Quantum Algorithms with Exponential Speedups

Leonard Schulman
Caltech

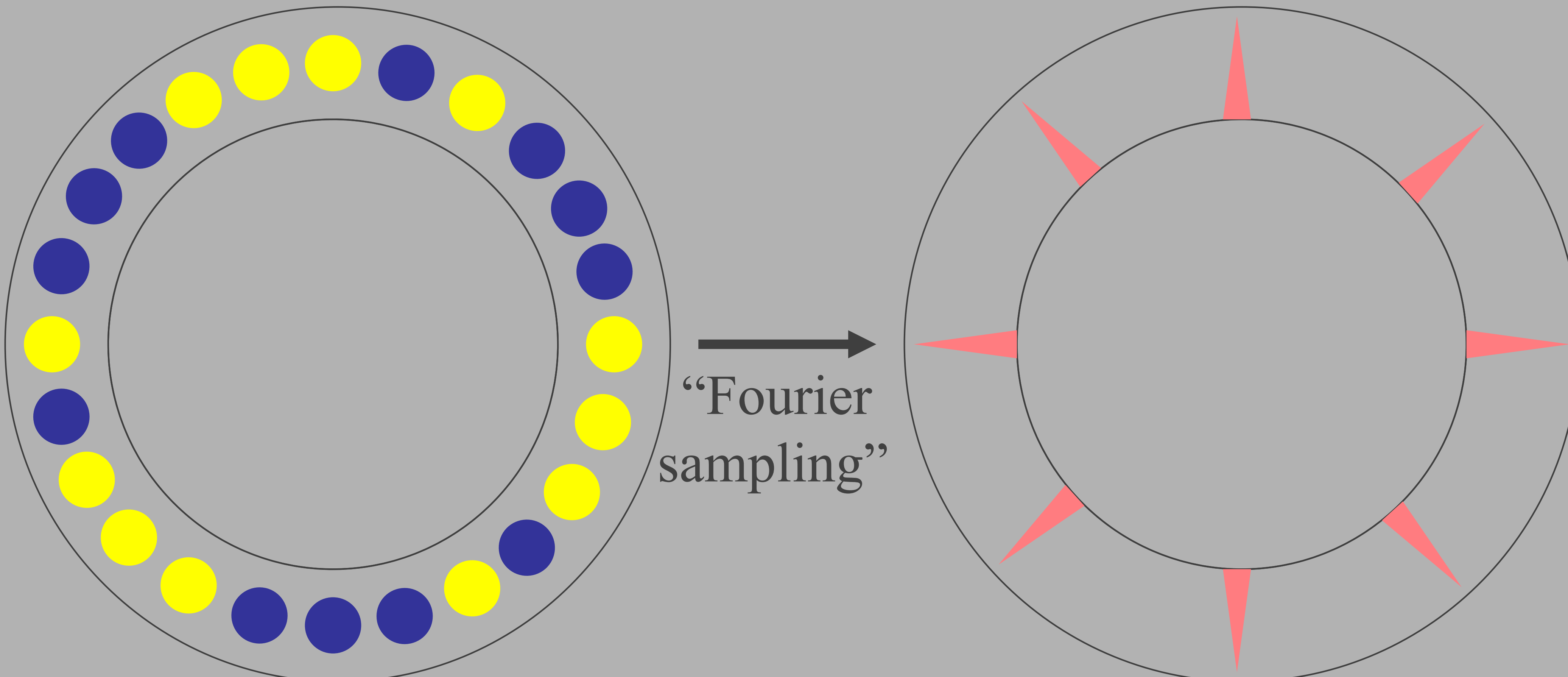
NSF workshop, Vienna VA, April 2009

Quantum computation

If you can maintain your computer in a *very* quiet environment, its state evolves under wave mechanics

Sometimes, we can design a computation so that the interference patterns reveal structure of a problem we want to solve

Example: hidden rotational symmetry



In: unif. superposition on H-periodic coloring of the group G=ℤ/N (for N ~ exp(n)). Here N=24, H=3.

Out: unif.-norms superposition on the subgroup of Ĝ perp. to the period (here ℤ/8). Sample, repeat, post-process to get H.

Design goal in quantum algorithms: create *huge* constructive interference

What kind of problems allow such constructive interference?

Need to create resonance

Bennett, Bernstein, Brassard, Vazirani ’94: Quantum search among 2^n items requires time $\geq 2^{n/2}$.

I.e. (relative to an oracle), *no subexponential-time algorithm for NP*.

Quantum computers, like classical ones, can quickly solve only structured problems.

Exponential speedup quantum algorithms

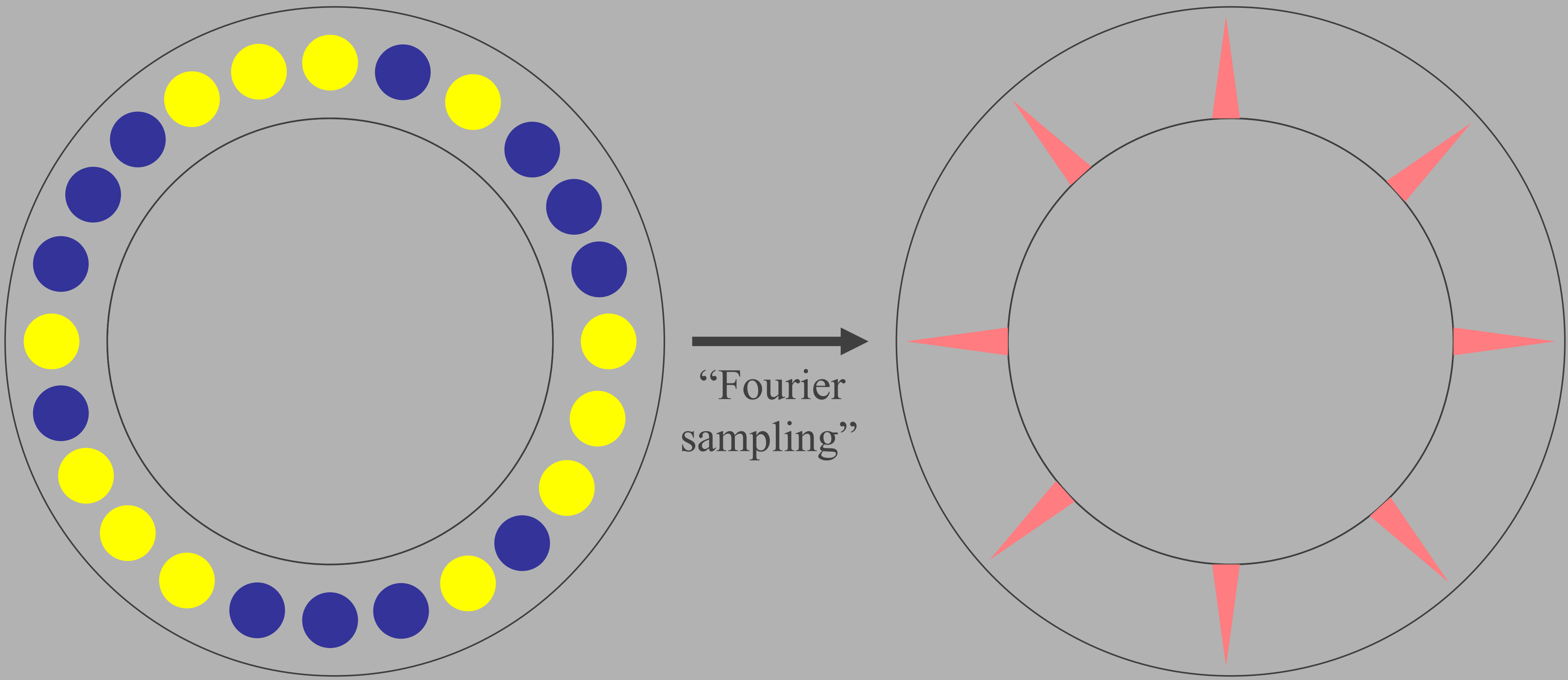
ABELIAN HIDDEN SUBGROUP PROBLEM
(+ closely related)

further abelian gps; cracks elliptic curve cryptosystem

discrete log, factoring; cracks RSA cryptosystem

superpolynomial speedup; not an HSP

cont. example: hidden rotational symmetry



For binary functions, Simon/Shor insufficient;
use also Hales Hallgren ’00.

Exponential speedup quantum algorithms

ABELIAN HIDDEN SUBGROUP PROBLEM
(+ closely related)

Hallgren '02: fin. gen. gps: Pell's eqn

van Dam Hallgren Ip '02: shifted quad. char.

Brassard Høyer '97, Mosca, Ekert '99

Boneh Lipton '95: Abelian HSP

Kitaev '95: Abelian Stabilizer

Simon '94; Shor '94: Abelian HSP

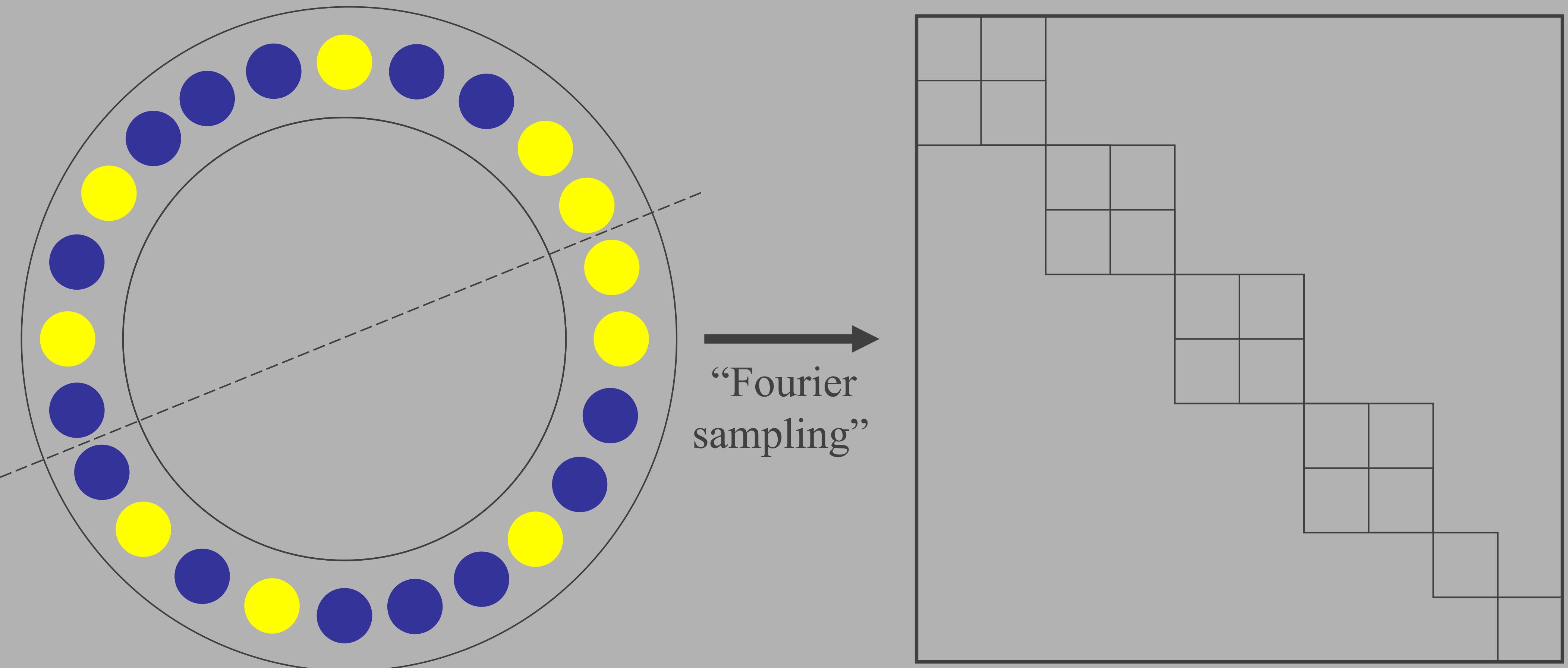
Bernstein Vazirani '93: Fourier sampling

further abelian gps; cracks elliptic curve cryptosystem

discrete log, factoring; cracks RSA cryptosystem

superpolynomial speedup; not an HSP

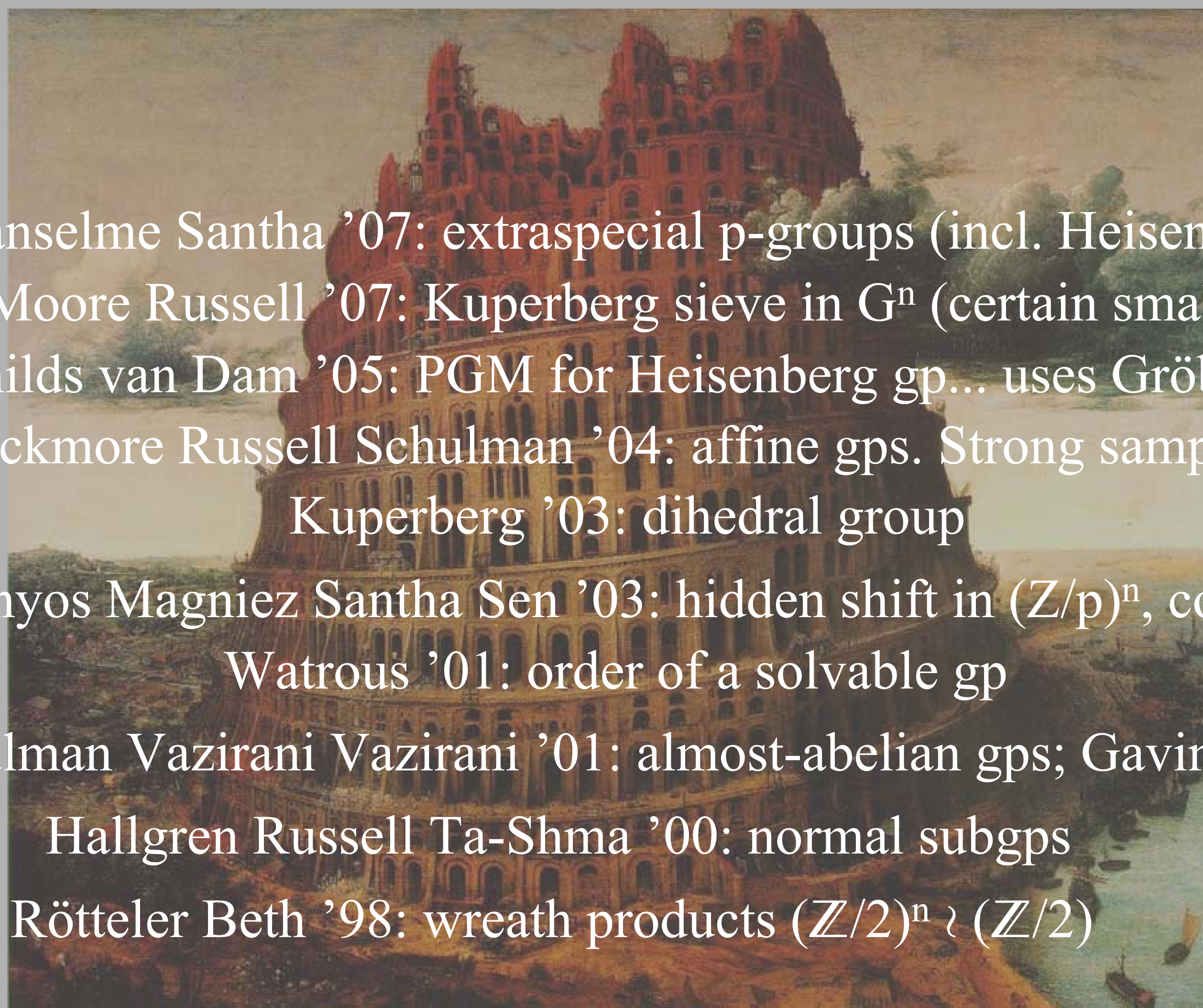
What about reflection symmetry?
Dihedral group: nonabelian



Instead of the dual group Ĝ, now use the nonabelian Fourier transform (decomposition of the group algebra into irreducible subspaces).
Ettinger Høyer ‘00: polynomially-many samples suffice. But no algorithm.

Exponential speedup quantum algorithms: beyond abelian HSP

NONABELIAN HIDDEN SUBGROUP PROBLEM
(+ closely related)



Ivanyos Sanselme Santha ’07: extraspecial p-groups (incl. Heisenberg)

Alagic Moore Russell ’07: Kuperberg sieve in G^n (certain small G)

Bacon Childs van Dam ’05: PGM for Heisenberg gp... uses Gröbner

Moore Rockmore Russell Schulman ’04: affine gps. Strong sampling

Kuperberg ’03: dihedral group

Friedl Ivanyos Magniez Santha Sen ’03: hidden shift in $(Z/p)^n$, const. p

Watrous ’01: order of a solvable gp

Grigni Schulman Vazirani Vazirani ’01: almost-abelian gps; Gavinsky ‘04

Hallgren Russell Ta-Shma ’00: normal subgps

Rötteler Beth ’98: wreath products $(\mathbb{Z}/2)^n \wr (\mathbb{Z}/2)$

Applications of the nonabelian HSP and related problems

1. Symmetric group:
   Graph Automorphism $\leq_{Cl}$ Symmetric Group HSP
2. Symmetric Group HSP $\leq_{Cl}$ Code Equivalence (McEliece '78,

   Petrank Roth '97)
3. Dihedral group: Regev '02:
   $n^{1.5}$-uSVP $\leq_{Qu}$ Dihedral HSP (single-register coset sampling)

   $\leq_{Qu}$ Avg-case Subset Sum

   Regev '04: for some constant c,
   n^{c}-uSVP $\leq_{Cl}$ Dihedral HSP (same sampling)

   uSVP is an important problem: Ajtai '96, Ajtai Dwork '96,

   Regev '04: public-key cryptosystem based on *worst-case*

   hardness of $n^{1.5}$-uSVP. Note, $n^{0.5}$-uSVP is NP-hard.

Limits to quantum algorithms for the HSP in S_n

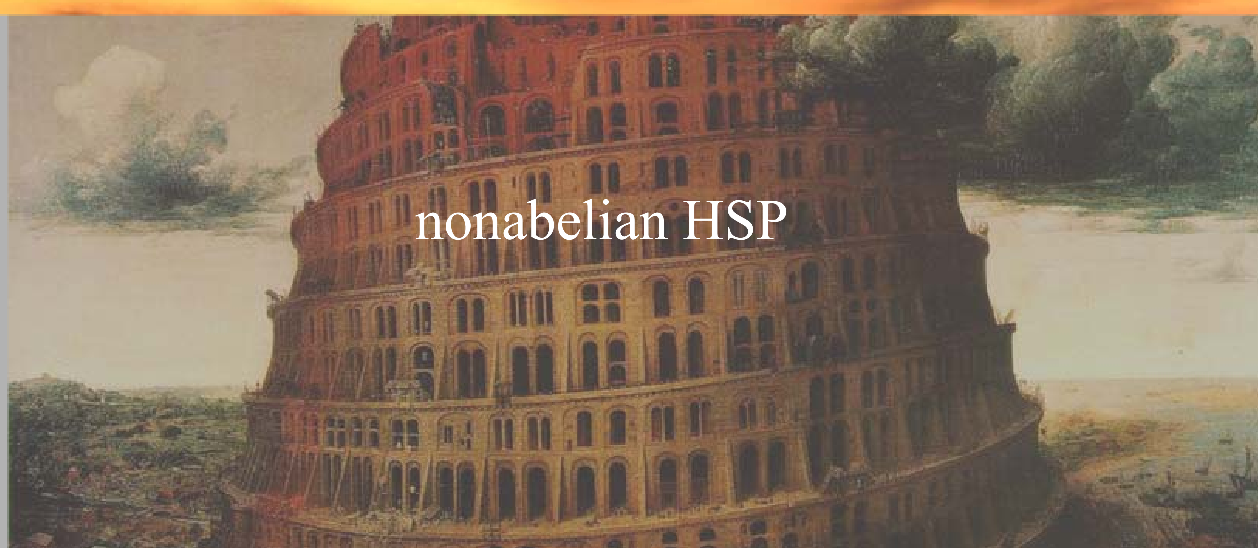
Hallgren Russell Ta-Shma ’00: weak sampling fails

Grigni Schulman Vazirani Vazirani ’01: random bases fail

Moore Russell Schulman ’05: single-register algs fail

Hallgren Moore Roetteler Russell Sen ’06: o(log n)-registers algs fail

Moore Russell Sniady ‘07: Kuperberg’s sieve fails



Obstacle to Kuperberg sieve for S_n: new representation theory inequality

Key is following inequality (Rattan Sniady '06): $\forall$ D>0 $\exists$ constant c such such that:

Let λ be an irrep of S_n whose Young Tableau has at most $Dn^{1/2}$ rows and and columns. Let $t(\pi)$ be the number of transpositions required to to generate permutation π.

Then

$|\chi_\lambda(\pi)/d_\lambda| \leq ((c \max\{1,t(\pi)^2/n\})/n^{1/2})^{t(\pi)}$.

(Here d_λ is the dimension, and χ_λ is the character, of irrep λ).

In Moore Russell Sniady '07 this ensures an upper bound on the variation variation distance between the statistics of the output of the algorithm algorithm when the hidden subgroup is trivial, and when it is nontrivial. nontrivial.

Other exponential speedup quantum algorithms

Childs Cleve Deotto Farhi Gutmann Spielman ’03: “quantum walk”

(but the most compelling walk alg is for polynomial improvement, Farhi Goldstone Gutmann ’07, Ambainis Childs Reichardt Spalek Zhang ‘07)

Kedlaya ’06: count pts on a genus g curve over GF(q) in time poly(g, log q)

Childs Schulman Vazirani ’07: nonlinear “hidden structure” problems (level sets of polynomials, sphere radius) in abelian groups

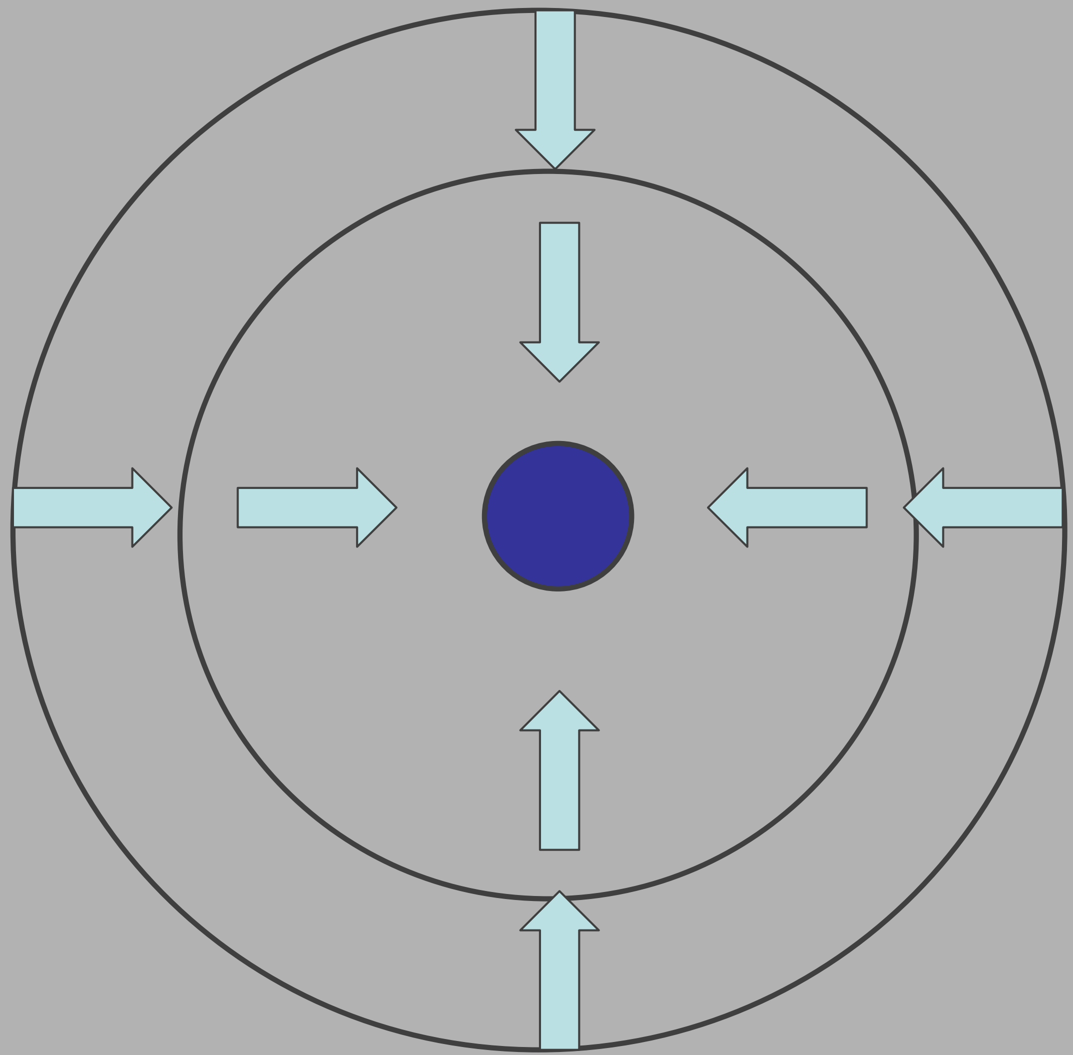
Freedman Kitaev Wang ‘02
Aharonov Jones Landau ’06: additively approximate Jones polynomial at roots of 1.

Aharonov Arad Eban Landau ‘07: additively approximate Tutte poly of planar graph

"Optically" driven algorithm design: find the centers of (a flat of) spheres

The plane here represents the finite geometry $(GF/q)^d$. Start w. wave on the "external" (meaningless for GF(q)) sphere

Can show: Prob. of landing at center is at least 1/polylog(q)



We find exponential speedup quantum algorithms in group algebras, not just any Hilbert space

Some potential targets

New algorithms for HSP in S_n. How to use highly entangled measurements?

"Post-quantum crypto:" try to rely on problems we really think aren't in BQP, e.g., HSP in S_n. New key exchange protocol to replace Diffie Hellman?

Improve dihedral alg; crack cryptosystems based on SVP.

Improve Gröbner basis, ideal membership computation. (Note: ideal membership is EXPSPACE-complete: Mayr Meyer '82)
{linear algebra, univariate gcd} $\leq$ Gröbner $\leq$ Knuth-Bendix

Many physical quantum systems are only "slightly quantum": e.g., low-entanglement 1D or 2D systems. (Motivates MPS, PEPS methods.) Simulate such quantum systems with quantum resources proportional only to this measure.

Further reading

Childs, van Dam ‘08:
Quantum algorithms for algebraic problems
arXiv:0812.0380

Image credits

South Island, New Zealand: Brewbooks 2006 (Flickr; Creative Commons license)

Great Wave off Kanagawa: Katsushika Hokusai, c. 1831

Lunar laser ranging: McDonald Observatory

Tower of Babel: Pieter Bruegel the Elder, c. 1563 (WebMuseum)

Lenticular/lee wave clouds: Roberta Johnson. Courtesy of Windows to the Universe, http://www.windows.ucar.edu

Kelvin-Helmholtz clouds: Terry Robinson/UCAR. Courtesy of Windows to the Universe, http://www.windows.ucar.edu

The Ancient Library of Alexandria: Wikimedia Commons

Electron cloud of a Silicon atom in GaA: M.C.M van der Wielen, A.J.A van Roij, and H. van Kempen, University of Nijmegen, http://qt.tn.tudelft.nl/publi/1998/stt/stt.html