbf{P}$ iff $\mathbf{P} = \mathbf{NP}$.

Functional classes are defined on relations between input and output $R \subseteq \Sigma^* \times \Sigma^*$.

xR denotes $\{y \in \Sigma^* \mid (x, y) \in R\}$.

Definition **FP (Functional Polynomial)**

$R \in \mathbf{FP}$ iff $\exists$ a PTTM M s.t. for $x \in \Sigma^*$

- ▷ if $xR \neq \varnothing$ then $M(x)$ accepts and outputs some $y \in xR$.
- ▷ if $xR = \varnothing$ then $M(x)$ rejects.

Definition **FNP (Functional Nondeterministic Polynomial)**

$R \in \mathbf{FNP}$ iff $\exists$ a PTTM M s.t. for $x \in \Sigma^*$

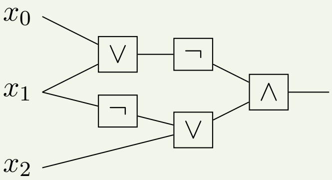
- ▷ if $xR \neq \varnothing$ then $\exists w \in \Sigma^*, M(x, w)$ accepts and outputs some $y \in xR$.
- ▷ if $xR = \varnothing$ then $\forall w \in \Sigma^*, M(x, w)$ rejects.

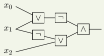
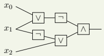
Example: FunctionalCircuitSAT

$(C, u) \in$ FunctionalCircuitSAT iff $C(u) = 1$

Example

$(x_0, x_1, x_2) = (0, 0, 1)$ and $(0, 0, 0)$ satisfy the circuit



So $\Bigg($  $, 001\Bigg), \Bigg($  $, 000\Bigg) \in$ FunctionalCircuitSAT.

FunctionalCircuitSAT $\in \mathbf{FNP}$ by checking the valuation and returning a *copy* of it.
FunctionalCircuitSAT $\in \mathbf{FP}$ iff $\mathbf{FP} = \mathbf{FNP}$.

Question

Are $\mathbf{FP}$ and $\mathbf{FNP}$ harder than $\mathbf{P}$ and $\mathbf{NP}$?

No.

Proposition **Equivalence between decision and search [BG94]**

$\mathbf{FP} = \mathbf{FNP}$ iff $\mathbf{P} = \mathbf{NP}$

Proof.
Let M be a PTTM solving FunctionalCircuitSAT.
The language $L = \{(x, w) \mid \exists w', M(x, w \cdot w') \text{ accepts}\}$ is in $\mathbf{NP}$.
So if $\mathbf{P} = \mathbf{NP}$ there is a PTTM M' recognizing L.
Construct a witness $w_1 \ldots w_k$ bit by bit with $w_i := 1$ iff $M'(x, w_1 \ldots w_{i-1})$ accepts.

[BG94] Mihir Bellare and Shafi Goldwasser. The complexity of decision versus search. **SIAM Journal on Computing, 23(1):97–119, 1994**

The same but quantum

- Quantum information
- Quantum decision classes
- State synthesis complexity classes

Kawazu (Shizuoka)

physical reality

Classical strings

$$u = b_1 \ldots b_n \in \{0,1\}^n$$

Quantum states

$$|\psi\rangle = \sum_{b_1 \ldots b_n \in \{0,1\}^n} \alpha_{b_1 \ldots b_n} |b_1 \ldots b_n\rangle \in \mathbb{C}^{2^n}$$

$$\sum |\alpha_{b_1 \ldots b_n}|^2 = 1$$

incomplete knowledge

Probabilistic strings

$$u = (p_1, \ldots, p_n) \in [0,1]^n$$

u <u>is</u> $b_1 \ldots b_n$ w.p. $\prod |b_i - p_i|$

Density matrices

$$\rho = \sum_{b_1 \ldots b_n \in \{0,1\}^n} \beta_{b_1 \ldots b_n} |b_1 \ldots b_n\rangle\langle b_1 \ldots b_n|$$

$$\sum \beta_{b_1 \ldots b_n} = 1$$

ρ <u>is</u> $|b_1 .. b_n\rangle\langle b_1 .. b_n|$ w.p. $\beta_{b_1 \ldots b_n}$

$|\psi\rangle = \sum \alpha_{b_1\dots b_n} |b_1\dots b_n\rangle$ is measured and projected on $|b_1\dots b_n\rangle$ w.p. $|\alpha_{b_1\dots b_n}|^2$.

Example **Measurement**

Let $|\psi\rangle = \sqrt{\frac{1}{3}}\,|001\rangle + \sqrt{\frac{2}{3}}\,|010\rangle$.

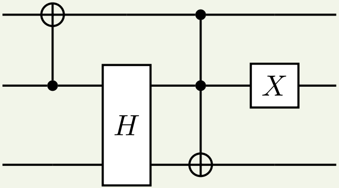
- ▷ projected on $|001\rangle$ w.p. $\frac{1}{3}$
- ▷ projected on $|010\rangle$ w.p. $\frac{2}{3}$

Example **Density matrices**

- ▷ complete knowledge of $|\psi\rangle$ is $\rho = |\psi\rangle\langle\psi| = \frac{1}{3}\,|001\rangle\langle 001| + \frac{2}{3}\,|010\rangle\langle 010|$
- ▷ knowledge on first two qubits of $|\psi\rangle$ is $\rho = \frac{1}{3}\,|00\rangle\langle 00| + \frac{2}{3}\,|01\rangle\langle 01|$
- ▷ if $|001\rangle$ w.p. $\frac{1}{3}$ and $|010\rangle$ w.p. $\frac{2}{3}$, we manipulate $\rho = \frac{1}{3}\,|001\rangle\langle 001| + \frac{2}{3}\,|010\rangle\langle 010|$

States are manipulated by circuits.

Example **Quantum circuit**



Fixed set of quantum gates are universal up to precision. E.g. $\left\{ H, \right.$  $\left. \right\}$ is universal.

States are approximated so we use a distance to characterize it.

Definition **Trace distance**

$$\mathrm{td}(\rho, \sigma) := \frac{1}{2}\mathrm{Tr}\left(\sqrt{(\rho - \sigma)^\dagger(\rho - \sigma)}\right) \in [0, 1]$$

Property **The trace distance characterizes distinguishability**

ρ and σ can be distinguished w.p. $\mathrm{td}(\rho, \sigma)$.

$|\psi\rangle = \sum_{b_1 \ldots b_n} \alpha_{b_1 \ldots b_n} |b_1 \ldots b_n\rangle$ cannot be written $|\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$, with $|\psi_i\rangle$ on 1 qubit.

Operators are linear: $C(\alpha |\psi_1\rangle + \beta |\psi_2\rangle) = \alpha C |\psi_1\rangle + \beta C |\psi_2\rangle$.

Quantum circuits (without measurement) are reversible.

Theorem **No-cloning theorem [Par70]**

There is no quantum circuit C s.t. $\forall |\psi\rangle, C |\psi\rangle |0^n\rangle = |\psi\rangle |\psi\rangle$.

[Par70] James L Park. The concept of transition in quantum mechanics. **Foundations of physics, 1:23–33, 1970**

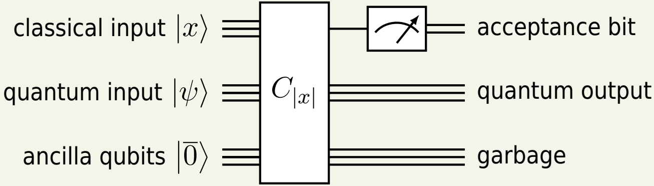
No quantum TM, but quantum circuits generated by TM.

Circuits have fixed size so family of circuits $(C_n)_{n\in\mathbb{N}}$.

Definition **Uniform family of circuits**

$(C_n)_{n\in\mathbb{N}}$ is uniform iff $\exists M$ PTTM s.t. $\forall n \in \mathbb{N}, M(1^n) = C_n$.

Example **Circuit with accepting bit and output state**



Definition QMA (Quantum Merlin Arthur)

$L \in \mathbf{QMA}[c, s]$ iff $\exists (C_n)_{n \in \mathbb{N}}$ uniform s.t.

- completeness: if $x \in L$ then $\exists \left|\psi\right\rangle, \Pr(C_n(\left|x\right\rangle \left|\psi\right\rangle)$ accepts$) \geqslant c(x)$
- soundness: if $x \notin L$ then $\forall \left|\psi\right\rangle, \Pr(C_n(\left|x\right\rangle \left|\psi\right\rangle)$ accepts$) \leqslant s(x)$

BQP (Bounded-error Quantum Polynomial)	no witness
QCMA (Quantum Classical-Merlin Arthur)	classical witness
QIP (Quantum Interactive Protocol)	quantum prover
QCIP (Quantum Classical Interactive Protocol)	classical prover

Theorem Relation between decision complexity classes [KSV02, JJUW11]

$$
\begin{tikzcd}
\mathbf{QIP} \arrow[r, phantom, "="] & \mathbf{PSPACE} \arrow[r, phantom, "="] & \mathbf{IP} \\
\mathbf{QMA} \arrow[u] & & \\
\mathbf{QCMA} \arrow[u] & \mathbf{NP} \arrow[l] \arrow[uu] & \\
\mathbf{BQP} \arrow[u] & \mathbf{P} \arrow[l] \arrow[u] &
\end{tikzcd}
$$

[KSV02] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. Classical and quantum computation. **Number 47. American Mathematical Soc., 2002**

[JJUW11] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. **J. ACM, 58(6), dec 2011**

	$\mathbf{FP}$	$\mathbf{FNP}$	$\mathbf{stateBQP}$	$\mathbf{stateQCMA}$	$\mathbf{stateQMA}$
Complexity	PTTM		Quantum circuit generated by PTTM		
Witness	$\varnothing$	String	$\varnothing$	String	Quantum state
Input	Classical string				
Output	Acceptance bit		Acceptance bit		
	String		Quantum state (density matrix)		

New parameter: inaccuracy δ.

Definition $\mathbf{stateQMA}$

$R \subseteq \Sigma^* \times \mathcal{Q}$ is in $\mathbf{stateQMA}_\delta[c, s]$ iff $\exists (C_n)_{n \in \mathbb{N}}$ uniform s.t.

- if $xR \neq \varnothing$ then
  - $\exists \left|\psi\right\rangle, \Pr(C_n(\left|x\right\rangle \left|\psi\right\rangle)$ accepts$) \geqslant c(x)$.
  - $\forall \left|\psi\right\rangle$, if $\mathrm{td}(C_n(\left|x\right\rangle \left|\psi\right\rangle), xR) > \delta(x)$ then $\Pr(C_n(\left|x\right\rangle \left|\psi\right\rangle)$ accepts$) \leqslant s(x)$.
- if $xR = \varnothing$ then $\forall \left|\psi\right\rangle, \Pr(C_n(\left|x\right\rangle \left|\psi\right\rangle)$ accepts$) \leqslant s(x)$.

$\mathbf{stateBQP}$, $\mathbf{stateQCMA}$, $\mathbf{stateQIP}$, $\mathbf{stateQCIP}$ are defined similarly.

Results


Kenroku-en (Ishikawa)

Previous results

For decision: $\mathbf{QIP} = \mathbf{PSPACE}$ [JJUW11]

Theorem $\mathbf{stateQIP} = \mathbf{statePSPACE}$ **[MY23]**

$\mathbf{stateQIP}_\delta \subseteq \mathbf{statePSPACE}_{\delta+1/\mathrm{poly}}$ and $\mathbf{statePSPACE}_\delta \subseteq \mathbf{stateQIP}_{\delta+1/\mathrm{poly}}$

For decision: $\mathbf{QIP}_\delta = \mathbf{QIP}_{\delta+1/\mathrm{poly}}(3)$ [Wat03]

Theorem $\mathbf{stateQIP}$ **has constant round protocols [Ros23]**

$\mathbf{stateQIP} = \mathbf{stateQIP}(6)$

[JJUW11] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. **J. ACM, 58(6), dec 2011**

[MY23] Tony Metger and Henry Yuen. stateqip= statepspace. **arXiv preprint arXiv:2301.07730, 2023**

[Ros23] Gregory Rosenthal. Efficient quantum state synthesis with one query. **arXiv preprint arXiv:2306.01723, 2023**

[Wat03] John Watrous. PSPACE has constant-round quantum interactive proof systems. **Theoretical Computer Science, 292(3):575-588, 2003**

Theorem **Inaccuracy preversing error-reduction [DGLM23]**

$$\mathbf{stateQMA}_\delta[c,s] \subseteq \mathbf{stateQMA}_\delta[1-2^{-\mathrm{poly}(n)}, 2^{-\mathrm{poly}(n)}]$$

For decision: $\mathbf{QCMA}[c,s] = \mathbf{QCMA}[1,\frac{1}{2}]$ [JKNN12]

Theorem $\mathrm{stateQCMA}$ **achieves perfect completeness [DGLM23]**

$$\mathbf{stateQCMA}_\delta[c,s] \subseteq \mathbf{stateQCMA}_{\delta+1/\exp}[1,\tfrac{1}{2}]$$

[DGLM23] Hugo Delavenne, Francois Le Gall, Yupan Liu, and Masayuki Miyamoto. Quantum merlin-arthur proof systems for synthesizing quantum states.
arXiv preprint arXiv:2303.01877, 2023

[JKNN12] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving Perfect Completeness in Classical-Witness Quantum Merlin-Arthur Proof Systems.
Quantum Info. Comput., 12(5–6):461–471, may 2012

Theorem **Impossibility to improve the inaccuracy**

For $0 < \varepsilon \leqslant \delta \leqslant 1 - 2^{-n}$, $\mathbf{stateBQP}_\delta \not\subset \mathbf{stateR}_{\delta-\varepsilon}$.

Proof idea for $\delta(n) := 1 - 2^{-n}$.
There exists $(u_n) \in \Sigma^*$ s.t. no TM can generate u_n w.p. $> 2^{-n}$.
With $xR := \{\left|u_{|x|}\right\rangle\}$, $R \in \mathbf{stateBQP}_{1-2^{-n}}[1,0]$ by synthesizing $2^{-n} \sum |\psi\rangle\langle\psi|$.
If $R \in \mathbf{stateR}_{1-2^{-n}-\varepsilon(n)}$ then by simulation u_n is generated w.p. $> 2^{-n}$.

Classes are defined as $\mathbf{stateQMA} := \bigcap_{p=\mathrm{poly}(n)} \mathbf{stateQMA}_{1/p}$.

Proposition **Equivalence with maximal inaccuracy**

For any R and $\mathbf{C}$, $L_R \in \mathbf{C}[c,s] \iff R \in \mathbf{stateC}_{1-2^{-n}}[c,s]$.

Proof idea.
Generate a maximally mixed state $2^{-n}\sum |b_1 \ldots b_n\rangle\langle b_1 \ldots b_n|$.
Use decision circuit for decision.

Can we do better?

Similarly to $\mathbf{P} = \mathbf{NP} \implies \mathbf{FP} = \mathbf{FNP}$, we guess the $\mathbf{QCMA}$ witness bit by bit.

Only issue is probabilities so we use promises.

Lemma Guessing a witness bit is QCMA

Input: circuit C, input x, partial witness w_0

Output: $\exists w, \Pr(C(|x\rangle\,|w_0 1 w\rangle$ accepts$) \geqslant p_0(|w_0|)$

Promise: for $b = 0$ or 1, $\forall w, \Pr(C(|x\rangle\,|w_0 b w\rangle)) \leqslant p_0(|w_0|) - 1/|x|^2$

is in $\mathbf{QCMA}$ for any p_0.

Proposition Generate a classical witness

If $\mathbf{BQP} = \mathbf{QCMA}$ then $\mathbf{stateBQP}_\delta = \mathbf{stateQCMA}_\delta$.

Conjecture Guessing a quantum state

If $\mathbf{BQP} = \mathbf{QMA}$ then $\mathbf{stateBQP}_{\delta} = \mathbf{stateQMA}_{\delta+1/\mathrm{poly}}$.

If an oracle poly-size circuit can generate $\mathbf{QMA}$ witnesses then $\mathbf{QCMA} = \mathbf{QMA}$.

However:

Conjecture Important conjecture in QCS

$\mathbf{QCMA} \neq \mathbf{QMA}$

My approach of synthesis classes is an extension of functional and decision classes.

The inaccuracy δ is a strict bottleneck.

Very nontrivial to know if synthesis is equivalent to decision.