Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy [1]

by MICHAEL J. BREMNER, RICHARD JOZSA AND DAN J. SHEPHERD

Report

FÜLÖP-BALOGH BEATRIX-EMŐKE
École Normale Supérieure de Lyon
January 4, 2017

Abstract

The main goal of the paper is to show that the classical efficient sampling of the IQP circuits' output probability distribution is equivalent with the collapse of the polynomial hierarchy to its third level Δ_3 i.e. it is highly improbable to be possible. Furthermore, it introduces the post-IQP class of languages (along with the IQP circuits augmented with post-selection) and proves that it is equal to the classical PP class. The paper also states that if the output of the IQP circuit is of $O(logn)$ size, then the efficient classical sampling of the distribution is possible.

1 Introduction

As a general point of view, quantum computing is expected to offer computational complexity speedup compared to classical algorithms, but there is no solid theoretical proof that any quantum algorithm can outperform the best classical algorithm for a task. This deficiency might be easily explained by the fact that the classical hardness problem is an extremely difficult issue to address. Because of this reason, the literature usually provides

conditional hardness proofs stating that if a widely believed to be unlikely problem is indeed hard, then the addressed problem is hard as well. This approach is used in the analyzed article as well, to prove the practical usefulness of the family of quantum circuits that is discussed.

On the other hand, quantum computing not only lacks theoretical proofs of its benefits but it's reported that there are difficulties in building a fault-tolerant and scalable quantum computer to practically prove the field's benefits.

The IQP circuits handled in this article aim to approach both of these issues. On one hand, the authors show that the class of problems that could be approached using these circuits are likely not efficiently computable by classical means. On the other hand, IQP circuits are physically restricted by only consisting of commuting gates which are, according to [2], relatively simple to implement using super- and semi-conductor qubit systems.

2 Definitions

In the following section, the definitions and the notations used in the article will be provided.

2.1 General Notions

Definition 2.1 (Computational Process)**.** *A computational process C computes the output of the computational task T, $T(w) = y_1 \cdots y_m$ of size m having the input $w = x_1 \cdots x_n$ of size n.*

Definition 2.2 (Bounded and unbounded error)**.** *C computes T with a bounded error if for all input w the following holds: $\exists \epsilon \in (0, \frac{1}{2})$ such that* $\text{prob}[C(w) = T(w)] \geq 1 - \epsilon$.
C computes T with a unbounded error if $\text{prob}[C(w) = T(w)] \geq \frac{1}{2}$.

Definition 2.3 (Language and decision task)**.** *If the size m of the output, $T(w)$ is 1, T is called a decision task and it is associated with the subset $\{w|T(w) = 1\}$ referred to as a language.*

Definition 2.4 (Circuit family)**.** *A circuit family is a set of circuits* $\{C_n\} = \{C_1, C_2, \cdots\}$*, where* C_n *is the circuit which computes the output for each input of size* n*.*

As seen in 2.4, circuit families are parameterised by the size of their input n, but for the purposes of this paper, it is more convenient to choose the inputs w as parameter of the circuit family $\{C_w\}$. Thus, the circuits will act on standard inputs, generally $0 \cdots 0$ for classical circuits and $|0\rangle \cdots |0\rangle$ for quantum circuits.

Definition 2.5 (Uniform family of circuits)**.** *A uniform family of circuits is a mapping* $w \to C_w$ *computable in* poly(n) *time. The description* C_w *includes the full layout of the gates used in the circuit, the input and the output lines and the description of every other register the circuit might need.*

Probability distributions $\{P_w\}$*, m-bit strings are associated to every uniform circuit family and are defined by the output of the computational process described by* C_w*.*

2.2 IQP Circuits

Definition 2.6 (IQP circuit)**.** *An IQP ("instantaneous quantum polynomial time" [3]) circuit is a commuting quantum circuit in which every commuting gate is diagonal in the X basis* $\{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$*, the input is* $w = |0\rangle\,|0\rangle \cdots |0\rangle$ *and the output is the measurement on the output lines.*

As it may be more convenient to work in the Z basis, one can note that it is enough to augment each line of the circuit at its beginning and at its end with a Hadamard (H) gate and work with diagonal gates in the Z basis in between. It is easily seen that this definition is equivalent with 2.6 since $HH = I$.

Definition 2.7 (Post-selected circuit)**.** *The post-selected circuit is a circuit that has, in addition to its output lines* O*, disjoint post-selection lines* P*. In this setting, the resulting output distribution will be* $\text{prob}[O = x | P = 00\ldots0]$*. Practically, result of the sampling of output of a post-selected circuit is equal to the output distribution measured only when the measurement on the post-selection lines yields* $00\ldots0$*.*

Definition 2.8 (post-IQP class)**.** *A language L is in the post-IQP class if and only if $\exists\{C_w\}$ uniform family of post-selected IPQ circuits with bounded error ϵ, a single output line O_w and post-selection lines P_w such that if $w \in L$ then* $\text{prob}[O_w = 1|P_w = 00\ldots0] \geq 1 - \epsilon$ *and if $w \notin L$ then* $\text{prob}[O_w = 0|P_w = 00\ldots0] \geq 1 - \epsilon$.

2.3 Classical Simulation of Quantum Circuits

In the article, the authors differentiates between two notions of classical simulation of quantum circuits, strong and weak. More than that, they define two types of weak simulations which they use in the proofs of the theorems presented in the paper.

Definition 2.9 (Strong simulation)**.** *A circuit family is strongly simulable if any output probability in P_w from the circuits' output probability distributions, and any of P_w's marginal probabilities can be computed with arbitrary precision in polynomial time.*

Definition 2.10 (Weak simulation)**.** *A circuit family is weakly simulable if the circuits' output probability distribution P_w can be classically sampled in polynomial time.*

Weak simulation can be further divided into subcategories based on the way its error bounds are defined as follows:

- A circuit family is *weakly simulable with multiplicative error $c \geq 1$* if there exist a family R_w of distributions on the same sample space as P_w that can be sampled in polynomial time and the following inequalities hold $\forall x, w$:

$$\frac{1}{c} prob[P_w = x] \leq prob[R_w = x] \leq c\, prob[P_w = x]. \tag{1}$$

- A circuit family is *weakly simulable within total variation distance ϵ* if the following inequality holds for the above defined R_w:

$$\sum_x |prob[P_w = x] - prob[R_w = x]| < \epsilon.$$

3 Results of the Paper

The results of the paper aim to show that IQP circuits, despite their restricted set of gates, are powerful tools in the sense that their results likely cannot be obtained by classical efficient computations.

The authors argue in the favor of this statement by providing proof that if the IQP circuits would be classically simulable, it would mean the collapse of the polynomial hierarchy to its third level which is highly unlikely.

The formal theorem can be stated as follows:

Theorem 3.1. *If the output probability distribution of a IQP circuit could be weakly classically simulated with a multiplicative error* $1 < c < \sqrt{2}$*, then the polynomial hierarchy* $PH = \Delta_3$*.*

In order to prove this theorem, the authors stated the following two theorems to be used in the final proof:

Theorem 3.2. *post-IQP = post-BQP = PP.*

Proof. The equality of the post-BQP and PP classes has been proven by Aaronson in [4], so in the following, the proof will focus on the post-IQP =post-BQP equality. The post-$IQP \subseteq$ *post-BQP* is trivial, so the proof focuses on the reverse inclusion.

It assumes an arbitrary uniform quantum circuit having the following universal set of gates H, Z, CZ and $P = e^{i\frac{\Pi}{8}Z}$ and it transforms it into a IQP circuit by replacing each Hadamard gate (since it is the only gate from the set that is not diagonal) with an equivalent subcircuit called Hadamard-gadget which is described by the following function:

$$|\psi\rangle_a |0\rangle_e \rightarrow H_a CZ_{ae} H_e |\psi\rangle_a |0\rangle_e .$$

After applying this transformation to every internal H gate, the resulting circuit will be a post-IQP circuit having as many additional post-selection lines as many H gates the initial circuit had (line a, on which the initial H gate was) and $H|\psi\rangle_a$ will be carried by newly added e lines. □

Theorem 3.3. *If the output probability distribution of the IQP circuits could be weakly classically simulated with a multiplicative error* $1 < c < \sqrt{2}$ *then post-BPP* $= PP$*.*

Proof. Let's consider $L \in$ *post-IQP* a language decided with bounded multiplicative error by the post-IQP circuit C_w and let $S_w(x) = \frac{prob[O_x=x \& P_w=00\cdots0]}{prob[P_w=00\cdots0]}$ be its output probability distribution. So the output distribution of C_w's simulation C'_w will be $S'_w(x) = \frac{prob[O'_x=x \& P'_w=00\cdots0]}{prob[P'_w=00\cdots0]}$.

By applying the inequality 1 from the definition of the multiplicative error to O_w and P_w one gets:

$$\frac{1}{c^2} S_w(x) \leq S'_w(x) \leq c^2 S_w(x).$$

From here, one can derive that C'_w can decide L with bounded multiplicative error if $c^2 < 1 + 2\delta$, where $\delta = \frac{1}{2} - \epsilon$, i.e. $c < \sqrt{2}$ suffices in order to guarantee that $L \in$ *post-BPP* (because post-IQP circuits are independent of the error ϵ meaning that ϵ can be arbitrarily chosen from the $(0, \frac{1}{2})$ interval).

Thus, by combining 3.2 with post-$BPP \subseteq$ *post-BQP*, the proof is complete. □

Now, that the above two theorems have been shown, the proof of the main theorem 3.1 of the paper is easily constructed as follows:

Proof. By applying Toda's theorem which states that $PH \subseteq P^{PP}$ and using the theorem 3.3, the proof is straightforward:

$$PH \subseteq P^{PP} = P^{post-BPP} \subseteq \Delta_3.$$

□

4 Discussion and Conclusions

As I have already mentioned it in the introduction, IQP circuits try to address the drawbacks of quantum computation both from theoretical and from practical points of view. Indeed, it is impressive that there exist a quantum circuit family that is fairly easily physically manufacturable and still most probably offers speedup compared to its classical counterparts (as it is proven in the article). This perspective makes the IQP circuits of great interest in the quantum complexity research field.

Since the publication of this paper, several other researchers approached this subject augmenting its theory by generalizing the theorems proposed by the authors to other, more general types of quantum circuits and complexity classes as in [5] or by further examining its limitations induced by the reduced set of allowed gates [5]. Moreover, already the authors mention it that the proofs provided in the article hold for any other circuit that is boosted to the PP class by post-selection. It is also easily seen that the introduction of the IQP class can induce new complexity classes, for example BPP^{IQP}.

As a conclusion, the IQP circuits are of great interest in quantum complexity theory because of their simplicity combined with their computational power. I also consider that their analysis could be useful when examining the properties of more complex but similar quantum circuits.

References

1. Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 467(2126):459–472, 2010.

2. P Aliferis, F Brito, D P DiVincenzo, J Preskill, M Steffen, and B M Terhal. Fault-tolerant computing with biased-noise superconducting qubits: a case study. *New Journal of Physics*, 11(1):013061, 2009.

3. Dan Shepherd and Michael J. Bremner. Temporally unstructured quantum computation. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 465(2105):1413–1439, 2009.

4. Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *CoRR*, abs/quant-ph/0412187, 2004.

5. Yasuhiro Takahashi, Seiichiro Tani, Takeshi Yamazaki, and Kazuyuki Tanaka. Commuting quantum circuits with few outputs are unlikely to be classically simulatable. *Quantum Information & Computation*, 16(3&4):251–270, 2016.