

Research Project Proposal: Quantum Computing and hardness of computation of combinatorial functions

MARCO VENERE, MARCO.VENERE@MAIL.POLIMI.IT

1. INTRODUCTION TO THE PROBLEM

This research project proposal builds at the intersection between EDA (Electronic Design Automation) and Quantum Computing.

The former is a research field dedicated to the development of algorithms and software tools for the automation of tasks related to the design of digital electronic circuits. In particular, the *frontend* of such instruments is the logic design flow which, given a high-level description of the circuit, produces a *netlist*, which is a document defining all the instances of the used blocks and their interconnections. Each of these blocks represents a specific Boolean function. The EDA *backend* is instead the physical design flow which, given a netlist, defines the final schematic of the circuits, i.e., establishing which library components to use, how to place them in the chip's core area (Placement) and how to interconnect them (Routing). The available combinatorial components of the libraries implement elementary Boolean functions, therefore each logic block of the netlist must be mapped to one or more library components (Technology Mapping), in such a way as to obtain an equivalent final circuit.

The latter is instead a model of computation whose operations can harness the phenomena of quantum mechanics, such as superposition, interference, and entanglement. Quantum algorithms have often proven to offer a noticeable speedup w.r.t. their analogue classical implementation, and are becoming an essential tool to tackle significant problems, whose complexity class prevents classical supercomputers from achieving correct solutions in a reasonable time.

In particular, the research topic here proposed relates to the implementation of a solver for the Boolean Matching Problem (BMP), based on quantum computing. The Boolean Matching Problem is a Technology Mapping problem regarding the comparison between a given Boolean function and those present in specific libraries. Equivalence under negation and permutation of inputs and negation of the output (NPN-equivalence) is considered [5].

The solution to such a problem is of paramount importance in EDA, since implementation costs for a digital circuit are noticeably reduced if the reuse of preexisting components is possible. Yet, the computational complexity of BMP solvers, which belong to the NP-hard class, is $O(2^{n+1}n!)$ in the size of the input for NPN-equivalence. Theoretically speaking, Quantum Computing has been proven to achieve at most a square-root speedup for NP-hard problems, which still results to be a desirable outcome, considering the current limits of classical solvers.

2. MAIN RELATED WORKS

The current State-of-the-Art for Boolean Matching Solvers considers three possible implementations, which exploit specific properties of the given Boolean Functions, in order to reduce the size of the search space in which to find NPN-equivalent functions:

1. Reduction to the canonical form: Boolean Functions can be associated with their canonical form, and it has been proven that functions belonging to the same equivalence class are associated with the same canonical

form. Therefore, computing such a form for the target Boolean Function and comparing it against the canonical forms of the functions belonging to the given libraries is theoretically proven to solve this task. Several ways have been implemented to output a correct canonical form. State-of-the-Art (SoA) solutions currently consider the Binary Decision Diagram (BDD) as a valid representation of the function, in order to improve performance [5] [4].

2. Signature Pruning: such a method performs a search in the space of the NPN-equivalent Boolean Functions after reducing it by pruning: indeed, there exist specific signatures, i.e., alternative representations for functions, which can be proven to be invariant for NPN-transformations. Therefore, pruning can be done on the search tree, based on comparison of signatures [3] [9] [8].
3. Spectral-based methods: they exploit the property that NPN-equivalence of Boolean Functions translates into equivalence under coefficient permutation in the sequence domain of the Walsh Transform. Therefore, an exploration of the permutation tree of the Walsh coefficients is performed [6].

Even though such algorithms manage to reduce the number of possible comparisons in order to find equivalence between the input function and the logic components of the libraries, an exponential complexity in the size of the input is still required, and only for a reduced amount of input bits computation is possible.

Finally, for what concerns quantum acceleration of EDA algorithms, a noticeable work regards the implementation of a quantum circuit addressing the Max-Cut Problem [7]. Yet, no relevant materials have been found directly related to the quantum acceleration of the Boolean Matching Problem.

3. RESEARCH PLAN

The goal of the research is to start from the classical implementation of solvers for the Boolean Matching Problem and find a corresponding quantum circuit version. Such a task is not trivial, especially for the usage of quantum superposition to manage input permutations. It may be required to find alternative approaches, that could better exploit quantum principles in order to achieve a valuable speedup.

The nature of the research is halfway between theory and application. Indeed, theoretical principles should be investigated in order to produce a functional design, and their application will produce a quantum circuit, which will be described as a proposed solver for the BMP. For what concerns the verification of the final product, functional testing will be performed. Obviously, because of the limits of current quantum computers, and because of the high amount of qubits required to implement BMP solvers, it will probably not be possible to test the algorithm on an input size effectively corresponding to current logic gates. This notwithstanding, it will be still possible to obtain a working circuit that will prove the correctness of the work.

The research may be split into the following stages:

1. completion of the study of the State of the Art: during this phase, further reports will be read, in order to understand, more in depth, the several possible strategies to tackle BMP. For each possible approach, key points to exploit for quantum acceleration will be investigated, and compared against SoA quantum acceleration techniques. As a final product of this phase, the more interesting path to follow will be recognized.
2. design of the solution: the main objective of this phase is to identify, for the specific algorithm to accelerate with a quantum computer, the main steps to implement as quantum circuits. A considerable aspect is related to the exploitation of quantum parallelism: in order to increase speedup w.r.t. classical implementations, it may be necessary to find alternative ways to solve the BMP, also by taking advantage of SoA cutting-edge techniques related to quantum superposition. The output of this task will be the complete design of a quantum circuit to subsequently implement.

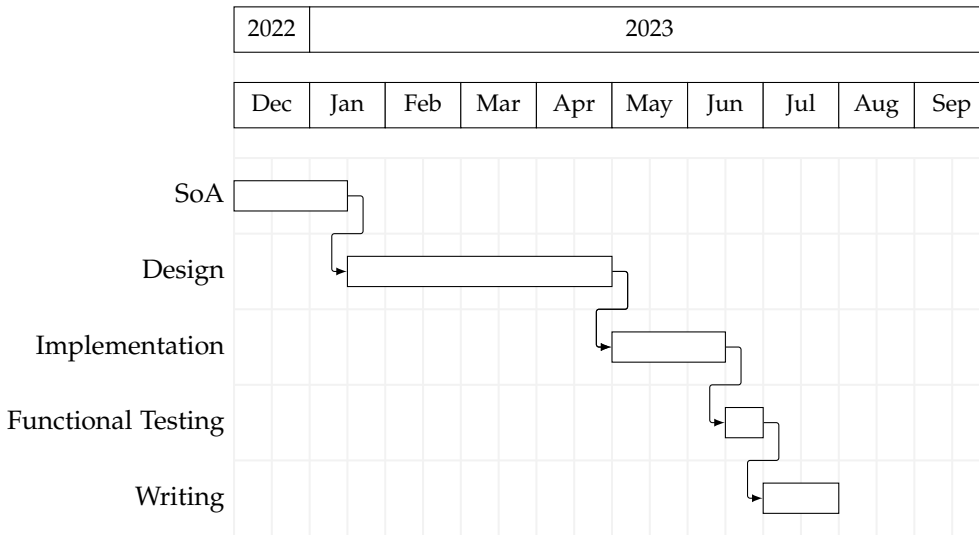


Figure 1: Gantt diagram of the tasks of the research project proposal

3. implementation: in this phase, the previously identified quantum circuit will be implemented by coding. Software suites for quantum development such as Qiskit [1] and QX Simulator [2] will be used to obtain a final code executable on both quantum simulators or real QPUs, according to quantum hardware availability.
4. functional testing: in this stage, the output of the implementation task will be used as a starting point to verify the correct functioning of the implemented quantum circuit. Because of the limitations of current QPUs, it may be not possible to properly test the circuit with real-world use cases, such as Boolean Matching comparing logic gates with tens of input bits. This notwithstanding, functional testing can verify the correctness of the developed circuit. The output of this task will consist of Key Performance Indicators (KPI) displaying the advantages implied by the quantum acceleration.
5. writing: in this phase, the proceeding of the previous tasks, their outputs, and their implications will be annotated, in order to elaborate the final thesis document and consider possibilities for submission of the work to journals or conferences.

For what concerns the duration of each task, the following Gantt diagram will describe the foreseen duration of each stage.

As it can be seen in Section 3, the SoA is foreseen to end at the beginning of 2023. The most intense task should be the Design, since it requires great mental efforts to better understand how to exploit quantum principles to obtain an effective acceleration. The subsequent stages of implementation and functional testing should require a reduced amount of time, once the design quantum circuit is available. The Writing stage will finally require a short duration. Please notice that, as in common waterfall development models, if a specific stage will highlight doubts or drawbacks related to the output of previous tasks, it may be required to turn back to previous milestones and review the work.

In order to evaluate the output of the research, it will be necessary to compare the performance of the newly produced quantum circuit and the classical implementation of solvers for the Boolean Matching Problem. Since we are considering quantum circuits, it may be useful to verify the number of quantum gates necessary to develop the circuit. It is important to pay attention to the fact that limits in the current quantum hardware will not allow to compare classical and quantum algorithms on a real-world problem scenario. Therefore, to obtain a clear speedup, it will be necessary to evaluate them on problems whose size is compatible with the number of available quantum bits.

REFERENCES

- [1] Qiskit. <https://qiskit.org/>. Accessed: 2022-11-29.
- [2] The qx simulator. <http://quantum-studio.net/>. Accessed: 2022-11-29.
- [3] ABDOLLAHI, A. Signature based boolean matching in the presence of don't cares. In *2008 45th ACM/IEEE Design Automation Conference (2008)*, pp. 642–647.
- [4] AGOSTA, G., BRUSCHI, F., PELOSI, G., AND SCIUTO, D. A transform-parametric approach to boolean matching. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 28, 6 (2009), 805–817.
- [5] BURCH, AND LONG. Efficient boolean function matching. In *1992 IEEE/ACM International Conference on Computer-Aided Design (1992)*, pp. 408–411.
- [6] MOORE, J., FAZEL, K., THORNTON, M. A., AND MILLER, D. M. Boolean function matching using walsh spectral decision diagrams. In *2006 IEEE Dallas/CAS Workshop on Design, Applications, Integration and Software (2006)*, pp. 127–130.
- [7] VERGHESE, A., BYRON, D., AMANN, A., AND POPOVICI, E. Max-cut problem implementation and analysis on a quantum computer. In *2022 33rd Irish Signals and Systems Conference (ISSC) (2022)*, IEEE, pp. 1–6.
- [8] ZHANG, J., YANG, G., HUNG, W., WU, J., AND ZHU, Y. A new pairwise npn boolean matching algorithm based on structural difference signature. *Symmetry* 11 (12 2018), 27.
- [9] ZHANG, J., YANG, G., HUNG, W. N., ZHANG, Y., AND WU, J. An efficient npn boolean matching algorithm based on structural signature and shannon expansion. *Cluster Computing* 22, 3 (2019), 7491–7506.