What is quantum good for? Unifications of quantum algorithms – Syllabus

Contrary to what we hear in the media, it is very unlikely that quantum computing unlocks a *universal* computation speedup: it seems there are only specific problems that it solves faster, sometimes dramatically so. Can we identify those problems, and understand why quantum algorithms perform so well on them? This is of course a question of prime importance, both foundational – for understanding the true power of quantum computing, beyond mere examples –, and practical – for instance for making sure that our post-quantum cryptography techniques will indeed remain quantum-secure. In this course, we will discover two strikingly different approaches to this question. The first, *Quantum Singular Value Transform* (QSVT), finds that quantum algorithms are good at polynomial transformations of matrices; the second, *Hidden Subgroup Problems* (HSP), finds that they perform well at spotting group-theoretic regularities. This will also be an occasion to discover some lesser-known quantum algorithms, such as the eigenvalue threshold, HHL, and discrete logarithms. The course will end on open research questions in these highly dynamic research domains.

Prerequisites: linear algebra, basic quantum algorithms (DJ, Grover, Shor). Having followed courses on group theory and representation theory is welcome, but these will in any case be covered at length in the lectures.

List of sessions

- Lecture 1 (3h) – Quantum signal processing, amplitude amplification, block encodings, and an application to Grover.
- Lecture 2 (3h) – Quantum Eigenvalue Transforms and the QSVT, applications to the eigenvalue threshold problem and to HHL
- TD 3 (3h) – Polynomial approximation for the QSVT with Chebyshev polynomials
- Lecture 4 (3h) – Groups and representations
- Lecture 5 (3h) – The regular representation and the Quantum Fourier Transform; HSPs and how they generalise Shor and the discrete logarithm
- Lecture 6 (3h) – Solving the abelian HSP
- TD 7 – Variations on the abelian HSP
- Lecture 8 – The HSP frontier: results and conjectures on the non-abelian case