Generators and Relations for $\mathrm{O}_n(\mathbb{Z}[1/2])$ and $\mathrm{U}_n(\mathbb{Z}[1/2, i])$

Xiaoning Bian, Sarah Meng Li, Neil J. Ross, and Peter Selinger

Department of Mathematics and Statistics
Dalhousie University, Halifax, Canada

QPL 2021

The Group $\mathrm{O}_n(\mathbb{Z}[1/2])$

- $\mathbb{Z}[\frac{1}{2}] = \left\{ \frac{u}{2^q} \middle| u \in \mathbb{Z}, q \in \mathbb{N} \right\}$ is the ring of *dyadic fractions*.

- $\mathrm{O}_n(\mathbb{Z}[1/2])$ is the group of orthogonal matrices over $\mathbb{Z}[\frac{1}{2}]$, namely, the group of *orthogonal dyadic matrices*.

- It consists of n-dimensional matrices of the form $\frac{1}{2^k}M$. For example,

$$U = \frac{1}{2^2}\begin{bmatrix} 3 & 1 & -1 & 1 & 2 \\ 1 & 3 & 1 & -1 & -2 \\ -1 & 1 & 3 & 1 & 2 \\ 1 & -1 & 1 & 3 & -2 \\ -2 & 2 & -2 & 2 & 0 \end{bmatrix} \in \mathrm{O}_5(\mathbb{Z}[1/2]).$$

The Group $\mathrm{U}_n(\mathbb{Z}[1/2, i])$

- $\mathbb{Z}[\frac{1}{2}, i] = \{r + si | r, s \in \mathbb{Z}[\frac{1}{2}]\}$ is a subring of $\mathbb{C}$, where an element has dyadic fractional real and imaginary part.
- $U_n(\mathbb{Z}[\frac{1}{2}, i])$ is the group of unitary matrices with entries from $\mathbb{Z}[\frac{1}{2}, i]$.
- It consists of n-dimensional matrices of the form $\frac{1}{2^k}N$. For example,

$$M = \frac{1}{2^2}\begin{bmatrix} -2i & -1-3i & 1-i \\ -2i & -1+i & 1+3i \\ 2-2i & 2i & -2i \end{bmatrix} \in U_3(\mathbb{Z}[\frac{1}{2}, i]).$$

The Circuit-Matrix Correspondence

Theorems (Amy, Glaudell, and Ross, 2020)

(a) A unitary M can be exactly represented by a circuit over $\{X, CX, CCX, H \otimes H\}$ if and only if $M \in \mathrm{O}_n(\mathbb{Z}[1/2])$.

(b) A unitary U can be exactly represented by a circuit over $\{X, CX, CCX, \omega^\dagger H, S\}$ if and only if $U \in \mathrm{U}_n(\mathbb{Z}[1/2, i])$.

- Restricted Clifford+T circuits correspond to a group of matrices.
- Studying matrix groups is a way to study quantum circuits.

Constructive Membership Problem (CMP)

Let $\mathcal{G}$ be a group of matrices with entries over some ring, and $\mathcal{S} = \{s_1, \ldots, s_q\}$ a set of generators for $\mathcal{G}$. Let $U \in \mathcal{G}$, find a sequence of generators $s_1, \ldots, s_\ell$ such that

$$U = s_1 \cdot \ldots \cdot s_\ell.$$

- The smaller the ℓ, the better the solution.
- A solution is optimal if the sequence is a shortest possible sequence.
- An algorithm to solve the CMP is called an **exact synthesis algorithm**.

Motivation

- Restricted Clifford+T circuits play an important role in many quantum algorithms.
- A good solution to CMP yields shorter quantum circuits.
- **Can we find a good solution to the CMP for** $\mathrm{O}_n(\mathbb{Z}[1/2])$ and $\mathrm{U}_n(\mathbb{Z}[1/2, i])$?

Basic Matrices in $\mathrm{O}_n(\mathbb{Z}[1/2])$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad (-1) = [-1],$$

$$K = H \otimes H = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \text{ where } H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Basic Matrices in $U_n(\mathbb{Z}[\frac{1}{2}, i])$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad (i) = [i],$$

$$\omega^\dagger H = \frac{\omega^\dagger}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1-i & 1-i \\ 1-i & -1+i \end{bmatrix}, \text{ where } \omega = \frac{1+i}{\sqrt{2}}.$$

Two-level Operators

Definition

Let $U = \begin{bmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{bmatrix}$. The action of $U_{[\alpha,\beta]}$, $1 \le \alpha < \beta \le n$, is defined as

$$U_{[\alpha,\beta]} v = w, \text{ where } \begin{cases} \begin{bmatrix} w_\alpha \\ w_\beta \end{bmatrix} = U \begin{bmatrix} v_\alpha \\ v_\beta \end{bmatrix}, \\ w_i = v_i, i \notin \{\alpha, \beta\}. \end{cases}$$

Let $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Then $X_{[2,4]} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ and $X_{[2,4]} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix} = \begin{bmatrix} v_1 \\ v_4 \\ v_3 \\ v_2 \end{bmatrix}$.

Four-level Operators

Create a four-level operator by embedding a 4×4 matrix U into an $n \times n$ identity matrix.

$$\text{Let } K = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \text{ Then } K_{[1,2,4,5]} = \begin{bmatrix} 1/2 & 1/2 & 0 & 1/2 & 1/2 \\ 1/2 & -1/2 & 0 & 1/2 & -1/2 \\ 0 & 0 & 1 & 0 & 0 \\ 1/2 & 1/2 & 0 & -1/2 & -1/2 \\ 1/2 & -1/2 & 0 & -1/2 & 1/2 \end{bmatrix}.$$

$$K_{[1,2,4,5]}\begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{bmatrix} = \begin{bmatrix} (v_1 + v_2 + v_4 + v_5)/2 \\ (v_1 - v_2 + v_4 - v_5)/2 \\ v_3 \\ (v_1 + v_2 - v_4 - v_5)/2 \\ (v_1 - v_2 - v_4 + v_5)/2 \end{bmatrix}.$$

Generators for $\mathrm{O}_n(\mathbb{Z}[1/2])$

Let $\mathcal{G} = \left\{(-1)_{[\alpha]}, X_{[\alpha,\beta]}, K_{[\alpha,\beta,\gamma,\delta]} : 1 \leq \alpha < \beta < \gamma < \delta \leq n\right\}$. Then $\mathcal{G}$ is a generating set for $\mathrm{O}_n(\mathbb{Z}[1/2])$:

Theorem (Amy et al., 2020)

Let M be a unitary $n \times n$ matrix. Then $M \in \mathrm{O}_n(\mathbb{Z}[1/2])$ if and only if M can be written as a product of elements of $\mathcal{G}$.

Proof

($\Leftarrow$) $\mathcal{G} \subseteq \mathrm{O}_n(\mathbb{Z}[1/2])$ and $\mathrm{O}_n(\mathbb{Z}[1/2])$ is closed under multiplication.

($\Rightarrow$) For every $M \in \mathrm{O}_n(\mathbb{Z}[1/2])$, construct a sequence of generators representing M.

The Exact Synthesis Algorithm

- The algorithm proceeds one column at a time, reducing each column to a corresponding basis vector.
- While outputting a word $\overrightarrow{G_\ell}$ after each iteration, the algorithm recursively acts on the input matrix until it is reduced to the identity matrix $\mathbb{I}$.

$$M \xrightarrow{\overrightarrow{G_1}} \left(\begin{array}{ccc|c} & & & 0 \\ & M' & & \vdots \\ & & & 0 \\ \hline 0 & \cdots & 0 & 1 \end{array}\right) \xrightarrow{\overrightarrow{G_2}} \left(\begin{array}{ccc|cc} & & & 0 & 0 \\ & M'' & & \vdots & \vdots \\ & & & 0 & 0 \\ \hline 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & 0 & 0 & 1 \end{array}\right) \xrightarrow{\overrightarrow{G_3}} \cdots \xrightarrow{\overrightarrow{G_\ell}} \mathbb{I}$$

$$\overrightarrow{G_\ell} \cdot \cdots \cdot \overrightarrow{G_1} M = \mathbb{I} \Rightarrow M = \overrightarrow{G_1}^{-1} \cdot \cdots \cdot \overrightarrow{G_\ell}^{-1}$$

The Least Denominator Exponent (LDE)

Let $t \in \mathbb{Z}[\frac{1}{2}]$. $t = \frac{a}{2^k}$, where $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. k is a *denominator exponent* of t. The minimal such k is called the *least denominator exponent* of t, written $\text{lde}(t)$.

$$v = \frac{1}{2^{7}} \begin{bmatrix} 54 \\ 62 \\ 98 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \end{bmatrix} = \frac{2}{2^7} \begin{bmatrix} 27 \\ 31 \\ 49 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2^6} \begin{bmatrix} 27 \\ 31 \\ 49 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$\text{lde}(v) = 6$$

$$U = \frac{1}{2} \begin{bmatrix} -1 & 1 & 1 & 0 & 1 & 0 \\ -1 & -1 & 0 & 1 & 0 & 1 \\ -1 & 1 & -1 & 0 & -1 & 0 \\ -1 & -1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 1 & -1 & -1 \\ 0 & 0 & 1 & -1 & -1 & 1 \end{bmatrix}$$

$$\text{lde}(U) = 1$$

Lemma (Base Case)

Let $v \in \mathbb{Z}[\frac{1}{2}]^n$ *be a unit vector. Let* $k = \operatorname{lde}(v)$*. If* $k = 0$*, then* $v = \pm e_j$ *for some* $j \in \{1, \ldots, n\}$*.*

Lemma (Count)

Let $v \in \mathbb{Z}[\frac{1}{2}]^n$ *be a unit vector, and* $\operatorname{lde}(v) = k > 0$*. Let* $w = 2^k v$*. Then the number of odd entries in* w *is a multiple of* 4*.*

Lemma (Parity Reduction)

Let u_1, u_2, u_3, u_4 *be odd integers. Then there exist* $\tau_1, \tau_2, \tau_3, \tau_4 \in \mathbb{Z}_2$ *such that*

$$K_{[1,2,3,4]}(-1)^{\tau_1}_{[1]}(-1)^{\tau_2}_{[2]}(-1)^{\tau_3}_{[3]}(-1)^{\tau_4}_{[4]} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix} = \begin{bmatrix} u_1' \\ u_2' \\ u_3' \\ u_4' \end{bmatrix},\ u_1', u_2', u_3', u_4' \text{ are even integers.}$$

Input: $v \in \mathbb{Z}[\frac{1}{2}]^8$ Output: G_1, G_2, G_3 Result: $G_3 \cdot G_2 \cdot G_1 \cdot v = e_1$

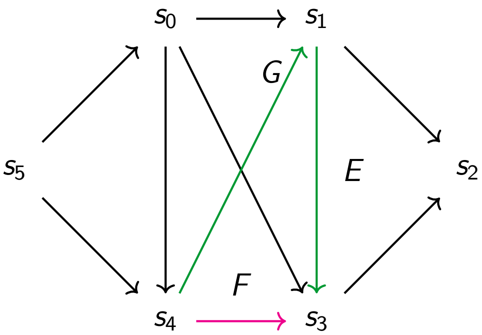
$$v : \frac{1}{4}\begin{pmatrix} -1 \\ 1 \\ -1 \\ -1 \\ 3 \\ 1 \\ 1 \\ 1 \end{pmatrix} \xrightarrow{G_1 = K_{[1,2,3,4]}(-1)_{[4]}(-1)_{[3]}(-1)_{[1]}} v' : \frac{1}{4}\begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 3 \\ 1 \\ 1 \\ 1 \end{pmatrix} \xrightarrow{G_2 = K_{[5,6,7,8]}(-1)_{[5]}}$$

$\text{lde}(v) = 2$ $\text{lde}(v') = 2$

$$v'' : \frac{1}{4}\begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 0 \\ -2 \\ -2 \\ -2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ -1 \\ -1 \end{pmatrix} \xrightarrow{G_3 = K_{[1,6,7,8]}(-1)_{[8]}(-1)_{[7]}(-1)_{[6]}} v''' : \frac{1}{2}\begin{pmatrix} 2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = e_1.$$

$\text{lde}(v'') = 1$ $\text{lde}(v''') = 0$

Cayley Graph of $\mathrm{O}_n(\mathbb{Z}[1/2])$



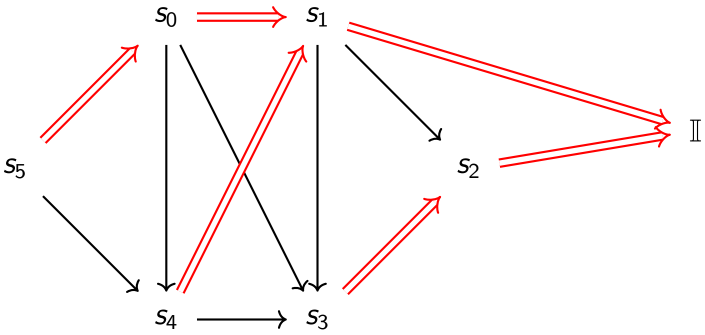
Vertex := group element (aka, operators, matrices, states).

Edge := a generator.

Cycle := relation.

Normal Form

The exact synthesis algorithm gives a canonical path from each group element to $\mathbb{I}$.



Semantic Equivalence

- A *word* is a sequence of generators. We write $\overrightarrow{G}$ for $G_q \ldots G_1$.
- Each operator has a unique *normal form*, which is the word output by the exact synthesis algorithm.
- The *interpretation* of $\overrightarrow{G}$ is $[\![\overrightarrow{G}]\!] = G_q \cdot \ldots \cdot G_1$.

Definition

Two words $\overrightarrow{G}$ and $\overrightarrow{F}$ are *semantically equivalent*, written $\overrightarrow{G} \sim \overrightarrow{F}$, if $[\![\overrightarrow{G}]\!] = [\![\overrightarrow{F}]\!]$.

Motivation

- Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two words where $\mathcal{C}_1 = X_{[1,2]}X_{[3,4]}X_{[1,2]}$ and $\mathcal{C}_2 = X_{[3,4]}$.
- To see if $\mathcal{C}_1 \sim \mathcal{C}_2$, we can check by direct computation or by simplifying $\mathcal{C}_1$.

$$\mathcal{C}_1 = X_{[1,2]}X_{[3,4]}X_{[1,2]} \sim X_{[1,2]}X_{[1,2]}X_{[3,4]} \sim \mathbb{I}X_{[3,4]} \sim X_{[3,4]} = \mathcal{C}_2.$$

Syntactic Equivalence

Definition

Two words $\overrightarrow{G}$ and $\overrightarrow{F}$ are *syntactically equivalent*, written $\overrightarrow{G} \approx \overrightarrow{F}$, where $\approx$ is the smallest congruence relation on words containing $R_1, \ldots, R_k$ and such that

$$\overrightarrow{G} \approx \overrightarrow{G'}, \overrightarrow{F} \approx \overrightarrow{F'} \Rightarrow \overrightarrow{G}\,\overrightarrow{F} \approx \overrightarrow{G'}\overrightarrow{F'}.$$

Question: Can we use syntactic and semantic relations interchangeably?

Soundness and Completeness

Theorem (Analogous to Greylyn's Theorem, 2014)

Let $\overrightarrow{G}$ *and* $\overrightarrow{F}$ *be words over* $\mathcal{G}$ *of* $\mathrm{O}_n(\mathbb{Z}[1/2])$*, then*

$$\overrightarrow{G} \approx \overrightarrow{F} \iff \overrightarrow{G} \sim \overrightarrow{F}.$$

Proof.

($\Rightarrow$) Soundness: By matrix multiplication.

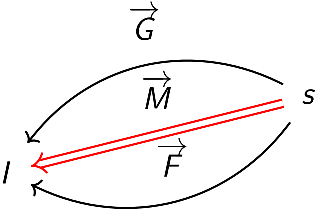
($\Leftarrow$) Completeness: Use induction to leverage **finitely** many syntactic relations such that an arbitrary path can be rewritten into its equivalent canonical path.

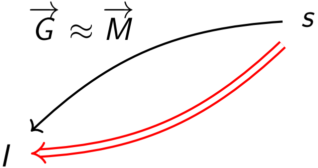
$\square$

Theorem (Completeness)

$\overrightarrow{G} \sim \overrightarrow{F} \Rightarrow \overrightarrow{G} \approx \overrightarrow{F}$

Proof Idea. If two words are semantically equivalent, they corresponds to the same normal form. If we can reduce an arbitrary path to its normal form using **syntactic relations**, this implies completeness.



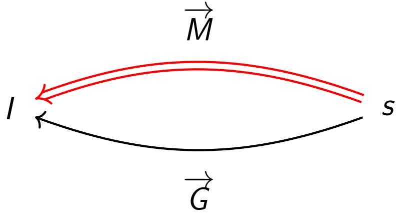


Proof of Completeness

Lemma 1

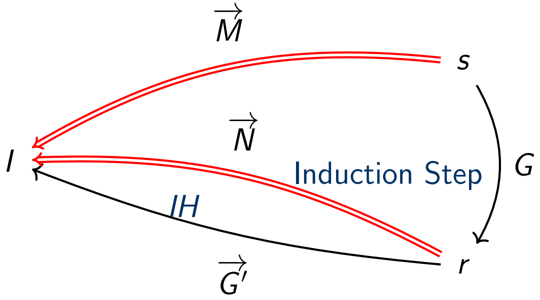
Let $s \xrightarrow{\overrightarrow{G}} I$ be any sequence of simple edges with final state I, and let $s \xRightarrow{\overrightarrow{M}} I$ be the unique sequence of normal edges from s to I. Then $\overrightarrow{G} \approx \overrightarrow{M}$.

Proof Idea. Proceed by induction on the length of $\overrightarrow{G}$.



Lemma 1

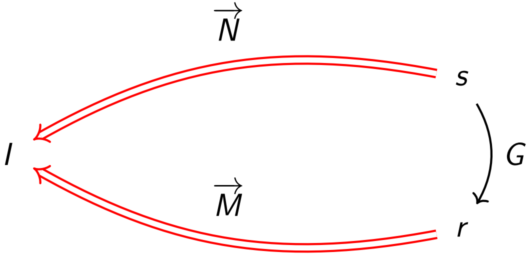
Let $s \xrightarrow{\overrightarrow{G}} l$ be any sequence of simple edges with final state l, and let $s \xRightarrow{\overrightarrow{M}} l$ be the unique sequence of normal edges from s to l. Then $\overrightarrow{G} \approx \overrightarrow{M}$.



Lemma 2

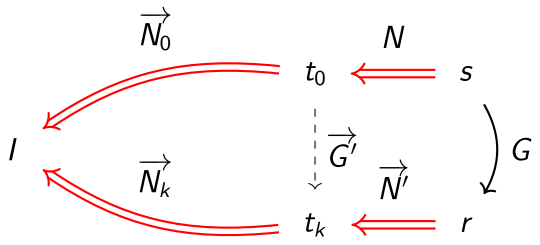
Let $s \xrightarrow{G} r$ be a simple edge. Let $s \xRightarrow{\overrightarrow{N}} l$ be the unique sequence of normal edges from s to l, $r \xRightarrow{\overrightarrow{M}} l$ be the unique sequence of normal edges from r to l. Then $\overrightarrow{M} G \approx \overrightarrow{N}$.

Proof Idea. Proceed by induction on the level of s.



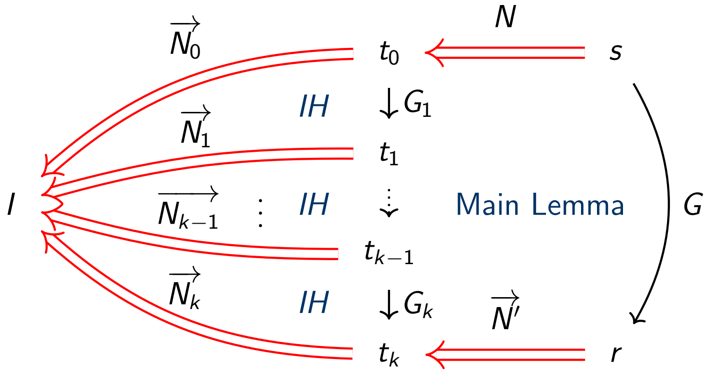
Lemma 2

Let $s \xrightarrow{G} r$ be a simple edge. Let $s \xRightarrow{\overrightarrow{N}} l$ be the unique sequence of normal edges from s to l, $r \xRightarrow{\overrightarrow{M}} l$ be the unique sequence of normal edges from r to l. Then $\overrightarrow{M}G \approx \overrightarrow{N}$.



Lemma 2

Let $s \xrightarrow{G} r$ be a simple edge. Let $s \xRightarrow{\overrightarrow{N}} I$ be the unique sequence of normal edges from s to I, $r \xRightarrow{\overrightarrow{M}} I$ be the unique sequence of normal edges from r to I. Then $\overrightarrow{M} G \approx \overrightarrow{N}$.



Main Lemma

Let s, t, and r be states, $N : s \Rightarrow t$ be a normal edge, and $G : s \rightarrow r$ be a simple edge. Then there exists a state q, a sequence of normal edges $\overrightarrow{N'} : r \Rightarrow q$ and a sequence of simple edges $\overrightarrow{G'} : t \rightarrow q$ such that the diagram

$$\begin{array}{ccc} s & \xrightarrow{\;G\;} & r \\ N \Big\Downarrow & & \Big\Downarrow \overrightarrow{N'} \\ & \overrightarrow{G'} & \\ t & \dashrightarrow & q \end{array}$$

commutes syntactically and $\text{level}(\overrightarrow{G'} : t \rightarrow q) < \text{level}(s)$.

Proof Idea. Since t and N are uniquely determined by s, and r is uniquely determined by G, it suffices to distinguish cases based on the pair (s, G).

Relations for $\mathrm{O}_n(\mathbb{Z}[1/2])$

$$X^2_{[a,b]} \approx \epsilon \quad (1a)$$

$$(-1)^2_{[a]} \approx \epsilon \quad (1b)$$

$$K^2_{[a,b,c,d]} \approx \epsilon \quad (1c)$$

$$X_{[a,b]}X_{[c,d]} \approx X_{[c,d]}X_{[a,b]} \quad (2a)$$

$$X_{[a,b]}(-1)_{[c]} \approx (-1)_{[c]}X_{[a,b]} \quad (2b)$$

$$X_{[a,b]}K_{[c,d,e,f]} \approx K_{[c,d,e,f]}X_{[a,b]} \quad (2c)$$

$$(-1)_{[a]}(-1)_{[b]} \approx (-1)_{[b]}(-1)_{[a]} \quad (2d)$$

$$(-1)_{[a]}K_{[b,c,d,e]} \approx K_{[b,c,d,e]}(-1)_{[a]} \quad (2e)$$

$$K_{[a,b,c,d]}K_{[e,f,g,h]} \approx K_{[e,f,g,h]}K_{[a,b,c,d]} \quad (2f)$$

$$X_{[a,a']}X_{[a,b]} \approx X_{[a',b]}X_{[a,a']} \quad (3a)$$

$$X_{[b,b']}X_{[a,b]} \approx X_{[a,b']}X_{[b,b']} \quad (3b)$$

$$X_{[a,b]}(-1)_{[b]} \approx (-1)_{[a]}X_{[a,b]} \quad (3c)$$

$$X_{[a,a']}K_{[a,b,c,d]} \approx K_{[a',b,c,d]}X_{[a,a']} \quad (3d)$$

$$X_{[b,b']}K_{[a,b,c,d]} \approx K_{[a,b',c,d]}X_{[b,b']} \quad (3e)$$

$$X_{[c,c']}K_{[a,b,c,d]} \approx K_{[a,b,c',d]}X_{[c,c']} \quad (3f)$$

$$X_{[d,d']}K_{[a,b,c,d]} \approx K_{[a,b,c,d']}X_{[d,d']} \quad (3g)$$

$$X_{[c,d]}K_{[a,b,c,d]} \approx K_{[a,b,c,d]}X_{[b,d]} \quad (4a)$$

$$X_{[b,c]}K_{[a,b,c,d]} \approx (-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]}K_{[a,b,c,d]}(-1)_{[a]} \quad (4b)$$

$$X_{[a,b]}K_{[a,b,c,d]} \approx K_{[a,b,c,d]}X_{[b,d]}(-1)_{[b]}(-1)_{[d]} \quad (4c)$$

$$K_{[a,b,c,d]}K_{[b,d,e,f]} \approx K_{[c,d,e,f]}K_{[a,b,c,e]} \quad (5a)$$

$$(-1)_{[a]}(-1)_{[e]}X_{[a,e]}K_{[e,f,g,h]}K_{[a,b,c,d]}X_{[d,e]}K_{[a,b,c,d]}K_{[e,f,g,h]}X_{[a,e]}(-1)_{[a]}(-1)_{[e]} \approx K_{[e,f,g,h]}K_{[a,b,c,d]}X_{[d,e]}K_{[a,b,c,d]}K_{[e,f,g,h]} \quad (6a)$$

Remark: The indices are distinct and the relations are well-formed. For example, in Relation (5a), we have $a < b < c < d < e < f$.

Relations for $U_n(\mathbb{Z}[\frac{1}{2}, i])$

$$
\begin{aligned}
i_{[j]}^4 &\approx \varepsilon && (1)\\
X_{[j,k]}^2 &\approx \varepsilon && (2)\\
K_{[j,k]}^8 &\approx \varepsilon && (3)
\end{aligned}
$$

$$
\begin{aligned}
i_{[j]} i_{[k]} &\approx i_{[k]} i_{[j]} && (4)\\
i_{[j]} X_{[k,\ell]} &\approx X_{[k,\ell]} i_{[j]} && (5)\\
i_{[j]} K_{[k,\ell]} &\approx K_{[k,\ell]} i_{[j]} && (6)\\
X_{[j,k]} X_{[\ell,m]} &\approx X_{[\ell,m]} X_{[j,k]} && (7)\\
X_{[j,k]} K_{[\ell,m]} &\approx K_{[\ell,m]} X_{[j,k]} && (8)\\
K_{[j,k]} K_{[\ell,m]} &\approx K_{[\ell,m]} K_{[j,k]} && (9)
\end{aligned}
$$

$$
\begin{aligned}
i_{[k]} X_{[j,k]} &\approx X_{[j,k]} i_{[j]} && (10)\\
X_{[k,\ell]} X_{[j,k]} &\approx X_{[j,k]} X_{[j,\ell]} && (11)\\
X_{[j,\ell]} X_{[k,\ell]} &\approx X_{[k,\ell]} X_{[j,k]} && (12)\\
K_{[k,\ell]} X_{[j,k]} &\approx X_{[j,k]} K_{[j,\ell]} && (13)\\
K_{[j,\ell]} X_{[k,\ell]} &\approx X_{[k,\ell]} K_{[j,k]} && (14)
\end{aligned}
$$

$$
\begin{aligned}
K_{[j,k]} i_{[k]}^2 &\approx X_{[j,k]} K_{[j,k]} && (15)\\
K_{[j,k]} i_{[k]}^3 &\approx i_{[k]} K_{[j,k]} i_{[k]} K_{[j,k]} && (16)\\
K_{[j,k]} i_{[j]} i_{[k]} &\approx i_{[j]} i_{[k]} K_{[j,k]} && (17)\\
K_{[j,k]}^2 i_{[j]} i_{[k]} &\approx \varepsilon && (18)\\
K_{[j,k]} K_{[\ell,m]} K_{[j,\ell]} K_{[k,m]} &\approx K_{[j,\ell]} K_{[k,m]} K_{[j,k]} K_{[\ell,m]} && (19)
\end{aligned}
$$

Remark: We redefine K to be $\omega^\dagger H$.

Future Work

- Improve the complexity of the exact synthesis algorithm.
- Investigate restricted Clifford+T circuit relations.
- Find a minimal set of syntactic relations for $\mathrm{O}_n(\mathbb{Z}[1/2])$ and $\mathrm{U}_n(\mathbb{Z}[1/2, i])$.
- Find syntactic relations for other restricted Clifford+T matrix groups such as the imaginary Clifford+T circuits.

Thank you!