Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets

Simon Forest
David Gosset
Vadym Kliuchnikov
David McKinnon

arXiv:1501.04944
They're swift and slippery, but researchers are beginning to get them under control.

Quantum Computers

Image source: Chemical and Engineering News, November 6, 2000
A fault-tolerant quantum computer will directly implement gates from some finite universal gate set $G$. Often we’ll want to approximate gates which are not in this set.

In theory we know that this can be done efficiently because of the Solovay-Kitaev theorem.

How efficiently? Can we reduce the resource requirements?
Approximate synthesis of single-qubit unitaries

Goal: efficiently approximate a given single-qubit unitary $U$ by a sequence of gates from some finite single-qubit universal gate set $\mathcal{G}$, to within an error tolerance $\epsilon$.

$$\|U - W_1 W_2 \ldots W_M\| \leq \epsilon \quad W_i \in \mathcal{G}$$
Goal: efficiently approximate a given single-qubit unitary $U$ by a sequence of gates from some finite single-qubit universal gate set $\mathcal{G}$, to within an error tolerance $\epsilon$.

$$\| U - W_1 W_2 \ldots W_M \| \leq \epsilon \quad W_i \in \mathcal{G}$$

To reduce quantum overhead we want $M$ as small as possible.
**Approximate synthesis of single-qubit unitaries**

**Goal:** efficiently approximate a given single-qubit unitary $U$ by a sequence of gates from some finite single-qubit universal gate set $\mathcal{G}$, to within an error tolerance $\epsilon$.

$$\|U - W_1 W_2 \ldots W_M\| \leq \epsilon \quad \forall W_i \in \mathcal{G}$$

To reduce quantum overhead we want $M$ as small as possible.

**Solution 1: Solovay-Kitaev algorithm**

**Pro:** Efficient for almost any finite universal gate set $\mathcal{G}$.

**Con:** Outputs gate sequence of length $M = O\left(\log^c \left(\frac{1}{\epsilon}\right)\right)$ where $c \sim 4$. Not asymptotically optimal! Want $c = 1$.

[Dawson, Nielsen 2006]
Approximate synthesis of single-qubit unitaries

**Goal:** Efficiently approximate a given single-qubit unitary $U$ by a sequence of gates from some finite single-qubit universal gate set $\mathcal{G}$, to within an error tolerance $\epsilon$.

$$\|U - W_1 W_2 ... W_M\| \leq \epsilon \quad W_i \in \mathcal{G}$$

To reduce quantum overhead we want $M$ as small as possible.

**Solution 2: New algorithms which exploit algebraic number theory**

**Pro:** Asymptotically optimal decompositions $M = O\left(\log \left(\frac{1}{\epsilon}\right)\right)$.

**Con:** Only works for specific gate sets $\mathcal{G}$. Efficiency contingent on number theory conjecture.
The first asymptotically optimal approximate synthesis algorithm (with no ancilla) was obtained in 2012 by Selinger, building on work of Kliuchnikov, Maslov, and Mosca.

It approximates a given single-qubit unitary over the “Clifford+T” gate set…
Clifford+T gate set

\[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \]

Single-qubit Clifford group \[ e = \langle H, S \rangle \]

Clifford+T group \[ G_4 = \langle e, T \rangle \]
Clifford+T gate set

\[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \]

Single-qubit Clifford group \( \mathcal{C} = \langle H, S \rangle \)

Clifford+T group \( G_4 = \langle \mathcal{C}, T \rangle \)

Unitaries \( U \in G_4 \) are said to be exactly synthesizable. Such unitaries can be written without error as a product of Clifford and T gates.
Overview of the approximate synthesis algorithm for Clifford+T

The approximate synthesis algorithm is based on three ingredients:

(a) Efficient exact synthesis algorithm [Kliuchnikov, Maslov, Mosca 2012]

\[ U \in G_4 \xrightarrow{	ext{Exact Synthesis}} C_1 T C_2 T \ldots T C_m \]

Optimal decomposition of \( U \)
Overview of the approximate synthesis algorithm for Clifford+T

The approximate synthesis algorithm is based on three ingredients:

(a) Efficient exact synthesis algorithm [Kliuchnikov, Maslov, Mosca 2012]

\[ U \in G_4 \quad \text{Exact Synthesis} \quad C_1 T C_2 T \ldots T C_m \]

Optimal decomposition of \( U \)

(b) Number-theoretic characterization of exactly synthesizable unitaries [Kliuchnikov, Maslov, Mosca 2012]

\[ G_4 = U_2(\mathcal{R}_4) = \text{Group of all } 2 \times 2 \text{ unitaries with entries in the ring } \mathcal{R}_4 = \mathbb{Z}[e^{i\pi/4}, 1/2] \]
Overview of the approximate synthesis algorithm for Clifford+T

The approximate synthesis algorithm is based on three ingredients:

(a) Efficient exact synthesis algorithm [Kliuchnikov, Maslov, Mosca 2012]

\[ U \in G_4 \rightarrow \text{Exact Synthesis} \rightarrow C_1TC_2T...TC_m \]

Optimal decomposition of \( U \)

(b) Number-theoretic characterization of exactly synthesizable unitaries [Kliuchnikov, Maslov, Mosca 2012]

\[ G_4 = U_2(\mathcal{R}_4) = \text{Group of all } 2 \times 2 \text{ unitaries with entries in the ring } \mathcal{R}_4 = \mathbb{Z}[e^{i\pi/4}, 1/2] \]

The smallest ring which contains the matrix elements of the generators.

Consists of numbers of the form \[ \frac{a+bi+c\sqrt{2}+di\sqrt{2}}{\sqrt{2}^k} \]
Overview of the approximate synthesis algorithm for Clifford+T

The approximate synthesis algorithm is based on three ingredients:

(a) Efficient exact synthesis algorithm [Kliuchnikov, Maslov, Mosca 2012]

\[ U \in G_4 \quad \text{Exact Synthesis} \quad C_1TC_2T \ldots TC_m \]

Optimal decomposition of \( U \)

(b) Number-theoretic characterization of exactly synthesizable unitaries [Kliuchnikov, Maslov, Mosca 2012]

\[ G_4 = U_2(\mathcal{R}_4) = \text{Group of all } 2 \times 2 \text{ unitaries with entries in the ring } \mathcal{R}_4 = \mathbb{Z}[e^{i\pi/4}, 1/2] \]

(c) Efficient rounding algorithm [Selinger 2012]

\[ W \in U_2(\mathcal{R}_4) = G_4 \]

\( \epsilon \)-approximation of \( V \)
Overview of the approximate synthesis algorithm for Clifford+T

Putting the ingredients together [Selinger 2012]

\[ V, \varepsilon \]

- **Rounding**
  \[ W \in U_2(\mathcal{R}_4) = G_4 \]
  \( \varepsilon \)-approximation of \( V \)

- **Optimal decomposition of** \( W \)

\[ C_1 TC_2 T \ldots TC_m \]

A similar strategy has since been developed for a handful of other gate sets.
In our paper we look at an infinite family of gate sets which includes Clifford+T as a special case. We are interested in whether the three ingredients can be generalized:

(a) Exact synthesis algorithm
(b) Number theoretic characterization of exactly synthesizable unitaries
(c) Efficient rounding algorithm

Summary:
We generalize (a) for each gate set we consider, show that (b) holds only for some of the gate sets, and we leave (c) as a question for future work.
Definitions and Results

Exact synthesis algorithm

Number theoretic characterization
Clifford-cyclotomic gate sets

Unconventional choice of global phase
Will matter only for the number theoretic characterization.

\[ H = \frac{e^{i\pi/4}}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad U_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/n} \end{pmatrix} \]

Single-qubit Clifford group \( \mathcal{E} = \langle H, S \rangle \)

Clifford-cyclotomic groups \( G_n = \langle \mathcal{E}, U_n \rangle \)
Clifford-cyclotomic gate sets

\[ H = \frac{e^{i\pi/4}}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad U_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/n} \end{pmatrix} \]

Single-qubit Clifford group \( e = \langle H, S \rangle \)

Clifford-cyclotomic groups \( G_n = \langle e, U_n \rangle \)
Clifford-cyclotomic gate sets

\[
H = \frac{e^{i\pi/4}}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad U_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/n} \end{pmatrix}
\]

Single-qubit Clifford group \( e = \langle H, S \rangle \)

Clifford-cyclotomic groups \( G_n = \langle e, U_n \rangle \)  
Take \( n \) to be an even positive integer (since \( G_n = G_{2n} \) for \( n \) odd)
We focus on exactly synthesizable unitaries (i.e., the groups $G_n$).

Clifford-cyclotomic gate sets

$$H = \frac{e^{i\pi/4}}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad U_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi n} \end{pmatrix}$$

Single-qubit Clifford group $\mathcal{E} = \langle H, S \rangle$

Clifford-cyclotomic groups $G_n = \langle \mathcal{E}, U_n \rangle$ Take $n$ to be an even positive integer (since $G_n = G_{2n}$ for $n$ odd)

We focus on exactly synthesizable unitaries (i.e., the groups $G_n$).
For each $n$ we present an efficient exact synthesis algorithm

$W \in G_n$  

Optimal decomposition of $W$ (up to global phase)

$C_1 U_n^{s_1} C_2 U_n^{s_2} \ldots U_n^{s_m} C_{m+1}$  

$C_i \in \mathcal{C}$
For each $n$ we present an efficient exact synthesis algorithm

\[ W \in G_n \]

\[ \text{Exact Synthesis} \quad \text{Optimal decomposition of } W \]

(up to global phase)

\[ C_1 U_n^{s_1} C_2 U_n^{s_2} \ldots U_n^{s_m} C_{m+1} \quad C_i \in \mathcal{C} \]

Our algorithm is optimal in the sense that it produces decompositions using the minimal number of non-Clifford gates.
For each $n$ we present an efficient exact synthesis algorithm

Our algorithm is optimal in the sense that it produces decompositions using the minimal number of non-Clifford gates.

$$\sum_j s_j$$
Number-theoretic characterization

The smallest ring which contains the matrix elements of the generators of $G_n$ is

$$R_n = \mathbb{Z}[e^{\frac{i\pi}{n}}, 1/2]$$
The smallest ring which contains the matrix elements of the generators of $G_n$ is

$$\mathcal{R}_n = \mathbb{Z}[e^{i\pi/n}, 1/2]$$

Therefore any element of $G_n$ has entries in this ring, i.e.,

$$G_n \subseteq U_2(\mathcal{R}_n)$$

Group of all $2 \times 2$ unitaries with entries in $\mathcal{R}_n$
Number-theoretic characterization

The smallest ring which contains the matrix elements of the generators of $G_n$ is

$$\mathcal{R}_n = \mathbb{Z}[e^{\frac{i\pi}{n}}, 1/2]$$

Therefore any element of $G_n$ has entries in this ring, i.e.,

$$G_n \subseteq U_2(\mathcal{R}_n)$$

Group of all $2 \times 2$ unitaries with entries in $\mathcal{R}_n$

**Theorem (good news)**

$$G_n = U_2(\mathcal{R}_n) \text{ for } n \in \{2, 4, 6, 8, 12\}$$
The smallest ring which contains the matrix elements of the generators of $G_n$ is

$$\mathcal{R}_n = \mathbb{Z}[e^{\frac{i\pi}{n}}, \frac{1}{2}]$$

Therefore any element of $G_n$ has entries in this ring, i.e.,

$$G_n \subseteq U_2(\mathcal{R}_n)$$

Group of all $2 \times 2$ unitaries with entries in $\mathcal{R}_n$

**Theorem (good news)**

$$G_n = U_2(\mathcal{R}_n) \text{ for } n \in \{2, 4, 6, 8, 12\}$$

Previously known

$n = 4$ \hspace{1cm} [Kliuchnikov Maslov Mosca 2012]
The smallest ring which contains the matrix elements of the generators of $G_n$ is
\[ R_n = \mathbb{Z}[e^{\frac{i\pi}{n}}, 1/2] \]
Therefore any element of $G_n$ has entries in this ring, i.e.,
\[ G_n \subseteq U_2(R_n) \]

Group of all $2 \times 2$ unitaries with entries in $R_n$

**Theorem (good news)**
\[ G_n = U_2(R_n) \text{ for } n \in \{2,4,6,8,12\} \]

Previously known

- $n = 4$ [Kliuchnikov Maslov Mosca 2012]
- $n = 6$ [Bocharov, Roetteler, Svore 2014]
The smallest ring which contains the matrix elements of the generators of $G_n$ is

$$\mathcal{R}_n = \mathbb{Z}[e^{\frac{i\pi}{n}}, \frac{1}{2}]$$

Therefore any element of $G_n$ has entries in this ring, i.e.,

$$G_n \subseteq U_2(\mathcal{R}_n)$$

Group of all $2 \times 2$ unitaries with entries in $\mathcal{R}_n$

**Theorem (good news)**

$$G_n = U_2(\mathcal{R}_n) \text{ for } n \in \{2, 4, 6, 8, 12\}$$

Previously known

$n = 4$ [Kliuchnikov Maslov Mosca 2012]

$n = 6$ [Bocharov, Roetteler, Svore 2014]

$n = 4, 6, 8$ [Serre 2009]

Our proof uses an exhaustive computer search.
Number-theoretic characterization

The smallest ring which contains the matrix elements of the generators of $G_n$ is

$$\mathcal{R}_n = \mathbb{Z}[e^{\frac{i\pi}{n}}, \frac{1}{2}]$$

Therefore any element of $G_n$ has entries in this ring, i.e.,

$$G_n \subseteq U_2(\mathcal{R}_n)$$

Group of all $2 \times 2$ unitaries with entries in $\mathcal{R}_n$

**Theorem (good news)**

$$G_n = U_2(\mathcal{R}_n) \text{ for } n \in \{2,4,6,8,12\}$$

**Theorem (bad news)**

Let $F_N$ be the fraction of even integers $n$ between 1 and $N$ for which $G_n = U_2(\mathcal{R}_n)$. Then

$$F_N \to 0 \text{ as } N \to \infty$$
Definitions and Results

Exact synthesis algorithm

Number theoretic characterization
Exact synthesis algorithm: strategy

Represent unitaries as rotations of the Bloch sphere
The image of the Clifford-cyclotomic group $G_n$ under this mapping is a discrete rotation group $\hat{G}_n$.

Derive a canonical form for elements of $\hat{G}_n$.
The canonical form is unique and can be obtained by a simple procedure.

Give algorithm which efficiently computes the canonical form.
An optimal decomposition over Clifford-cyclotomic gate set can be recovered from the canonical form.

This generalizes a strategy which was used in [G., Kliuchnikov, Mosca, Russo 2014] for the Clifford+T case $n = 4$. 
Bloch sphere representation

\[ G_n = \langle \mathcal{E}, \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/n} \end{pmatrix} \rangle \quad \Rightarrow \quad \widehat{G}_n = \langle \widehat{\mathcal{E}}, R_z \rangle \]

\[ \widehat{\mathcal{E}} = \text{Subgroup of SO}(3) \text{ consisting of signed permutation matrices} \]

\[ R_z = \begin{pmatrix} \cos(\pi/n) & \sin(\pi/n) & 0 \\ -\sin(\pi/n) & \cos(\pi/n) & 0 \\ 0 & 0 & 1 \end{pmatrix} \]
\[ G_n = \langle \mathcal{E}, \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/n} \end{pmatrix} \rangle \]

Represent as rotation of Bloch sphere

\[ \widehat{G}_n = \langle \widehat{\mathcal{E}}, R_z \rangle \]

\[ \widehat{\mathcal{E}} = \text{Subgroup of SO}(3) \text{ consisting of signed permutation matrices} \]

\[ R_z = \begin{pmatrix} \cos(\pi/n) & \sin(\pi/n) & 0 \\ -\sin(\pi/n) & \cos(\pi/n) & 0 \\ 0 & 0 & 1 \end{pmatrix} \]

The group \( \widehat{G}_n \) is a discrete subgroup of SO(3) of the type studied in [Radin, Sadun 1998]. Canonical forms and the relations in this group are previously known.

The exact synthesis algorithm can be viewed as an algorithmic extension of those results.
Canonical form

Define $R_x, R_y, R_z$ to be $3 \times 3$ rotation matrices corresponding to a rotation by $\pi/n$ about the $x, y, z$ axes respectively.

Lemma

Any $M \in \widehat{G}_n$ can be decomposed as

$$M = (R_{p_1}^{a_1} R_{p_2}^{a_2} \ldots R_{p_L}^{a_L})C$$

where $p_i \in \{x, y, z\}$ satisfy $p_i \neq p_{i+1}$, $C \in \widehat{E}$, and $1 \leq a_i < \frac{n}{2}$. 

Any $M \in \overline{G}_n$ can be decomposed as

$$M = (R_{p_1}^{a_1}R_{p_2}^{a_2} \cdots R_{p_L}^{a_L})C$$

where $p_i \in \{x, y, z\}$ satisfy $p_i \neq p_{i+1}$, $C \in \hat{C}$, and $1 \leq a_i < \frac{n}{2}$. 
Canonical form

Lemma

Any $M \in \widehat{G}_n$ can be decomposed as

$$M = (R_{p_1}^{a_1}R_{p_2}^{a_2} \ldots R_{p_L}^{a_L})C$$

where $p_i \in \{x, y, z\}$ satisfy $p_i \neq p_{i+1}$, $C \in \widehat{C}$, and $1 \leq a_i < \frac{n}{2}$.

Proof sketch (for case $n = 4$)

Start with decomposition

$$M = C_1 R_z C_2 R_z \ldots C_m R_z C_{m+1}$$
Canonical form

Lemma

Any $M \in \overline{G}_n$ can be decomposed as

$$M = (R_{p_1}^{a_1} R_{p_2}^{a_2} \ldots R_{p_L}^{a_L})C$$

where $p_i \in \{x, y, z\}$ satisfy $p_i \neq p_{i+1}$, $C \in \hat{C}$, and $1 \leq a_i < \frac{n}{2}$.

Proof sketch (for case $n = 4$)

Start with decomposition

$$M = C_1 R_z C_2 R_z \ldots C_m R_z C_{m+1}$$

$$= (D_1 R_z D_1^\dagger)(D_2 R_z D_2^\dagger) \ldots (D_m R_z D_m^\dagger)D_{m+1}$$

where $D_j = C_1 C_2 \ldots C_j$
Lemma

Any $M \in \widehat{G}_n$ can be decomposed as

$$M = (R_{p_1}^{a_1} R_{p_2}^{a_2} ... R_{p_L}^{a_L})C$$

where $p_i \in \{x, y, z\}$ satisfy $p_i \neq p_{i+1}$, $C \in \widehat{C}$, and $1 \leq a_i < \frac{n}{2}$.

Proof sketch (for case $n = 4$)

Start with decomposition

$$M = C_1 R_z C_2 R_z ... C_m R_z C_{m+1}$$

$$= (D_1 R_z D_1^\dagger)(D_2 R_z D_2^\dagger) ... (D_m R_z D_m^\dagger)D_{m+1} \quad \text{where } D_j = C_1 C_2 ... C_j$$

$$= R_{p_1}^{b_1} R_{p_2}^{b_2} ... R_{p_m}^{b_m} D_{m+1} \quad \text{where } b_i \in \{1, -1\}$$
Lemma

Any \( M \in \hat{G}_n \) can be decomposed as

\[
M = (R_{p_1}^{a_1}R_{p_2}^{a_2} \ldots R_{p_L}^{a_L})C
\]

where \( p_i \in \{x, y, z\} \) satisfy \( p_i \neq p_{i+1} \), \( C \in \hat{C} \), and \( 1 \leq a_i < \frac{n}{2} \).

Proof sketch (for case \( n = 4 \))

Start with decomposition

\[
M = C_1R_zC_2R_z \ldots C_mR_zC_{m+1}
= (D_1R_zD_1^\dagger)(D_2R_zD_2^\dagger) \ldots (D_mR_zD_m^\dagger)D_{m+1}
\]

where \( D_j = C_1C_2 \ldots C_j \)

\[
= R_{p_1}^{b_1}R_{p_2}^{b_2} \ldots R_{p_m}^{b_m}D_{m+1}
\]

where \( b_i \in \{1, -1\} \)

We want all \( b_i = 1 \). Suppose \( b_1 = -1 \). To get rid of it, use the fact that \( R_{p_1}^{-1} = R_{p_1}C \) where \( C \in \hat{C} \).

\[
= R_{p_1}(CR_{p_2}^{b_2} \ldots R_{p_m}^{b_m}D_{m+1})
\]
Any $M \in \mathcal{G}_n$ can be decomposed as

$$M = (R_{p_1}^{a_1}R_{p_2}^{a_2} ... R_{p_L}^{a_L})C$$

where $p_i \in \{x, y, z\}$ satisfy $p_i \neq p_{i+1}$, $C \in \mathcal{E}$, and $1 \leq a_i < \frac{n}{2}$.

Proof sketch (for case $n = 4$)

Start with decomposition

$$M = C_1 R_z C_2 R_z ... C_m R_z C_{m+1}$$

$$= (D_1 R_z D_1^\dagger)(D_2 R_z D_2^\dagger)...(D_m R_z D_m^\dagger)D_{m+1} \quad \text{where} \quad D_j = C_1 C_2 ... C_j$$

$$= R_{p_1}^{b_1} R_{p_2}^{b_2} ... R_{p_m}^{b_m} D_{m+1} \quad \text{where} \quad b_i \in \{1, -1\}$$

We want all $b_i = 1$. Suppose $b_1 = -1$. To get rid of it, use the fact that $R_{p_1}^{-1} = R_{p_1} C$ where $C \in \mathcal{E}$.

$$= R_{p_1} (C R_{p_2}^{b_2} ... R_{p_m}^{b_m} D_{m+1})$$

Now start again to decompose expression in parentheses. Procedure terminates after at most $m$ steps.
Any $M \in \widehat{G}_n$ can be decomposed as

$$M = (R_{p_1}^{a_1} R_{p_2}^{a_2} \ldots R_{p_L}^{a_L})\mathcal{C}$$

where $p_i \in \{x, y, z\}$ satisfy $p_i \neq p_{i+1}$, $\mathcal{C} \in \widehat{C}$, and $1 \leq a_i < \frac{n}{2}$.

Our main result is an algorithm to compute this canonical form (up next).

It deterministically recovers the canonical form from a given $M$, thus it is unique.

It is then straightforward to obtain an optimal decomposition in the original gate set.
Computing the canonical form: Clifford+T example

Consider the Clifford+T case $n = 4$, where

$$R_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \quad R_y = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \quad R_z = \begin{pmatrix} 1 & 1 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{pmatrix}$$

Our goal is to compute the canonical form of a given matrix $M$.

$$M = (R_{p_1} R_{p_2} ... R_{p_L}) C$$

Key idea: look at the pattern of “denominator exponents” in the entries of $M$...
Computing the canonical form: Clifford+T example

Definition of denominator exponent, Clifford+T case

All entries of $M$ have the form

$$z = \frac{a + b\sqrt{2}}{\sqrt{2}^k}$$

$k$ is the denominator exponent

The denominator exponent for a row of $M$ is the maximum denominator exponent of one of the entries in the row.
Computing the canonical form: Clifford+T example

Example: denominator exponent pattern of $M = R_{p_1}$

$$R_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$R_y = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$R_z = \begin{pmatrix} 1 & 1 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
Computing the canonical form: Clifford+T example

Example: denominator exponent pattern of $M = R_{p_1}$

$$R_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \quad R_y = \begin{pmatrix} 1 & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 1 \\ 1 & \frac{1}{\sqrt{2}} & 0 \end{pmatrix} \quad R_z = \begin{pmatrix} 1 & 1 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{pmatrix}$$

Each matrix has two rows with denominator exponent $k = 1$ and one row with denominator exponent $k = 0$.

The row with $k = 0$ in $R_{p_1}$ is the one labeled $p_1$. 
Computing the canonical form: Clifford+T example

Example: Denominator exponent pattern of $M = R_{p_1}R_{p_2}$

$$R_xR_y = \begin{pmatrix} 1 & 0 & -1 \\ \frac{1}{\sqrt{2}} & 1 & \frac{1}{\sqrt{2}} \\ \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{2} \end{pmatrix} \quad R_yR_z = \begin{pmatrix} 1 & 1 & -1 \\ \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{2} & \frac{1}{\sqrt{2}} & \frac{1}{2} \end{pmatrix} \quad R_zR_x = \begin{pmatrix} 1 & 1 & 1 \\ \frac{1}{\sqrt{2}} & \frac{2}{2} & \frac{1}{2} \\ 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \quad \ldots \text{ETC}$$
Computing the canonical form: Clifford+T example

Example: Denominator exponent pattern of $M = R_{p_1} R_{p_2}$

$$R_x R_y = \begin{pmatrix} 1 & 0 & -1 \\ \frac{1}{\sqrt{2}} & 0 & -1 \end{pmatrix} \quad R_y R_z = \begin{pmatrix} 1 & 1 & -1 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{pmatrix} \quad R_z R_x = \begin{pmatrix} 1 & 1 & 1 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \end{pmatrix} \quad \ldots \text{ETC}$$

Each matrix has two rows with denominator exponent $k = 2$ and one row with denominator exponent $k = 1$.

The row with $k = 1$ in $R_{p_1} R_{p_2}$ is the one labeled $p_1$. 
Lemma (Denominator exponent pattern, Clifford+T case)

Let

\[ M = \left( R_{p_1} R_{p_2} ... R_{p_L} \right) C \quad p_i \neq p_{i+1} \]

Then \( M \) has two rows with denominator exponent \( k = L \) and one row with \( k = L - 1 \). The row with \( k = L - 1 \) is the one labeled \( p_1 \).
**Lemma (Denominator exponent pattern, Clifford+T case)**

Let

\[ M = \left( R_{p_1} R_{p_2} \ldots R_{p_L} \right) C \quad p_i \neq p_{i+1} \]

Then \( M \) has two rows with denominator exponent \( k = L \) and one row with \( k = L - 1 \). The row with \( k = L - 1 \) is the one labeled \( p_1 \).

**Two line inductive proof:**

We saw the base case \( L = 1 \) already. So suppose it holds for \( M \) (with decomposition as above) and show it holds for \( R_q M \) where \( q \neq p_1 \). Suppose \( q = z \) and \( p_1 = x \) (other cases are symmetric).
Lemma (Denominator exponent pattern, Clifford+T case)

Let

\[ M = (R_{p_1} R_{p_2} \ldots R_{p_L})C \quad p_i \neq p_{i+1} \]

Then \( M \) has two rows with denominator exponent \( k = L \) and one row with \( k = L - 1 \). The row with \( k = L - 1 \) is the one labeled \( p_1 \).

Two line inductive proof:

We saw the base case \( L = 1 \) already. So suppose it holds for \( M \) (with decomposition as above) and show it holds for \( R_q M \) where \( q \neq p_1 \). Suppose \( q = z \) and \( p_1 = x \) (other cases are symmetric).

\[
R_z M = \begin{pmatrix}
1 & 1 & 0 \\
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\
-1 & 1 & 0 \\
-\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\
0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
\vec{r}_1 \\
\vec{r}_2 \\
\vec{r}_3
\end{pmatrix}
\]

Rows of \( M \)—both \( \vec{r}_2, \vec{r}_3 \) have denom. exponent \( L \) and \( \vec{r}_1 \) has denominator exponent \( L - 1 \) (by inductive hypothesis)
Lemma (Denominator exponent pattern, Clifford+T case)

Let

\[ M = (R_{p_1} R_{p_2} \ldots R_{p_L}) C \quad p_i \neq p_{i+1} \]

Then \( M \) has two rows with denominator exponent \( k = L \) and one row with \( k = L - 1 \). The row with \( k = L - 1 \) is the one labeled \( p_1 \).

Two line inductive proof:
We saw the base case \( L = 1 \) already. So suppose it holds for \( M \) (with decomposition as above) and show it holds for \( R_q M \) where \( q \neq p_1 \). Suppose \( q = z \) and \( p_1 = x \) (other cases are symmetric).

\[
R_z M = \begin{pmatrix}
1 & 0 & 0 \\
\frac{1}{\sqrt{2}} & 1 & 0 \\
-\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\
0 & 0 & 1
\end{pmatrix} \begin{pmatrix}
\vec{r}_1 \\
\vec{r}_2 \\
\vec{r}_3
\end{pmatrix} = \begin{pmatrix}
\frac{1}{\sqrt{2}} (\vec{r}_1 + \vec{r}_2) \\
\frac{1}{\sqrt{2}} (-\vec{r}_1 + \vec{r}_2) \\
\vec{r}_3
\end{pmatrix}
\]

Rows of \( M \)—both \( \vec{r}_2, \vec{r}_3 \) have denom. exponent \( L \) and \( \vec{r}_1 \) has denominator exponent \( L - 1 \) (by inductive hypothesis)
Lemma (Denominator exponent pattern, Clifford+T case)

Let

\[ M = \left( R_{p_1} R_{p_2} \ldots R_{p_L} \right) C \quad p_i \neq p_{i+1} \]

Then \( M \) has two rows with denominator exponent \( k = L \) and one row with \( k = L - 1 \).
The row with \( k = L - 1 \) is the one labeled \( p_1 \).

Two line inductive proof:

We saw the base case \( L = 1 \) already. So suppose it holds for \( M \) (with decomposition as above) and show it holds for \( R_q M \) where \( q \neq p_1 \). Suppose \( q = z \) and \( p_1 = x \) (other cases are symmetric).

\[
R_z M = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \vec{r}_1 \\ \vec{r}_2 \\ \vec{r}_3 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} (\vec{r}_1 + \vec{r}_2) \\ \frac{1}{\sqrt{2}} (\vec{r}_1 - \vec{r}_2) \\ \vec{r}_3 \end{pmatrix}
\]

This row (labeled \( z \)) has denominator exponent \( L \)

Rows of \( M \)—both \( \vec{r}_2, \vec{r}_3 \) have denom. exponent \( L \) and \( \vec{r}_1 \) has denominator exponent \( L - 1 \) (by inductive hypothesis)
Lemma (Denominator exponent pattern, Clifford+T case)

Let

$$M = \left( R_{p_1} R_{p_2} \ldots R_{p_L} \right) C \quad p_i \neq p_{i+1}$$

Then $M$ has two rows with denominator exponent $k = L$ and one row with $k = L - 1$.
The row with $k = L - 1$ is the one labeled $p_1$.

Two line inductive proof:
We saw the base case $L = 1$ already. So suppose it holds for $M$ (with decomposition as above) and show it holds for $R_q M$ where $q \neq p_1$. Suppose $q = z$ and $p_1 = x$ (other cases are symmetric).

$$R_z M = \begin{pmatrix} 1 & 1 & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \overrightarrow{r_1} \\ \overrightarrow{r_2} \\ \overrightarrow{r_3} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} (\overrightarrow{r_1} + \overrightarrow{r_2}) \\ \frac{1}{\sqrt{2}} (-\overrightarrow{r_1} + \overrightarrow{r_2}) \\ \overrightarrow{r_3} \end{pmatrix}$$

These rows have
denominator exponent $L + 1$
This row (labeled $z$) has
denominator exponent $L$

Rows of $M$—both $\overrightarrow{r_2}, \overrightarrow{r_3}$ have denom. exponent $L$ and $\overrightarrow{r_1}$ has
denominator exponent $L - 1$ (by inductive hypothesis)
Lemma (Denominator exponent pattern, Clifford+T case)

Let

\[ M = (R_{p_1} R_{p_2} ... R_{p_L})C \quad p_i \neq p_{i+1} \]

Then \( M \) has two rows with denominator exponent \( k = L \) and one row with \( k = L - 1 \). The row with \( k = L - 1 \) is the one labeled \( p_1 \).

**Implication 1:** we can determine \( L \) (the number of terms in the canonical form) by looking at the entries of \( M \)!
Lemma (Denominator exponent pattern, Clifford+T case)

Let

\[
M = \left(R_{p_1} R_{p_2} \ldots R_{p_L}\right)C \quad p_i \neq p_{i+1}
\]

Then \( M \) has two rows with denominator exponent \( k = L \) and one row with \( k = L - 1 \).

The row with \( k = L - 1 \) is the one labeled \( p_1 \).

**Implication 1:** we can determine \( L \) (the number of terms in the canonical form) by looking at the entries of \( M \)!

**Implication 2:** Let \( q \in \{x, y, z\} \). The matrix \( R_q^{-1}M \) has denominator exponent smaller than that of \( M \) only when \( q = p_1 \).
Lemma (Denominator exponent pattern, Clifford+T case)

Let

\[ M = (R_{p_1} R_{p_2} \ldots R_{p_L})C \quad p_i \neq p_{i+1} \]

Then \( M \) has two rows with denominator exponent \( k = L \) and one row with \( k = L - 1 \). The row with \( k = L - 1 \) is the one labeled \( p_1 \).

**Implication 1:** we can determine \( L \) (the number of terms in the canonical form) by looking at the entries of \( M \)!

**Implication 2:** Let \( q \in \{x, y, z\} \). The matrix \( R_q^{-1}M \) has denominator exponent smaller than that of \( M \) only when \( q = p_1 \). To see this, note that

\[
R_q^{-1}M = C'R_qM = \begin{cases} 
(R_{p_2} \ldots R_{p_L})C, & \text{if } q = p_1 \\
C'(R_qR_{p_1}R_{p_2} \ldots R_{p_L})C, & \text{if } q \neq p_1 
\end{cases}
\]
Lemma (Denominator exponent pattern, Clifford+T case)

Let

$$M = (R_{p_1} R_{p_2} \ldots R_{p_L})C \quad p_i \neq p_{i+1}$$

Then $M$ has two rows with denominator exponent $k = L$ and one row with $k = L - 1$. The row with $k = L - 1$ is the one labeled $p_1$.

**Implication 1:** we can determine $L$ (the number of terms in the canonical form) by looking at the entries of $M$!

**Implication 2:** Let $q \in \{x, y, z\}$. The matrix $R_q^{-1}M$ has denominator exponent smaller than that of $M$ only when $q = p_1$. To see this, note that

$$R_q^{-1}M = C'R_qM = \begin{cases} (R_{p_2} \ldots R_{p_L})C, & \text{if } q = p_1 \\ C'(R_{q R_{p_1}} R_{p_2} \ldots R_{p_L})C, & \text{if } q \neq p_1 \end{cases}$$

With these two facts in hand, computing the canonical form is easy…
Computing the canonical form: Clifford+T example

Algorithm to compute the canonical form (idea: greedily reduce denominator exponent)

1. Compute the maximum denominator exponent appearing in the given matrix $M$. If it is zero then set $C = M$ and stop.

2. Recall that $q = p_1$ is the only choice for which the maximum denominator exponent in $R_q^{-1}M$ is less than that of $M$. So determine $p_1$ by looking at the three matrices $R_x^{-1}M$, $R_y^{-1}M$, $R_z^{-1}M$.

3. Set $M \to R_{p_1}^{-1}M$ and go back to step 1.
How does this algorithm generalize to larger values of $n$?

We will define a generalization of the denominator exponent.

We will see that the canonical form can be recovered using the denominator exponent pattern of $M$, just like in the Clifford+T case.
Computing the canonical form: general case

Aside: Definition of divisibility for algebraic integers

An algebraic integer is a root of a polynomial with integer coefficients and leading coefficient equal to 1.

An algebraic integer $b$ is said to divide another algebraic integer $a$ if and only if $\frac{a}{b}$ is an algebraic integer.
Aside: Definition of divisibility for algebraic integers

An **algebraic integer** is a root of a polynomial with integer coefficients and leading coefficient equal to 1.

An algebraic integer $b$ is said to divide another algebraic integer $a$ if and only if $\frac{a}{b}$ is an algebraic integer.
Computing the canonical form: general case

**Denominator exponent.** Write $n = 2^r s$ where $s$ is odd. Define

$$\beta = \begin{cases} 
2, & \text{if } r = 1 \\
2 \cos \left( \frac{\pi}{2^r} \right), & \text{otherwise.}
\end{cases}$$

$\beta$ is an algebraic integer

We define the denominator exponent to be “the number of factors of $\beta$ in the denominator” (we’ll make this more precise soon)
Computing the canonical form: general case

Denominator exponent example:

For each $1 \leq a < \frac{n}{2}$ we can write

$$R_z^a = \begin{pmatrix} \cos(\pi a/n) & \sin(\pi a/n) & 0 \\ -\sin(\pi a/n) & \cos(\pi a/n) & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{x_a}{\beta^{qa}} & \frac{y_a}{\beta^{qa}} & 0 \\ \frac{-y_a}{\beta^{qa}} & \frac{x_a}{\beta^{qa}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Where $q_a$ is a positive integer that depends on $a$ and $n$, and where $x_a, y_a$ are algebraic integers which are not divisible by $\beta$. 
Computing the canonical form: general case

Denominator exponent example:

For each $1 \leq a < \frac{n}{2}$ we can write

$$R^a_z = \begin{pmatrix} \cos(\pi a/n) & \sin(\pi a/n) & 0 \\ -\sin(\pi a/n) & \cos(\pi a/n) & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{x_a}{\beta^{q_a}} & \frac{y_a}{\beta^{q_a}} & 0 \\ -\frac{y_a}{\beta^{q_a}} & \frac{x_a}{\beta^{q_a}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Where $q_a$ is a positive integer that depends on $a$ and $n$, and where $x_a, y_a$ are algebraic integers which are not divisible by $\beta$.

Explicitly, $q_a = \begin{cases} 2^{r-1} - 2^{-j}, & \text{if } \frac{n}{\gcd(a, n)} = 2^j \\ 2^{r-1}, & \text{otherwise.} \end{cases}$
Computing the canonical form: general case

Denominator exponent example:

For each $1 \leq a < \frac{n}{2}$ we can write

$$R_z^a = \begin{pmatrix} \cos(\pi a/n) & \sin(\pi a/n) & 0 \\ -\sin(\pi a/n) & \cos(\pi a/n) & 0 \end{pmatrix} = \begin{pmatrix} \frac{x_a}{\beta^{q_a}} & \frac{y_a}{\beta^{q_a}} & 0 \\ -\frac{y_a}{\beta^{q_a}} & \frac{x_a}{\beta^{q_a}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Has two rows with denominator exponent $k = q_a$ and one row with denominator exponent $k = 0$.

Where $q_a$ is a positive integer that depends on $a$ and $n$, and where $x_a, y_a$ are algebraic integers which are not divisible by $\beta$.

Explicitly,

$$q_a = \begin{cases} 2^{r-1} - 2^{r-j}, & \text{if } \frac{n}{\gcd(a, n)} = 2^j \\ 2^{r-1}, & \text{otherwise.} \end{cases}$$
Lemma (Denominator exponent pattern)

Let the canonical form of $M \in \tilde{G}_n$ be given by

$$M = \left( R_{p_1}^{a_1} R_{p_2}^{a_2} \ldots R_{p_L}^{a_L} \right) C$$

Define $N = \sum_{i=1}^{L} q_{a_i}$. Then:
Computing the canonical form: general case

**Lemma (Denominator exponent pattern)**

Let the canonical form of $M \in \hat{G}_n$ be given by

$$M = \left( R_{p_1}^{a_1} R_{p_2}^{a_2} \ldots R_{p_L}^{a_L} \right) C$$

Define $N = \sum_{i=1}^{L} q_{a_i}$. Then:

1. Each nonzero entry of $M$ can be written as $\frac{w}{\beta^k}$ where $k \in \mathbb{Z}_{\geq 0}$ and $w$ is an algebraic integer not divisible by $\beta$. 
Lemma (Denominator exponent pattern)

Let the canonical form of \( M \in \mathcal{G}_n \) be given by

\[
M = \left( R_{p_1}^{a_1} R_{p_2}^{a_2} \ldots R_{p_L}^{a_L} \right) C
\]

Define \( N = \sum_{i=1}^{L} q_{a_i} \). Then:

1. Each nonzero entry of \( M \) can be written as \( \frac{w}{\beta^k} \) where \( k \in \mathbb{Z}_{\geq 0} \) and \( w \) is an algebraic integer not divisible by \( \beta \).

2. The maximum denominator exponent \( k \) which appears in \( M \) is equal to \( N \). Exactly two rows have an entry with this denominator exponent.
Computing the canonical form: general case

**Lemma (Denominator exponent pattern)**

Let the canonical form of $M \in \widehat{G}_n$ be given by

$$M = \left( R_{p_1}^{a_1} R_{p_2}^{a_2} \ldots R_{p_L}^{a_L} \right) C$$

Define $N = \sum_{i=1}^{L} q_{a_i}$. Then:

1. Each nonzero entry of $M$ can be written as $\frac{w}{\beta^k}$ where $k \in \mathbb{Z}_{\geq 0}$ and $w$ is an algebraic integer not divisible by $\beta$.

2. The maximum denominator exponent $k$ which appears in $M$ is equal to $N$. Exactly two rows have an entry with this denominator exponent.

3. There is one row of $M$ in which the maximum denominator exponent is $N - q_{a_1}$. This row is the one labeled $p_1$. 
Computing the canonical form: general case

Lemma (Denominator exponent pattern)

Let the canonical form of $M \in \widehat{G}_n$ be given by

$$M = (R_{p_1}^{a_1}R_{p_2}^{a_2} \ldots R_{p_L}^{a_L})C$$

Define $N = \sum_{i=1}^{L} q_{a_i}$. Then:

1. Each nonzero entry of $M$ can be written as $\frac{w}{\beta^k}$ where $k \in \mathbb{Z}_{\geq 0}$ and $w$ is an algebraic integer not divisible by $\beta$.

2. The maximum denominator exponent $k$ which appears in $M$ is equal to $N$. Exactly two rows have an entry with this denominator exponent.

3. There is one row of $M$ in which the maximum denominator exponent is $N - q_{a_1}$. This row is the one labeled $p_1$.

Just like in the Clifford+T case this lemma gives us an algorithm to compute the canonical form, based on greedily reducing the maximum denominator exponent appearing in $M$. 
Computing the canonical form: general case

Algorithm to compute the canonical form

1. Compute the maximum denominator exponent appearing in the given matrix $M$. If it is zero then set $C = M$ and stop.

2. Look at the matrices $R_q^{-b}M$ for $1 \leq b < \frac{n}{2}$ and $q \in \{x, y, z\}$ and compute the maximum denominator exponent appearing in each of them. The one where this number is smallest corresponds to the choice $q = p_1$ and $b = a_1$.

3. Set $M \rightarrow R_{p_1}^{-a_1}M$ and go back to step 1.
Number-theoretic characterization

\[ U_2(\mathcal{R}_n) = \text{group of all } 2 \times 2 \text{ unitaries with entries in the ring } \mathcal{R}_n = \mathbb{Z}[e^{\frac{in}{n}}, 1/2] \]

\[ G_n = \text{Group generated by Cliffords plus } \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/n} \end{pmatrix}. \]

**Theorem (bad news)**
Let \( F_N \) be the fraction of even integers \( n \) between 1 and \( N \) for which \( G_n = U_2(\mathcal{R}_n) \). Then

\[ F_N \to 0 \text{ as } N \to \infty \]
Number-theoretic characterization

$U_2(\mathcal{R}_n) =$ group of all $2 \times 2$ unitaries with entries in the ring $\mathcal{R}_n = \mathbb{Z}[e^{i\pi n}, 1/2]$

$G_n =$ Group generated by Cliffords plus $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/n} \end{pmatrix}$.

**Theorem (bad news)**

Let $F_N$ be the fraction of even integers $n$ between 1 and $N$ for which $G_n = U_2(\mathcal{R}_n)$. Then

$$F_N \to 0 \text{ as } N \to \infty$$

**Proof strategy:**

Focus on the subgroups of diagonal $z$-axis rotations in each group $U_2(\mathcal{R}_n), G_n$.

Establish a necessary and sufficient condition for these subgroups to be equal.

Then show that this condition is violated for almost all even positive integers.
What is the subgroup $D_n$ of $z$-axis rotations in $G_n$?

Definition:

$$D_n = \{U_z(\theta): U_z(\theta) \in G_n\}$$

$$U_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$
Number-theoretic characterization

What is the subgroup $D_n$ of $z$-axis rotations in $G_n$?

Definition: 
\[ D_n = \{ U_z(\theta) : U_z(\theta) \in G_n \} \]
\[ U_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \]

Lemma 
\[ D_n = \{ U_z(\pi j/n) : 0 \leq j \leq 2n - 1 \} \]
What is the subgroup $D_n$ of $z$-axis rotations in $G_n$?

**Definition:**

$$D_n = \{ U_z(\theta) : U_z(\theta) \in G_n \}$$

$$U_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

**Lemma**

$$D_n = \{ U_z(\pi j/n) : 0 \leq j \leq 2n - 1 \}$$

**Proof:** The Bloch sphere representation of $U_z(\theta) \in D_n$ is

$$\begin{pmatrix} \cos(\theta) & \sin(\theta) & 0 \\ -\sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
Number-theoretic characterization

What is the subgroup $D_n$ of z-axis rotations in $G_n$?

Definition: $D_n = \{ U_z(\theta) : U_z(\theta) \in G_n \}$

$$U_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Lemma

$$D_n = \{ U_z(\pi j/n): 0 \leq j \leq 2n - 1 \}$$

Proof: The Bloch sphere representation of $U_z(\theta) \in D_n$ is

$$\begin{pmatrix} \cos(\theta) & \sin(\theta) & 0 \\ -\sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The last row of this matrix has denominator exponent 0. Using what we know about denominator exponent patterns, this severely constrains its canonical form. We infer

$$\begin{pmatrix} \cos(\theta) & \sin(\theta) & 0 \\ -\sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix} = R_z^a C \quad 0 \leq a < \frac{n}{2}$$

$C$ is a signed permutation matrix.
Number-theoretic characterization

What is the subgroup $D_n$ of z-axis rotations in $G_n$?

**Definition:**

\[
D_n = \{ U_z(\theta) : U_z(\theta) \in G_n \} \quad \text{where} \quad U_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}
\]

**Lemma**

\[
D_n = \{ U_z(\pi j/n) : 0 \leq j \leq 2n - 1 \}
\]

**Proof:** The Bloch sphere representation of $U_z(\theta) \in D_n$ is

\[
\begin{pmatrix}
\cos(\theta) & \sin(\theta) & 0 \\
-\sin(\theta) & \cos(\theta) & 0 \\
0 & 0 & 1
\end{pmatrix}
\]

The last row of this matrix has denominator exponent 0. Using what we know about denominator exponent patterns, this severely constrains its canonical form. We infer

\[
\begin{pmatrix}
\cos(\theta) & \sin(\theta) & 0 \\
-\sin(\theta) & \cos(\theta) & 0 \\
0 & 0 & 1
\end{pmatrix} = R_z^a C \quad 0 \leq a < \frac{n}{2}
\]

C is a signed permutation matrix

From this we see that $C$ must also be a $z$-rotation. The only $z$-rotations which are signed permutation matrices are powers of $R_z$. Therefore $\theta = \pi j/n$. 
What is the subgroup $\Delta_n$ of $z$-axis rotations in $U_2(R_n)$?

$$
\Delta_n = \{ U_z \in (\theta): e^{i\theta} \in R_n \} \\
U_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}
$$
What is the subgroup $\Delta_n$ of $z$-axis rotations in $U_2(\mathcal{R}_n)$?

$$\Delta_n = \{ U_z \in (\theta) : e^{i\theta} \in \mathcal{R}_n \}$$

$$U_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

So, what is the set of complex phases in $\mathcal{R}_n$? When is it equal to $\{ e^{i\pi j / n} : 0 \leq j \leq 2n - 1 \}$?
Number-theoretic characterization

What is the subgroup $\Delta_n$ of $z$-axis rotations in $U_2(\mathcal{R}_n)$?

$$\Delta_n = \{U_z \in (\theta): e^{i\theta} \in \mathcal{R}_n\} \quad U_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

So, what is the set of complex phases in $\mathcal{R}_n$? When is it equal to $\{e^{i\pi j/n}: 0 \leq j \leq 2n - 1\}$?

**Lemma**

Write $n = 2^r s$ where $s$ is odd. Suppose there exists a positive integer $t$ such that $2^t = -1 \pmod{s}$. Then the set of complex phases in $\mathcal{R}_n$ is

$$\{e^{i\pi j/n}: 0 \leq j \leq 2n - 1\}.$$

Conversely if there is no such positive integer $t$ then $\mathcal{R}_n$ contains complex phases of infinite order.
What is the subgroup $\Delta_n$ of $z$-axis rotations in $U_2(\mathcal{R}_n)$?

$$\Delta_n = \{ U_z \in (\theta) : e^{i\theta} \in \mathcal{R}_n \}$$

$$U_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

So, what is the set of complex phases in $\mathcal{R}_n$? When is it equal to $\{ e^{i\pi j/n} : 0 \leq j \leq 2n - 1 \}$?

**Lemma**

Write $n = 2^r s$ where $s$ is odd. Suppose there exists a positive integer $t$ such that $2^t = -1 \pmod{s}$. Then the set of complex phases in $\mathcal{R}_n$ is

$$\{ e^{i\pi j/n} : 0 \leq j \leq 2n - 1 \}.$$

Conversely if there is no such positive integer $t$ then $\mathcal{R}_n$ contains complex phases of infinite order.

Therefore $U_2(\mathcal{R}_n) \neq G_n$ whenever the above condition is not satisfied. We show that the proportion of positive integers $n \leq N$ which satisfy this condition approaches zero as $N \to \infty$. 

**Number-theoretic characterization**
Open questions

What can be said about approximate synthesis?

For exactly which $n$ is $G_n = U_2(\mathcal{R}_n)$?

Can we fault-tolerantly implement $\pi/n$ z-rotation gates?

Can any of these results be extended to multi-qubit unitaries?

Is there a unified way to handle exact synthesis in general (ad for the next talk!)?