Reg. No: 2021/41/N/ST6/03907; Principal Investigator: mgr Piotr Kawałek

MODULAR CIRCUITS - ALGORITHMS AND LOWER BOUNDS

Popular Science Summary

Circuits are among the basic objects of computer science. Their structure consists of gates between which connections, called wires, are drawn. This structure represents in fact some computation. A number of wires enters the circuit from outside, through which raw data will be sent. This data then flows through the circuit, and the interconnected gates are like neurons processing the information and sending it on. Finally, the processed information gets out through the output gates.

Depending on which types of operations are allowed in building of such a network we have to deal with different computational capabilities of the circuit. Sometimes, it may turn out that some calculations cannot be expressed with a certain type of gates, because they have not enough *expressive power*. A slightly better, but still unfavorable scenario is when the computation we are interested in requires a circuit of very large size, which basically means that the solution to the problem is *inefficient*. The most important problems in complexity theory, including solving the famous millennium problem P vs NP, require a thorough understanding of what the capabilities and limitations of various circuits are.

Thus, **the goal of the project** will be to study the expressive power of circuits depending on the set of admissible gates. We will seek for *lower bounds*, which imply either the impossibility of expressing certain functions using circuits of a given type, or the necessity of using a large size for this purpose. *Algorithms* will also be created to investigate important properties of such networks.

The methods used include the application of advanced algebraic techniques such as commutator theory or tame congruence theory. They are well-suited for the study of the so-called modular circuits which are of great importance in complexity theory.

As a result, through experimental studies and mathematical proofs, a complete or partial classification of modular structures will be created, depending on their expressive power. The main measure used will usually be the size in which such circuits compute some particular function.