Some quantum algorithms for black-box algebraic structures

Guillermo Lugilde[1], Elías F. Combarro[2], Ignacio F. Rúa[1]
[1]Mathematics Department, University of Oviedo, Spain
[2]Computer Science Department, University of Oviedo, Spain

Introduction and preliminaries

- Some algorithms will be provided for black-box structures: for a structure M, its elements are represented as strings of n qubits; we assume efficient access to an oracle that implements the operations in M. This implies that $|M| \leq 2^n$. We focus on QMA^B and BQP^B.

  Definition 1 (BQP^B). *A language $L \subset \{0,1\}^*$ is in BQP^B if there exists a uniform family of quantum poly-generated circuits $\{Q_n\}$ with poly-width and efficient access to an oracle B, such that, $\forall x \in \{0,1\}^n$: if $x \in L$, Q_n accepts x in poly-time with probability $\geq 2/3$; if $x \notin L$, Q_n accepts x in poly-time with probability $< 1/3$.*

  Definition 2 (QMA^B). *A language $L \subset \{0,1\}^*$ is in QMA^B if there exists a uniform family of quantum poly-generated circuits $\{Q_n\}$ with poly-width and efficient access to an oracle B, such that, $\forall x \in \{0,1\}^n$: if $x \in L$, there exists $|\psi\rangle \in (\mathbb{C}^2)^{\otimes q(n)}$ so that Q_n accepts $(x, |\psi\rangle)$ in poly-time with probability $\geq 2/3$; if $x \notin L$, then for all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes q(n)}$, Q_n accepts $(x, |\psi\rangle)$ in poly-time with probability $< 1/3$.*

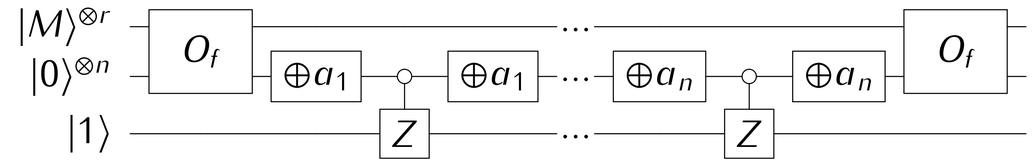
- Initial result: for any magma M, the state $|M\rangle := 1/\sqrt{|M|}\sum_{m\in M}|m\rangle$ can be created:
  1. *Prepare the state $|+\rangle^n$ in register **R** and $|0\rangle$ in register **S**.*
  2. *Check if register **R** belongs to M, storing the output in register **S**.*
  3. *Measure the register **S**.*

Ring problems in QMA^B or BQP^B

- Finding a generating set of a group G: generate from $|G\rangle$ a total of n^2 random elements.
- Finding additive generators for a subring $S = \langle s_0, \ldots, s_k\rangle$: let H_0 be the group generated by $\tilde{H}_0 := \{s_0, \ldots, s_k\}$ and set $l = 0$.
  1. *For all $s_i \in \tilde{H}_0$ and $h_j \in \tilde{H}_l$, check, one by one, if $s_i h_j \in H_l$ [1].*
  2. *If $s_i h_j \notin H_l$, define $\tilde{H}_{l+1} = \tilde{H}_l \cup \{s_i h_j\}$ and start again for $l = l + 1$.*
  3. *Continue until $s_i h_j \in H_l, \forall i, j$.*
- Hence, any result applicable to abelian subgroups is also applicable to subrings, such as creating the state $|S\rangle$ for any subring S [1].
- Combining the previous three results, we can deduce:
  - → Membership to a subring: given an element $r \in R$, we can efficiently determine if $r \in S$ [1].
  - → Equality of subrings: construct $|S\rangle$, $|T\rangle$ and perform a swap test.
  - → Elimination of redundant generators.
  - → Generators for the intersection of two subrings: the function $f(s) = |s + T\rangle$ hides the subgroup $(S \cap T)^+$ inside S^+. The hidden subgroup problem can be solved for abelian groups [2].
- Left-ideality of a subring I:
  1. Prepare $|R\rangle$, $|I\rangle$ and $|0\rangle$ in registers **R**, **I** and **M**, respectively.
  2. Multiply $|R\rangle$ and $|I\rangle$ on register **M** and measure **M**.
  3. Declare that I is an ideal only if the result belongs to I.
- 'Non-division ring' in QMA^B: let **S** be the certificate register.
  1. Measure **S** and reject if the result is not in R or is equal to 0.
  2. In **S**, we are left with an $r \in R$. Accept if and only if $rR \neq R$.

Magmas: existence problems

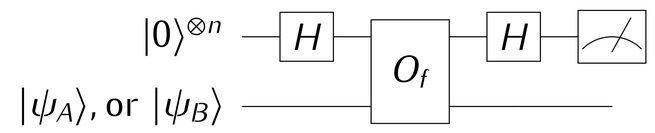
- Given $f : M^r \longrightarrow \{0,1\}^n$, we want to decide if there exists an element in a fixed $A \subseteq \{0,1\}^n$ such that $A \cap f(M^r) \neq \emptyset$.
- This includes the problems of deciding if an element is invertible, if its annihilator is different from 0, the existence of divisors of 0 or idempotent elements, if an element behaves like a 0 for the product, or if M is commutative, associative, distributive, etc.
- Approach based on Quantum Abstract Detecting Systems [3]:



- Exact if $A \cap f(M^r) \neq \emptyset$ or if $|\{\vec{x} \in M^r \text{ such that } f(\vec{x}) \in A\}| = |f(M^r)|/2$. Overall behavior equivalent to the classical random pooling method: if we repeat it R times, the probability of error is $\frac{1}{2R+1}$.
- However, if we repeat our quantum method $R-1$ times and then apply the classical method just once, the probability of error is $\frac{R}{(2R-1)(2R+1)}$.

Deutsch-Jozsa generalization

- We are given $f : \{0,1\}^n \longrightarrow \{0,1\}^m$ and two disjoint subsets of $\{0,1\}^m$, $A = \{a_1, a_2, \ldots, a_{d_A}\}$ and $B = \{b_1, b_2, \ldots, b_{d_B}\}$. We assume that $f(\{0,1\}^n)$ is either contained in one of both sets, or balanced between both, and must decide which is the case.



- For $A = \{a_1\}, B = \{b_1, b_2\}$, $|\psi_A\rangle$ and $|\psi_B\rangle$ are, respectively:

$$\frac{1}{\sqrt{2^{1+2}}}(|0\rangle - |a_1\rangle + |b_1\rangle + |b_2\rangle - |a_1 \oplus b_1\rangle - |a_1 \oplus b_2\rangle + |b_1 \oplus b_2\rangle - |a_1 \oplus b_1 \oplus b_2\rangle);$$

$$\frac{1}{\sqrt{2^{1+2}}}(|0\rangle + |a_1\rangle - |b_1\rangle - |b_2\rangle - |a_1 \oplus b_1\rangle - |a_1 \oplus b_2\rangle + |b_1 \oplus b_2\rangle + |a_1 \oplus b_1 \oplus b_2\rangle)$$

Definition 3. *We say A and B are $\oplus$-incoherent if an equation of the form $\bigoplus_{p=1}^{k} a_{i_p} = \bigoplus_{q=1}^{l} b_{j_q}$ holds, being both k and l odd.*

Theorem 1. *The $\oplus$-coherence of A and B can be deterministically decided in $O(m(d_A + d_B)^2)$ operations. At least one of $|\psi_A\rangle$ or $|\psi_B\rangle$, is deterministically constructible $\Leftrightarrow$ A and B are $\oplus$-coherent.*

Conclusions and future works

- Every quantum procedure that works for abelian subgroups, works for any subring as well.
- Connection between magmas and the QADS paradigm.
- New generalization of the Deutsch-Jozsa algorithm, where the function is either balanced between two sets or constant on one.
- Other approaches to the construction of $|\psi_A\rangle$ or $|\psi_B\rangle$ might gain efficiency. Starting an algorithm with a random distribution of amplitude signs in $|M\rangle$ could mitigate the arbitrariness of a magma operation.

References

[1] John Watrous, "Quantum algorithms for solvable groups," in *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, 2001, pp. 60–67.
[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, 2011.
[3] Elías F Combarro, José Ranilla, and Ignacio Fernández Rúa, "Quantum abstract detecting systems," *Quantum Information Processing*, vol. 19, no. 8, pp. 258, 2020.

Acknowledgements

This work was partially supported by MCIN/AEI/10.13039/501100011033 under grant PID2021-123461NB-C22 and by MCIU/AEI/10.13039/501100011033/FEDER, EU under grant PID2023-146520OB-C22; by Gobierno del Principado de Asturias under Grant FC-GRUPIN-IDI/2021/000047 and AYUD/2021/50994, by the Spanish National Institute of Cybersecurity (INCIBE) under MRR-MAETD-24-INCIBE-001, and by the Quantum Spain project funded by the Ministry of Economic Affairs and Digital Transformation of the Spanish Government and the European Union through the Recovery, Transformation and Resilience Plan - NextGenerationEU. The first and third authors, members of the Universidad de Oviedo research team GACYC, have also been supported by the Spanish Network of Mathematics in the Information Society (MatSI).