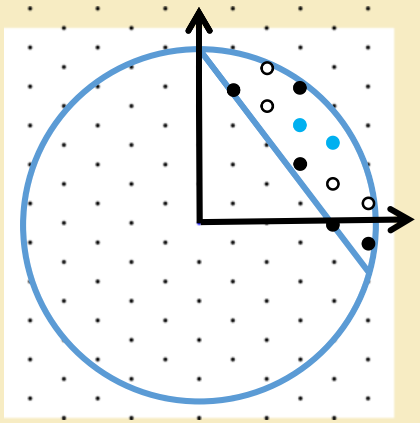
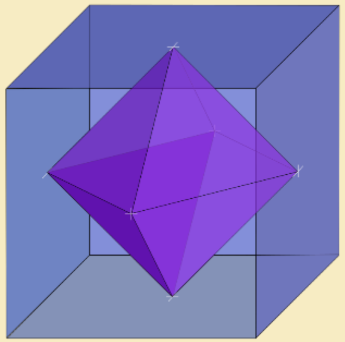
A framework for approximating qubit unitaries





Jon Yard

with

Vadym Kliuchnikov, Alex Bocharov, Martin Roetteler

Microsoft Research

Quantum Architectures and Computation Group (QuArC)

QIP 2016

Banff International Research Station, Alberta, Canada

January 14, 2016

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

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

My collaborators

Vadym Kliuchnikov

Martin Roetteler

Alex Bocharov

A FRAMEWORK FOR EXACT SYNTHESIS

VADYM KLIUCHNIKOV[1] AND JON YARD[1]

Abstract. Exact synthesis is a tool used in algorithms for approximating an arbitrary qubit unitary with a sequence of quantum gates from some finite set. These approximation algorithms find asymptotically optimal approximations in probabilistic polynomial time, in some cases even finding the optimal solution in probabilistic polynomial time given access to an oracle for factoring integers. In this paper, we present a common mathematical structure underlying all results related to the exact synthesis of qubit unitaries known to date, including Clifford+T, Clifford-cyclotomic and V-basis gate sets, as well as gates sets induced by the braiding of Fibonacci anyons in topological quantum computing. The framework presented here also provides a means to answer questions related to the exact synthesis of unitaries for wide classes of other gate sets, such as Clifford+T+V and $SU(2)_k$ anyons.

arXiv:1504.04350
``the first paper''

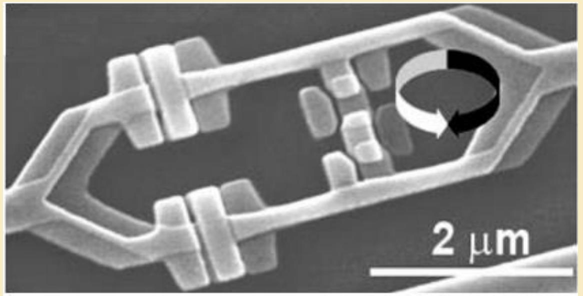
A FRAMEWORK FOR APPROXIMATING QUBIT UNITARIES

VADYM KLIUCHNIKOV[1], ALEX BOCHAROV[1], MARTIN ROETTELER[1], AND JON YARD[1]

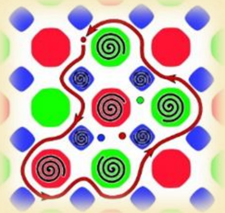
Abstract. We present an algorithm for efficiently approximating of qubit unitaries over gate sets derived from totally definite quaternion algebras. It achieves ε-approximations using circuits of length $O(\log(1/\varepsilon))$, which is asymptotically optimal. The algorithm achieves the same quality of approximation as previously-known algorithms for Clifford+T [arXiv:1212.6253], V-basis [arXiv:1303.1411] and Clifford+$\pi/12$ [arXiv:1409.3552], running on average in time polynomial in $O(\log(1/\varepsilon))$ (conditional on a number-theoretic conjecture). Ours is the first such algorithm that works for a wide range of gate sets and provides insight into what should constitute a "good" gate set for a fault-tolerant quantum computer.

arXiv:1510.03888
``the second paper''

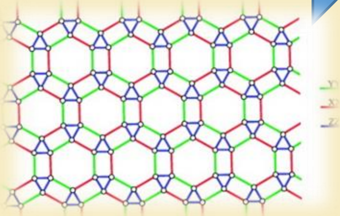
Fault-tolerant quantum gates



Physical error < 10^{-2}

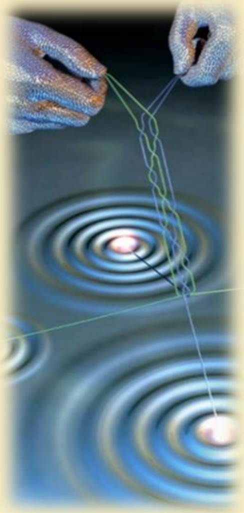


quantum code

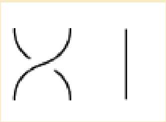


$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Fault tolerant



braiding



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

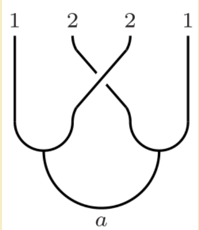
What do I do with all these gates?

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

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

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

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



$\mathrm{SU}(2)_4$ + measurement

$\sigma_1 = \begin{pmatrix} -\zeta_{10} & 0 \\ 0 & \zeta_{10}^3 \end{pmatrix} \quad \sigma_2 = \frac{1}{\phi} \begin{pmatrix} \zeta_{10}^4 & -\zeta_5 \sqrt{\phi} \\ -\zeta_5 \sqrt{\phi} & -1 \end{pmatrix} \quad \phi = \frac{1+\sqrt{5}}{2}$

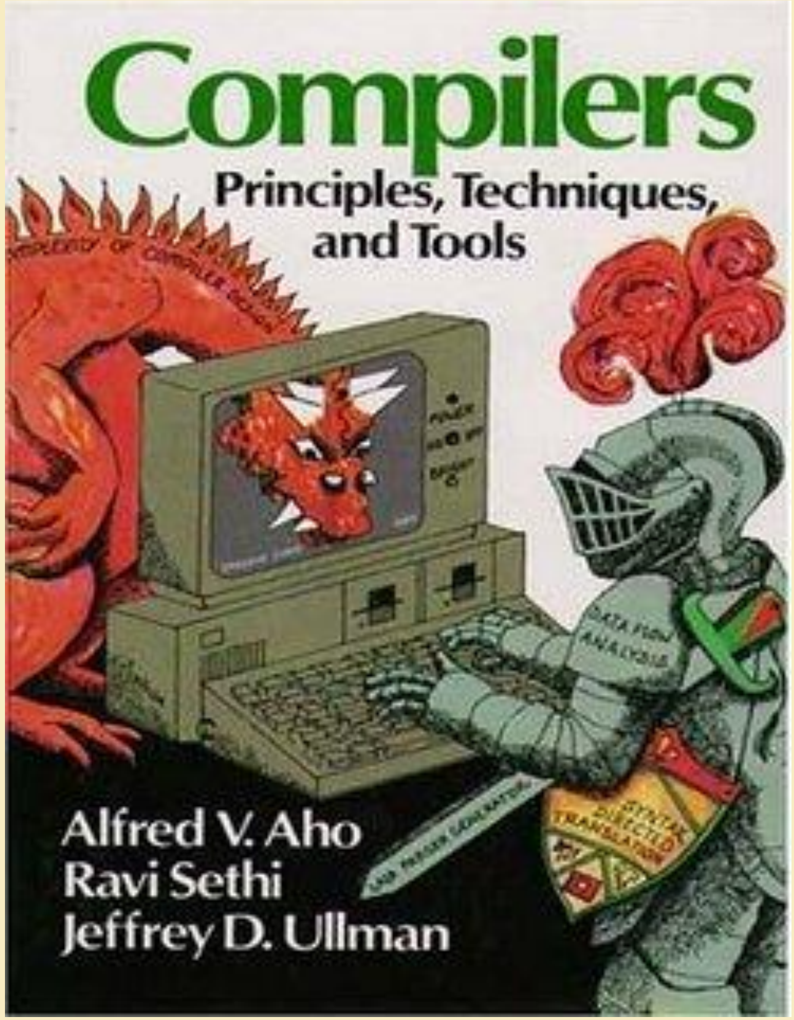
Fibonacci anyons

$B = \frac{1}{2} \begin{pmatrix} 1 & -\sqrt{-3} \\ -\sqrt{-3} & 1 \end{pmatrix} \quad K = \begin{pmatrix} 1 & 0 \\ 0 & \frac{-1+4\sqrt{-3}}{7} \end{pmatrix}$

Levaillant, Bauer, Freedman, Wang, Bonderson ‘15

Compile them!

- **This talk**: polynomial-time algorithm for ε-approximating a given unitary $U \in \mathrm{SU}_2(\mathbb{C})$ with an $O\big(\log(1/\varepsilon)\big)$-length circuit over a very general gate set
- i.e. for gate sets derived from maximal orders in totally-definite quaternion algebras over number fields.
- **Optimal** up to constant factors
- Generalizes most existing known algorithms for specific gate sets



The general compiling problem:

Fault-tolerant quantum computer

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

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

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 $\mathrm{cost}\left(U_{m_n} \cdots U_{m_2} U_{m_1}\right) = \sum_i \mathrm{cost}(U_{m_i})$

Q: When does this problem have a solution?

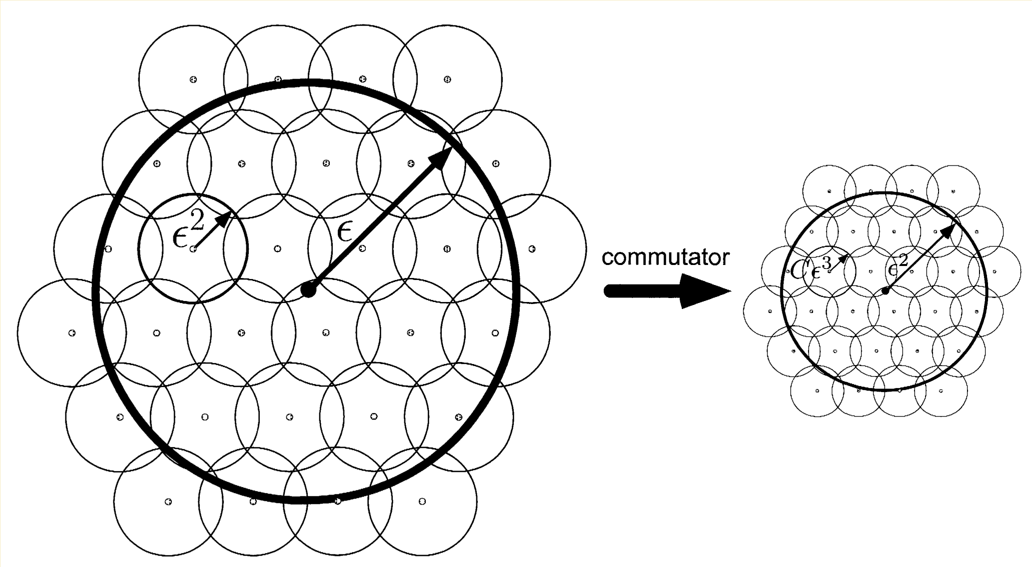
A: When $\langle \mathcal{G} \rangle \subset \mathrm{SU}(2)$ is dense

Brute-force search is impractical (exponential memory)

Solovay-Kitaev algorithm to the rescue!

Standard approach until 2012

Basic idea: Successive refining of a net using commutators



Implementations:

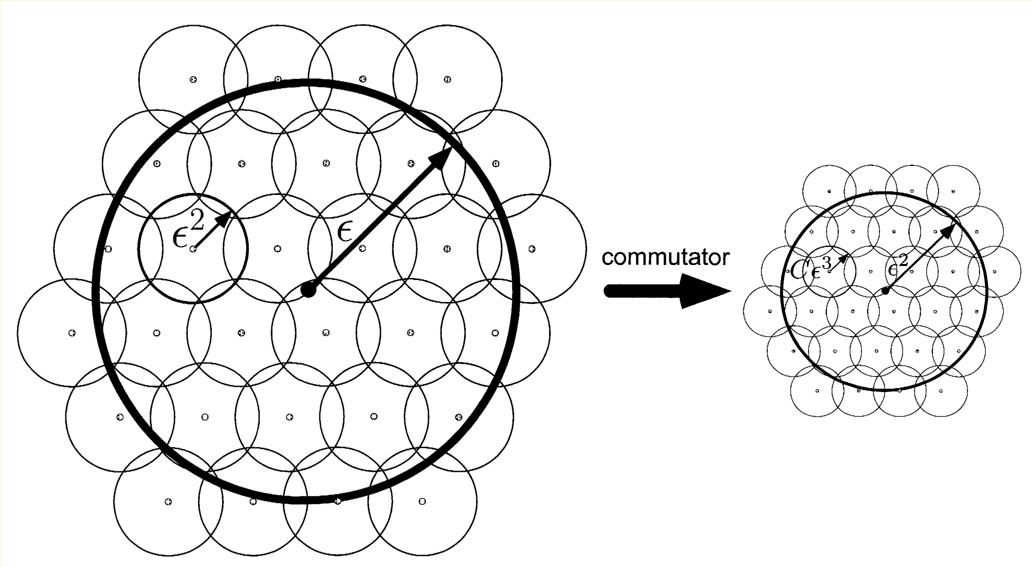
- [Kitaev, Shen, Vyalyi, AMS 2002]: $n = \log^{3+\delta}(1/\varepsilon)$ in $\log^{3+\delta}(1/\varepsilon)$ time
- [Dawson, Nielsen, quant-ph/0505030]: $n = \log^{3.97}(1/\varepsilon)$ in $\log^{2.71}(1/\varepsilon)$ time

[Image source: Nielsen/Chuang, CUP 2000]

Solovay-Kitaev algorithm to the rescue?

Standard approach 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, $\varepsilon = 10^{-16}$ needs $n = 15000$
- Volume argument: $O(\log(1/\varepsilon))$ lower bound on length – can we achieve it?

[Image source: Nielsen/Chuang, CUP 2000]

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



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)



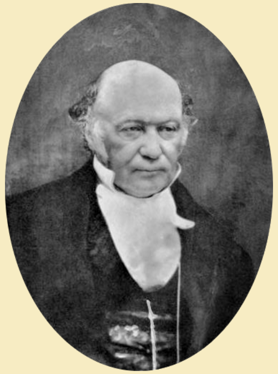
Fibonacci anyons

Kliuchnikov-Bocharov-Svore 1310.4150 PRL’14

Dramatic improvement: $\varepsilon = 10^{-16}$ requires $n = 150$ (or even $n = 50$ with extra tricks)

Is there a common generalization?

Quaternions



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

$$\mathbb{H}^\times \to \mathrm{SU}(2) \to \mathrm{SO}(3)$$

$$q \quad \mapsto \quad U_q \quad \mapsto \quad R_q$$

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

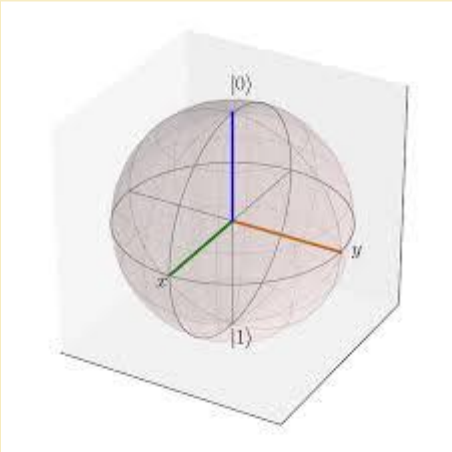
unitary normalization

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 $a \in \mathbb{R}$

Covering map $R_q(v_1\boldsymbol{i} + v_2\boldsymbol{j} + v_3\boldsymbol{k}) = q(v_1\boldsymbol{i} + v_2\boldsymbol{j} + v_3\boldsymbol{k})q^{-1}$

Integral quaternions and the V-basis



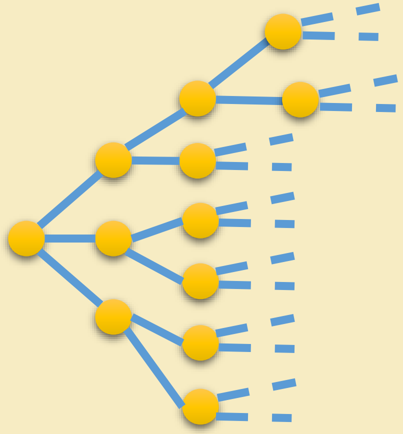
Lipschitz quaternion order

Rudolph Lipschitz

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

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

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



There are **six** norm-5 quaternions: $1 \pm 2\boldsymbol{i}, 1 \pm 2\boldsymbol{j}, 1 \pm 2\boldsymbol{k}$

$$U_{\mathcal{L}_5} = \langle V_x, V_y, V_z \rangle$$

Compiling by trial division: ``factoring on steroids''

$$V_x \to R_x\left(\arccos\left(-\frac{3}{5}\right)\right), R_y\left(\arccos\left(-\frac{3}{5}\right)\right), R_z\left(\arccos\left(-\frac{3}{5}\right)\right)$$

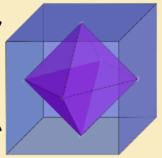
$$V_x = U_{2\boldsymbol{i}+1} = \frac{1}{\sqrt{5}}\begin{pmatrix} 1+2i & 0 \\ 0 & 1-2i \end{pmatrix},\ V_y = U_{2\boldsymbol{j}+1} = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & 2i \\ 2i & 1 \end{pmatrix},\ V_z = U_{2\boldsymbol{k}+1} = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$$

Used in Bocharov-Gurevich-Svore 1303.1411 PRA'13

The Clifford quaternions

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

$$\mathcal{C}^\times = \left\{\pm 1, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}, \frac{\pm 1 \pm \boldsymbol{i}}{\sqrt{2}}, \frac{\pm 1 \pm \boldsymbol{j}}{\sqrt{2}}, \frac{\pm 1 \pm \boldsymbol{k}}{\sqrt{2}}, \frac{\pm \boldsymbol{i} \pm \boldsymbol{j}}{\sqrt{2}}, \frac{\pm \boldsymbol{j} \pm \boldsymbol{k}}{\sqrt{2}}, \frac{\pm \boldsymbol{k} \pm \boldsymbol{i}}{\sqrt{2}}, \frac{\pm 1 \pm \boldsymbol{i} \pm \boldsymbol{j} \pm \boldsymbol{k}}{2}\right\}$$

$\simeq U_{\mathcal{C}^\times} = \mathrm{Aut}\Big($  $\Big)$ = binary octahedral group = ``qubit Clifford group''

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

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

$$N\left(1+\frac{1+\boldsymbol{i}}{\sqrt{2}}\right)\mathbb{Z}[\sqrt{2}] = \sqrt{2}\mathbb{Z}[\sqrt{2}] \quad \mathcal{C}_{\sqrt{2}} = \{q \in \mathcal{C} : N(q)\mathbb{Z}[\sqrt{2}] = 2^{L/2}\mathbb{Z}[\sqrt{2}]\ \exists L \in \mathbb{Z}\}$$

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

KMM ‘12

Gosset-Kliuchnikov-Mosca-Russo ‘14

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

Optimal approximations – when do they exist at all?

Hecke operator

$$T_{\mathcal{G}}: L^2(\mathrm{SU}_2) \to L^2(\mathrm{SU}_2)$$

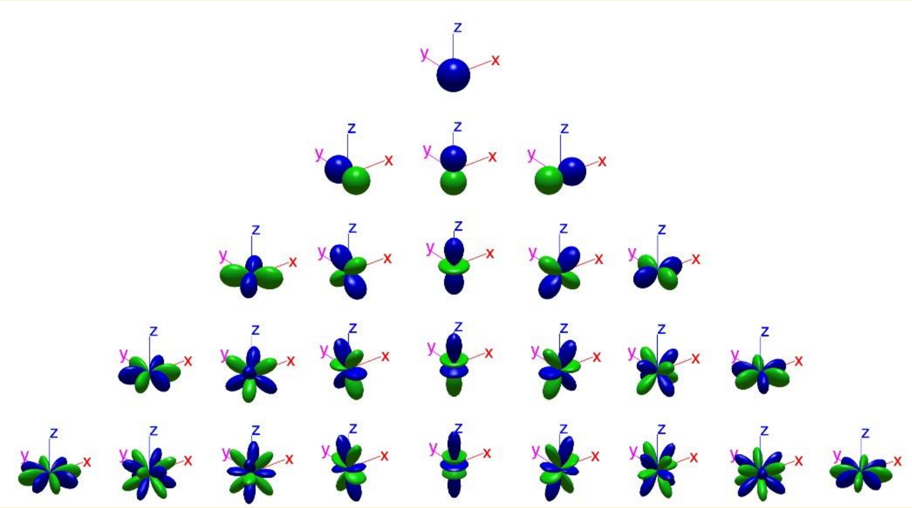
$$(T_{\mathcal{G}} f)(g) = \frac{1}{|\mathcal{G}|} \sum_{U \in \mathcal{G}} f(U^{-1}x)$$

$$\begin{array}{ccc} & & L^2(\mathrm{SU}_2) \simeq L^2(S^3) \simeq \bigoplus_{j\in\frac{1}{2}\mathbb{N}} \mathbb{C}^{2j+1} \\ S^1 \to S^3 & & \uparrow \\ \text{Hopf fibration} \downarrow & & \\ S^2 & & L^2(S^2) \simeq \bigoplus_{j\in\mathbb{N}} \mathbb{C}^{2j+1} \quad \text{spherical harmonics} \end{array}$$

$\langle \mathcal{G} \rangle$ 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

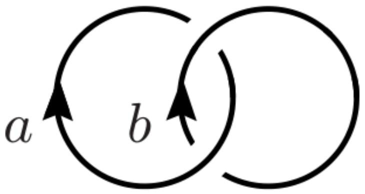
- [Harrow-Recht-Chuang quant-ph/0111031, JMP ’02]
- [Lubotzky-Phillips-Sarnak CPAM ’86]
- [Bourgain-Gamburd Inventiones Math. ’08] (**algebraic** entries)

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



“Everything” is algebraic!

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



Vafa’s theorem: Topological spins θ_a algebraic

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

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

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

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

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

$$\sigma_1 = \begin{pmatrix} -\zeta_{10} & 0 \\ 0 & \zeta_{10}^3 \end{pmatrix} \quad \sigma_2 = \frac{1}{\phi} \begin{pmatrix} \zeta_{10}^4 & -\zeta_5\sqrt{\phi} \\ -\zeta_5\sqrt{\phi} & -1 \end{pmatrix} \quad \phi = \frac{1+\sqrt{5}}{2} \quad B = \frac{1}{2} \begin{pmatrix} 1 & -\sqrt{-3} \\ -\sqrt{-3} & 1 \end{pmatrix} \quad K = \begin{pmatrix} 1 & 0 \\ 0 & \frac{-1+4\sqrt{-3}}{7} \end{pmatrix}$$

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

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?

Maximal orders in quaternion algebras over number fields

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

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

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

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

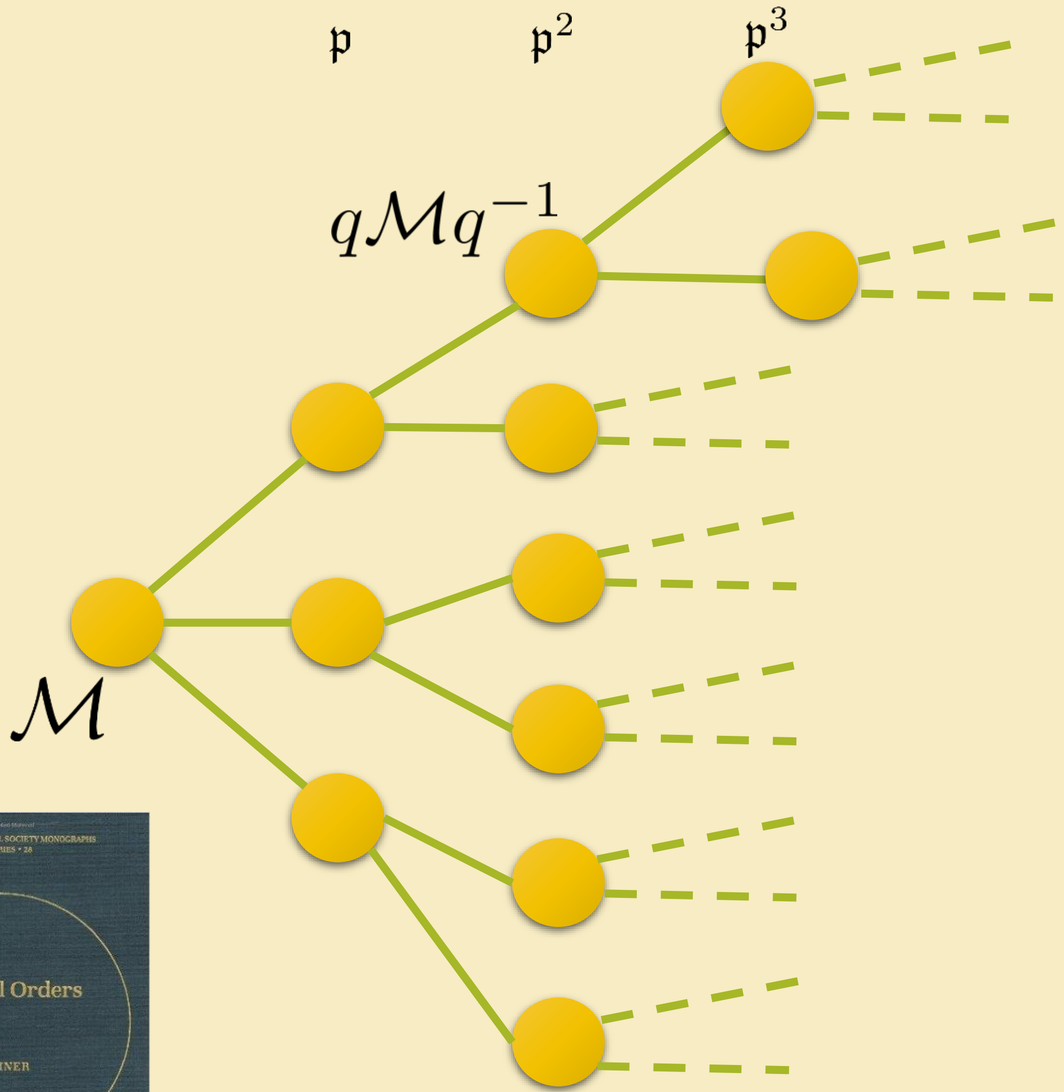
where $S =$ finite set of prime ideals in $\mathbb{Z}_F$, $\mathcal{M}_S = \{q \in \mathcal{M} : \mathrm{supp}(N(q)\mathbb{Z}_F) \subset S\}$

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 give (arXiv:1504.04350 [KY]) first explicit effective method for computing a complete set of generators when $|S| \geq 1$ and when the algebra has at most one embedding into $\mathbb{R}^{2\times 2}$

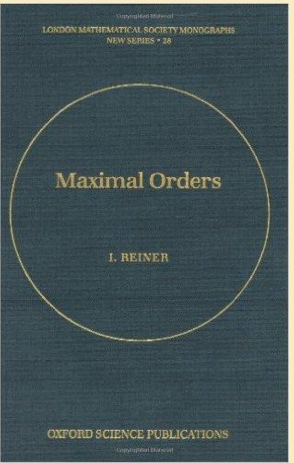
Algorithms: factorization: simple case



Idea: there is as vertex of a tree corresponding to each quaternion

Factorization: path finding

The tree is $N(\mathfrak{p})+1$ regular



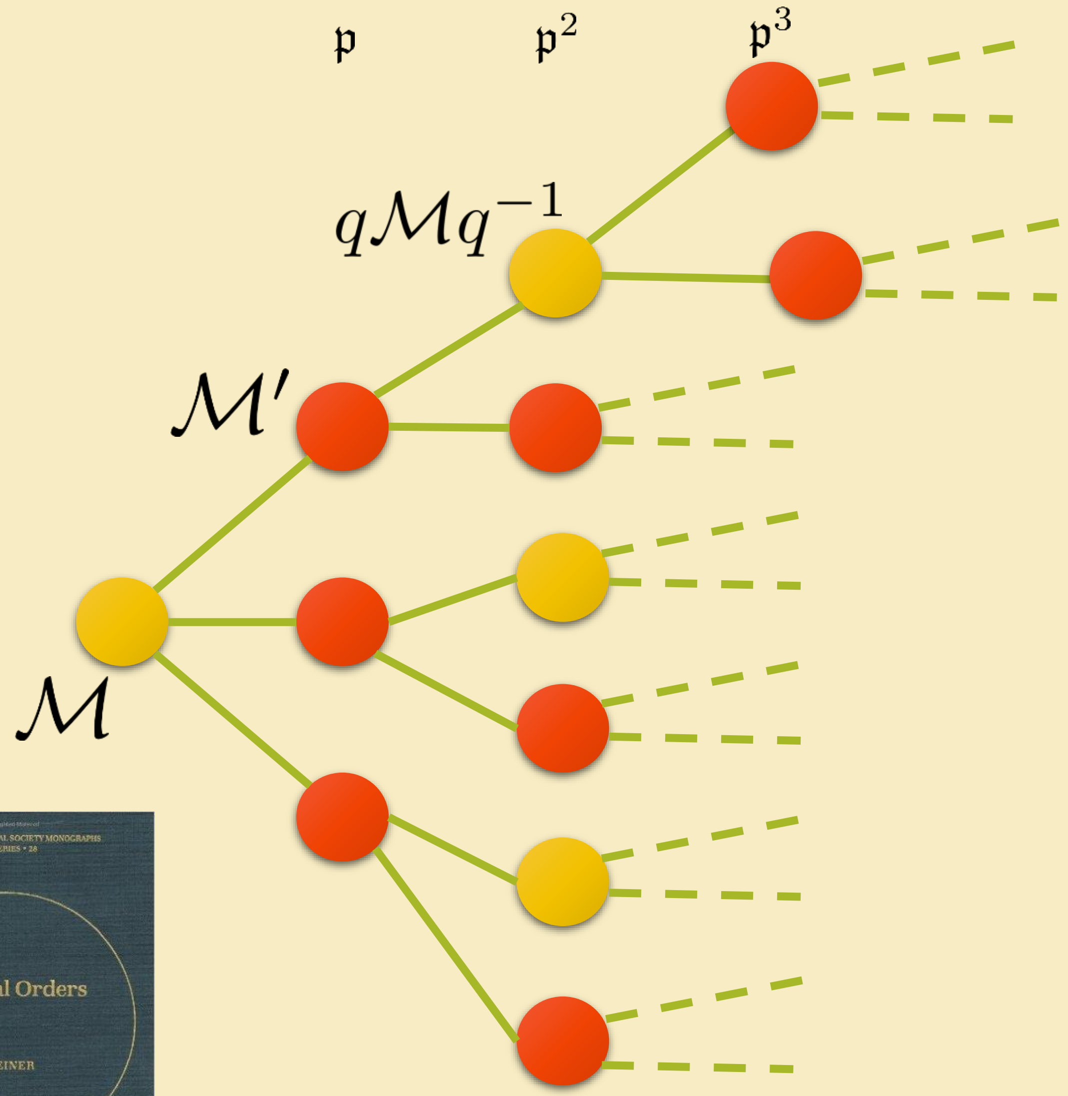
$\left(\frac{a,b}{F}\right)$ = quaternion algebra over number field F

$\mathcal{M}$ = maximal order

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

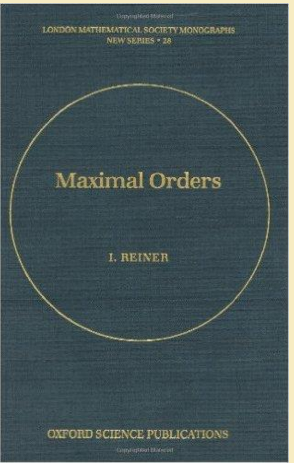
$\mathrm{SU}(\mathcal{M},\mathfrak{p}) = \{U_q : q \in \mathcal{M}, N(q)\mathbb{Z}_F = \mathfrak{p}^n, n \in \mathbb{N}\}$

Algorithms: factorization: class set



Issue: not all vertices are conjugate to $\mathcal{M}$

Relevant for Clifford+$\sqrt{T}$, Clifford+$R_z\left(\frac{2\pi}{n}\right)$



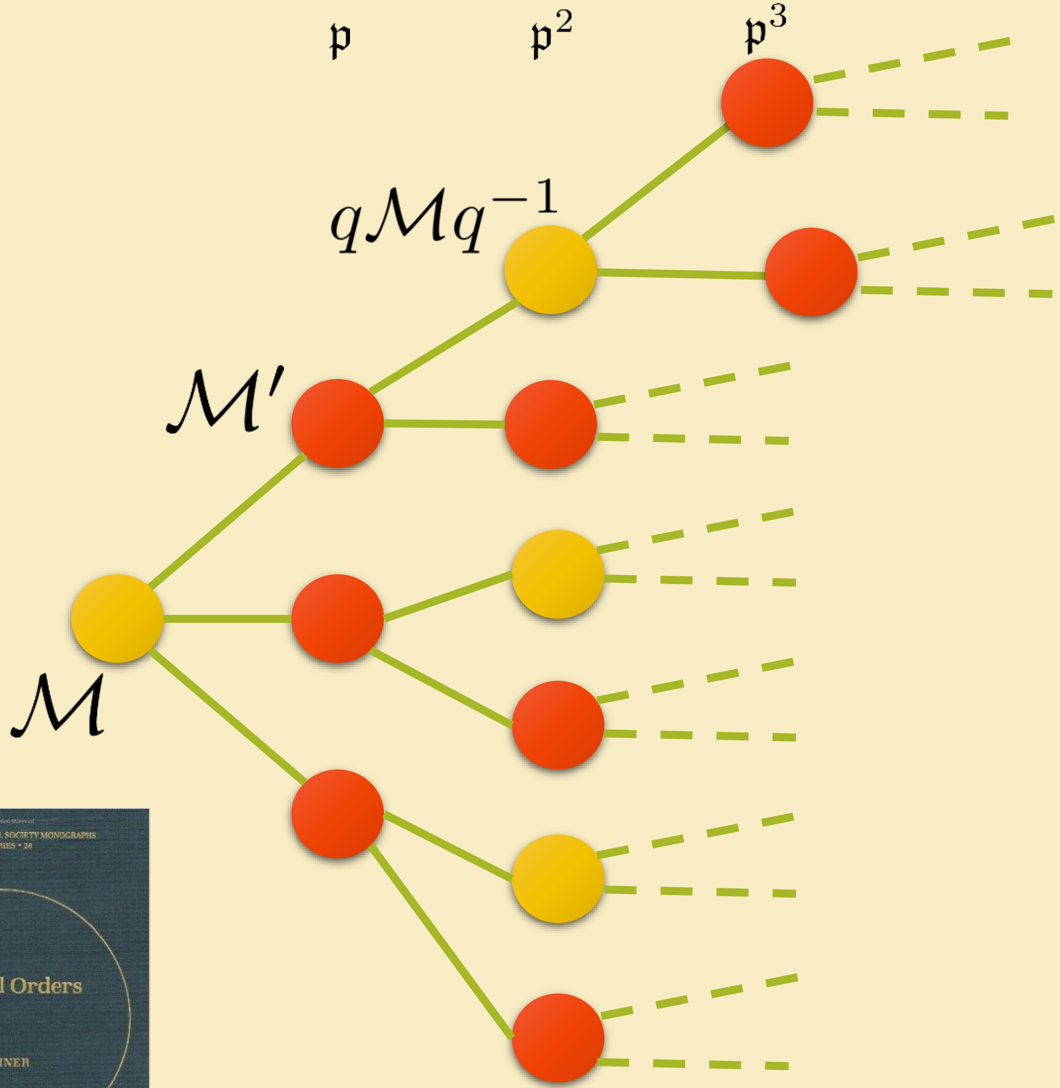
$\left(\frac{a,b}{F}\right)$ = quaternion algebra over number field F

$\mathcal{M}$ = maximal order

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

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

Algorithms: factorization: class set



Issue: not all vertices are conjugate to $\mathcal{M}$

Relevant for Clifford+$\sqrt{T}$, Clifford+$R_z\left(\frac{2\pi}{n}\right)$

Can also compile for e.g.:

Fibonnaci anyons: $\mathfrak{p} = \sqrt{5}\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$,

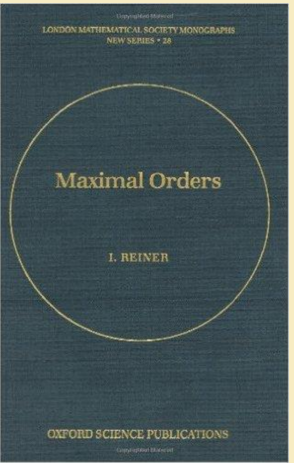
Clifford+T+V: $S = \{\sqrt{2}\mathbb{Z}[\sqrt{2}], 5\mathbb{Z}[\sqrt{2}]\}$

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

$\mathcal{M}$ = maximal order

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

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



Algorithms : approximation (back to step 1)

Input:

$\left(\frac{a,b}{F}\right)$ = 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

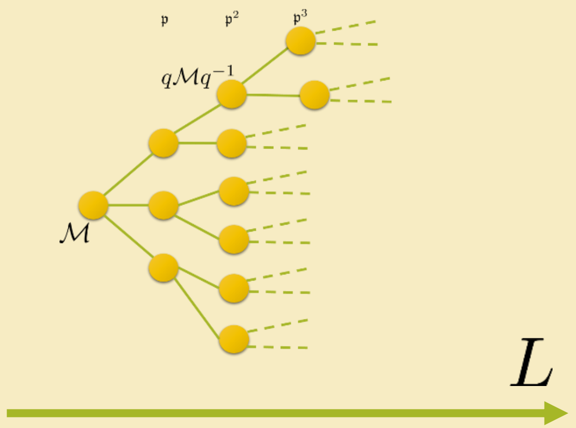
Target qubit unitary

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

Output:

q from $\mathcal{M}$

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



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

Algorithms : approximation: idea

$\left(\frac{a,b}{F}\right)$

$$q = \overbrace{a_1 + a_2\boldsymbol{i}}^{K/F} + \overbrace{a_3\boldsymbol{j} + a_4\boldsymbol{k}}^{K/F}$$

Step 1. Sampling

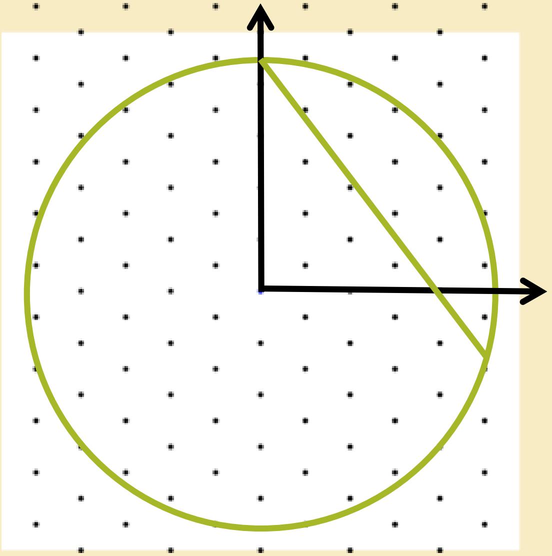
$\|U_q - R_z(\varphi)\| \le \varepsilon$

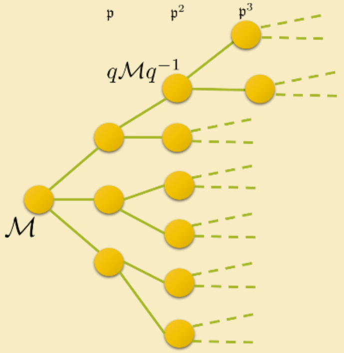
Step 2. Norm equation

$N(q)\mathbb{Z}_F = \mathfrak{p}^L$

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

Lattice from K





Solve integral relative norm equation K/F

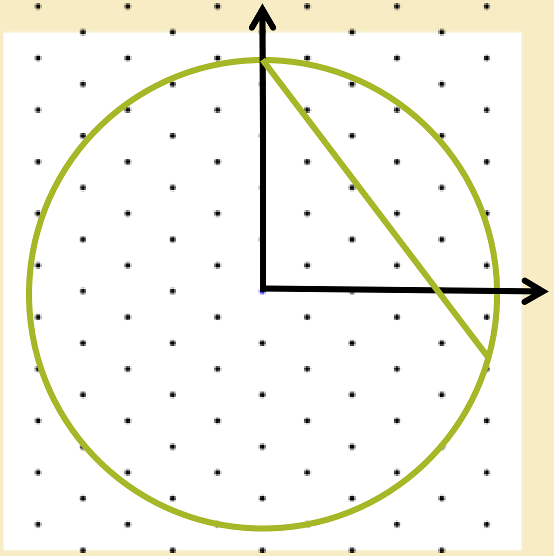
Algorithms : approximation: sampling

Step 1.

$$q = \underbrace{a_1 + a_2\boldsymbol{i}} + a_3\boldsymbol{j} + a_4\boldsymbol{k}$$

$$\|U_q - R_z(\varphi)\| \leq \varepsilon$$

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



Algorithms : relative norm equation

$\left(\frac{a,b}{F}\right)$

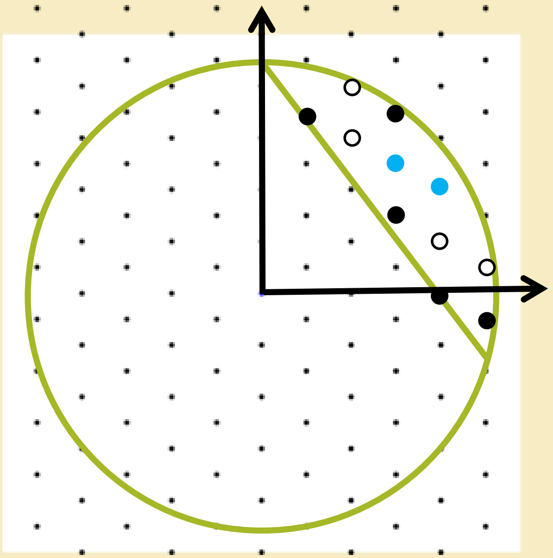
$$q = \underbrace{a_1 + a_2\boldsymbol{i}}_{} + \underbrace{a_3\boldsymbol{j} + a_4\boldsymbol{k}}_{}$$

Step 1. Sampling

$$\|U_q - R_z(\varphi)\| \le \varepsilon$$

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

Lattice from K



Step 2. Norm equation

$$N(q)\mathbb{Z}_F = \mathfrak{p}^L$$

Solve integral relative norm equation in K/F

Idea 1: Do post selection for easy instances

Idea 2: Reduce arbitrary easy instance to constant size instance using LLL

Issue: Algorithm's performance is conjectural

Thanks for listening!

- Polynomial-time algorithm for compiling $O(\log(1/\varepsilon))$-length ε-approximations, which is optimal
- Now we can approximate for Clifford+$\sqrt{T}$, Clifford+T+V and many others
- A general quaternionic framework for producing complete sets of qubit gates that can be compiled by trial division
- The future: qudit, multi-qubit, codes
- Other applications?