Arithmetic golden gates

organized by
Vadym Kliuchnikov, Ori Parzanchevski, and Peter Selinger

Workshop Summary

This workshop was devoted to understanding new developments in unitary approximation, which is a topic at the interface between quantum computing and number theory. To this end, about half of the workshop participants were quantum computing researchers, and the other half number theorists.

For the first few days, the main focus was to bring the two communities together. Following the AIM format, we started each day with one or two tutorials whose purpose was either to teach the relevant basics of quantum computing to number theorists or vice versa. The tutorials were deliberately addressed not to the half of the audience who were specialists but to the other half. Luckily all of the participants were on board with this, and slowed down every speaker by asking a lot of basic questions. In the beginning it was especially important for each community to learn the other's terminology and way of thinking.

Peter Selinger and Vadym Kliuchnikov gave an overview of approximation problems in quantum computing. Ori Parzanchevski gave an introduction to Bruhat-Tits buildings and how the unitary group acts on them. John Voigt gave an introduction to algorithmic algebraic number theory. Sebastian Schoennenbeck explained a new method for doing multi-qubit exact synthesis over the Clifford+T and similar gate sets using Bruhat-Tits buildings. Kristin Lauter gave a tutorial on cryptographic applications of path-finding on expander graphs. Cristina Ballantine gave an introduction to Ramanujan graphs.

In addition to prepared tutorials, on some mornings we also had "flash tutorials", which were spontaneous talks explaining a concept of interest to the audience. To facilitate this, we made a list of possible topics and how many minutes each topic would require, then voted on which topics we would like to hear about each day. There were flash tutorials on quantum error correction by Robert Raussendorf, on quantum algorithms by Sean Hallgren, on generator-finding for S-arithmetic groups by Aurel Page, on how to prove approximation exponents by Alex Gamburd, on repeat-until-success methods by Vadym Kliuchnikov, on dynamic systems of continued fractions by Katherine Stange, and on mixing rates in ergodic theory by Amos Nevo.

In the afternoons, we followed the AIM workshop style by working on problems in groups. Here are the problems that were worked on:

- **Approximation for non-diagonal operators.** The best known approximation algorithms achieve optimal approximation exponents if the operator to be approximated is diagonal. For example, in the case of Clifford+T approximation, these algorithms achieve T-counts between $3\log(1/\epsilon)$ in the typical case and $4\log(1/\epsilon)$ in the worst case. However, non-diagonal operators must be approximated by Euler decomposition, yielding an approximation exponent that is 3 times worse than the information-theoretic lower bound. A group of participants worked on the problem of finding better approximation algorithms in the non-diagonal case.

- **Super strong approximation over number fields** The optimal covering rate of Golden Gate sets in one qubit is obtained from "super strong approximation" results for quadratic forms in four variables. A group of participants received a crash course on this subject from Naser Talebizadeh Sardari, and then worked on the question of generalizing these results to multi-qubit gate sets.
- **Characterizing the large holes in approximation.** When approximating elements of $PSU(2)$ by members of a finitely generated subgroup, one often finds large holes: elements that are significantly harder to approximate than average. For example, in the case of Clifford+T approximation, it heuristically appears that the operators $e^{-i\theta Z}$ can be approximated with T-count $3\log_2(1/\epsilon) + K$ for $\epsilon \to \infty$, unless $\tan(\theta) \in \mathbf{Q}(\sqrt{2})$, in which case a T-count of $4\log_2(1/\epsilon) + K$ is required. A group of participants worked on the problem of characterizing exactly where these holes occur.
- **Which super golden gates are feasible for error correction.** One reason the Clifford+T gate set is preferred in quantum computing is that there is a known method for performing such gates fault-tolerantly on noisy quantum hardware using quantum error correction. Also, as a set of "golden" gates, the Clifford+T gates have good number-theoretic approximation algorithms. The purpose of this working group was to investigate which other sets of golden gates, if any, could be suitable for error correction.
- **The hyperbolic case.** Gates which arise from S-arithmetic lattices act on a non-archimedean space (the Bruhat-Tits building). Similarly, arithmetic lattices in a unitary group with a non-compact completion act on an archimedean symmetric space (the hyperbolic plane in the case of U(2)). A group of participants studied the application of this action to navigation and covering exponent in such gates.
- **Generators that guarantee hardness.** In the context of cryptographic hash functions, it would be desirable to have sets of generators for which the problem of finding short paths along expander graphs (in the p-adic case) or finding short approximations up to ϵ (in the Archimedean case) is provably hard. Such gates would in a sense be the opposite of golden. A group worked on the problem of finding such provably hard gate sets.
- **Multi-qubit exact synthesis.** In the case of 2×2 Clifford+T operators, each operator has a unique normal form which is moreover of minimal T-count. Also, there is an efficient algorithm for computing the normal form of an operator. In the case of operators of size $n \times n$, there are algorithms for computing a circuit from an operator, but there is no known normal form for such circuits, and there is no efficient method for minimizing such circuits. However, as shown in Sebastian Schoennenbeck's tutorial, it is possible to design exact synthesis algorithms using Bruhat-Tits buildings. The group worked on finding better exact synthesis algorithms in the multi-qubit case.
- **Relationship to continued fraction type algorithms.** Pythagorean triples are integer points on the surface $a^2 + b^2 - c^2 = 0$, and are acted on by a finitely generated group of integer matrices giving the set of pythagorean triples the structure of a tree. As shown by Romik, the algorithm for finding the shortest path to a given

triple can also be applied to arbitrary real solutions of $a^2 + b^2 - c^2 = 0$, giving good approximations of points in projective space, in a way that is essentially isomorphic to continued fractions. As shown by Chaubey, Fuchs, Hines, and Stange, the algorithm can be generalized to n-tuples for $n \geq 4$. The group investigated whether these ideas can yield a better Clifford+T approximate synthesis algorithm in the non-diagonal case.

Participants often joined different working groups on different days, although some groups stayed together for two or three days. In many of the groups, significant time was spent understanding and better defining the problems. While many groups made some progress, the problems were typically hard and were not solved within the allotted time. Several of the groups are planning to continue collaborating on their respective topics.