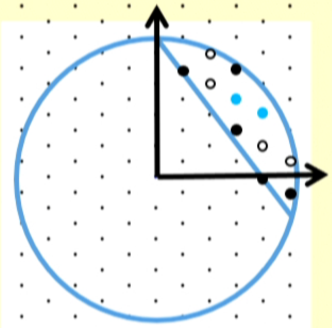
Title: Quantum gates

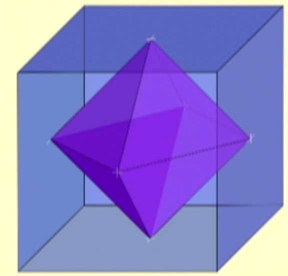
Date: Jun 08, 2016 02:00 PM

URL: http://pirsa.org/16060049

Abstract: <p>Fault-tolerant quantum computers will compute by applying
 a sequence of elementary unitary operations, or gates, to an
 error-protected subspace. While algorithms are typically expressed
 over arbitrary local gates, there is unfortunately no known theory
 that can correct errors for a continuous set of quantum gates.
 However, theory does support the fault-tolerant construction of
 various finite gate sets, which in some cases generate circuits that
 can approximate arbitrary gates to any desired precision. In this
 talk, I will present a framework for approximating arbitrary qubit
 unitaries over a very general but natural class of gate sets derived
 from the theory of integral quaternions over number fields, where the
 complexity of a unitary is algebraically encoded in the length of a
 corresponding quaternion. Then I will explore the role played by
 higher-dimensional generalizations of the Pauli gates in various
 physical and mathematical settings, from classifying bulk-boundary
 correspondences of abelian fractional quantum Hall states to
 generating optimal symmetric quantum measurements with surprising
 connections to Hilbert's 12th problem on explicit class field theory
 for real quadratic number fields.</p>



Quantum gates



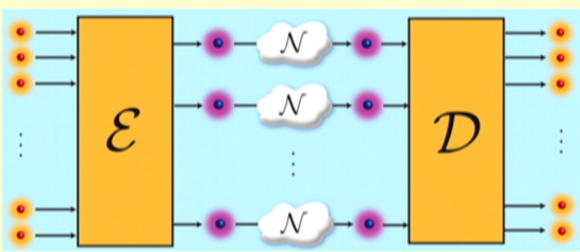
Codes, compiling and arithmetic

Jon Yard

Microsoft Research Station Q

Quantum Architectures and Computation Group (QuArC)

$$\begin{pmatrix} 1 & 0 \\ 0 & \zeta_8 \end{pmatrix}$$



Perimeter Institute
Waterloo, ON
June 8, 2016

$$\frac{1}{\sqrt{5}}\begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix}$$

Quantum mechanics

$$|\langle a|U|\psi\rangle|^2 = \Pr(\mathrm{a}|\psi)$$

3. Measurement

$$|1\rangle = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \cdots, |d\rangle = \begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}$$

$$\langle\psi| = (\psi_1^* \quad \cdots \quad \psi_d^*)$$

Probabilistic result

2. Unitary evolution

$$U^\dagger = U^{-1}$$

$$U \in \mathrm{U}(\mathbb{C}^d)$$

$\langle \quad | \quad \rangle \;=\; \langle \quad , \quad \rangle$

Bra-Ket = Bracket

1. Preparation

$$|\psi\rangle = \begin{pmatrix}\psi_1\\\vdots\\\psi_d\end{pmatrix} \in \mathbb{C}^d$$

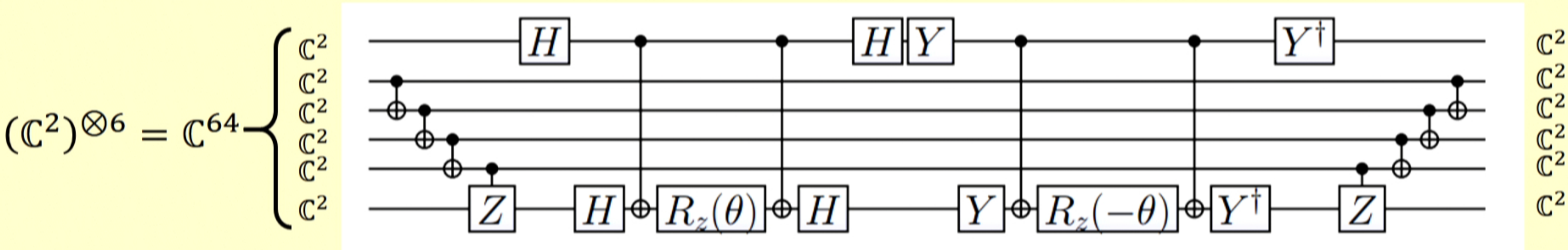
$$|\psi_1|^2 + \cdots + |\psi_d|^2 = 1$$

Often $d = 2$ or 2^n

Probabilities depend on $\mathbb{P}(\mathbb{C}^d)$

Quantum circuits

Sequence of 1-qubit $U_2(\mathbb{C})$ or 2-qubits $U_4(\mathbb{C})$ unitary gates producing an element of $U_{2^n}(\mathbb{C})$.



$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

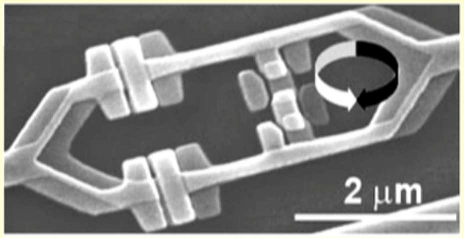
$$Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

$$R_z(\theta) = \begin{pmatrix} e^{i\pi\theta/2} & 0 \\ 0 & e^{-i\pi\theta/2} \end{pmatrix}$$

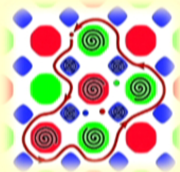
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

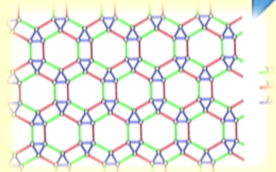
Fault-tolerant quantum gates



Physical error < 10^{-2}

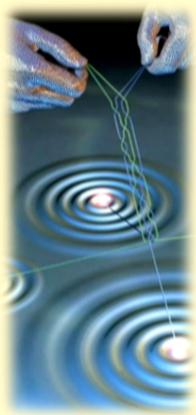


quantum code



$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

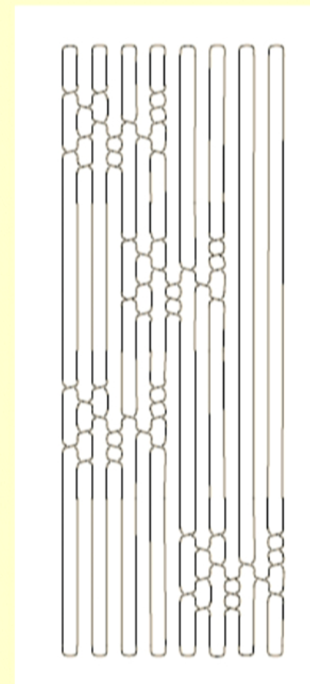
Fault tolerant



braiding

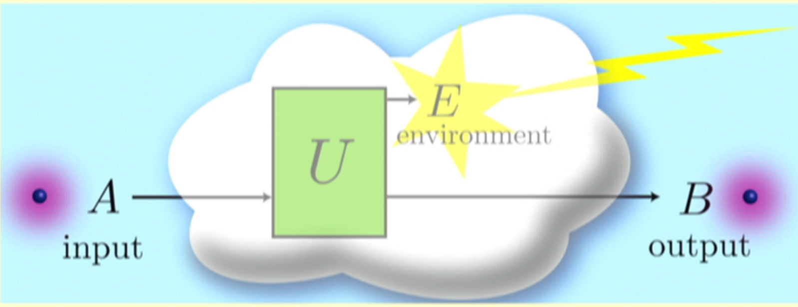
$$= \begin{pmatrix} -e^{i\pi/5} & 0 \\ 0 & e^{i3\pi/5} \end{pmatrix}$$

Nonabelian representation of braid group B_n defined by $\mathrm{SU}(2)_k$ Chern-Simons TQFT



Quantum capacity

Noisy quantum channel



reversible interaction with inaccessible environment

$U: A \to B \otimes E$

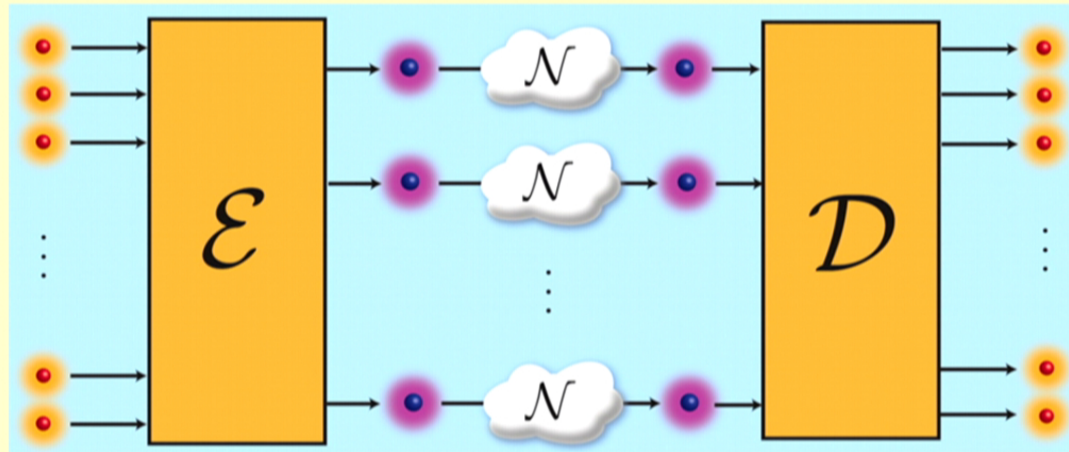
$\mathcal{N}(\rho) = \mathrm{Tr}_E U^\dagger \rho U$

Density matrix $\mathrm{Tr}\,\rho = 1, \rho \geq 0$

$$\rho = \sum_x p(x) |\psi_x\rangle\langle\psi_x| = \mathrm{Tr}_R |\Psi\rangle\langle\Psi|$$

Purification $|\Psi\rangle \in A \otimes R$

Encoder Decoder



encoded data qubits noisy physical qubits

Quantum capacity $Q(\mathcal{N}) = \max \frac{\#\text{encoded qubits}}{\#\text{physical qubits}}$

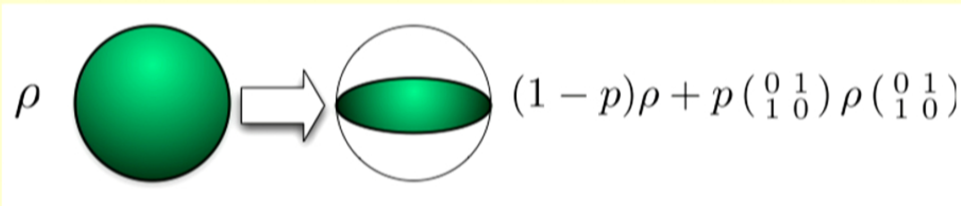
Ultimate limit to our ability to correct quantum errors

Contrary to classical case, **no general formula** known

Some examples

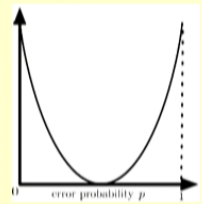
Quantum capacity $Q(\mathcal{N}) = \max \frac{\#\text{encoded qubits}}{\#\text{physical qubits}}$

Qubit flip channel



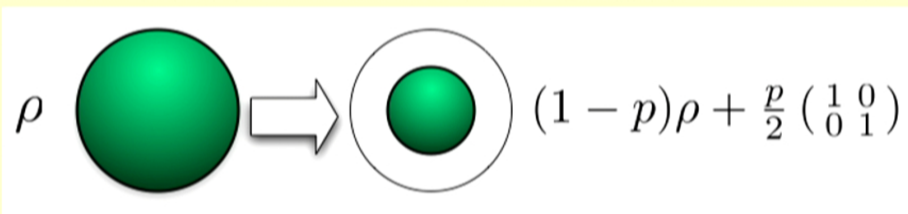
$$Q = 1 - p\log(p) - (1-p)\log(1-p)$$

$=$



Qubit depolarizing channel

(popular model for studying fault-tolerant gates)



$Q = ???$

In particular, we don't even know when $Q = 0$.
All we know is that the threshold p^* such that $Q = 0$ for every $p \geq p^*$ satisfies
$.2552 \leq p^* \leq 1/3$.

Superactivation of quantum capacity

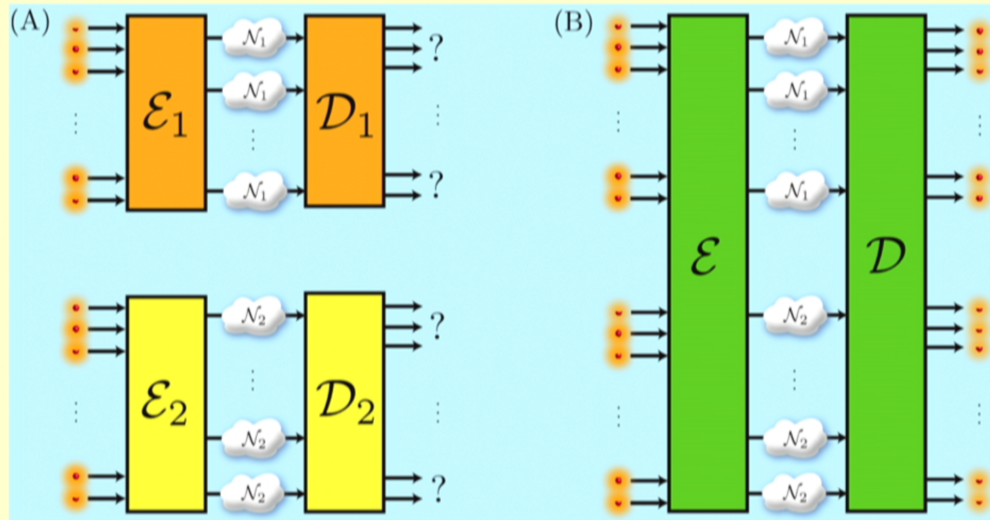
26 SEPTEMBER 2008 VOL 321 SCIENCE www.sciencemag.org

REPORTS

Quantum Communication with Zero-Capacity Channels

Graeme Smith[1*] and Jon Yard[2]

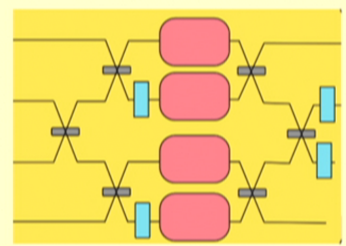
$$0 + 0 > 0$$



nature photonics

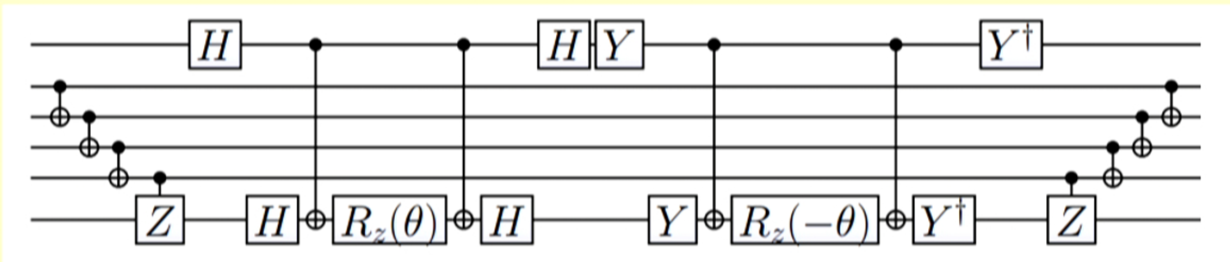
Quantum communication with Gaussian channels of zero quantum capacity

Graeme Smith[1*], John A. Smolin[1] and Jon Yard[2]

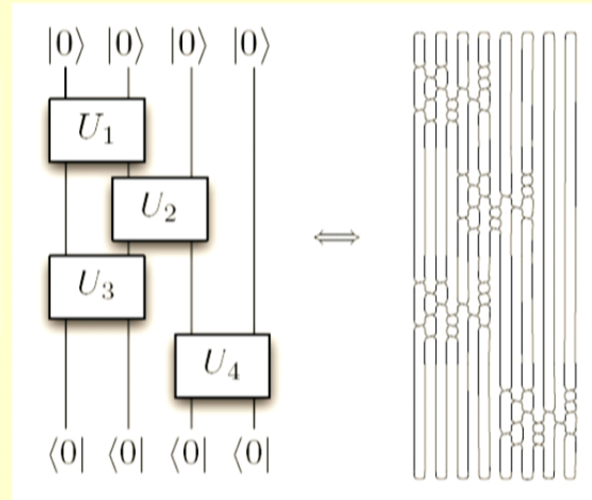


$\in U(L^2(\mathbb{R}^4))$ via metaplectic representation of $Sp_8(\mathbb{R})$

Error-correcting unitaries



Wecker et al. PRA **92**, 062318



In practice, e.g. quantum chemistry algorithms claim to be useful if errors $\varepsilon = 10^{-6} - 10^{-16}$

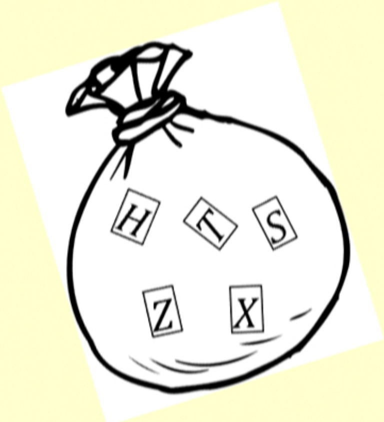
Open question: how to correct errors for a continuous family of gates???

Fault-tolerant gates

Fortunately, we do know how to error-correct certain discrete gate sets

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$



$$T = \begin{pmatrix} 1 & 0 \\ 0 & \zeta_8 \end{pmatrix} \quad \sqrt{T} = \begin{pmatrix} 1 & 0 \\ 0 & \zeta_{16} \end{pmatrix} \quad T^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & \zeta_{32} \end{pmatrix} \quad \zeta_n = e^{2\pi i/n}$$

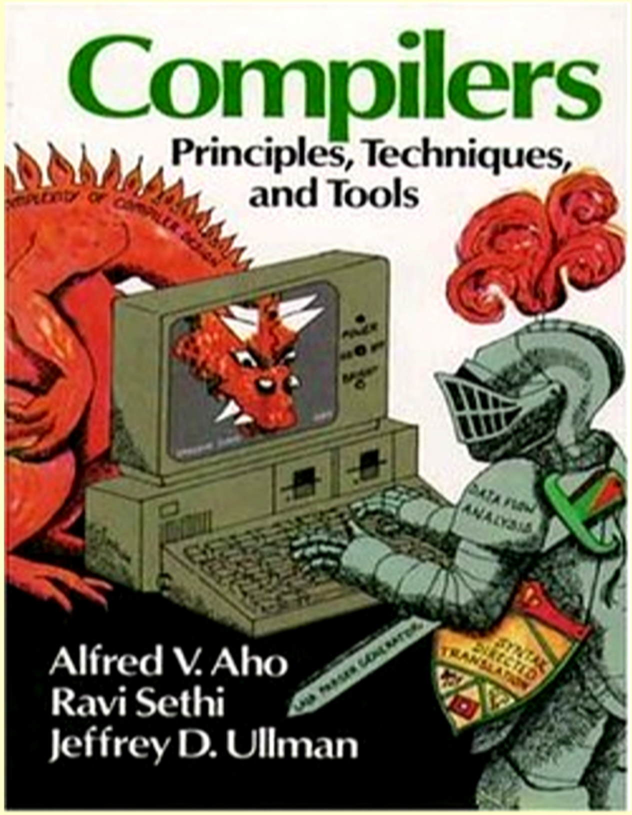
$$V_x = \frac{1}{\sqrt{5}} \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix} \; V_y = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix} \; V_z = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} -\zeta_{10} & 0 \\ 0 & \zeta_{10}^3 \end{pmatrix} \quad \sigma_2 = \frac{1}{\phi} \begin{pmatrix} \zeta_{10}^4 & -\zeta_5\sqrt{\phi} \\ -\zeta_5\sqrt{\phi} & -1 \end{pmatrix} \quad \phi = \frac{1+\sqrt{5}}{2} \qquad X_d = \begin{pmatrix} 0 & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}, \; Z_d = \begin{pmatrix} 1 & & & \\ & \zeta_d & & \\ & & \ddots & \\ & & & \zeta_d^{d-1} \end{pmatrix}$$

Fibonacci anyons

Get arbitrary gates by *compiling*

- **This talk:** Poly-time algorithm for ε-approximating a given unitary $U \in \mathrm{SU}(2)$ with an $O\big(\log(1/\varepsilon)\big)$-length circuit over a very general class of gate sets
- **Optimal** up to constant factors
- Generalizes most existing known algorithms for specific gate sets
- Underlying mathematics has roots in computer science – constructing explicit expanding graphs
- May lead to new quantum algorithms or new tools for designing fault-tolerant protocols
- Science of quantum gate sets



The general compiling problem:

Fault-tolerant quantum computer

$$\mathcal{G} = \{U_1, \dots, U_M\} \subset \mathrm{SU}(2)$$

$$\mathrm{cost}(U_{m_i}) \geq 0$$

Target unitary
$U \in \mathrm{SU}(2)$

How?

Compiled unitary
$U_{m_n} \cdots U_{m_2} U_{m_1}$ satisfying
$\left\| U - U_{m_n} \cdots U_{m_2} U_{m_1} \right\|_2 \leq \varepsilon$

Given ε, want to minimize length n, or otherwise $\mathrm{cost}(U_{m_n} \cdots U_{m_2} U_{m_1}) = \sum_i \mathrm{cost}(U_{m_i})$

Q: When does this problem have a solution?

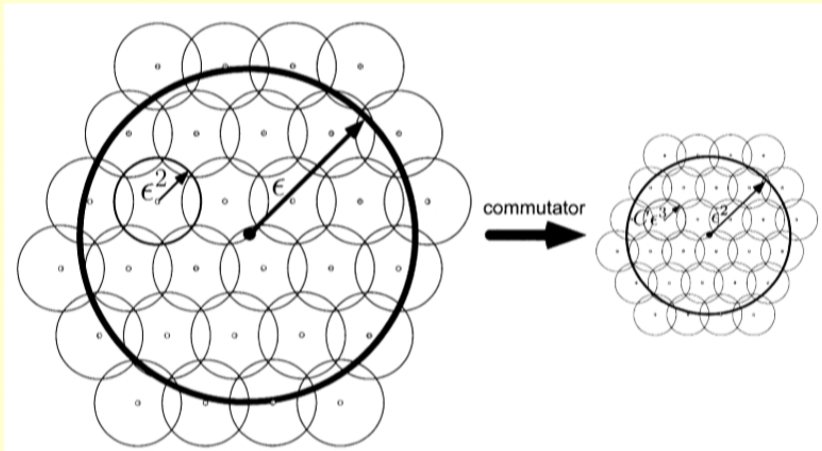
A: When $\langle \mathcal{G} \rangle \subset \mathrm{SU}(2)$ is dense

Brute-force search is impractical (exponential memory)

Solovay-Kitaev algorithm to the rescue?

Textbook approach - standard until 2012

Basic idea: Successive refining of a net using commutators



Implementations:

- [Kitaev, Shen, Vyalyi, AMS 2002]: $n = \log^{3+\delta}(1/\varepsilon)$ in $\log^{3+\delta}(1/\varepsilon)$ time
- [Dawson, Nielsen, quant-ph/0505030]: $n = \log^{3.97}(1/\varepsilon)$ in $\log^{2.71}(1/\varepsilon)$ time

However:

- Depressing gate counts – in practice, $R_z\left(\frac{2\pi}{64}\right)$ to error $\varepsilon = 10^{-16}$ needs $n \approx 15000$ T-gates
- Volume argument: $O(\log(1/\varepsilon))$ lower bound on length – can we achieve it? **[Image source: Nielsen/Chuang, CUP 2000]**

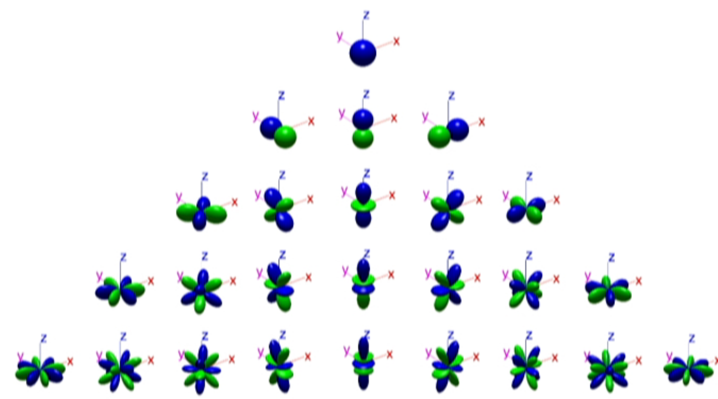
Optimal approximations – when do they exist at all?

Hecke operator averages functions $f : S^2 \to \mathbb{C}$ over finite gate set $\mathcal{G}$

$$(T_{\mathcal{G}} f)(x) = \frac{1}{|\mathcal{G}|} \sum_{U \in \mathcal{G}} f(U^{-1} x)$$

spherical harmonics

$$f \in L^2(S^2) \simeq \bigoplus_{j \in \mathbb{N}} \mathbb{C}^{2j+1}$$



$\langle \mathcal{G} \rangle$ has **exponential growth** if $T_{\mathcal{G}}$ is gapped:
For every $U \in \mathrm{SU}(2)$, $\| U - \mathcal{G}^n \|_2 \leq \exp(-O(n))$
i.e. $O(\log(1/\varepsilon))$ scaling

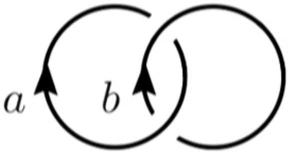
- [Lubotzky-Phillips-Sarnak CPAM ’86]
- [Harrow-Recht-Chuang quant-ph/0111031, JMP ’02]
- [Bourgain-Gamburd Inventiones Math. ’08] (**algebraic** entries)

(Algebraic = root of a polynomial over $\mathbb{Z}$)

But “everything” is algebraic!

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$S_{ab} = \mathcal{D}^{-1} \sum_c N_{\bar{a}b}^c \frac{\theta_c}{\theta_a \theta_b} d_c = \frac{1}{\mathcal{D}}\, a\, b$$



$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

Vafa’s theorem: Topological spins θ_a algebraic

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \zeta_8 \end{pmatrix} \quad \sqrt{T} = \begin{pmatrix} 1 & 0 \\ 0 & \zeta_{16} \end{pmatrix} \quad T^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & \zeta_{32} \end{pmatrix}$$

$$\zeta_n = e^{2\pi i/n}$$

$$V_x = \frac{1}{\sqrt{5}} \begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix} \quad V_y = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix} \quad V_z = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} -\zeta_{10} & 0 \\ 0 & \zeta_{10}^3 \end{pmatrix} \quad \sigma_2 = \frac{1}{\phi} \begin{pmatrix} \zeta_{10}^4 & -\zeta_5\sqrt{\phi} \\ -\zeta_5\sqrt{\phi} & -1 \end{pmatrix} \quad \phi = \frac{1+\sqrt{5}}{2} \quad X_d = \begin{pmatrix} 0 & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}, \; Z_d = \begin{pmatrix} 1 & & & \\ & \zeta_d & & \\ & & \ddots & \\ & & & \zeta_d^{d-1} \end{pmatrix}$$

But can we **find** an approximation efficiently?

$O(\log(1/\varepsilon))$-length ε-approximations in $O(\text{polylog}(1/\varepsilon))$-time!

Dramatic improvement: $R_z\left(\frac{2\pi}{64}\right)$ to $\varepsilon = 10^{-16}$ with 150 T gates (or even 50 with other tricks)



Clifford + T

Kliuchnikov-Maslov-Mosca 1212.0822 PRL '13

Selinger 1212.6253

Ross-Selinger 1403.2975




V-basis

Bocharov-Gurevich-Svore 1303.1411 PRA'13

(+ others)



Fibonacci anyons

Kliuchnikov-Bocharov-Svore 1310.4150 PRL'14

Is there a common generalization?

General method

Requirements:

- $\langle \mathcal{G} \rangle \subset \mathrm{SU}(2)$ dense (so we can approximate)
- Characterize $\mathcal{G}^n$ and $\langle \mathcal{G} \rangle$ (so we can round)
- Factoring in $\langle \mathcal{G} \rangle$ (so we can compile)

Two-step process:

- Step 1: (Approximate synthesis) Round U to $\lfloor U \rceil_n \in \mathcal{G}^n$

  [Kliuchnikov-Bocharov-Roetteler-Yard 1510.03888]
- Step 2: (Exact synthesis) Compile $\lfloor U \rceil_n = U_{m_n} \cdots U_{m_1}$

  [Kliuchnikov-Yard 1504.04350]

Clifford + T

Kliuchnikov-Maslov-Mosca 1212.0822 PRL '13

Selinger 1212.6253

Ross-Selinger 1403.2975

V-basis

Bocharov-Gurevich-Svore 1303.1411 PRA'13

Fibonacci anyons

Kliuchnikov-Bocharov-Svore 1310.4150 PRL'14

Natural data structure?

Quaternions

$$\mathbb{H} = \{q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}, q_i \in \mathbb{R} : \boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1, \boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k}\}$$

$$\begin{array}{ccccc} \mathbb{H}^\times & \to & \mathrm{SU}(2) & \to & \mathrm{SO}(3) \\ q & \mapsto & U_q & \mapsto & R_q \end{array}$$

$$U_q = \frac{q_0 I + i(q_1 Z + q_2 Y + q_3 X)}{\sqrt{N(q)}}$$

unitary normalization

Quaternion norm $N(q) = q_0^2 + q_1^2 + q_2^2 + q_3^2$ measures length, or complexity

homomorphism: $U_{q_1}U_{q_2} = U_{q_1 q_2}$, $U_{aq} = \pm U_q$ for $a \in \mathbb{R}^\times$

covering map: $R_q(v_1\boldsymbol{i} + v_2\boldsymbol{j} + v_3\boldsymbol{k}) = q(v_1\boldsymbol{i} + v_2\boldsymbol{j} + v_3\boldsymbol{k})q^{-1}$, $R_{aq} = R_q$ for $a \in \mathbb{R}^\times$

Integral quaternions and the V-basis

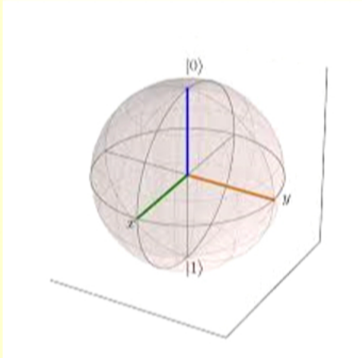
Rudolph Lipschitz

Lipschitz quaternion order

$$\mathcal{L} = \mathbb{Z} + \mathbb{Z}\boldsymbol{i} + \mathbb{Z}\boldsymbol{j} + \mathbb{Z}\boldsymbol{k}$$

$\mathcal{L}^\times = \{\pm 1, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\} = Q_8 =$ quaternion group

$U_{\mathcal{L}^\times} = \{\pm I, \pm iX, \pm iY, \pm iZ\} \to R_{\mathcal{L}^\times} = \langle R_x(\pi), R_z(\pi) \rangle \simeq (\mathbb{Z}/2)^2$



24 norm-5 quaternions: $\{1 \pm 2\boldsymbol{i}, 1 \pm 2\boldsymbol{j}, 1 \pm 2\boldsymbol{k}\} \cdot \mathcal{L}^\times$

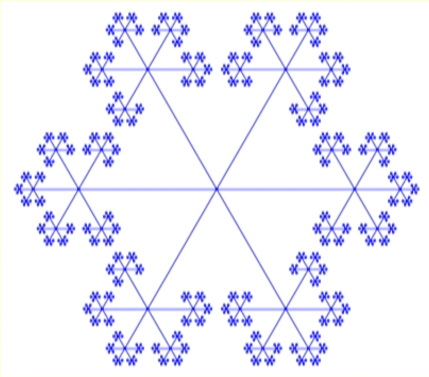
$$\theta = \arccos\left(-\tfrac{3}{5}\right)$$

$$V_x = U_{2\boldsymbol{i}+1} = \frac{1}{\sqrt{5}}\begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix} \to R_{2\boldsymbol{i}+1} = R_x(\theta)$$

$$V_y = U_{2\boldsymbol{j}+1} = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix} \to R_{2\boldsymbol{j}+1} = R_y(\theta)$$

$$V_z = U_{2\boldsymbol{k}+1} = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \to R_{2\boldsymbol{k}+1} = R_z(\theta)$$

This all works for any prime $p \equiv 1 \bmod 4$



Applications: BT, LPS, HRC, BGS

Compile by trial division *noncommutative* factoring

$$\mathcal{L}_5 = \{q \in \mathcal{L} : N(q) \in 5^{\mathbb{N}}\}$$

$$U_{\mathcal{L}_5} = \pm\langle V_x, V_y, V_z\rangle \to R_{\mathcal{L}_5} = \langle R_x(\theta), R_y(\theta), R_z(\theta)\rangle = \mathrm{SO}_3\left(\mathbb{Z}\left[\frac{1}{5}\right]\right) \simeq \mathrm{PSU}_2\left(\mathbb{Z}\left[i, \frac{1}{\sqrt{5}}\right]\right) \simeq \mathbb{F}^3$$

The Clifford quaternions

$$\mathcal{C} = \mathbb{Z}[\sqrt{2}]\frac{1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2} + \mathbb{Z}[\sqrt{2}]\frac{1+\boldsymbol{i}}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}]\frac{1+\boldsymbol{j}}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}]\frac{1+\boldsymbol{k}}{\sqrt{2}}$$

Isometric to E_8 root lattice: $\left(\mathcal{C}, \frac{\mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(N(x))}{4+2\sqrt{2}}\right) \simeq (E_8, x^2)$

where the **field trace** is $\mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}\,(x+y\sqrt{2}) = (x+y\sqrt{2}) + (x-y\sqrt{2}) = 2x.$

$U_{\mathcal{C}^\times}$ = binary octahedral group = ``qubit Clifford group'' = $\mathcal{C}^\times/\langle 1+\sqrt{2}\rangle \subset \mathrm{SU}(2)$

$$\equiv \left\{\pm 1, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}, \frac{\pm 1\pm\boldsymbol{i}}{\sqrt{2}}, \frac{\pm 1\pm\boldsymbol{j}}{\sqrt{2}}, \frac{\pm 1\pm\boldsymbol{k}}{\sqrt{2}}, \frac{\pm\boldsymbol{i}\pm\boldsymbol{j}}{\sqrt{2}}, \frac{\pm\boldsymbol{j}\pm\boldsymbol{k}}{\sqrt{2}}, \frac{\pm\boldsymbol{k}\pm\boldsymbol{i}}{\sqrt{2}}, \frac{\pm 1\pm\boldsymbol{i}\pm\boldsymbol{j}\pm\boldsymbol{k}}{2}\right\} \bmod \langle 1+\sqrt{2}\rangle$$

$\propto X \quad Y \quad Z \quad\quad H \quad\quad P$

$\rightarrow R_{\mathcal{C}^\times} = \mathrm{Aut}($  $) = \mathrm{Aut}($  $)$ = octahedral group = $\mathcal{C}^\times/\mathbb{Z}[\sqrt{2}]^\times \subset \mathrm{SO}(3)$

But where is the T-gate???

$$\mathcal{C} = \mathbb{Z}[\sqrt{2}]\frac{1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}}{2} + \mathbb{Z}[\sqrt{2}]\frac{1+\boldsymbol{i}}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}]\frac{1+\boldsymbol{j}}{\sqrt{2}} + \mathbb{Z}[\sqrt{2}]\frac{1+\boldsymbol{k}}{\sqrt{2}}$$

$$\boxed{T = U_{1+\frac{1+\boldsymbol{i}}{\sqrt{2}}}}$$

six such operators up to units $\mathbb{Z}[\sqrt{2}]^{\times} = \pm\langle 1+\sqrt{2}\rangle$

$\left(N\left(1+\frac{1+\boldsymbol{i}}{\sqrt{2}}\right)\right) = (\sqrt{2})$, where $(x) \coloneqq x\mathbb{Z}[\sqrt{2}]$ is principal ideal generated by $x \in \mathbb{Z}[\sqrt{2}]$

$$\mathcal{C}_{\sqrt{2}} = \left\{q \in \mathcal{C}: \left(N(q)\right) = \left(\sqrt{2}\right)^{n} \exists n \in \mathbb{N}\right\}$$

$$\langle \mathrm{Cliff}, T\rangle = U_{\mathcal{C}_{\sqrt{2}}} \to \mathrm{PU}_2\left(\mathbb{Z}\left[i, \tfrac{1}{\sqrt{2}}\right]\right) = \mathrm{PU}_2\left(\mathbb{Z}\left[\zeta_8, \tfrac{1}{2}\right]\right) \simeq \mathrm{SO}_3\left(\mathbb{Z}\left[\tfrac{1}{\sqrt{2}}\right]\right) = R_{\mathcal{C}_{\sqrt{2}}}$$

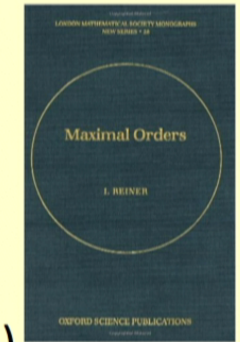
KMM '12

Gosset-Kliuchnikov-Mosca-Russo '14

Sarnak: ``A miracle that Clifford+T is arithmetic'' [IQC talk June '15]

A general framework: maximal orders in simple $\mathbb{Q}$-algebras

$\left(\frac{a,b}{F}\right) = \{q_0 + q_1\boldsymbol{i} + q_2\boldsymbol{j} + q_3\boldsymbol{k}, q_i \in F : \boldsymbol{i}^2 = a, \boldsymbol{j}^2 = b, \boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k}\}$



F = **number field** with ring of integers $\mathbb{Z}_F$

e.g. Out[6]= Root[14 − 72 #1 + 25 #1^2 − 144 #1^3 − 88 #1^4 − 8 #1^5 + 62 #1^6 − 14 #1^8 + #1^{10} &, 2]

Maximal order $\mathcal{M} \subset \left(\frac{a,b}{F}\right)$ is a noncommuting ring of integers (a spanning $\mathbb{Z}_F$-lattice)

Our application: a machine for producing S-arithmetic groups $\mathrm{SU}(\mathcal{M}, S) = U_{\mathcal{M}_S}$

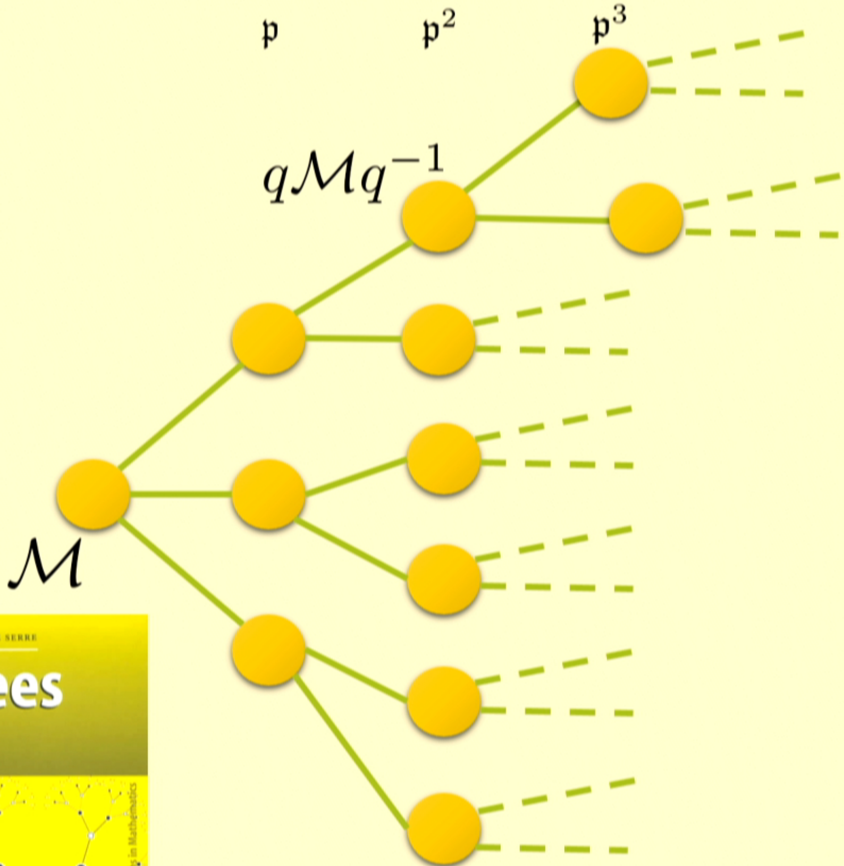
where S = finite set of prime ideals in $\mathbb{Z}_F$, $\mathcal{M}_S = \{q \in \mathcal{M} : (N(q)) = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n_\mathfrak{p}}, n_\mathfrak{p} \in \mathbb{N}\}$

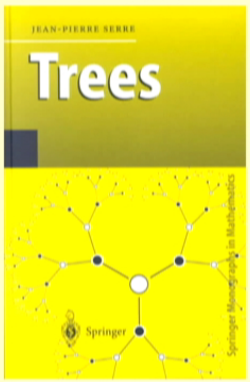
e.g. $S = \{5\mathbb{Z}\}$ (V-basis), $S = \{\sqrt{2}\mathbb{Z}[\sqrt{2}]\}$ (Clifford+T),

Deep theorems: S-arithmetic groups are finitely generated [Borel & Harish-Chandra '61]
and finitely presented [Grunewald-Segal '80]

We gave (arXiv:1504.04350 [KY]) first explicit effective method for computing generators allowing trial division when $|S| \geq 1$ and when the algebra has at most one embedding into $\mathbb{R}^{2\times 2}$

Exact synthesis (step 2) example: factoring on a tree





When $S = \{\mathfrak{p}\}$ can build a $(N(\mathfrak{p}) + 1)$-regular tree with a vertex for each quaternion

Factoring = path finding

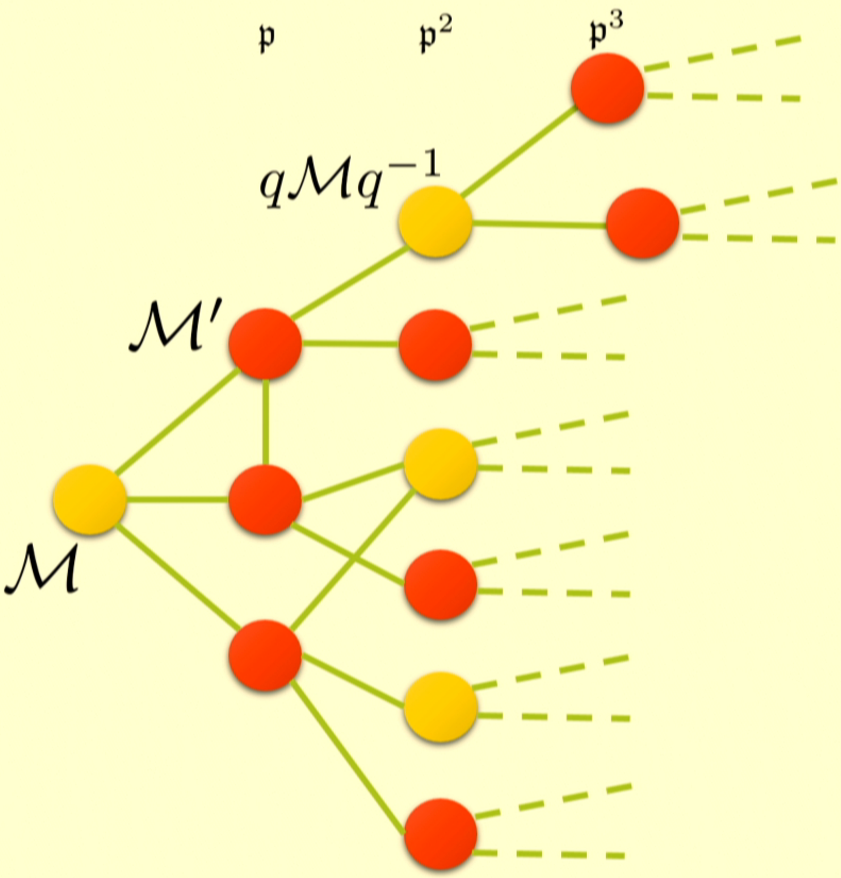
$\left(\frac{a,b}{F}\right)$ = quaternion algebra over number field F

$\mathcal{M}$ = maximal order

$\mathfrak{p}$ = prime ideal of $\mathbb{Z}_F$

$\mathrm{SU}(\mathcal{M}, \mathfrak{p}) = \{U_q : q \in \mathcal{M}, N(q)\mathbb{Z}_F = \mathfrak{p}^n, n \in \mathbb{N}\}$

Exact synthesis (step 2) example: $|S| > 1$



Can also compile for e.g.:
Cliff+T+V: $S = \{\sqrt{2}\mathbb{Z}[\sqrt{2}], 5\mathbb{Z}[\sqrt{2}]\}$
(but now it is no longer a tree)

$\left(\frac{a,b}{F}\right)$ = quaternion algebra over number field F
$\mathcal{M}$ = maximal order
$\mathfrak{p}$ = prime ideal of $\mathbb{Z}_F$
$\mathrm{SU}(\mathcal{M}, \mathfrak{p}) = \{U_q : q \in \mathcal{M}, N(q)\mathbb{Z}_F = \mathfrak{p}^n, n \in \mathbb{N}\}$

Approximate synthesis (step 1)

Input:

F = totally real number field

$\left(\frac{a,b}{F}\right)$ = totally-definite quaternion algebra over number field F

$\mathcal{M}$ = maximal order

$\mathfrak{p}$ = prime ideal of $\mathbb{Z}_F$

$\mathrm{SU}(\mathcal{M},\mathfrak{p}) = \{U_q : q \in \mathcal{M}, N(q)\mathbb{Z}_F = \mathfrak{p}^n, n \in \mathbb{N}\}$

ε = quality of approximation

φ = z-rotation angle

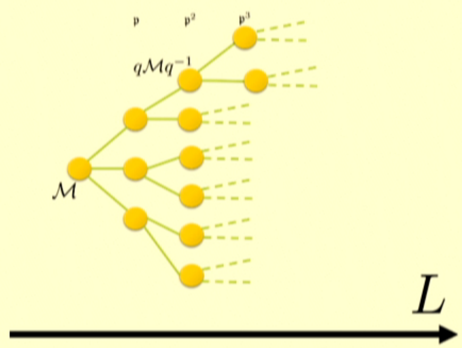
Target qubit unitary

$$R_z(\varphi) = \begin{pmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{pmatrix}$$

Output:

$q \in \mathcal{M}$ such that

1. $\left\| U_q - R_z(\varphi) \right\|_2 \le \varepsilon$
2. $N(q)\mathbb{Z}_F = \mathfrak{p}^L$, where

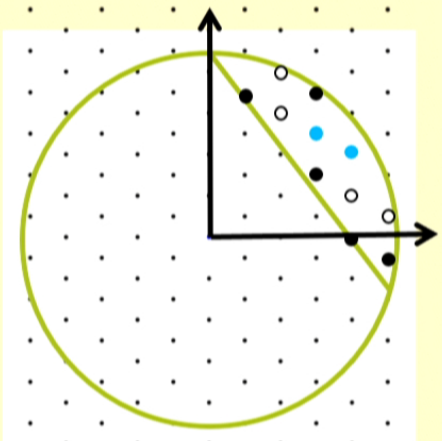


$$L \log(N(\mathfrak{p})) \le 4 \log(1/\varepsilon) + C$$

Approximate synthesis (step 1)

$$q = q_0 + q_3\boldsymbol{k} + q_1\boldsymbol{i} + q_2\boldsymbol{j} \in \mathbb{Z}_F\mathcal{L} \simeq \mathbb{Z}_K \oplus \mathbb{Z}_K \subset \mathcal{M} \subset \left(\frac{a,b}{F}\right)$$

CM field
$K = F(\sqrt{a})$



$\left\|U_q - R_z(\varphi)\right\|_2 \leq \varepsilon$

1. Sample lattice points $\mathbb{Z}_K$ from convex body

2. Solve integral norm equation $N(q)\mathbb{Z}_F = \mathfrak{p}^L$ over to ensure that $q \in \mathcal{M}_S$

- Reshape convex body by solving approximate CVP in unit lattice $\mathbb{Z}_F^\times/\{\pm 1\}$

- Postselect for easy instances
- Reduce arbitrary easy instance to constant size instance using LLL
- Efficient algorithm assuming number-theoretical conjecture

A Fibonacci quaternion order

$$\mathcal{F} = \mathbb{Z}\left[\frac{\sqrt{5}+1}{2}\right] + \mathbb{Z}\left[\frac{\sqrt{5}+1}{2}\right]\frac{1+\boldsymbol{i}}{2} + \mathbb{Z}\left[\frac{\sqrt{5}+1}{2}\right]\boldsymbol{j} + \mathbb{Z}\left[\frac{\sqrt{5}+1}{2}\right]\frac{\boldsymbol{j}+\boldsymbol{k}}{2} \subset \left(\frac{\frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+3}{2}}{\mathbb{Q}(\sqrt{5})}\right)$$

$U_{\mathcal{F}^\times} =$ image of ``even'' subgroup of B_3 (infinite unit group)

Full image of B_3 with $S = \sqrt{5}\mathcal{F}$

Only unitary for some embeddings since $\mathbb{Q}\left(\sqrt{\frac{\sqrt{5}-1}{2}}\right)$ not a CM field

Exist further generalizations for $\mathrm{SU}(2)_k$ CS-theory

Asymptotically Optimal Topological Quantum Compiling

Vadym Kliuchnikov[†], Alex Bocharov[*], and Krysta M. Svore[*]
[†] *Institute for Quantum Computing and David R. Cheriton School of Computer Science, Univ. of Waterloo, Waterloo, Ontario (Canada)*
Quantum Architectures and Computation Group, Microsoft Research, Redmond, WA (USA)

Computing fundamental domains for Fuchsian groups

par John Voight

Maximal sets of equiangular complex lines (SIC-POVMs)

Consider n equiangular lines in $\mathbb{C}^d$ spanned by unit vectors $|\psi_1\rangle, \ldots, |\psi_n\rangle \in \mathbb{C}^d$ i.e. satisfying $\left|\langle\psi_i, \psi_j\rangle\right|^2 = \begin{cases} 1, & i = j \\ \alpha, & i \neq j \end{cases}$ for $\alpha < 1$.

Easy to prove that $n \leq d^2$, and if $n = d^2$ then $\alpha = \frac{1}{d+1}$.

SIC-POVM in $d = 2$

There are computer-assisted proofs in huge number fields that orbits of Heisenberg group $\langle X_d, Z_d\rangle$ achieve $n = d^2$ for $d = 2 - 20, 24, 28, 35, 48$

Inexact numerical evidence up to d=323 [Scott, Scott-Grassl, RBSC, Zauner]

$$X_d = \begin{pmatrix} 0 & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}, \quad Z_d = \begin{pmatrix} 1 & & & \\ & \zeta_d & & \\ & & \ddots & \\ & & & \zeta_d^{d-1} \end{pmatrix}$$

Exists $|\psi\rangle \in \mathbb{C}^d$ generating SIC-POVM is such that Galois closure of $\mathbb{Q}\left(\frac{\psi_1}{\psi_d}, \cdots \frac{\psi_{d-1}}{\psi_d}\right)$ equals ray class field of $\mathbb{Q}(\sqrt{(d-3)(d+1)})$ with conductor $(d)\infty$.

GENERATING RAY CLASS FIELDS OF REAL QUADRATIC FIELDS VIA COMPLEX EQUIANGULAR LINES

MARCUS APPLEBY, STEVEN FLAMMIA, GARY MCCONNELL, AND JON YARD

ABSTRACT. Let K be a real quadratic field. For certain K with sufficiently small discriminant we produce explicit unit generators for specific ray class fields of K using a numerical method that arose in the study of complete sets of equiangular lines in $\mathbb{C}^d$ (known in quantum information as symmetric informationally complete measurements or SICs). The construction in low dimensions suggests a general recipe for producing unit generators in infinite towers of ray class fields above arbitrary K and we summarise this in a conjecture. Such explicit generators are notoriously difficult to find, so this recipe may be of some interest.

arXiv:1604.06098v1 [math.NT] 20 Apr 2016

Thanks for listening!

- Quantum capacity can be superactivated
- Poly-time algorithm for compiling $O\big(\log(1/\varepsilon)\big)$-length ε-approximations, which is optimal
- A general quaternionic framework for producing qubit gate sets generating arithmetic groups.
- SIC-POVMs -> Hilbert's 12^{th} problem for real quadratic fields, a holy grail of class field theory

The future:

- Qudit, and multi-qubit codes.
- Fault-tolerant protocols and Clifford hierarchy.
- New algorithms?
- Explicit quantum expanders?
- Existence of SIC-POVMs via arithmetic models of Weil representation constructed via Galois cohomology?