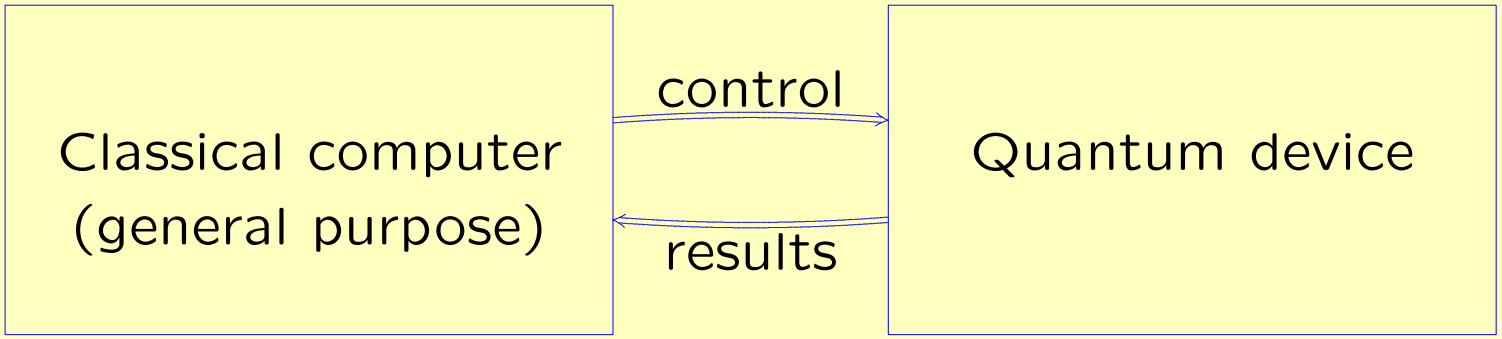
Overview of approximation problems in quantum computing

Peter Selinger

Dalhousie University

Part 1: 10-minute introduction to quantum computing

A schematic quantum computer [Knill96]



- General-purpose classical computer controls a special quantum hardware device
- Quantum device provides a bank of individually addressable qubits.
- Left-to-right: instructions: unitary transformations and measurements.
- Right-to-left: results of the measurements.

Quantum computation: States

- state of one qubit: $\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ (*superposition* of $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$).

- state of two qubits: $\alpha|\mathbf{00}\rangle + \beta|\mathbf{01}\rangle + \gamma|\mathbf{10}\rangle + \delta|\mathbf{11}\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$.

- *independent*: $(a|\mathbf{0}\rangle + b|\mathbf{1}\rangle) \otimes (c|\mathbf{0}\rangle + d|\mathbf{1}\rangle) = ac|\mathbf{00}\rangle + ad|\mathbf{01}\rangle + bc|\mathbf{10}\rangle + bd|\mathbf{11}\rangle.$

- otherwise *entangled*.

Quantum computation: Operations

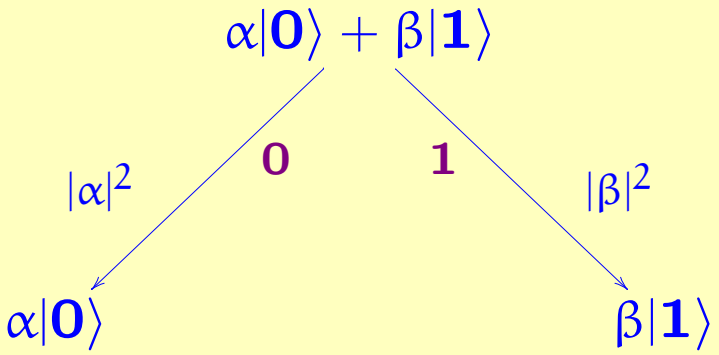
- unitary transformation
- measurement

Some standard unitary gates

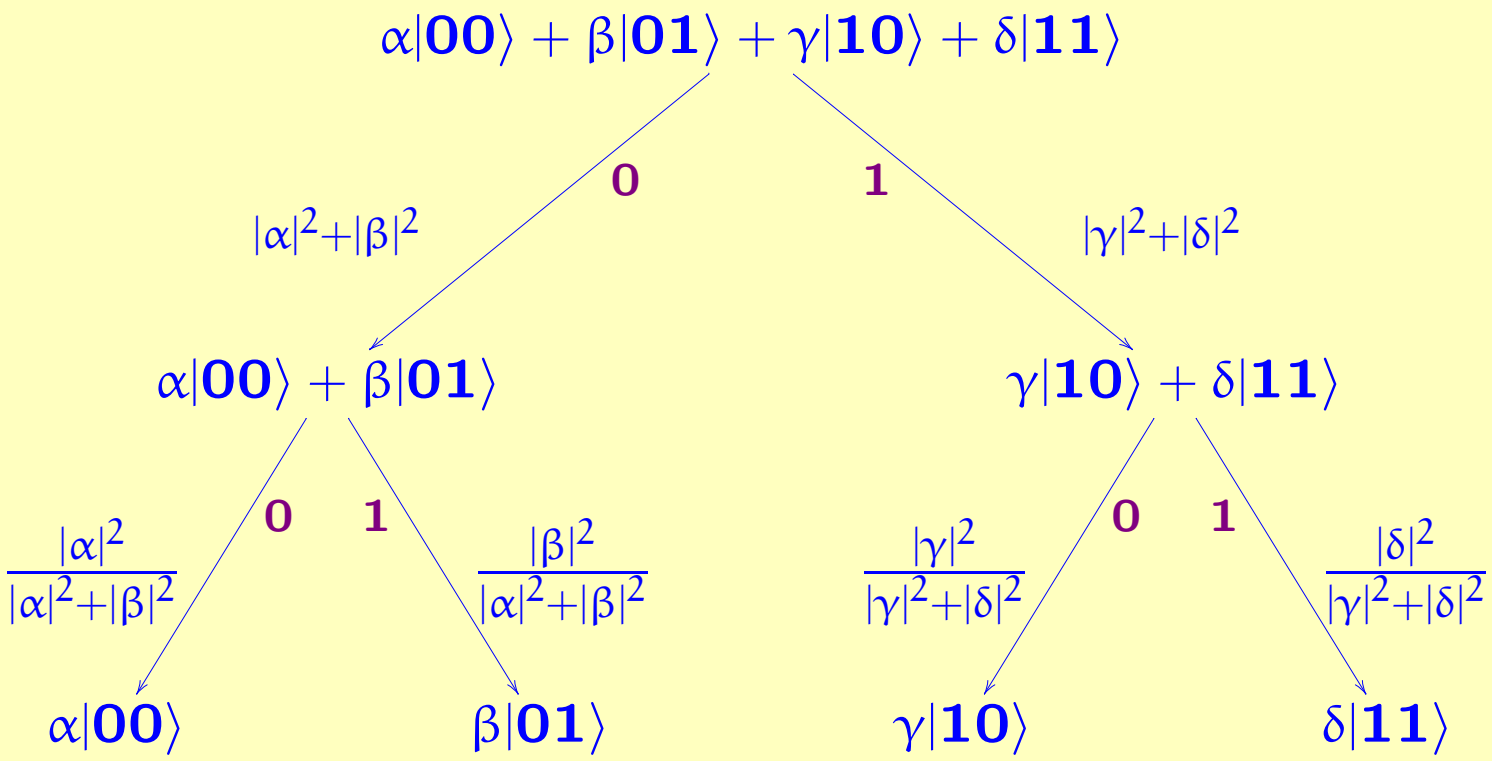
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}, \quad \omega = e^{i\pi/4}$$

Measurement



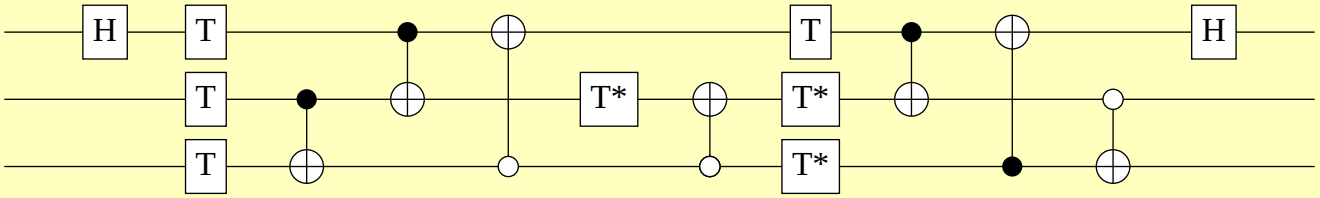
Two Measurements



Note: Normalization convention.

Quantum circuits

A quantum circuit is "a word in the generators".



Motivation for the Clifford+T gate set

- Gottesman-Knill Theorem
- Quantum error correction
- Buhrman-Cleve-Laurent-Linden-Schrijver-Unger 2006.

Part II: The synthesis problems

The synthesis problems

- The *exact synthesis problem* is: given an operator U in the Clifford+T group, decompose it into an actual sequence of gates.

- The *approximate synthesis problem* is: given a unitary operator U and an $\epsilon > 0$, find a sequence of gates that approximates U to within ϵ.

  Moreover, the sequence should be short, and the solution should be computed by an efficient algorithm.

A very brief history

- Lubotzky, Phillips, Sarnak 1986, 1987: Proved that there exist gate sequences of length $O(\log(1/\epsilon))$. The proof is not constructive (no algorithm).
- Solovay, Kitaev, 1995: gave an algorithm for general gate sets that finds sequences of length $O(\log^c(1/\epsilon))$, where $c > 3$.
- Whether c can be reduced to 1 remained open for 17 years.
- Charles, Goren, Lauter 2008: proposed a cryptographic hash function based on the difficulty of this problem (in the p-adic setting: path finding in LPS graphs).
- Petit, Lauter, Quisquater 2008: broke the cryptographic hash function.
- 2012+: new class of efficient number-theoretic algorithms solve the approximate synthesis problem with $O(\log(1/\epsilon))$ gates [Kliuchnikov-Maslov-Mosca, Ross-Selinger, ...]

Some relevant rings

- $\mathbb{Z}$, the ring of *integers*;
- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, the ring of *quadratic integers* with radicand 2;
- $\mathbb{Z}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a, b, c, d \in \mathbb{Z}\}$, the ring of *cyclotomic integers* of degree 8.
- $\mathbb{D}[\omega] = \mathbb{Z}[\delta^{-1}, \omega]$, where $\delta = 1 + \omega$.

Normal form (Matsumoto and Amano)

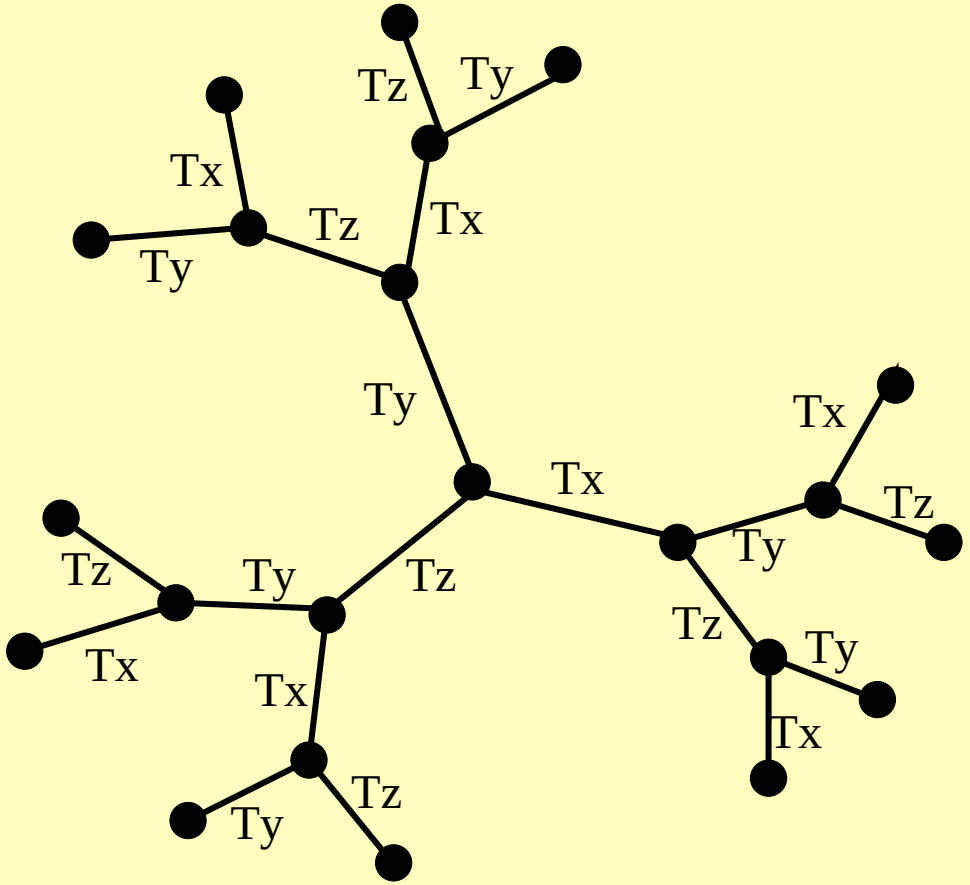
Let $T_x = HTH$, $T_y = SHTHS^{-1}$, and $T_z = T$.

Theorem. Every 2×2 Clifford+T operator can be *uniquely* written in the form

$$T_1 T_2 \dots T_k C,$$

where each $T_i \in \{T_x, T_y, T_z\}$, no two consecutive T_i's are equal, and C is a Clifford operator.

Another way to say this is that the set of Clifford+T operators has the structure of a *regular tree*.



Algebraic characterization of Clifford+T operators

Theorem (Kliuchnikov, Maslov, Mosca 2012a)**.** *The group of 2×2 Clifford+T operators is exactly $U_2(\mathbb{D}[\omega])$.*

Moreover, if $\det U = 1$, the T-count is exactly equal to $k - 2$, where k is minimal such that $U \in \frac{1}{\delta^k}\mathbb{Z}[\omega]$.

Corollary (Exact synthesis)**.** *There is an efficient algorithm for decomposing a Clifford+T operator into a circuit of minimal T-count.*

Approximate synthesis: the Solovay Kitaev algorithm

Solovay-Kitaev algorithm (ca. 1995): *Geometry*.

$$ABA^{-1}B^{-1}.$$

Precision	Solovay-Kitaev	Lower bound
	$O(\log^{3.97}(1/\epsilon))$	$3\log_2(1/\epsilon) + K$
$\epsilon = 10^{-10}$	$\approx 4,000$	≈ 102
$\epsilon = 10^{-20}$	$\approx 60,000$	≈ 198
$\epsilon = 10^{-100}$	$\approx 37,000,000$	≈ 998
$\epsilon = 10^{-1000}$	$\approx 350,000,000,000$	≈ 9966

Information-theoretic lower bound on the T-count

Corollary (Matsumoto and Amano 2008)**.** *There are exactly* $192 \cdot (3 \cdot 2^n - 2)$ *distinct single-qubit Clifford+T operators of T-count at most* n*.*

Corollary. *To approximate an arbitrary operator up to* ϵ *requires T-count at least* $K + 3\log_2(1/\epsilon)$ *in the typical case.*

Proof. Since $SU(2)$ is a 3-dimensional real manifold, it requires $\Omega(1/\epsilon^3)$ epsilon-balls to cover. Let n be the T-count. We have

$$192 \cdot (3 \cdot 2^n - 2) \geq \frac{c}{\epsilon^3},$$

hence

$$n \geq K + 3\log_2(1/\epsilon).$$

Approximate synthesis: Ross-Selinger algorithm

The main idea: We will only approximate diagonal operators, specifically operators of the form:

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

We will approximate them by matrices of the form

$$U = \frac{1}{\sqrt{2}^k} \begin{pmatrix} u & -t^\dagger \\ t & u^\dagger \end{pmatrix},$$

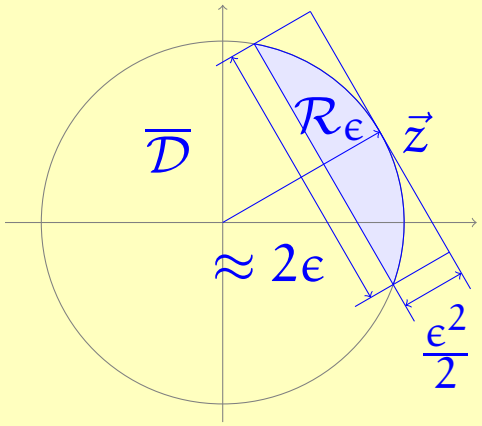
where $u, t \in \mathbb{Z}[\omega]$.

Fact. The error ϵ only depends on u (and not on t). If we set $z = e^{-i\theta/2}$, $u' = \frac{u}{\sqrt{2}^k}$, and $t' = \frac{t}{\sqrt{2}^k}$, the error is:

$$\begin{aligned} \|U - R_z(\theta)\|^2 &= |z - u'|^2 + |t'|^2 \\ &= (z - u')(\bar{z} - \bar{u}')^\dagger + t\bar{t}' \\ &= z\bar{z} - z\bar{u}' - u'\bar{z} + u\bar{u}' + t\bar{t}' \\ &= 2 - 2\,\mathrm{Re}(z\bar{u}'), \end{aligned}$$

therefore

$$\|U - R_z(\theta)\| \leq \epsilon \quad \text{iff} \quad \vec{u}' \cdot \vec{z} \geq 1 - \frac{\epsilon^2}{2}.$$



Moreover, the condition $\mathfrak{u}\mathfrak{u}^\dagger + \mathfrak{t}\mathfrak{t}^\dagger = 1$ implies that $|\mathfrak{u}^\bullet| \leq 1$; here $\bullet : \mathbb{D}[\omega] \to \mathbb{D}[\omega]$ is the automorphism mapping $\omega \to -\omega$.

The exact synthesis problem then reduces to:

(1) **Grid problem:** Finding $\mathfrak{u} \in \mathbb{D}[\omega]$ with small denominator exponent such that $\mathfrak{u} \in \mathbb{R}_\epsilon$ and $|\mathfrak{u}^\bullet| \leq 1$.

(2) **Diophantine problem:** Solving $\mathfrak{t}^\dagger\mathfrak{t} + \mathfrak{u}^\dagger\mathfrak{u} = 1$.

Solutions to problem (1) can be enumerated efficiently in order of increasing k, because this reduces to the problem of finding integer lattice points in a convex set of dimension 4.

Solutions to problem (2) can be calculated efficiently provided that there is an integer factoring oracle. Without factoring, it can still be done efficiently in the *average case* — but this requires a heuristic assumption on the distribution of primes among the solutions to (1).

Results

- In the presence of a factoring oracle (e.g., a quantum computer), the algorithm is *optimal* in an absolute sense: it finds the solution with the smallest possible T-count whatsoever, for the given θ and ϵ.

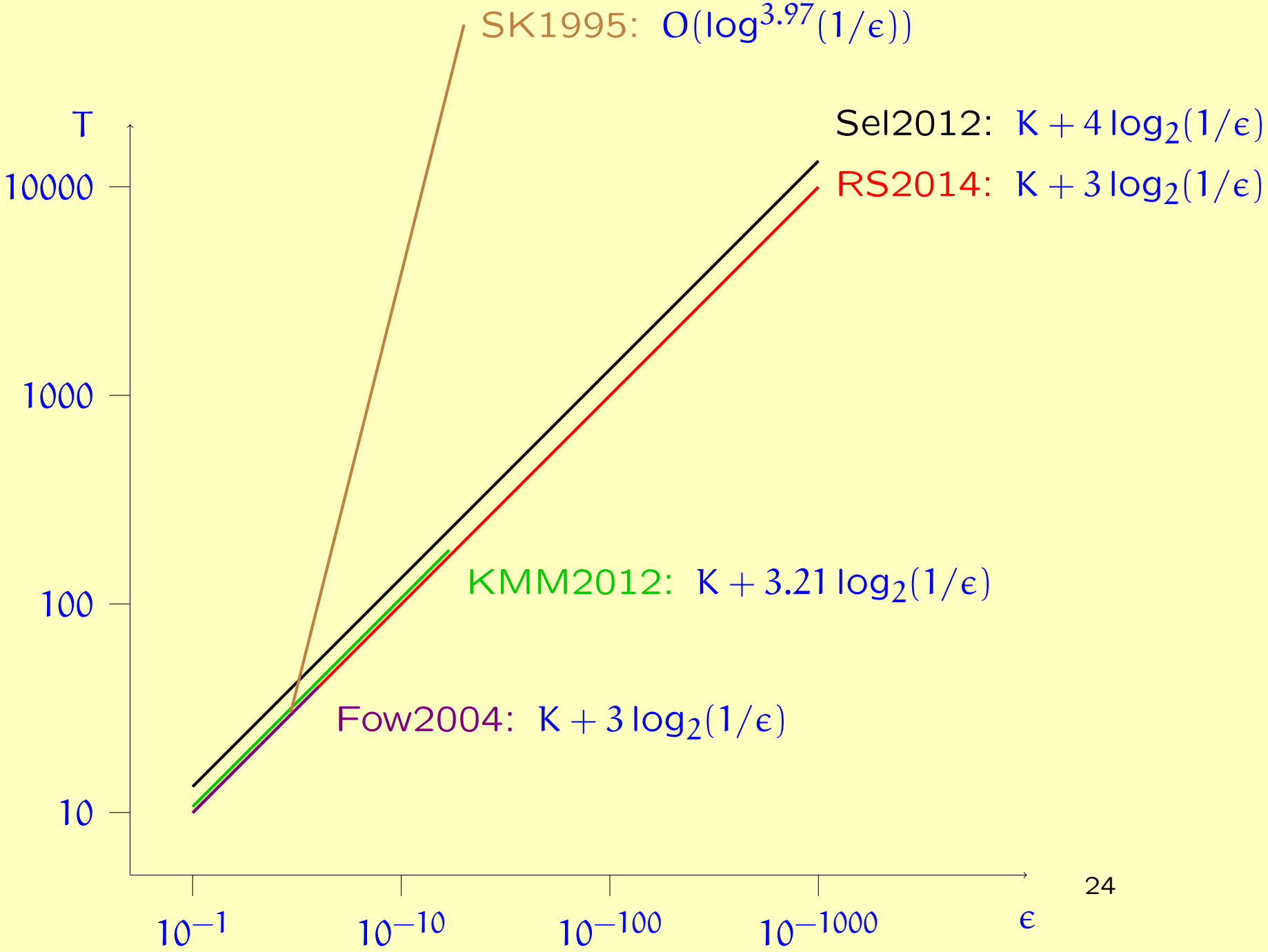
- In the absence of a factoring oracle, the algorithm is *heuristically nearly optimal*: it yields T-counts of $m + O(\log(\log(1/\epsilon)))$, where m is the second-to-optimal T-count.

- The algorithm yields an *upper bound* and a *lower bound* for the T-count of each problem instance.

- The runtime is polynomial in $\log(1/\epsilon)$.

Gate complexity, in numbers.

Precision	Solovay-Kitaev	Lower bound	This algorithm
$\epsilon = 10^{-10}$	$\approx 4,000$	102	102
$\epsilon = 10^{-20}$	$\approx 60,000$	198	200
$\epsilon = 10^{-100}$	$\approx 37,000,000$	998	1000
$\epsilon = 10^{-1000}$	$\approx 350,000,000,000$	9966	9974


SK1995: $O(\log^{3.97}(1/\epsilon))$
Sel2012: $K + 4\log_2(1/\epsilon)$
RS2014: $K + 3\log_2(1/\epsilon)$
KMM2012: $K + 3.21\log_2(1/\epsilon)$
Fow2004: $K + 3\log_2(1/\epsilon)$
T
10000
1000
100
10
10^{-1}
10^{-10}
10^{-100}
10^{-1000}
ϵ

Part III: Problems

- Runtime bound requires strong heuristic assumptions about the distribution of primes. Can these be removed?
- Better synthesis in the non-diagonal case? $3\log(1/\epsilon)$ vs. $4\log(1/\epsilon)$ vs. $6\log(1/\epsilon)$ vs. $9\log(1/\epsilon)$.
- There are "gaps" in the covering, apparently for angles θ satisfying $\tan(\theta/2) \in \mathbf{Q}(\sqrt{2})$, which require $4\log(1/\epsilon)$ gates, whereas all others require $3\log(1/\epsilon)$. Make precise?
- Better synthesis in $n \times n$ case.
- Other approximation methods, such as repeat-until-success, also are subject to similar number-theoretic methods.
- Other gate sets, e.g., Fibonacci (Kliuchnikov, Bocharov, Svore 2013), Clifford+V (Bocharov, Gurevich, Svore 2013; Ross 2015), Clifford+$\sqrt{\mathrm{T}}$. General results e.g. Kliuchnikov, Bocharov, Roetteler, Yard; Parzanchevski, Sarnak.

The end.

[Matsumoto and Amano 2008] K. Matsumoto and K. Amano. Representation of quantum circuits with Clifford and $\pi/8$ gates. arXiv:0806.3834, June 2008.

[Amy et al, 2012] M. Amy, D. Maslov, M. Mosca, and M. Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. arXiv:1206.0758, June 2012.

[Kliuchnikov et al. 2012a] V. Kliuchnikov, D. Maslov, and M. Mosca. Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates. arXiv:1206.5236v2, June 2012.

[Selinger 2012a] P. Selinger. Quantum circuits of T-depth one. *Physical Review A* 87, 042302, 2013. Available from arXiv:1210.0974.

[Giles and Selinger 2012] B. Giles and P. Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Physical Review A* 87, 032332, 2013. Available from arXiv:1212.0506.

[Kliuchnikov et al. 2012b] V. Kliuchnikov, D. Maslov, and M. Mosca. Asymptotically optimal approximation of single qubit unitaries by Clifford and t circuits using a constant number of ancillary qubits. arXiv:1212.0822, Dec. 2012.

[Selinger 2012b] P. Selinger. Efficient Clifford+T approximation of single-qubit operators. arXiv:1212.6253.

[Bocharov et al. 2013] A. Bocharov, Y. Gurevich, K. M. Svore. Efficient Decomposition of Single-Qubit Gates into V Basis Circuits. *Physical Review A* 88, 012303, 2013. Available from arXiv:1303.1411.

[Kliuchnikov 2013] V. Kliuchnikov, Synthesis of unitaries with Clifford+T circuits. arXiv:1306.3200, June 2013.

[Kliuchnikov et al. 2013] V. Kliuchnikov, A. Bocharov, K. M. Svore. Asymptotically Optimal Topological Quantum Compiling. arXiv:1310.4150, October 2013.

[Ross and Selinger 2014] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. arXiv:1403.2975, March 2014.