Efficient quantum pseudorandomness with simple graph states

Rawad Mezher [1, 2], Joe Ghalbouni [1], Joseph Dgheim [1], and Damian Markham [2]

[1] Laboratoire de Physique Appliquée, Faculty of Sciences 2, Lebanese University, 90656 Fanar, Lebanon.

[2] LIP6-CNRS, Université Pierre et Marie Curie, Sorbonne Universités, 4 place Jussieu, 75252 Paris Cedex 05, France.

Measurement based quantum computation (MBQC) allows for universal quantum computing by measuring individual qubits prepared in entangled multipartite states, known as graph states. Unless corrected for, the randomness of the measurements leads to the generation of ensembles of random unitaries, where each random unitary is identified with a string of possible measurement results. We show that repeating an MB scheme an efficient number of times, on a simple graph state, with measurements at fixed angles and no feed-forward corrections, produces a random unitary ensemble that is an ε-approximate t-design on n-qubits. Unlike previous constructions, the graph is regular and is also a universal resource for measurement based quantum computing, closely related to the brickwork state.

Our construction is very similar to the brickwork state, which is a universal resource for MBQC - it is basically the brickwork state but with regular holes. In MBQC these holes would simply teleport the inputs through, so that the proofs of universality easily extend to our graph - that is, concatenations of our graph form also a universal resource for MBQC. In addition to being pleasing from a practical point of view, this opens the door to applications of techniques for delegation of ensemble generation, as done for computation, and indeed the possibility to hide whether one is sampling unitaries or performing some deterministic computation.

Keywords: Measurement based quantum computation, graph states, random unitary ensemble, ε-approximate t-design, brickwork state.