CENTRE DE RECHERCHES MATHÉMATIQUES

Tenseurs : information quantique, complexité et combinatoires quantiques

Tensors: Quantum Information, Complexity and Combinatorics

Robert Robere
(McGill University)

Duality Theorems for Amortized Circuit Complexity

Some of the central questions in complexity theory address the amortized complexity of computation (often under the name of "direct sum problems"). While these questions appear in many contexts, they are all variants of the following:

Is the best way of performing a task T many times in parallel to compute T independently each time, or, can we achieve an economy of scale and compute all copies of T more efficiently on average?

In this talk, we discuss some results studying the amortized circuit complexity of computing boolean functions in various circuit models. The amortized circuit complexity of a boolean function f is defined to be the limit, as m tends to infinity, of the circuit complexity of computing f on the same input m times, divided by m. We prove a new duality theorem for amortized circuit complexity in any circuit model, showing that the amortized circuit complexity of computing f is equal to the best lower bound achieved by any "formal complexity measure" applied to f. This new duality theorem is inspired by, and closely related to, Strassen's duality theorem for semirings, which has been fruitfully used to characterize the matrix multiplication exponent, the Shannon Capacity of graphs, as well as other important parameters in combinatorics and complexity. We discuss how our new duality theorem can be used to give alternative proofs of upper bounds on amortized circuit complexity, and also the close relationship between amortized circuit complexity and catalytic algorithms, in which an algorithm is provided with an extra input of advice bits that it is free to use, as long as it outputs a new copy of the extra advice on termination.

This is based on joint work with Jeroen Zuiddam.