Invariants of groups and universality of quantum gate sets

Gábor Ivanyos, MTA SZTAKI

Universality of a set of n-qubit quantum gates (that is, unitary transformations of $\mathbf{C}^{2^n}$) is a notion which reflects usefulness of the collection in building circuits for quantum computing. A set of n-qubit quantum gates is called universal if there exists $N_0 \geq n$ such that for every $N \geq N_0$ every N-qubit unitary operation can be approximated with arbitrary precision by a circuit built of permutations of the N qubits and of gates from the collection. In other words, the permutations of the N qubits together with the gates should generate a dense subgroup of the underlying projective unitary group. We remark that, using the Kitaev–Solovay theorem (see e.g. [4] and also [6, 7] for an implementation), if a gate set is universal then approximations of arbitrary unitary operations can be built efficiently.

One can show [2] that if an n-qubit gate set is universal then the smallest N_0 with the above property is at most $2^8 n$. The proof combines Jeandel's density criterion [3] based on Lie theory with a recent result of Guralnick and Tiep [1] on invariants of finite linear groups and with Lazard's bound [5] on regularity of the Hilbert function of zero dimensional ideals.

In this talk we give an exposition of the proof by outlining an analogous result for universality in the closely related model of reversible computing. (We are indebted to E. Jeandel for drawing our attention to this analogy). We also discuss some related open questions as well as certain experimental results obtained using GAP and Macaulay 2.

References

[1] R. M. Guralnick, P. H. Tiep, Decompositions of small tensor powers and Larsen's conjecture, *Represent. Theory 9 (2005), 138–208.*

[2] G. Ivanyos, Deciding universality of quantum gates, *J. Algebra 310 (2007), 49–56.*

[3] E. Jeandel, Universality in quantum computation, *in: Proc. 31th ICALP, Springer LNCS 3142: 793–804 2004.*

[4] A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi (2002), *Classical and quantum computation, AMS Graduate Studies in Mathematics, Vol. 47, 2002.*

[5] D. Lazard, Résolution des systèmes d'équations algébriques, *Theoret. Comput. Sci. 15 (1981), no. 1, 77–110.*

[6] A. B. Nagy, On an implementation of the Solovay-Kitaev algorithm, *Proc. RWCA 2006 Basel, 201–208.*

[7] A. B. Nagy, Cs. Schneider, SKA: An implementation of the Solovay-Kitaev Algorithm, Version 0.1. *http://www.sztaki.hu/∼schneider/Research/SKA.*