Beyond Solovay-Kitaev

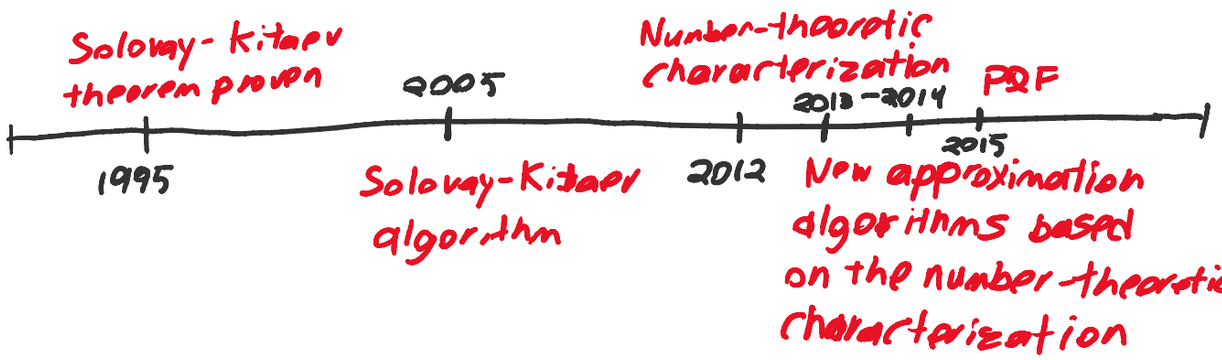
Since gate approximation produces long circuits with many T gates, optimizing single qubit gate approximations in Clifford+T is a fundamental problem in circuit compilation

For many years, the best-known constructive (i.e. produces a circuit) method (Dawson & Nielsen 2005) gave $C > 3$ for $\{H, T\}$. An information-theoretic lower bound of $3\log(1/\epsilon)$ suggested better was possible but wasn't met until the Number theoretic method was developed in 2013-2014. To this day, for $\{H, T\}$ the best known (pure circuit) algorithm is Ross & Selinger (2014)'s Grid-Synth which produces approximations of length

$$3\log(1/\epsilon) + O(\log\log 1/\epsilon)$$

If measurement is allowed, the PQF method of Bocharov, Roetteler & Svore (2015) reduces this to an expected length

$$\log(1/\epsilon) + O(\log\log 1/\epsilon)$$



The Number-theoretic Method

The Number-theoretic method which has resulted in the proliferation of single-qubit approximation algorithms over Clifford+T, other gate sets, new (efficient) gate sets, and a deeper understanding of circuit groups, combines two parts:

1. A (constructive) characterization of circuits over a gate set G as unitaries over an (algebraic number) ring R
2. Approximation of unitaries by "rounding off" into the ring R

We will cover the first part in depth, and sketch a method for part 2.

Thm. (Giles-Selinger)

Let $\mathbb{Z}[i, 1/\sqrt{2}] = \{\frac{1}{\sqrt{2}^n}(a+ib+(c+id)\sqrt{2}) \mid n \in \mathbb{N}, a,b,c,d \in \mathbb{Z}\}$.

A $2^n \times 2^n$ unitary matrix U can be implemented as a Clifford+T circuit, possibly with ancillas, if and only if $U \in M_{2^n}(\mathbb{Z}[i, 1/\sqrt{2}])$. That is, U has all entries contained in $\mathbb{Z}[i, 1/\sqrt{2}]$.

(historical context)

The Giles-Selinger theorem was first proven in the 1-qubit case and conjectured to hold for n-qubits by Kliuchnikov, Maslov, & Mosca (2012, arXiv:1206.5236). The Giles-Selinger presentation (2012, arXiv:1212.0506) is much cleaner however so we follow it.

Algebra

(Rings)

A ring $R = (S, +, \cdot)$ is a set S equipped with binary operators $+, \cdot$ such that

$$\left.\begin{aligned} (a+b)+c &= a+(b+c) \\ a+b &= b+a \\ a+0 &= a \\ a+(-a) &= 0 \end{aligned}\right\} (S,+) \text{ is a group}$$

$$\left.\begin{aligned} (a\cdot b)\cdot c &= a\cdot(b\cdot c) \\ a\cdot 1 &= a = 1\cdot a \end{aligned}\right\} (S,\cdot) \text{ is a monoid}$$

$$\left.\begin{aligned} a\cdot(b+c) &= ab+ac \\ (b+c)\cdot a &= ba+ca \end{aligned}\right\} \cdot \text{ distributes over } +$$

Ex.
The following are rings:

$\mathbb{Z}$ (the integers)
$\mathbb{R}$ (real numbers)
$\mathbb{Q}$ (rational numbers)

$\mathbb{Z}_2 = (\{0,1\}, \oplus, \cdot)$ i.e. addition & mult. mod 2

$\mathbb{Z}_n = (\{0,\dots,n-1\}, a+b \bmod n, a\cdot b \bmod n)$

$\mathbb{D} = (\{a/2^b \mid a,b \in \mathbb{Z}\}, +, \cdot)$ ← regular add & mult

↖ Dyadic fractions like $1/2$, $5/1028$, 17, $1/64$

(Ring extensions)

Roughly speaking, for a ring R and $\alpha \notin R$, $R[\alpha]$ denotes the ring obtained by "adding α to R."

Ex. The following are ring extensions

$\mathbb{Z}[1/2] = \mathbb{D}$ (note that $1/2 \in \mathbb{Z}[1/2]$, so $1/2 \cdot 1/2 \in \mathbb{Z}[1/2]$)

$\mathbb{Z}[i, 1/\sqrt{2}] = \mathbb{Z}[i][1/\sqrt{2}]$

$\mathbb{D}[w] = \{aw^3 + bw^2 + cw + d \mid w = e^{i\pi/4}, a,b,c,d \in \mathbb{D}\}$

Unitaries over rings

Fact

Any circuit over $\{H, CNOT, T\}$ (Clifford+T) corresponds to a unitary with entries in the ring $\mathbb{Z}[i, 1/\sqrt{2}]$. In particular,

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & w \end{bmatrix}$$

Note that $w = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}$, so each gate is a unitary over $\mathbb{Z}[i, 1/\sqrt{2}]$. Since $\mathbb{Z}[i, 1/\sqrt{2}]$ is a ring, multiplying two matrices over $\mathbb{Z}[i, 1/\sqrt{2}]$ produces a matrix over $\mathbb{Z}[i, 1/\sqrt{2}]$.

Note

Since $w = \frac{1+i}{\sqrt{2}}$, $w^* = w^7 = \frac{1-i}{\sqrt{2}}$, hence $\frac{w+w^*}{2} = \frac{1}{\sqrt{2}}$.

So it follows that $\mathbb{Z}[i, 1/\sqrt{2}] = \mathbb{D}[w]$ which is more convenient to work with.

We have one direction of the proof with the above fact. To prove the other direction, we want a procedure (exact synthesis algorithm) that takes a unitary over $\mathbb{D}[w]$ and produces a circuit over Clifford+T.

the basic idea is the same as CNOT + single qubit unitary synthesis: use two-level matrices to reduce one column v to $\begin{bmatrix} ! \\ ? \\ \vdots \\ 0 \end{bmatrix}$ at a time

Exact Synthesis

In CNOT + single qubit Synthesis, we had access to any two-level matrix which could be used to map

$$\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \xrightarrow{U} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

In Clifford + T, we only have 2 moves:

$$\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \xrightarrow{H} \frac{1}{\sqrt{2}} \begin{bmatrix} u_1 + u_2 \\ u_1 - u_2 \end{bmatrix}$$

$$\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \xrightarrow{T} \begin{bmatrix} u_1 \\ \omega u_2 \end{bmatrix}$$

The game is to alternate between rotating the phases of rows and then adding rows of similar magnitudes so that we can hopefully zero them out

(think 2048...)

Ex.

Consider the column $u = \begin{bmatrix} 1/\sqrt{2} \\ 1/2 \\ \omega/2 \\ 0 \end{bmatrix}$

To get $u \to \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ we intuitively need to sum the 2nd and 3rd rows first since they have the same magnitudes

However,

$$1 + \omega \neq 0$$
$$1 - \omega \neq 0$$

so we first need to rotate their relative phases.

$$\begin{bmatrix} 1/\sqrt{2} \\ 1/2 \\ \omega/2 \\ 0 \end{bmatrix} \xrightarrow{T_{2,3}} \begin{bmatrix} 1/\sqrt{2} \\ 1/2 \\ \omega/2 \\ 0 \end{bmatrix} \xrightarrow{H_{2,3}} \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \\ 0 \end{bmatrix} \xrightarrow{H_{1,2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

We use powers of $\frac{1}{\sqrt{2}}$ (the lde) to guide pairing

Denominator exponents

Defn

$\mathbb{Z}[w] = \{aw^3 + bw^2 + cw + d \mid a,b,c,d \in \mathbb{Z}\}$
is the ring of integers of $\mathbb{D}[w]$

Ex.
The following are elements of $\mathbb{Z}[w]$:
$\sqrt{2} = -w^3 + w$ $\quad w^4 = -1$
$i = w^2$ $\quad w^* = w^7 = -w^3$
However, $1/\sqrt{2} \notin \mathbb{Z}[w]$

Fact

For any $u \in \mathbb{D}[w]$, there exists k s.t.
$\sqrt{2}^k u \in \mathbb{Z}[w]$

Explicitly, if $q/2^b \in \mathbb{D}$, then $\sqrt{2}^k \, q/2^b \in \mathbb{Z}$
for any $k \geq 2b$

Defn (lde)

– roughly, high lde means small magnitude. Highest lde's paired first

Let $u \in \mathbb{D}[w]$. The least denominator exponent of u is the smallest k s.t. $\sqrt{2}^k u \in \mathbb{Z}[w]$, denoted by $\text{lde}(u)$

Ex.
$\text{lde}(1/\sqrt{2}) = 1$ since $\sqrt{2} \cdot 1/\sqrt{2} = 1 \in \mathbb{Z}[w]$
$\text{lde}(i/2 + w/\sqrt{2}) = 2$ since $\sqrt{2}^2 \cdot (i/2 + w/\sqrt{2}) = i + \sqrt{2}w \in \mathbb{Z}[w]$
$= 1 + 2i$
↖ higher lde / smaller magnitude

Denominator exponents of vectors

(lde of a vector)

Let $\vec{u}$ be a vector over $\mathbb{D}[\omega]$. $\text{lde}(\vec{u})$ is the smallest k s.t. $\sqrt{2}^k * \vec{u}$ is a vector over $\mathbb{Z}[\omega]$

Ex.

$\text{lde}\left(\begin{bmatrix}1\\0\end{bmatrix}\right) = 0$

$\text{lde}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\right) = 1$ (note: $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = H\begin{bmatrix}1\\0\end{bmatrix}$)

$\text{lde}\left(\begin{bmatrix}1\\1/\sqrt{3}\\1/\sqrt{6}\end{bmatrix}\right) = 1$ (since $\sqrt{2} \in \mathbb{Z}[\omega]$)

$\text{lde}\left(\frac{1}{2}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}\right) = 2$

Single-qubit synthesis

Armed with the lde, we can now tackle the problem of single qubit synthesis over $\mathbb{D}[w]$.
Recall that a single-qubit unitary can be written as

$$U = \begin{bmatrix} a & -e^{i\theta}b^* \\ b & e^{i\theta}a^* \end{bmatrix}$$

We focus on the first column for now, i.e. finding some $U_1 \cdots U_k \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Lemma (lde-0-case)

Let u be a 2-dimensional unit vector over $\mathbb{Z}[w]$.
Then $u = \begin{bmatrix} w^k \\ 0 \end{bmatrix}$ or $\begin{bmatrix} 0 \\ w^k \end{bmatrix}$ for some $k \geq 0$

Pf

The idea is to use the constraints imposed by $\|u\| = 1$
Note that if $u = [u_1 \; u_2]^T$,

$$\|u\|^2 = u_1 u_1^* + u_2 u_2^* = |u_1|^2 + |u_2|^2$$

It can be shown that if $u = aw^3 + bw^2 + cw + d$, then

$$|u|^2 = a^2 + b^2 + c^2 + d^2 + (cd + bc + ab - da)\sqrt{2} \quad \text{(important)}$$

Since $\|u\|^2 = 1$, the $\sqrt{2}$ parts of $|u_1|^2$ & $|u_2|^2$ cancel. Now, $a^2 + b^2 + c^2 + d^2 \in \mathbb{Z}^+$ when $a, b, c, d \in \mathbb{Z}$, so only 1 of u_1 & u_2 can be non-zero - i.e. $u = \begin{bmatrix} v \\ 0 \end{bmatrix}$ or $\begin{bmatrix} 0 \\ v \end{bmatrix}$, $|v|^2 = 1$
Now, $|v|^2 = 1 \Rightarrow a^2 + b^2 + c^2 + d^2 = 1 \Rightarrow$ only one entry is non-zero, and in particular $v = w^k$, $0 \leq k \leq 7$.

Note: if $u = \begin{bmatrix} w^k \\ 0 \end{bmatrix}$, then $XT^{-k}Xu = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

$u = \begin{bmatrix} 0 \\ w^k \end{bmatrix}$, then $XT^{-k}u = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Single-qubit cont.

Lemma (lde-k-case)

weather condition suffices...

Let u be a 2-dimensional ~~unit~~ vector in $\mathbb{D}[\omega]$ with $lde(u) > 0$. Then there exists a sequence of H & T gates $U_1 \cdots U_k$ s.t. $lde(U_1 \cdots U_k u) < lde(u)$.

(reducibility)

For this proof it will be helpful to define reducibility (mod $\sqrt{2}$). We say a vector v in $\mathbb{Z}[\omega]^2$ is reducible if $v = \sqrt{2}\, v'$, v' in $\mathbb{Z}[\omega]^2$.

Given $v = \sqrt{2}^{lde(u)} u$, our goal is to find $U_1 \cdots U_k$ s.t. $U_1 \cdots U_k v$ is reducible, since

$$U_1 \cdots U_k v = \sqrt{2}\, v' = \sqrt{2}^{lde(u)} U_1 \cdots U_k u$$

$$\Downarrow$$

$$v' = \sqrt{2}^{lde(u)-1} U_1 \cdots U_k u$$

Ex.

Let $u = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ i \end{bmatrix}$ and let $v = \sqrt{2}u = \begin{bmatrix} 1 \\ i \end{bmatrix}$. Then

$$Hv = \frac{1}{\sqrt{2}}\begin{bmatrix} 1+i \\ 1-i \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 2 \\ 0 \end{bmatrix} = \sqrt{2}\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Proof of lde-k-case

Let $v = \sqrt{2}^{\,lde(u)}\, u$, so v has entries in $\mathbb{Z}[w]$.

We know $\|v\| = \|\sqrt{2}^{\,lde(u)} u\| = 2^m$ for $m > 0$.

Now if $v = [v_1\ v_2]^T$, then we know:

① The $\sqrt{2}$-parts of $|v_1|^2$ & $|v_2|^2$ cancel

② $|v_1|^2 \equiv |v_2|^2 \bmod 2$

Notice that if $v_1 \equiv v_2 \bmod 2$, then $v_1 \pm v_2 \equiv 0 \bmod 2$, hence Hv is reducible:

$$Hv = \frac{1}{\sqrt{2}} \begin{bmatrix} v_1 + v_2 \\ v_1 - v_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 2v_1' \\ 2v_2' \end{bmatrix} = \sqrt{2}\, v'$$

Our immediate goal is to "make" $v_1 \equiv v_2 \bmod 2$.

Let $|v_1|^2 = a + b\sqrt{2}$, $|v_2|^2 = c + d\sqrt{2}$, $a, b, c, d \in \mathbb{Z}$. By ② above,

③ $a \equiv b \bmod 2$

④ $c \equiv d \bmod 2$

Case 1: $a \equiv b \equiv c \equiv d \equiv 0 \bmod 2$

Let $v_1 = a_1 w^3 + a_2 w^2 + a_3 w + a_4$, so $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$

$$b = a_1 a_2 + a_2 a_3 + a_3 a_4 - a_1 a_4$$

That $a \equiv b \equiv 0 \bmod 2$ tells us that either

① all of a_i are even, so v_1 is reducible

② all of a_i are odd, so

$$\sqrt{2}\, v_1 = (w - w^3) v_1 = (a_0 - a_4) w^3 + (a_0 + a_1) w^2 + (a_4 + a_3) w + (a_3 - a_1)$$
$$\equiv 2 v_1'$$
$$\therefore v_1 = \sqrt{2}\, v_1', \text{ i.e. } v_1 \text{ is reducible}$$

③ only non-adjacent a_i, a_j are odd. Then

$v_1 \equiv w^k (1 + i) \bmod 2$ for some k.

Since $w^k (1+i) = w^k \sqrt{2}$, $v_1 = \sqrt{2}(w^k + \sqrt{2} v_1')$, hence v_1 is reducible

So, both v_1 & v_2 are reducible and the case is finished

Ide-k-case cont.

Case 2: $a \equiv c \equiv 0 \bmod 2$, $b \equiv d \equiv 1 \bmod 2$.

Letting $v_1 = a_1w^3 + a_2w^2 + a_3w + a_4$ again, we know evenly many a_i are odd. $a_1a_2 + a_2a_3 + a_3a_4 - a_4a_1 \equiv 1 \bmod 2$ tells us that

$$v_1 \equiv w^k(1+w) \bmod 2 \text{ for some } k$$

By the same argument, $v_2 \equiv w^j(1+w) \bmod 2$. Now

$$w^{k-j}v_2 \equiv v_1 \bmod 2.$$

since $T^{k-j}\begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = \begin{bmatrix} v_1 \\ w^{k-j}v_2 \end{bmatrix}$, $T^{k-j}V$ is reducible.

Case 3: $a \equiv b \equiv c \equiv d \equiv 1 \bmod 2$

Letting $v_1 = a_1w^3 + a_2w^2 + a_3w + a_4$, we see that an odd number of a_i's are odd. Any such choice gives $b = a_1a_2 + a_2a_3 + a_3a_4 - a_4a_5 \equiv 0 \bmod 2$, so this case is impossible.

LDE-k-cast cont.

Case 3: $a \equiv c \equiv 1 \bmod 2$, $b \equiv d \equiv 0 \bmod 2$

Letting $v_1 = a_1 w^3 + a_2 w^2 + a_3 w + a_4$, $a \equiv 1 \bmod 2$ & $b \equiv 0 \bmod 2$ imply that an odd number of a_i's are odd, so

$$v_1 \equiv w^k \text{ or } w^k(1+w+i) \bmod 2$$
$$v_2 \equiv w^j \text{ or } w^j(1+w+i) \bmod 2$$

If $v_1 \equiv w^k \bmod 2$ & $v_2 \equiv w^j \bmod 2$ or
$v_1 \equiv w^k(1+w+i) \bmod 2$ & $v_2 \equiv w^j(1+w+i) \bmod 2$,
then $v_1 \equiv w^{k-j} v_2 \bmod 2$, so $T^{k-j} v$ is reducible

Otherwise, WLOG $v_1 \equiv w^k \bmod 2$ & $v_2 = w^j(1+w+i) \bmod 2$.

Let $v_1' = v_1 + w^{k-i+1} v_2$, $v_2' = v_1 - w^{k-i+1} v_2$, so

$$v_1' \equiv w^k + w^{k+1}(1+w+i) \bmod 2$$
$$\equiv w^k(1+w+i+w) \bmod 2$$
$$\equiv 1+w+i+w^3 \bmod 2$$

$$v_2' \equiv w^k + w^{k+1}(1+w+i) \bmod 2$$
$$\equiv w^k(1+w+i+w^3) \bmod 2$$
$$\equiv 1+w+i+w^3 \bmod 2$$

By the first case, v_1' & v_2' are both reducible, and if $v_1' = \sqrt{2}\, v_1''$, then

$$1+w+i+w^3 \equiv (w-w^2)(aw^3+bw^2+cw+d) \bmod 2$$
$$\equiv (b-d)w^3 + (c+a)w^2 + (d+b)w + (c-a) \bmod 2$$

So $b+d \equiv c+a \equiv 1 \bmod 2$, hence $v_1'' \equiv w^n(1+w) \bmod 2$
$v_2'' \equiv w^n(1+w) \bmod 2$

So $v_1'' \equiv w^{m-n} v_2'' \bmod 2$, and

$$T^{m-n} H T^{k-i+1} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = T^{m-n} \frac{1}{\sqrt{2}} \begin{bmatrix} v_1' \\ v_2' \end{bmatrix} = T^{m-n} \begin{bmatrix} v_1'' \\ v_2'' \end{bmatrix}$$
$$= \begin{bmatrix} v_1'' \\ w^{m-n} v_2'' \end{bmatrix}$$

$\therefore$ $T^{m-n} H T^{k-i+1} v$ is reducible

Exact synthesis

The hard part is over now ☺
Let's start with single qubit case

Thm

Let u be a unit vector in $\mathbb{D}[w]^2$. Then $\exists U_1 \cdots U_k$ from $\{H, T\}$ such that $U_1 \cdots U_k u = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

Pf

By induction on $lde(u)$ using the previous two lemmas.

For the n-qubit case, we extend this to a column lemma using two-level operators of the form $H_{i,j}$ & $T_{i,j}$

Thm (column lemma)

Let u be a unit vector in $\mathbb{D}[w]^d$. Then there exists
- sequence $U_1 \cdots U_k$ of two-level, dxd gates $H_{i,j}$ & $T_{i,j}$

such that $U_1 \cdots U_k u = \begin{bmatrix} 1 \\ \vdots \\ 0 \end{bmatrix}$

Pf

By induction on $lde(u)$. If $lde(u) = 0$, then $u = w^k e_i$, so $X_{a,i} T_{a,i}^k = H_{b,i} T_{a,i}^4 H_{a,i} T_{a,i}^k$ suffices.

If $lde(u) = k \geq 1$, let $v = \sqrt{2}^k u$. Then

$$2^k = \|v\|^2 = |v_1|^2 + \cdots + |v_d|^2$$

$$\Rightarrow |v_1|^2 + \cdots + |v_d|^2 \equiv 0 \bmod 2$$

Since for any $|v|^2 = a + b\sqrt{2}$, we can't have $a \equiv b \equiv 1 \bmod 2$, there exist i, j s.t. $|v_i|^2 \equiv |v_j|^2 \bmod 2$. Use the lde-k lemma with $u = \begin{bmatrix} u_i \\ u_j \end{bmatrix}$ and repeat in pairs until every v_i is reducible.

Finishing the job

Recall that all we need to synthesize over two-level operators is a column lemma, so here's where we are

Unitaries over $\mathbb{D}[\omega]$

↓ Done!

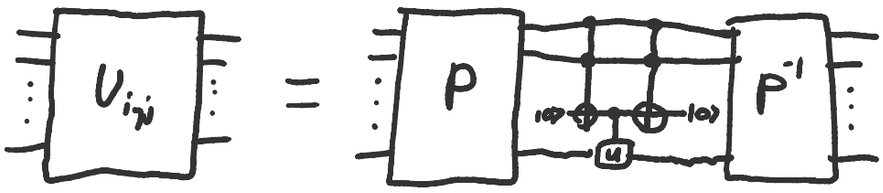
Two-level $\{H, T\}$ matrices

↓ still need to do

Clifford + T

(Decomposition of two-level H & T)

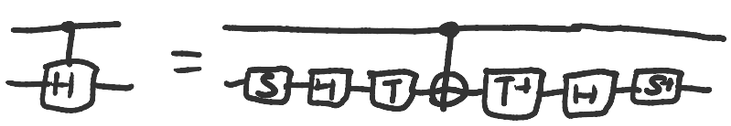
Recall that any 2-level unitary can be decomposed as a controlled gate and Toffolis, i.e.



Since the Toffoli has a known Clifford+T implementation, we only need controlled-H and-T.

For controlled-T, note that T is actually controlled-ωI, so

For controlled-H, $H = S^\dagger H T^\dagger X T H S$ ← why? so



Complexity analysis

It turns out that this is optimal for single-qubit unitaries
For n-qubit unitaries however it produces very inefficient circuits.

Prop.

For an n-qubit matrix U over $\mathbb{D}[\omega]$, The Giles-Selinger algorithm produces circuits of size $O(3^{2n}k)$ where $k = lde(U)$

Note

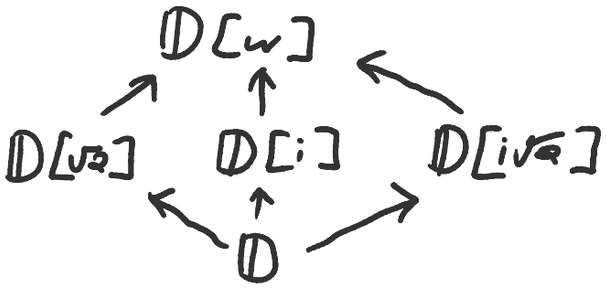
Kliuchnikov 2013 - Synthesis of unitaries with Clifford+T (arXiv:1306.3200)

reduced this to $O(4^n nk)$ using reflection operators.

(this is a really cool method ☺)

Other correspondences

Number-theoretic characterization has led to some other interesting correspondences. In particular, the (partial) lattice of sub-rings



of $\mathbb{D}[\omega]$ has similarly been characterized:

- $\mathbb{D}[\sqrt{2}] \equiv \{X, CX, CCX, H, CH\}$
- $\mathbb{D} \equiv \{X, CX, CCX, H \otimes H\}$
- $\mathbb{D}[i] \equiv \{X, CX, CCX, \omega H, S\}$
- $\mathbb{D}[i\sqrt{2}] \equiv \{X, CX, CCX, F \propto \sqrt{H}\}$

Ring round-off & Grid-synth

Since a circuit over Clifford+T corresponds precisely to a unitary over $\mathbb{D}[\omega]$, we can approximate U by finding V with entries in $\mathbb{D}[\omega]$ such that

$$\|U - V\| \leq \epsilon$$

This is called the round-off problem. Ross & Selinger (2014, arXiv:1403.2975) famously gave an effectively optimal algorithm for rounding off $R_z(\theta)$ rotations into $\mathbb{D}[\omega]$, called Grid-synth.

Thm (Ross-Selinger) (over Clifford+T)

An $R_z(\theta)$ gate can be approximated optimally via $\mathbb{D}[\omega]$ and exact synthesis given a factoring oracle, or with typical length $3\log_2(1/\epsilon) + O(\log(\log(1/\epsilon)))$.

Pf

Very far outside our scope...

The idea is to find some $u \in \mathbb{D}[\omega]$ in an ϵ-region of the unit circle with minimal lde

This is shown to be poly-time enumerable.

Then, try to find $t \in \mathbb{D}[\omega]$ s.t. $\begin{bmatrix} u \\ t \end{bmatrix}$ is a unit vector.

requires solving a diophantine equation $|t|^2 = 1 - |u|^2$