Reg. No: 2015/18/E/ST1/00200; Principal Investigator: dr Adam Sawicki

A memory of a classical computer stores bits, where each bit can be either 1 or 0 corresponding to the logical truth or false. On the very basic level, a computer program is a sequence of operations, encoded by Boolean aka switching functions, performed on bits for the completion of a specific task. Boolean functions are realized by logical gates - electronic devices which perform logical operations. A set of gates which allows implementation of any logical function is called a universal set of gates. Universal sets of gates are given for example by {AND, OR, NOT} which realize conjunction, disjunction and negation respectively or {NAND} which is the negation of conjunction. There are only finitely many Boolean function operating on n bits.

One can think of a quantum computer as a machine which operates on qubits - quantum bits. A qubit is the simplest quantum mechanics system with only two basis states which one can think of as states of truth and false. Qubit can be realized physically as polarization of light (vertical or horizontal) or spin (up or down). Quantum mechanics says that the state of a qubit can be any superposition of the state of truth with probability p1 and the state of false with a probability p2, where p1+p2=1. Therefore the set of quantum states for a single qubit is much bigger than for the classical bit. This is actually why quantum computers can perform various tasks much faster than classical ones. All one qubit quantum gates, that is, operations which send one superposition of truth and false states into another superposition of truth and false states, preserving the sum of probabilities, have a nice mathematical structure: they form the two-dimensional unitary group SU(2). This group contains uncountable number of elements. Producing uncountable number of gates in a laboratory is unrealistic. Typically we have access only to a finite set of gate types which compositions give other gates. This way we can create only countably many SU(2) gates. They can, however, still be dense in SU(2) - that is approximate any gate we want with an arbitrary precision. For example the famous set consisting of Hadamard gate H and the so-called phase gate T have this property, and therefore we call it a universal set of gates for one qubit. Of course quantum computer operates on many qubits and one need to add additional gates to form a set which is universal for n-qubit quantum computing. This is the simplest theoretical setting to start speaking about quantum computing.

This project focus on various aspects of both one- and many- qudit universality problems - an inevitable part of any sort of quantum computation. The aim is to lay the foundations for the uniform understanding and description of the universality problems and question stemming from them. A qudit is a d-level quantum system and for d>2 can be physically implemented using optical lattices that couple modes of light. For this implementation, gates that operate on qudit states are called d-mode beamsplitters and they form d-dimensional unitary SU(d) (or orthogonal SO(d) in real case) group. Recently, there has been some attempts to understand which optical gates can generate dense sets of d-mode gates. It is know, for example, that any 2-mode beamsplitter, when we let it to operate on all possible pairs of d modes of light, densely generate SU(d) (SO(d)). There are also similar result for real 3-mode beamsplitters. Our aim is to develop new methods and techniques that would allow better understanding of qudit universality problems. We want to find out what are conditions for a d-mode beamsplitter to be universal. Characterization of universal sets for many qdits quantum computation is our anther goal. Finally we wish to understand which optical gates can be exactly realized by beamsplitters and what is the optimal choice of a beamsplitter which lead to the most efficient realization of a given quantum operation. In order to achieve these goals we plan to use already developed methods and techniques from control theory, geometry and algebraic number theory but a new approaches might be needed too. Above all the distinguishing feature of the proposal is the highly ambitious goal, unusual combination of methods, techniques and people involved.