On finding substructures of finite algebras with quantum algorithms

J.M. Hernández Cáceres, University of Oviedo, Department of Mathematics, C/ Leopoldo Calvo Sotelo 18, Spain, 985103187 jmhernandez@uniovi.es
I.F.Rúa University of Oviedo, Department of Mathematics, C/ Leopoldo Calvo Sotelo 18, Spain, 985103344, rua@uniovi.es
Elías F. Combarro University of Oviedo, Department of Computer Science, C/ Jesús Arias de Velasco, Oviedo, Spain, 985103177, efernandezca@uniovi.es

Let A be a non-associative and non-commutative $\mathbb{F}_p$-algebra with $\mathbb{F}_p$ a finite field of prime cardinality p, with a fixed basis $\beta = \{e_1, \ldots, e_n\}$. There exists a unique set of constants $\{M_{ijk}\}_{i,j,k=1}^{n} \subseteq K$ such that $e_i \cdot e_j = \sum_{k=1}^{n} M_{ijk} e_k$, for all $i, j \in \{1, \ldots, n\}$. That set is known as the multiplication table of the algebra. Consider the additive group $G = (A, +)$, i.e., the elements of the algebra with the addition operation. G is a finite abelian group, moreover $G \cong (\mathbb{Z}/p\mathbb{Z})^n$. The right, middle, and left nuclei, the nucleus and the center of A are sets which can be written in terms of the $\mathbb{F}_p$-basis β and the multiplication table, and they provide information about the algebra. For instance, when A is a finite semifield, i.e., a finite division ring, these sets are related to properties of the corresponding coordinates projective planes [1]. Finding those sets (which are substructures of A) can be stated in terms of the Hidden Subgroup Problem (HSP), and it is clearly important in the context of the classification of finite semifields, see for instance [3]. In fact, finding each substructure can be transformed into an instance of the HSP, which in general can be stated as: Given the multiplication table of a finite dimensional $\mathbb{F}_p$-algebra A, and a function f which is constant on a subgroup $H = \langle s_1, s_2, \ldots, s_l \rangle$ of G and is distinct on cosets of H, find $s_1, s_2, \ldots, s_l$. In order to solve it, we explicitly and efficiently construct quantum circuits that, from the multiplication table of A, implement hiding functions f that can be used to determine these sets using only a polynomial number of quantum gates, in fact of order $O(n^5 r^3)$, with $O(nr)$ queries to the oracle, where $r = \lceil \log_2(p) \rceil$ (i.e., with an asymptotically linear number of evaluations of the function f). Additionally we prove that, in general, this can not be achieved classically with a polynomial number of accesses to the function f if given only access to a black box oracle to evaluate f, without additional information on the algebra.

References

[1] A. A. Albert, Finite division algebras and finite planes, *Proc. Symp. Appl. Math* 10 (1960) 53–70.

[2] A. A. Albert, Generalized twisted fields, *Pac. J. of Math.* 11 (1961) 1-8.

[3] J.M. Hernández Cáceres, I.F.Rúa, An approach to the Classification of Finite Semifields by Quantum Computing, Non-Associative Algebras and Related Topics:NAART II, Coimbra, Portugal, July 18-22,2022. (to appear)