# Optimal ancilla-free Clifford+T approximation of z-rotations
# 実装ノート

量子プログラミングコンテスト　出題者一同

2024 年 10 月 6 日

本ノートは、Pauli rotation の Clifford+T 分解を行う nearl-optimal な手法を与えた論文 [4] の実装 (特に grid problem の解法) に関するノートである。流れは原論文に従って書かれているが、Ross-Selinger による Haskell 実装 [1] を参考に一部加筆されている。本ノートの内容はすでに `pygridsynth` として実装されている。

コンテスト課題については、`problem.ipynb` を参照されたい。

## 1 Some algebra

**Definition 1.1** ([4, Definition 3.1])**.** (Extensions of $\mathbb{Z}$)
$\omega = (1+i)/\sqrt{2}$.

- $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$,
- $\mathbb{Z}[\omega] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a, b, c, d \in \mathbb{Z}\}$,
- $\mathbb{D} = \mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^k} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$,
- $\mathbb{D}[\sqrt{2}] = \mathbb{Z}[\frac{1}{\sqrt{2}}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{D}\}$,
- $\mathbb{D}[\omega] = \mathbb{Z}[\frac{1}{\sqrt{2}}, i] = \{a\omega^3 + b\omega^2 + c\omega + d \mid a, b, c, d \in \mathbb{D}\}$.

$\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Z}[\omega]$, $\mathbb{D} \subseteq \mathbb{D}[\sqrt{2}] \subseteq \mathbb{D}[\omega]$, $\mathbb{Z} \subseteq \mathbb{D}$, $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{D}[\sqrt{2}]$, $\mathbb{Z}[\omega] \subseteq \mathbb{D}[\omega]$. $\mathbb{Z}[\sqrt{2}]$ と $\mathbb{Z}[\omega]$ は $\mathbb{R}$, $\mathbb{C}$ 上で dense.

**Definition 1.2** ([4, Definition 3.2])**.** (Automorphisms)

- Complex conjugation:
$$(a\omega^3 + b\omega^2 + c\omega + d)^\dagger = -c\omega^3 - b\omega^2 - a\omega + d \tag{1}$$
- $\sqrt{2}$-conjugation:
$$(a\omega^3 + b\omega^2 + c\omega + d)^\bullet = -a\omega^3 + b\omega^2 - c\omega + d \tag{2}$$

$\lambda = 1 + \sqrt{2}$ と定義する．このとき，$\lambda^{-1} = -1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, $\lambda^\bullet = 1 - \sqrt{2} = -\lambda^{-1} \in \mathbb{Z}[\sqrt{2}]$.

**Definition 1.3** ([4, Definition 3.4])**.** $t \in \mathbb{D}[\omega]$, $k \in \mathbb{N}$ とする．$\sqrt{2}^k t \in \mathbb{Z}[\omega]$ のとき，$k$ を $t$ の denominator exponent と呼ぶ．$k \geq 0$ での $k$ の最小値を $t$ の least denominator exponent と呼ぶ.

## 2 One-dimensional grid problem ([4, Section 4])

**Definition 2.1** ([4, Definition 4.3])**.** $I, J \subseteq \mathbb{R}$ とする．

**One-dimensional grid problem (ODGP):** $\alpha \in I$ かつ $\alpha^\bullet \in J$ を満たす $\alpha \in \mathbb{Z}[\sqrt{2}]$ を見つける．

$\mathbb{R}$ 上の閉区間の組 $I, J$ に対する one-dimensional grid problem の解集合を $S_{\mathrm{ODGP}}(I, J)$ とする．$\mathbb{R}$ 上の閉区間 $I = [I_l, I_r]$ に対して，$\Delta_I \coloneqq I_r - I_l$ と定義する．

**Algorithm 2.2.** $\mathbb{R}$ 上の閉区間の組 $I = [I_l, I_r], J = [J_l, J_r]$ に対して，$S_{\mathrm{ODGP}}(I, J)$ を求めるアルゴリズム (gridpoints in [6], solve_ODGP in [7]):

1. $\Delta_I < 0$ または $\Delta_J < 0$ のとき，解なし．
2. $a_0 = \lfloor (I_l + J_l)/2 \rfloor$, $b_0 = \left\lfloor (I_l - J_l)/\sqrt{2}^3 \right\rfloor$, $\alpha_0 = a_0 + b_0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ を計算し，$I' = I - \alpha_0$, $J' = J - \alpha_0^\bullet$ に対する ODGP の解集合の候補 $S'$ を計算する．
3. $S = \{\alpha + \alpha_0 \mid \alpha \in S', \alpha + \alpha_0 \in I, (\alpha + \alpha_0)^\bullet \in J\}$ が求める集合である．

$I, J$ に対する ODGP の解集合の候補を求めるアルゴリズム (gridpoints_internal in [6], _solve_ODGP_internal in [7]):

1. $\Delta_I < 0$ または $\Delta_J < 0$ のとき，空集合を返す．
2. $\Delta_I > 0$ かつ $\Delta_J \leq 0$ のとき，$J, I$ に対する ODGP の解集合の候補 $S'$ をこのアルゴリズムによって求め，$S = \{\alpha^\bullet \mid \alpha \in S'\}$ を返す．
3. $\Delta_I \leq 0$ かつ $\Delta_J \leq 0$ のとき，6 に進む．
4. $\Delta_J > 0$ のとき，$n = \lfloor \log_\lambda \Delta_J \rfloor$ を計算し，$n \neq 0$ のとき 5 に進み，$n = 0$ のとき 6 に進む．
5. $I' = \lambda^n I$, $J' = (\lambda^\bullet)^n J$ に対する ODGP の解集合の候補 $S'$ をこのアルゴリズムによって求め，$S = \{\lambda^{-n}\alpha \mid \alpha \in S'\}$ を返す．
6. $S$ を空集合で初期化し，$a_{\min} = \lceil (I_l + J_l)/2 \rceil$, $a_{\max} = \lfloor (I_r + J_r)/2 \rfloor$ を計算する．
7. $a = a_{\min}, \ldots, a_{\max}$ について，$b_{\min} = \left\lceil (a - J_r)/\sqrt{2} \right\rceil$, $b_{\max} = \left\lfloor (a - J_l)/\sqrt{2} \right\rfloor$ を計算し，$b = b_{\min}, \ldots, b_{\max}$ について，$a + b\sqrt{2}$ を $S$ に追加する．
8. $S$ を返す．

**Lemma 2.3.** $a_0 \coloneqq \lfloor (I_l + J_l)/2 \rfloor$, $b_0 \coloneqq \left\lfloor (I_l - J_l)/\sqrt{2}^3 \right\rfloor$, $\alpha_0 \coloneqq a_0 + b_0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, $I' \coloneqq I - \alpha_0$, $J' \coloneqq J - \alpha_0$ と定義する．このとき，$0 \leq I'_l < \lambda$, $-\sqrt{2} < J'_l < 1$ が成り立つ．

*Proof.*

$$I'_l = I_l - \left\lfloor \frac{I_l + J_l}{2} \right\rfloor - \left\lfloor \frac{I_l - J_l}{\sqrt{2}^3} \right\rfloor \sqrt{2} \geq I_l - \frac{I_l + J_l}{2} - \frac{I_l - J_l}{\sqrt{2}^3} \cdot \sqrt{2} = 0, \tag{3}$$

$$I'_l = I_l - \left\lfloor \frac{I_l + J_l}{2} \right\rfloor - \left\lfloor \frac{I_l - J_l}{\sqrt{2}^3} \right\rfloor \sqrt{2} < I_l - \left( \frac{I_l + J_l}{2} - 1 \right) - \left( \frac{I_l - J_l}{\sqrt{2}^3} - 1 \right) \cdot \sqrt{2} = \lambda, \tag{4}$$

$$J'_l = J_l - \left\lfloor \frac{I_l + J_l}{2} \right\rfloor + \left\lfloor \frac{I_l - J_l}{\sqrt{2}^3} \right\rfloor \sqrt{2} > J_l - \frac{I_l + J_l}{2} + \left( \frac{I_l - J_l}{\sqrt{2}^3} - 1 \right) \cdot \sqrt{2} = -\sqrt{2}, \tag{5}$$

$$J_l' = J_l - \left\lfloor \frac{I_l + J_l}{2} \right\rfloor + \left\lfloor \frac{I_l - J_l}{\sqrt{2}^3} \right\rfloor \sqrt{2} < J_l - \left( \frac{I_l + J_l}{2} - 1 \right) + \frac{I_l - J_l}{\sqrt{2}^3} \cdot \sqrt{2} = 1. \tag{6}$$

□

$\mathbb{R}$ 上の閉区間 $I, J$ と任意の $\alpha_0 \in \mathbb{Z}[\sqrt{2}]$ について，$\alpha + \alpha_0 \in S_{\mathrm{ODGP}}(I, J) \Leftrightarrow \alpha \in S_{\mathrm{ODGP}}(I - \alpha_0, J - \alpha_0^\bullet)$ であるから，$S_{\mathrm{ODGP}}(I, J)$ を求める問題は $S_{\mathrm{ODGP}}(I - \alpha_0, J - \alpha_0^\bullet)$ を求める問題に帰着できる．このとき，Lemma 2.3 で定めた $\alpha_0$ を選ぶことで，以降のアルゴリズムでの数値的不安定性が避けられる．

**Lemma 2.4** ([4, Proposition 4.5] の補足)**.** $\mathbb{R}$ 上の閉区間 $I, J$ に対して，$S_{\mathrm{ODGP}}(I, J) = \lambda S_{\mathrm{ODGP}}(\lambda^{-1} I, (\lambda^\bullet)^{-1} J)$, $S_{\mathrm{ODGP}}(I, J) = \lambda^{-1} S_{\mathrm{ODGP}}(\lambda I, \lambda^\bullet J)$ が成り立つ．

*Proof.* $\alpha \in S_{\mathrm{ODGP}}(I, J)$ を任意にとると，$\alpha \in I$, $\alpha^\bullet \in J$ より，

$$\lambda^{-1}\alpha \in \lambda^{-1} I, \tag{7}$$
$$(\lambda^{-1}\alpha)^\bullet = (\lambda^{-1})^\bullet \alpha^\bullet \in (\lambda^\bullet)^{-1} J \tag{8}$$

であるから，$\lambda^{-1}\alpha \in S_{\mathrm{ODGP}}(\lambda^{-1} I, (\lambda^\bullet)^{-1} J)$ より，$\alpha \in \lambda S_{\mathrm{ODGP}}(\lambda^{-1} I, (\lambda^\bullet)^{-1} J)$．一方，$\beta \in \lambda S_{\mathrm{ODGP}}(\lambda^{-1} I, (\lambda^\bullet)^{-1} J)$ を任意にとると，$\lambda^{-1}\beta \in \lambda^{-1} I$, $(\lambda^{-1}\beta)^\bullet \in (\lambda^\bullet)^{-1} J$ より，

$$\beta = \lambda(\lambda^{-1}\beta) \in \lambda(\lambda^{-1} I) = I, \tag{9}$$
$$\beta^\bullet = (\lambda^\bullet)^{-1}(\lambda^{-1}\beta)^\bullet \in (\lambda^\bullet)^{-1}((\lambda^\bullet)^{-1} J) = J \tag{10}$$

であるから，$\beta \in S_{\mathrm{ODGP}}(I, J)$．したがって，$S_{\mathrm{ODGP}}(I, J) = \lambda S_{\mathrm{ODGP}}(\lambda^{-1} I, (\lambda^\bullet)^{-1} J)$.

$S_{\mathrm{ODGP}}(I, J) = \lambda^{-1} S_{\mathrm{ODGP}}(\lambda I, \lambda^\bullet J)$ は，$\lambda$ を $\lambda^{-1}$ に置き換えて同様の議論を行えば証明できる． □

**Lemma 2.5.** $\mathbb{R}$ 上の閉区間 $I = [I_l, I_r], J = [J_l, J_r]$ に対して，

$$S_{\mathrm{ODGP}}(I, J) \subseteq \left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Z}, \frac{I_l + J_l}{2} \le a \le \frac{I_r + J_r}{2}, \frac{a - J_r}{\sqrt{2}} \le b \le \frac{a - J_l}{\sqrt{2}} \right\}. \tag{11}$$

*Proof.* $\alpha \in S_{\mathrm{ODGP}}(I, J) \subseteq \mathbb{Z}[\sqrt{2}]$ を任意にとり，$a, b \in \mathbb{Z}$ を用いて $\alpha = a + b\sqrt{2}$ と表せるとする．$a - b\sqrt{2} \in [J_l, J_r]$ より，$(a - J_r)/\sqrt{2} \le b \le (a - J_l)/\sqrt{2}$ が成り立つ．$a = (\alpha + \alpha^\bullet)/2$ と，$I_l \le \alpha \le I_r$, $J_l \le \alpha^\bullet \le J_r$ より，$(I_l + J_l)/2 \le a \le (I_r + J_r)/2$ が成り立つ．したがって，

$$a + b\sqrt{2} \in S_{\mathrm{ODGP}}(I, J) \Rightarrow \frac{I_l + J_l}{2} \le a \le \frac{I_r + J_r}{2} \wedge \frac{a - J_r}{\sqrt{2}} \le b \le \frac{a - J_l}{\sqrt{2}}. \tag{12}$$

□

**Proposition 2.6.** Algorithm 2.2 によって，$\mathbb{R}$ 上の閉区間の組 $I, J$ に対する one-dimensional grid problem の解集合，つまり，$\alpha \in I$ かつ $\alpha^\bullet \in J$ を満たす $\alpha \in \mathbb{Z}[\sqrt{2}]$ の集合 $S_{\mathrm{ODGP}}(I, J)$ が計算可能である．

*Proof.* まず，$\Delta_J = J_r - J_l > 0$ を仮定する．Lemma 2.4 より，$1 \le \lambda^{-n}\Delta_J < \lambda$ となるような $n \in \mathbb{Z}$ をとり，$I' \coloneqq \lambda^n I$, $J' \coloneqq (\lambda^\bullet)^n J$ と定義すると，$S_{\mathrm{ODGP}}(I, J) = \lambda^{-n} S_{\mathrm{ODGP}}(I', J')$ であるから，$S_{\mathrm{ODGP}}(I', J')$ を求める問題に帰着される．Lemma 2.5 より，$I' = [I_l', I_r']$, $J' = [J_l', J_r']$ に対して，

$$\frac{I_l' + J_l'}{2} \le a \le \frac{I_r' + J_r'}{2} \wedge \frac{a - J_r'}{\sqrt{2}} \le b \le \frac{a - J_l'}{\sqrt{2}} \tag{13}$$

を満たす全ての $(a,b)\in\mathbb{Z}^2$ のうち，$\alpha'=a+b\sqrt{2}$ が $\alpha'\in I'$ かつ $\alpha'^{\bullet}\in J'$ を満たすものからなる集合を $S_{\mathrm{ODGP}}(I',J')$ とすればよい．$a,b\in\mathbb{Z}$ より，

$$a=\left\lceil\frac{I'_l+J'_l}{2}\right\rceil,\dots,\left\lfloor\frac{I'_r+J'_r}{2}\right\rfloor, \tag{14}$$

$$b=\left\lceil\frac{a-J'_r}{\sqrt{2}}\right\rceil,\dots,\left\lfloor\frac{a-J'_l}{\sqrt{2}}\right\rfloor. \tag{15}$$

を調べればよい．

次に，$\Delta_J<0$ のとき，明らかに $S_{\mathrm{ODGP}}(I,J)=\emptyset$.

最後に，$\Delta_J=0$ のときを考える．$\Delta_I<0$ のとき，明らかに $S_{\mathrm{ODGP}}(I,J)=\emptyset$. $\Delta_I>0$ のとき，$\alpha\in S_{\mathrm{ODGP}}(I,J)\Leftrightarrow\alpha^{\bullet}\in S_{\mathrm{ODGP}}(J,I)$ より，$S_{\mathrm{ODGP}}(I,J)=\{\alpha^{\bullet}\mid\alpha\in S_{\mathrm{ODGP}}(J,I)\}$．よって，$S_{\mathrm{ODGP}}(J,I)$ を求める問題に帰着される．$\Delta_I=0$ のとき，$n=0$ として $\Delta_J>0$ の場合と同じように解けばよい． □

**Lemma 2.7** ([4, Proposition 4.5] の補足)**.** $\mathbb{R}$ 上の閉区間 $I=[I_l,I_r],J=[J_l,J_r]$ に対して，$\Delta_I\coloneqq I_r-I_l$, $\Delta_J\coloneqq J_r-J_l$ と定義すると，$|S_{\mathrm{ODGP}}(I,J)|=\Omega(\Delta_I\Delta_J)$.

証明は Appendix A を参照.

**Proposition 2.8.** $\mathbb{R}$ 上の閉区間 $I=[I_l,I_r],J=[J_l,J_r]$ に対して，$\Delta_I\coloneqq I_r-I_l$, $\Delta_J\coloneqq J_r-J_l$ と定義すると，Algorithm 2.2 の時間計算量は $O(\Delta_I\Delta_J)$ であり，オーダーの意味で最善である.

*Proof.* $1\le\lambda^{-n}\Delta_J<\lambda$ となるような $n\in\mathbb{Z}$ をとり，$I'\coloneqq\lambda^n I$, $J'\coloneqq(\lambda^{\bullet})^n J$ と定義する．$\Delta_{I'}=I'_l-I'_r$, $\Delta_{J'}=J'_l-J'_r$ とおくと，Algorithm 2.2 で調べる $a$ の個数は $(I'_r+J'_r)/2-(I'_l+J'_l)/2+1=(\Delta_{I'}+\Delta_{J'})/2+1$ で抑えられ，それぞれについて，調べる $b$ の個数は $(a-J'_l)/\sqrt{2}-(a-J'_r)/\sqrt{2}+1=\Delta_{J'}/\sqrt{2}+1$ で抑えられる．$1\le\Delta'_J<\lambda=1+\sqrt{2}$ より，$(\Delta_{I'}+\Delta_{J'})/2+1<\Delta_{I'}/2+3$, $\Delta_{J'}/\sqrt{2}+1<3$ であるから，Algorithm 2.2 の時間計算量は $O(\Delta_{I'})$ である．$\Delta_{I'}=\lambda^n\Delta_I$, $\Delta_{J'}=|(\lambda^{\bullet})^n|\Delta_J=\lambda^{-n}\Delta_J$ より，$\Delta_{I'}\Delta_{J'}=\Delta_I\Delta_J$ であるから，$O(\Delta_{I'})=O(\Delta_{I'}\Delta_{J'})=O(\Delta_I\Delta_J)$ となる．

一方，Lemma 2.7 より，解の個数は $\Omega(\Delta_I\Delta_J)$ であるから，解を全て列挙するには $\Omega(\Delta_I\Delta_J)$ 時間必要である． □

# 3 Two-dimensional grid problem ([4, Section 5])

以降，$(x,y)\in\mathbb{R}^2$ と $x+yi\in\mathbb{C}$ を対応させることで，$\mathbb{C}$ と $\mathbb{R}^2$ を同一視する.

**Definition 3.1** ([4, Definition 5.3])**.** $A,B\subseteq\mathbb{R}^2$ とする.

**Two-dimensional grid problem:** $u\in A$ かつ $u^{\bullet}\in B$ を満たす $u\in\mathbb{Z}[\omega]$ を見つける.

$A,B\subseteq\mathbb{R}^2$ に対して，two-dimensional grid problem の解集合を $S_{\mathrm{TDGP}}(A,B)$ とする．つまり，

$$S_{\mathrm{TDGP}}(A,B)=\{u\in\mathbb{Z}[\omega]\mid u\in A,u^{\bullet}\in B\}. \tag{16}$$

## 3.1 Upright rectangles

$\mathcal{I}\subseteq\mathbb{R}^2$ が $[I_{x,l},I_{x,r}]\times[I_{y,l},I_{y,r}]$ の形で書けるとき，$\mathcal{I}$ を upright rectangle と呼ぶ.

**Algorithm 3.2.** upright rectangle の組 $\mathcal{I} = I_x \times I_r, \mathcal{J} = J_x \times J_r$ に対して，$S_{\mathrm{ODGP}}(\mathcal{I}, \mathcal{J})$ を求めるアルゴリズム (solve_TDGP_for_upright_rectangle in [7]):

1. $S_\alpha = \text{solve\_ODGP}(I_x, J_x)$ と $S_\beta = \text{solve\_ODGP}(I_y, J_y)$ を計算する．
2. $I'_x = I_x - 1/\sqrt{2}$, $I'_y = I_y - 1/\sqrt{2}$, $J'_x = J_x + 1/\sqrt{2}$, $J'_y = J_y + 1/\sqrt{2}$ と定義し，$S'_\alpha = \text{solve\_ODGP}(I'_x, J'_x)$ と $S'_\beta = \text{solve\_ODGP}(I'_y, J'_y)$ を計算する．
3. $S = \{\alpha + \beta i \mid \alpha \in S_\alpha, \beta \in S_\beta\} \cup \left\{\alpha + \beta i + \omega \;\middle|\; \alpha \in S'_\alpha, \beta \in S'_\beta\right\}$ を返す．

**Lemma 3.3** ([4, Lemma 5.5])**.** $u \in \mathbb{C}$ について，$\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ を用いて $u = \alpha + \beta i$ または $u = \alpha + \beta i + \omega$ と書けるとき，かつそのときに限り，$u \in \mathbb{Z}[\omega]$ である．

*Proof.* ‘if’ part は $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Z}[\omega]$ と $\mathbb{Z}[\omega]$ が和と積に関して閉じていることより従う．

‘only if’ part について，$u \in \mathbb{Z}[\omega]$ のとき，$a, b, c, d \in \mathbb{Z}$ を用いて $u = a\omega^3 + b\omega^2 + c\omega + d$ と表せるから，

$$u = a\frac{-1+i}{\sqrt{2}} + bi + c\frac{1+i}{\sqrt{2}} + d = \left(d + \frac{c-a}{2}\sqrt{2}\right) + \left(b + \frac{c+a}{2}\sqrt{2}\right)i. \tag{17}$$

$c - a$ が偶数のとき，$\frac{c-a}{2}, \frac{c+a}{2} \in \mathbb{Z}$ より，

$$\alpha \coloneqq d + \frac{c-a}{2}\sqrt{2} \in \mathbb{Z}[\sqrt{2}], \tag{18}$$

$$\beta \coloneqq b + \frac{c+a}{2}\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \tag{19}$$

と定義すれば，$u = \alpha + \beta i$ の形で書ける．$c - a$ が奇数のとき，$\frac{c-a-1}{2}, \frac{c+a-1}{2} \in \mathbb{Z}$ より，

$$\alpha \coloneqq d + \frac{c-a-1}{2}\sqrt{2} \in \mathbb{Z}[\sqrt{2}], \tag{20}$$

$$\beta \coloneqq b + \frac{c+a-1}{2}\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \tag{21}$$

と定義すれば，$u = \alpha + \beta i + \omega$ の形で書ける． □

**Proposition 3.4** ([4, Lemma 5.6])**.**

*Proof.* $\mathcal{I}$ と $\mathcal{J}$ が upright rectangle のとき，閉区間 $I_x, I_y, J_x, J_y \subseteq \mathbb{R}$ を用いて $\mathcal{I} = I_x \times I_y$, $\mathcal{J} = J_x \times J_y$ と表せる．Lemma 3.3 より，任意の解は $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ を用いて $u = \alpha + \beta i$ または $u = \alpha + \beta i + \omega$ の形で書ける．前者の場合，

$$u = \alpha + \beta i \in \mathcal{I} = I_x \times I_y \Leftrightarrow \alpha \in I_x \wedge \beta \in I_y, \tag{22}$$

$$u^\bullet = \alpha^\bullet + \beta^\bullet i \in \mathcal{J} = J_x \times J_y \Leftrightarrow \alpha^\bullet \in J_x \wedge \beta^\bullet \in J_y \tag{23}$$

より，

$$\begin{aligned} u \in S_{\mathrm{TDGP}}(\mathcal{I}, \mathcal{J}) &\Leftrightarrow u \in \mathcal{I} \wedge u^\bullet \in \mathcal{J} \\ &\Leftrightarrow \alpha \in I_x \wedge \beta \in I_y \wedge \alpha^\bullet \in J_x \wedge \beta^\bullet \in J_y \\ &\Leftrightarrow \alpha \in S_{\mathrm{ODGP}}(I_x, J_x) \wedge \beta \in S_{\mathrm{ODGP}}(I_y, J_y). \end{aligned} \tag{24}$$

後者の場合，

$$u = \left(\alpha + \frac{1}{\sqrt{2}}\right) + \left(\beta + \frac{1}{\sqrt{2}}\right)i \in \mathcal{I} = I_x \times I_y \Leftrightarrow \alpha \in \left(I_x - \frac{1}{\sqrt{2}}\right) \wedge \beta \in \left(I_y - \frac{1}{\sqrt{2}}\right), \tag{25}$$

$$u^\bullet = \left(\alpha^\bullet - \frac{1}{\sqrt{2}}\right) + \left(\beta^\bullet - \frac{1}{\sqrt{2}}\right) i \in \mathcal{J} = J_x \times J_y \Leftrightarrow \alpha^\bullet \in \left(J_x + \frac{1}{\sqrt{2}}\right) \wedge \beta^\bullet \in \left(J_y + \frac{1}{\sqrt{2}}\right) \tag{26}$$

より，$I'_x, I'_y, J'_x, J'_y$ を

$$I'_{x/y} \coloneqq I_{x/y} - 1/\sqrt{2} = [I_{x/y,l} - 1/\sqrt{2}, I_{x/y,r} - 1/\sqrt{2}] \tag{27}$$
$$J'_{x/y} \coloneqq J_{x/y} + 1/\sqrt{2} = [J_{x/y,l} + 1/\sqrt{2}, J_{x/y,r} + 1/\sqrt{2}] \tag{28}$$

と定義すれば，

$$\begin{aligned} u \in S_{\mathrm{TDGP}}(\mathcal{I}, \mathcal{J}) &\Leftrightarrow u \in \mathcal{I} \wedge u^\bullet \in \mathcal{J} \\ &\Leftrightarrow \alpha \in I'_x \wedge \beta \in I'_y \wedge \alpha^\bullet \in J'_x \wedge \beta^\bullet \in J'_y \\ &\Leftrightarrow \alpha \in S_{\mathrm{ODGP}}(I'_x, J'_x) \wedge \beta \in S_{\mathrm{ODGP}}(I'_y, J'_y). \end{aligned} \tag{29}$$

□

## 3.2 Upright sets

$\mathbb{R}^2$ の有界凸集合 $A$ について，$A$ の uprightness を表す $\mathrm{up}(A)$ は，

$$\mathrm{up}(A) \coloneqq \frac{\mathrm{area}(A)}{\mathrm{area}(\mathrm{BBox}(A))} \tag{30}$$

で定義される．ただし，$\mathrm{area}(A)$ は $A$ の面積を表し，$\mathrm{BBox}(A)$ は $A$ を含む面積最小の upright rectangle を表す．$\mathrm{up}(A) \geq M$ のとき，$A$ は $M$-upright であると言う．

**Lemma 3.5** ([4, Lemma 5.8])**.** $A$, $B$ が $\mathbb{R}^2$ の有界凸集合で $M$-upright であるとき，解の個数の $O(1/M^2)$ 倍の計算時間で解を求められる．

*Proof.* Algorithm 3.2 より，$S_{\mathrm{TDGP}}(\mathrm{BBox}(A), \mathrm{BBox}(B))$ に含まれる点は格子上に並ぶことから，$|S_{\mathrm{TDGP}}(A, B)|$: $|S_{\mathrm{TDGP}}(\mathrm{BBox}(A), \mathrm{BBox}(B))|$ が $M^2$: 1 程度になるため．(厳密な証明ではない？ $A$, $B$ 内部の長方形で面積比が定数以上のものが存在することが言えればよさそう？) □

## 3.3 Grid operators ([4, Section 5.3])

**Definition 3.6** ([4, Definition 5.10])**.** 実線形演算子 $G$: $\mathbb{R}^2 \to \mathbb{R}^2$ が $G(\mathbb{Z}[\omega]) \subseteq \mathbb{Z}[\omega]$ を満たすとき，$G$ を *grid operator* と呼ぶ．更に，行列式が $\pm 1$ のとき，$G$ を *special grid operator* と呼ぶ．

**Lemma 3.7** ([4, Definition 5.11])**.** 実線形演算子 $G$: $\mathbb{R}^2 \to \mathbb{R}^2$ を $2 \times 2$ 実行列で表すとすると，$G$ が grid operator となる必要十分条件は，

$$G = \begin{pmatrix} a + a'/\sqrt{2} & b + b'/\sqrt{2} \\ c + c'/\sqrt{2} & d + d'/\sqrt{2} \end{pmatrix} \tag{31}$$

と表せ，$a, b, c, d, a', b', c', d' \in \mathbb{Z}$, $a + b + c + d \equiv 0 \pmod 2$, $a' \equiv b' \equiv c' \equiv d' \pmod 2$ が成り立つことである．

*Proof.* Lemma 3.3 より，$u \in \mathbb{R}^2$ が $u \in \mathbb{Z}[\omega]$ となる必要十分条件は,

$$u = \begin{pmatrix} x + x'/\sqrt{2} \\ y + y'/\sqrt{2} \end{pmatrix} \tag{32}$$

と表せ，$x, x', y, y' \in \mathbb{Z}$, $x' \equiv y' \pmod 2$ が成り立つことである．

まず，'if' part を示す．$u \in \mathbb{Z}[\omega]$ を任意にとると,

$$\begin{aligned} G(u) &= \begin{pmatrix} a + a'/\sqrt{2} & b + b'/\sqrt{2} \\ c + c'/\sqrt{2} & d + d'/\sqrt{2} \end{pmatrix} \begin{pmatrix} x + x'/\sqrt{2} \\ y + y'/\sqrt{2} \end{pmatrix} \\ &= \begin{pmatrix} (ax + by + (a'x' + b'y')/2) + (ax' + a'x + by' + b'y)/\sqrt{2} \\ (cx + dy + (c'x' + d'y')/2) + (cx' + c'x + dy' + d'y)/\sqrt{2} \end{pmatrix}. \end{aligned} \tag{33}$$

$a'x' \equiv b'y' \equiv c'x' \equiv d'y' \pmod 2$ より，$ax + by + (a'x' + b'y')/2, cx + dy + (c'x' + d'y')/2 \in \mathbb{Z}$. $ax' + a'x + by' + b'y, cx' + c'x + dy' + d'y \in \mathbb{Z}$ は明らか.

$$\begin{aligned} (ax' + a'x + by' + b'y) + (cx' + c'x + dy' + d'y) &\equiv (ax' + a'x + bx' + a'y) + (cx' + a'x + dx' + a'y) \\ &\equiv (a + b + c + d)x' + 2a'(x + y) \\ &\equiv 0 \pmod 2 \end{aligned} \tag{34}$$

より，$ax' + a'x + by' + b'y \equiv cx' + c'x + dy' + d'y \pmod 2$. ゆえに，$G(u) \in \mathbb{Z}[\omega]$.

次に，'only if' part を示す．$G(1) \in \mathbb{Z}[\omega]$, $G(i) \in \mathbb{Z}[\omega]$ が必要であるから,

$$G = \begin{pmatrix} a + a'/\sqrt{2} & b + b'/\sqrt{2} \\ c + c'/\sqrt{2} & d + d'/\sqrt{2} \end{pmatrix} \tag{35}$$

と表せ，$a, b, c, d, a', b', c', d' \in \mathbb{Z}$, $a' \equiv c' \pmod 2$, $b' \equiv d' \pmod 2$ が成り立つことが必要である．更に，$G(\omega) \in \mathbb{Z}[\omega]$ が必要であるから,

$$\begin{pmatrix} \frac{a'+b'}{2} + \frac{a+b}{\sqrt{2}} \\ \frac{c'+d'}{2} + \frac{c+d}{\sqrt{2}} \end{pmatrix} \in \mathbb{Z}[\omega], \tag{36}$$

つまり，$a + b \equiv c + d \pmod 2$ かつ $a' + b' \equiv c' + d' \equiv 0 \pmod 2$ が必要である．これらを合わせると，$a + b + c + d \equiv 0 \pmod 2$, $a' \equiv b' \equiv c' \equiv d' \pmod 2$ が得られる． □

**Lemma 3.8.** 実線形演算子 $G\colon \mathbb{R}^2 \to \mathbb{R}^2$ が grid operator となる必要十分条件は,

$$G = \begin{pmatrix} d + (c - a)/\sqrt{2} & d' + (c' - a')/\sqrt{2} \\ b + (c + a)/\sqrt{2} & b' + (c' + a')/\sqrt{2} \end{pmatrix} \tag{37}$$

と表せ，$a, b, c, d, a', b', c', d' \in \mathbb{Z}$, $a + c + a' + c' \equiv b + d + b' + d' \equiv 0 \pmod 2$ が成り立つことである．

*Proof.* Lemma 3.7 について，$a, b, c, d, a', b', c', d'$ を $d_2, d'_2, b_2, b'_2, c_2 - a_2, c'_2 - a'_2, c_2 + a_2, c'_2 + a'_2$ に置換すると,

$$a, b, c, d \in \mathbb{Z} \Leftrightarrow d_2, d'_2, b_2, b'_2 \in \mathbb{Z}, \tag{38}$$

$$a', c', a' \equiv c' \pmod 2 \in \mathbb{Z} \Leftrightarrow a_2, c_2 \in \mathbb{Z}, \tag{39}$$

$$b', d', b' \equiv d' \pmod 2 \in \mathbb{Z} \Leftrightarrow a'_2, c'_2 \in \mathbb{Z}, \tag{40}$$

$$a + b + c + d \equiv 0 \pmod 2 \Leftrightarrow b_2 + d_2 + b'_2 + d'_2 \equiv 0 \pmod 2, \tag{41}$$

$$a' \equiv b' \pmod 2 \Leftrightarrow a_2 + c_2 + a'_2 + c'_2 \equiv 0 \pmod 2 \tag{42}$$

より，$G$ が grid operator となる必要十分条件は，

$$G = \begin{pmatrix} d_2 + (c_2 - a_2)/\sqrt{2} & d_2' + (c_2' - a_2')/\sqrt{2} \\ b_2 + (c_2 + a_2)/\sqrt{2} & b_2' + (c_2' + a_2')/\sqrt{2} \end{pmatrix} \tag{43}$$

と表せ，$a_2, b_2, c_2, d_2, a_2', b_2', c_2', d_2' \in \mathbb{Z}$, $a_2 + c_2 + a_2' + c_2' \equiv b_2 + d_2 + b_2' + d_2' \equiv 0 \pmod 2$ が成り立つことである．□

Lemma 3.8 の表記のとき，$G(1) = a\omega^3 + b\omega^2 + c\omega + d$, $G(i) = a'\omega^3 + b'\omega^2 + c'\omega + d'$ である．また，$G(\omega) = (G(1) + G(i))/\sqrt{2}$, $G(\omega) = (-G(1) + G(i))/\sqrt{2}$ である．$u = a_0\omega^3 + b_0\omega^2 + c_0\omega + d_0 \in \mathbb{Z}[\omega]$ に対して，$Gu = a_1\omega^3 + b_1\omega^2 + c_1\omega + d_1 \in \mathbb{Z}[\omega]$ は，

$$\begin{aligned} Gu &= a_0 G(\omega^3) + b_0 G(\omega^2) + c_0 G(\omega) + d_0 G(1) \\ &= \left(d_0 + \frac{c_0 - a_0}{\sqrt{2}}\right) G(1) + \left(b_0 + \frac{c_0 + a_0}{\sqrt{2}}\right) G(i) \\ &= \left(d_0 + \frac{c_0 - a_0}{2}(\omega - \omega^3)\right) G(1) + \left(b_0 + \frac{c_0 + a_0}{2}(\omega - \omega^3)\right) G(i) \\ &= d_0(a\omega^3 + b\omega^2 + c\omega + d) \\ &\qquad + \frac{c_0 - a_0}{2}(b\omega^3 + c\omega^2 + d\omega - a) \\ &\qquad + \frac{c_0 - a_0}{2}(-d\omega^3 + a\omega^2 + b\omega + c) \\ &\qquad + b_0(a'\omega^3 + b'\omega^2 + c'\omega + d') \\ &\qquad + \frac{c_0 + a_0}{2}(b'\omega^3 + c'\omega^2 + d'\omega - a') \\ &\qquad + \frac{c_0 + a_0}{2}(-d'\omega^3 + a'\omega^2 + b'\omega + c') \end{aligned} \tag{44}$$

より，

$$a_1 = ad_0 + a'b_0 + (b' - d' + b - d)c_0/2 + (b' - d' - b + d)a_0/2, \tag{45}$$
$$b_1 = bd_0 + b'b_0 + (c' + a' + c + a)c_0/2 + (c' + a' - c - a)a_0/2, \tag{46}$$
$$c_1 = cd_0 + c'b_0 + (b' + d' + b + d)c_0/2 + (b' + d' - b - d)a_0/2, \tag{47}$$
$$d_1 = dd_0 + d'b_0 + (c' - a' + c - a)c_0/2 + (c' - a' - c + a)a_0/2 \tag{48}$$

によって計算できる．

また，$\det G = \mathrm{Re}[G(1)]\,\mathrm{Im}[G(i)] - \mathrm{Im}[G(1)]\,\mathrm{Re}[G(i)] = \mathrm{Im}[G(1)^\dagger G(i)]$ より，$G$ が special grid operator となる条件は，$\mathrm{Im}[G(1)^\dagger G(i)] = \pm 1$ である．

$\det G = 1$ のとき，$G^{-1}$ については，

$$G^{-1} = \begin{pmatrix} b' + (c' + a')/\sqrt{2} & -d' - (c' - a')/\sqrt{2} \\ -b - (c + a)/\sqrt{2} & d + (c - a)/\sqrt{2} \end{pmatrix} \tag{49}$$

より，

$$\begin{aligned} G^{-1}(1) &= \Big(b' + (c' + a')/\sqrt{2}\Big) + i\Big(-b - (c + a)/\sqrt{2}\Big) \\ &= \frac{-c' - a' - c - a}{2}\omega^3 - b\omega^2 + \frac{c' + a' - c - a}{2}\omega + b', \\ G^{-1}(i) &= \Big(-d' - (c' - a')/\sqrt{2}\Big) + i\Big(d + (c - a)/\sqrt{2}\Big) \end{aligned} \tag{50}$$

$$= \frac{c'-a'+c-a}{2}\omega^3 + d\omega^2 + \frac{-c'+a'+c-a}{2}\omega - d' \tag{51}$$

によって計算できる．$\det G = -1$ のときは，全体が $-1$ 倍されたものとなる．

$G^\dagger$ については，

$$G^\dagger = \begin{pmatrix} d+(c-a)/\sqrt{2} & b+(c+a)/\sqrt{2} \\ d'+(c'-a')/\sqrt{2} & b'+(c'+a')/\sqrt{2} \end{pmatrix} \tag{52}$$

より，

$$\begin{aligned} G^{-1}(1) &= \Big(d+(c-a)/\sqrt{2}\Big) + i\Big(d'+(c'-a')/\sqrt{2}\Big) \\ &= \frac{c'-a'-c+a}{2}\omega^3 + d'\omega^2 + \frac{c'-a'+c-a}{2}\omega + d, \end{aligned} \tag{53}$$

$$\begin{aligned} G^{-1}(i) &= \Big(b+(c+a)/\sqrt{2}\Big) + i\Big(b'+(c'+a')/\sqrt{2}\Big) \\ &= \frac{c'+a'-c-a}{2}\omega^3 + b'\omega^2 + \frac{c'+a'+c+a}{2}\omega + b \end{aligned} \tag{54}$$

によって計算できる．

**Remark 3.9** ([4, Remark 5.12])**.** (special) grid operator の積も (special) grid operator となる．$G$ が special grid operator のとき，$G^{-1}$ も special grid operator となる．$G$ が (special) grid operator のとき，$G^\bullet$ も (special) grid operator である．ただし，$G^\bullet$ は $G^\bullet u = (Gu^\bullet)^\bullet$ によって定義される．

**Proposition 3.10.** $A, B \subseteq \mathbb{R}^2$, $G$ を special grid operator とする．

$$G(A) = \{Gu \mid u \in A\}, \tag{55}$$

$$G^\bullet(B) = \{G^\bullet u \mid u \in B\} \tag{56}$$

と表すとすると，$u \in S_{\mathrm{TDGP}}(A,B) \Leftrightarrow Gu \in S_{\mathrm{TDGP}}(G(A), G^\bullet(B))$.

*Proof.* $u \in \mathbb{Z}[\omega]$ とする．$G$ は可逆で $G^{-1}, G^\bullet, (G^\bullet)^{-1}$ も special grid operator であるから，

$$\begin{aligned} u \in S_{\mathrm{TDGP}}(A,B) &\Leftrightarrow u \in A \wedge u^\bullet \in B \\ &\Leftrightarrow Gu \in G(A) \wedge (Gu)^\bullet = G^\bullet u^\bullet \in G^\bullet(B) \\ &\Leftrightarrow Gu \in S_{\mathrm{TDGP}}(G(A), G^\bullet(B)). \end{aligned} \tag{57}$$

□

## 3.4 Ellipse ([4, Section 5.4])

**Definition 3.11** ([4, Definition 5.15])**.** $D$ は $2\times 2$ 実行列で行列式が非ゼロの正定値対称行列とする．$p \in \mathbb{R}^2$ を点とする．このとき，中心 $p$ と行列 $D$ によって定義される *ellipse* とは，以下の集合 $E$ である．

$$E = \big\{u \in \mathbb{R}^2 \;\big|\; (u-p)^\dagger D(u-p) \le 1\big\}. \tag{58}$$

**Theorem 3.12.** $E_A, E_B \subseteq \mathbb{R}^2$ を ellipse とする．このとき，$G(E_A)$ と $G^\bullet(E_B)$ が 1/6-upright であるような grid operator $G$ が存在する．更に，$E_A$ と $E_B$ が $M$-upright であるとき，この $G$ は $O(\log(1/M))$ 時間で計算できる．

詳しくは Appendix B.

**Algorithm 3.13.** ここでは，grid operator $G$ を $G(1), G(i) \in \mathbb{Z}[\omega]$ を用いて，$[G(1), G(i)]$ と書き表すとする．

state $(D, \Delta)$ が与えられたとき，$\mathrm{Skew}(G \cdot (D, \Delta)) < 15$ を満たす special grid operator $G$ を求めるアルゴリズム (step_lemma in [6], step_lemma in [7]):

1. $\beta < 0$ のとき，$Z = [1, -i]$ を用いて，$(D', \Delta') = Z \cdot (D, \Delta)$ を計算する．$(D', \Delta')$ に対して再帰的に grid operator $G'$ を計算し，$G'X$ を返す．
2. そうでなく，$\mathrm{Bias}(A)\,\mathrm{Bias}(B) < 1$ のとき，$X = [i, 1]$ を用いて，$(D', \Delta') = X \cdot (D, \Delta)$ を計算する．$(D', \Delta')$ に対して再帰的に grid operator $G'$ を計算し，$G'X$ を返す．
3. そうでなく，$\mathrm{Bias}(D, \Delta) > 33.971$ または $\mathrm{Bias}(D, \Delta) < 0.029437$ のとき，$n = \mathrm{round}((\log_\lambda \mathrm{Bias}(D, \Delta))/8)$, $S = [\lambda, i\lambda^{-1}]$ を用いて，$(D', \Delta') = S^n \cdot (D, \Delta)$ を計算する．$(D', \Delta')$ に対して再帰的に grid operator $G'$ を計算し，$G'S^n$ を返す．
4. そうでなく，$\mathrm{Skew}(D, \Delta) \leq 15$ のとき，$I = [1, i]$ を返す．
5. そうでなく，$\mathrm{Bias}(D, \Delta) > 5.8285$ または $\mathrm{Bias}(D, \Delta) < 0.17157$ のとき，$n = \mathrm{round}((\log_\lambda \mathrm{Bias}(D, \Delta))/4)$ を用いて，
$$(D', \Delta') = \left( \begin{pmatrix} e\lambda^{-z-n} & b \\ b & e\lambda^{z+n} \end{pmatrix}, \begin{pmatrix} \epsilon\lambda^{-\zeta+n} & (-1)^n\beta \\ (-1)^n\beta & \epsilon\lambda^{\zeta-n} \end{pmatrix} \right) \tag{59}$$
を計算する．$(D', \Delta')$ に対して再帰的に grid operator $G'$ を計算し，$\sigma_l = [\lambda, i]$, $\sigma_r = [1, i\lambda^{-1}]$ を用いて，$\sigma_l^n G' \sigma_r^n$ を返す．
6. そうでなく，$0.24410 \leq \mathrm{Bias}(D) \leq 4.0968$ かつ $0.24410 \leq \mathrm{Bias}(\delta) \leq 4.0968$ のとき，$R = [\omega, \omega^3]$ を用いて，$(D', \Delta') = R \cdot (D, \Delta)$ を計算する．$(D', \Delta')$ に対して再帰的に grid operator $G'$ を計算し，$G'R$ を返す．
7. そうでなく，$b \geq 0$ かつ $\mathrm{Bias}(D) \leq 1.6969$ のとき，$K = [-\omega^3 - \omega^2, -\omega^2 + \omega]$ を用いて，$(D', \Delta') = K \cdot (D, \Delta)$ を計算する．$(D', \Delta')$ に対して再帰的に grid operator $G'$ を計算し，$G'K$ を返す．
8. そうでなく，$b \geq 0$ かつ $\mathrm{Bias}(\Delta) \leq 1.6969$ のとき，$K^\bullet = [\omega^3 - \omega^2, -\omega^2 - \omega]$ を用いて，$(D', \Delta') = K^\bullet \cdot (D, \Delta)$ を計算する．$(D', \Delta')$ に対して再帰的に grid operator $G'$ を計算し，$G'K^\bullet$ を返す．
9. そうでなく，$b \geq 0$ のとき，$n = \max\Big(1, \Big\lfloor \sqrt{\min(\mathrm{Bias}(D), \mathrm{Bias}(\Delta))/4} \Big\rfloor\Big)$, $A^n = [1, \omega^2 + 2n]$ を用いて，$(D', \Delta') = A^n \cdot (D, \Delta)$ を計算する．$(D', \Delta')$ に対して再帰的に grid operator $G'$ を計算し，$G'A^n$ を返す．
10. そうでないとき，$n = \max\Big(1, \Big\lfloor \sqrt{\min(\mathrm{Bias}(D), \mathrm{Bias}(\Delta))/2} \Big\rfloor\Big)$, $B^n = [1, n\omega^3 + \omega^2 - n\omega]$ を用いて，$(D', \Delta') = B^n \cdot (D, \Delta)$ を計算する．$(D', \Delta')$ に対して再帰的に grid operator $G'$ を計算し，$G'B^n$ を返す．

## 3.5 General solution of the two-dimensional grid problem ([4, Section 5.6])

**Algorithm 3.14.** 内部が非空の有界凸集合 $A, B \subseteq \mathbb{R}^2$ が与えられたとき，$u \in A$ かつ $u^\bullet \in B$ を満たす全ての $u \in \mathbb{Z}[\omega]$ からなる集合 $S$ を求めるアルゴリズム:

1. $N \leftarrow \frac{4\pi}{3\sqrt{3}}$ として，$A \subseteq E_A$ かつ $\mathrm{area}(E) \leq N\,\mathrm{area}(A)$ を満たす楕円 $E_A$ と $B \subseteq E_B$ かつ $\mathrm{area}(E) \leq$

$N\,\mathrm{area}(B)$ を満たす楕円 $E_B$ を見つける．(ad hoc)

2. $G(E_A)$ と $G^\bullet(E_B)$ が 1/6-upright であるような grid operator $G$ を見つける．
3. $S' = \text{solve\_TDGP\_for\_upright\_rectangles}(\mathrm{BBox}(G(E_A)), \mathrm{BBox}(G^\bullet(E_B)))$ を計算する．
4. $S = \left\{ G^{-1}u \;\middle|\; u \in S', u \in G(A), u^\bullet \in G^\bullet(B) \right\}$ を返す．

**Proposition 3.15.** 内部が非空の有界凸集合 $A, B \subseteq \mathbb{R}^2$ が与えられたとき，$A, B$ が $M$-upright であるとすると，Algorithm 3.14 によって，$S_{\mathrm{TDGP}}(A, B)$ が $O(\log(1/M))$ 時間と解の個数に対する線形時間の和で計算可能である．ただし，$E_A$, $E_B$ は定数時間で計算可能であると仮定する．

*Proof.* Theorem 3.12 より，$G$ は $O(\log(1/M))$ 時間で求められる．$G(E_A)$ と $G^\bullet(E_B)$ は 1/6-upright より，$G(A)$ と $G(B)$ は $N$/6-upright であるから，Lemma 3.5 より，$S_{\mathrm{TDGP}}(G(A), G^\bullet(B))$ は解の個数に対する線形時間で求められる．Proposition 3.10 より，$G^{-1}S_{\mathrm{TDGP}}(G(A), G^\bullet(B))$ によって $S_{\mathrm{TDGP}}(A, B)$ が計算可能である． □

## 3.6 Scaled grid problems ([4, Section 5.7])

**Definition 3.16** ([4, Definition 5.3])**.** $A, B \subseteq \mathbb{R}^2$ とする．

- **Two-dimensional scaled grid problem for fixed $k$:** $u \in A$ かつ $u^\bullet \in B$ を満たす $u \in \mathbb{Z}[\omega]/\sqrt{2}^k$ を見つける．
- **Two-dimensional scaled grid problem for arbitary $k$:** $u \in A$ かつ $u^\bullet \in B$ を満たす $u \in \mathbb{D}[\omega]$ を見つける．

$A, B \in \mathbb{R}^2$, $k \in \mathbb{Z}_{\geq 0}$ に対して，two-dimensional scaled grid problem for $k$ の解集合を $S_{\mathrm{TDSGP}}(k, A, B)$, two-dimensional scaled grid problem の解集合を $S_{\mathrm{TDSGP}}(A, B)$ とする．

**Algorithm 3.17.** 内部が非空の有界凸集合 $A, B \subseteq \mathbb{R}^2$ が与えられたとき，$S_{\mathrm{TDSGP}}(k, A, B)$ を求めるアルゴリズム:

1. $A' = \sqrt{2}^k A$, $B' = (-\sqrt{2})^k B$ について，$S' = \text{solve\_TDGP}(A', B')$ を求める．
2. $S = \left\{ u/\sqrt{2}^k \;\middle|\; u \in S' \right\}$ を返す．

**Proposition 3.18.** 内部が非空の有界凸集合 $A, B \subseteq \mathbb{R}^2$ と $k \in \mathbb{Z}_{\geq 0}$ が与えられたとき，$A, B$ が $M$-upright であるとすると，Algorithm 3.17 によって，$S_{\mathrm{TDGP}}(A, B)$ が $O(\log(1/M))$ 時間と解の個数に対する線形時間の和で計算可能である．

*Proof.* $u \in \mathbb{Z}[\omega]$, $A' = \sqrt{2}^k A$, $B' = (-\sqrt{2})^k B$ とすると，

$$\begin{aligned} u \in S_{\mathrm{TDSGP}}(k, A', B') &\Leftrightarrow u \in \sqrt{2}^k A \wedge u^\bullet \in (-\sqrt{2})^k B \\ &\Leftrightarrow \frac{u}{\sqrt{2}^k} \in A \wedge \left(\frac{u}{\sqrt{2}^k}\right)^\bullet = \frac{1}{(-\sqrt{2})^k} u^\bullet \in B \\ &\Leftrightarrow \frac{u}{\sqrt{2}^k} \in S_{\mathrm{TDGP}}(A, B). \end{aligned} \tag{60}$$

□

**Lemma 3.19** ([4, Proposition 5.22])**.** $u \in \mathbb{Z}[\omega]/\sqrt{2}^k$ が $a,b,c,d \in \mathbb{Z}$ を用いて $u = (a\omega^3+b\omega^2+c\omega+d)/\sqrt{2}^k$ と表されるとする．このとき，

$$u \in \mathbb{Z}[\omega]/\sqrt{2}^k - \mathbb{Z}[\omega]/\sqrt{2}^{k-1} \Leftrightarrow a-c\colon \text{odd} \vee b-d\colon \text{odd}. \tag{61}$$

*Proof.* $u \in \mathbb{Z}[\omega]/\sqrt{2}^k$, $a,b,c,d \in \mathbb{Z}$ として，$u = (a\omega^3+b\omega^2+c\omega+d)/\sqrt{2}^k$ と表されるとき，

$$u \in \mathbb{Z}[\omega]/\sqrt{2}^{k-1} \Leftrightarrow b-d \equiv a-c \equiv 0 \mod 2 \tag{62}$$

を示せばよい．

$$\begin{aligned}\sqrt{2}^{k-1}u &= \frac{1}{\sqrt{2}}(a\omega^3+b\omega^2+c\omega+d)\\ &= \frac{1}{2}(\omega+\omega^{-1})(a\omega^3+b\omega^2+c\omega+d)\\ &= \frac{1}{2}((b-d)\omega^3+(c+a)\omega^2+(d+b)\omega+(-a+c))\end{aligned}$$

より，

$$\begin{aligned}u \in \mathbb{Z}[\omega]/\sqrt{2}^{k-1} &\Leftrightarrow \sqrt{2}^{k-1}u \in \mathbb{Z}[\omega]\\ &\Leftrightarrow b-d \equiv c+a \equiv d+b \equiv -a+c \equiv 0 \mod 2\\ &\Leftrightarrow b-d \equiv a-c \equiv 0 \mod 2.\end{aligned} \tag{63}$$

□

two-dimensional scaled grid problem for arbitary $k$ を解くには，$k$ の昇順に two-dimensional scaled grid problem for $k$ を解き，Lemma 3.19 を用いて重複する解を取り除けばよい．(解の個数は $k$ の指数関数に従って増えていくので，重複する解を毎回求めていても時間計算量は同じになりそう．ODGP を解く時点で適切に要らない解を捨てる，$k$ について指数探索を行うなどすると，時間計算量が定数倍改善できそう？) このとき，grid operator $G$ は共通に取れるので，$G$ の計算は最初に一度行うだけでよいことに留意する．

# 4 Solving a Diophantine equation ([4, Section 6])

**Definition 4.1. Diophantine equation:** $\xi \in \mathbb{D}[\sqrt{2}]$ が与えられたとき，$t \in \mathbb{D}[\omega]$ が $t^\dagger t = \xi$ を満たす．

**Algorithm 4.2.** $\xi \in \mathbb{Z}[\sqrt{2}], k \in \mathbb{Z}_{\geq 0}$ が与えられたとき，$t^\dagger t = \xi/\sqrt{2}^k$ を満たす $t \in \mathbb{D}[\omega]$ を求めるアルゴリズム (diophantine_dyadic in [7]):

1. $k' = \lfloor k/2 \rfloor$, $k'' = k - 2k'$ とする．
2. ${t'}^\dagger t' = \lambda^{k''}\xi$ を満たす $t' \in \mathbb{Z}[\omega]$ を求める．(Algorithm 4.3)
3. $t'$ が存在しなければ「解なし」を返す．$t'$ が存在すれば，$t = (\omega-\omega^2)^{k''}t'/\sqrt{2}^{k'+k''}$ を返す．

**Algorithm 4.3.** $\xi \in \mathbb{Z}[\sqrt{2}]$ が与えられたとき，$t^\dagger t = \xi$ を満たす $t \in \mathbb{Z}[\omega]$ を求めるアルゴリズム (diophantine in [7]):

1. $\xi = 0$ ならば，$t = 0$ を返す．
2. $\xi < 0$ または $\xi^\bullet < 0$ ならば，「解なし」を返す．

3. $t'^{\dagger}t' \sim \xi$ を満たす $t' \in \mathbb{Z}[\omega]$ を求める．(Algorithm 4.4)
4. $t'$ が存在しなければ「解なし」を返す．$t'$ が存在すれば，$v = \sqrt{\xi/t^{\dagger}t}$ を計算し，$t = vt'$ を返す．

**Algorithm 4.4.** $\xi \in \mathbb{Z}[\sqrt{2}]$ が与えられたとき，$t^{\dagger}t \sim \xi$ を満たす $t \in \mathbb{Z}[\omega]$ を求めるアルゴリズム (adj_decompose in [7]):

1. $\xi = 0$ ならば，$t = 0$ を返す．
2. $d = \gcd(\xi, \xi^{\bullet})$ を計算する．
3. $t_1^{\dagger}t_1 \sim d$ を満たす $t_1 \in \mathbb{Z}[\omega]$ を求める．(Algorithm 4.5)
4. $t_2^{\dagger}t_2 \sim \xi/d$ を満たす $t_2 \in \mathbb{Z}[\omega]$ を求める．(Algorithm 4.9)
5. $t_1$ または $t_2$ が存在しなければ「解なし」を返す．$t_1$ と $t_2$ が存在すれば，$t = t_1t_2$ を返す．

**Algorithm 4.5.** $\xi \sim \xi^{\bullet}$ を満たす $\xi \in \mathbb{Z}[\sqrt{2}]$ が与えられたとき，$t^{\dagger}t \sim \xi$ を満たす $t \in \mathbb{Z}[\omega]$ を求めるアルゴリズム (adj_decompose_selfassociate in [7]):

1. $\xi = 0$ ならば，$t = 0$ を返す．
2. $\xi = a + b\sqrt{2}$ と表し，$n = \gcd(a, b)$ を計算する．
3. $t_1^{\dagger}t_1 \sim n$ を満たす $t_1 \in \mathbb{Z}[\omega]$ を求める．(Algorithm 4.6)
4. $\xi/n$ が $\sqrt{2}$ の整数倍のとき，$t_2 = 1 + \omega$，そうでないとき，$t_2 = 1$ と定義する．
5. $t_1$ が存在しなければ「解なし」を返す．$t_1$ が存在すれば，$t = t_1t_2$ を返す．

**Algorithm 4.6.** $n \in \mathbb{Z}$ が与えられたとき，$t^{\dagger}t \sim n$ を満たす $t \in \mathbb{Z}[\omega]$ を求めるアルゴリズム (adj_decompose_int in [7]):

1. $n < 0$ ならば，$n \leftarrow -n$ とする．
2. $n = 0$ または $n = 1$ ならば，$t = n$ を返す．
3. 整数の範囲で，$n$ を $n = p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m}$ の形に素因数分解する．
4. $i = 1, \ldots, m$ について，$t_i^{\dagger}t_i \sim p_1^{k_1}$ を満たす $t_i \in \mathbb{Z}[\omega]$ を求める．(Algorithm 4.7) $t_i$ が存在しなければ「解なし」を返す．
5. $t_1, \ldots, t_m$ が存在すれば，$t = t_1 \cdots t_m$ を返す．

**Algorithm 4.7.** 素数 $p \in \mathbb{Z}_{>0}$, $k \in \mathbb{Z}_{\geq 0}$ が与えられたとき，$t^{\dagger}t \sim p^k$ を満たす $t \in \mathbb{Z}[\omega]$ を求めるアルゴリズム (adj_decompose_int_prime_power in [7]):

1. $k$ が偶数ならば，$t = p^{k/2}$ を返す．
2. $k$ が奇数ならば，$t' \dagger t' \sim p$ を満たす $t' \in \mathbb{Z}[\omega]$ を求める．(Algorithm 4.8) $t'$ が存在しなければ「解なし」を返す．$t'$ が存在すれば，$t'^k$ を返す．

**Algorithm 4.8.** 素数 $p \in \mathbb{Z}$ が与えられたとき，$t^{\dagger}t \sim p$ を満たす $t \in \mathbb{Z}[\omega]$ を求めるアルゴリズム (adj_decompose_int_prime in [7]):

1. $p < 0$ ならば，$p \leftarrow -p$ とする．
2. $p = 0$ または $p = 1$ ならば，$t = p$ を返す．
3. $p = 2$ ならば，$t = -\omega^3 + \omega = \sqrt{2}$ を返す．
4. $p \equiv 1 \pmod 4$ ならば，$h^2 \equiv -1 \pmod p$ を満たす $h \in \mathbb{Z}$ を求め，$t = \gcd(\omega^2 + h, p)$ を返す．

5. $p \equiv 3 \pmod 8$ ならば，$h^2 \equiv -2 \pmod p$ を満たす $h \in \mathbb{Z}$ を求め，$t = \gcd(\omega^3 + \omega + h, p)$ を返す．
6. $p \equiv 7 \pmod 8$ ならば，「解なし」を返す．

**Algorithm 4.9.** $\gcd(\xi, \xi^\bullet) = 1$ を満たす $\xi \in \mathbb{Z}[\sqrt{2}]$ が与えられたとき，$t^\dagger t \sim \xi$ を満たす $t \in \mathbb{Z}[\omega]$ を求めるアルゴリズム (adj_decompose_selfcoprime in [7]):

1. $n = \xi^\bullet \xi$ を計算する．
2. $n < 0$ ならば，$n \leftarrow -n$ とする．
3. $n = 0$ または $n = 1$ ならば，$t = n$ を返す．
4. 整数の範囲で，$n$ を $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ の形に素因数分解する．
5. $i = 1, \ldots, m$ について，$t_i^\dagger t_i \sim \gcd(\xi, p_i)^{k_1}$ を満たす $t_i \in \mathbb{Z}[\omega]$ を求める．(Algorithm 4.10) $t_i$ が存在しなければ「解なし」を返す．
6. $t_1, \ldots, t_m$ が存在すれば，$t = t_1 \cdots t_m$ を返す．

**Algorithm 4.10.** 素数 $\eta \in \mathbb{Z}[\sqrt{2}]$, $k \in \mathbb{Z}_{\geq 0}$ が与えられたとき，$t^\dagger t \sim \eta^k$ を満たす $t \in \mathbb{Z}[\omega]$ を求めるアルゴリズム (adj_decompose_zomega_prime_power in [7]):

1. $k$ が偶数ならば，$t = \eta^{k/2}$ を返す．
2. $k$ が奇数ならば，$t' \dagger t' \sim \eta$ を満たす $t' \in \mathbb{Z}[\omega]$ を求める．(Algorithm 4.11) $t'$ が存在しなければ「解なし」を返す．$t'$ が存在すれば，$t'^k$ を返す．

**Algorithm 4.11.** 素数 $\eta \in \mathbb{Z}[\sqrt{2}]$ が与えられたとき，$t^\dagger t \sim \eta$ を満たす $t \in \mathbb{Z}[\omega]$ を求めるアルゴリズム (adj_decompose_zomega_prime in [7]):

1. $p = \eta^\bullet \eta$ を計算する．
2. $p < 0$ ならば，$p \leftarrow -p$ とする．
3. $p = 0$ または $p = 1$ ならば，$t = p$ を返す．
4. $p = 2$ ならば，$t = \omega + 1$ を返す．
5. $p \equiv 1 \pmod 4$ ならば，$h^2 \equiv -1 \pmod p$ を満たす $h \in \mathbb{Z}$ を求め，$t = \gcd(\omega^2 + h, \eta)$ を返す．
6. $p \equiv 3 \pmod 8$ ならば，$h^2 \equiv -2 \pmod p$ を満たす $h \in \mathbb{Z}$ を求め，$t = \gcd(\omega^3 + \omega + h, \eta)$ を返す．
7. $p \equiv 7 \pmod 8$ ならば，「解なし」を返す．

# 5 The approximate synthesis algorithm ([4, Section 7])

## 5.1 The approximate synthesis problem ([4, Section 7.1])

**Definition 5.1** ([4])**.** $\theta$ と精度 $\epsilon > 0$ が与えられたとき，the *approximate synthesis problem for z-rotations* とは，the single-qubit Clifford+T gate set で表現可能な operator $U$ であって，

$$\|R_z(\theta) - U\| \leq \epsilon \tag{64}$$

を満たすものを見つけることである．

Clifford+T circuit の T-count とはそれに現れる T-gate の個数であり，operator $U$ の T-count を可能な限り最小化したい．

**Lemma 5.2** ([3])**.** single-qubit operator が Clifford+T gate set で正確に表現可能な条件は，$u, t \in \mathbb{D}[\omega]$, $l \in \mathbb{Z}$ として以下の形で書けることである．

$$U = \begin{pmatrix} u & -t^\dagger \omega^l \\ t^\dagger & u^\dagger \omega^l \end{pmatrix} \tag{65}$$

*Proof.* [3] を参照. □

**Lemma 5.3** ([4, Lemma 7.2])**.** $\epsilon < \left|1 - e^{i\pi/8}\right|$ ならば，approximate synthesis problem の全ての解は，$u, t \in \mathbb{D}[\omega]$ として以下の形で書ける．

$$U = \begin{pmatrix} u & -t^\dagger \\ t^\dagger & u^\dagger \end{pmatrix} \tag{66}$$

$\epsilon \geq \left|1 - e^{i\pi/8}\right|$ ならば，T-count 0 の解が存在して，式 (66) の形で書ける．

*Proof.* □

つまり，一般性を失わずに $l = 0$ と仮定してよいということ．

**Lemma 5.4** ([4, Lemma 7.3], [2])**.** $k$ を $u$ の the least denominator exponent とすると，$U$ の T-count は $\max(0, 2k - 2)$ となる．

*Proof.* [2] を参照. □

$z = e^{-i\theta/2}$ とおくと，$u^\dagger u + t^\dagger t = 1$, $z^\dagger z = 1$ より，

$$\|R_z(\theta) - U\|^2 = \|u - z\|^2 + \|t\|^2 = 2 - 2\,\mathrm{Re}(z^\dagger u) \tag{67}$$

であるから，

$$\|R_z(\theta) - U\| \leq \epsilon \Leftrightarrow \mathrm{Re}(z^\dagger u) \geq 1 - \frac{\epsilon^2}{2}. \tag{68}$$

$z = x + yi$ と $u = a + bi$ を $z = (x, y)^\top$, $u = (a, b)^\top$ と同一視すると，これは

$$z \cdot u \geq 1 - \frac{\epsilon^2}{2} \tag{69}$$

と書ける．

**Problem 5.5** ([4, Problem 7.4])**.** angle $\theta$ と精度 $\epsilon > 0$ が与えられたとき, 以下の条件を見つける $u, t \in \mathbb{D}[\omega]$ を見つける．

(a) $t^\dagger t + u^\dagger u = 1$,
(b) $z = e^{-i\theta/2}$ として，$z \cdot u \geq 1 - \epsilon^2/2$,
(c) $u$ は the denominator exponent が条件を満たすうちで最小.

## 5.2 Reduction to a grid problem and a Diophantine equation

**Lemma 5.6** ([4, Lemma 7.5])**.**

$$t^\dagger t + u^\dagger u = 1 \Rightarrow u, u^\bullet \in \overline{\mathcal{D}} \tag{70}$$

よって，$u \in \mathcal{R}_\epsilon = \left\{u \in \overline{\mathcal{D}} \;\middle|\; u \cdot z \geq 1 - \epsilon^2/2\right\}, u^\bullet \in \overline{\mathcal{D}}$ が必要条件である．

## 6 Main Algorithm

**Algorithm 6.1** ([4, Algorithm 7.6])**.** $\theta$ と $\epsilon > 0$ が与えられたとき，approximate synthesis problem を解くアルゴリズム:

1. $\overline{\mathcal{D}}$ を the closed unit disk とする．$A = \mathcal{R}_\epsilon$, $B = \overline{\mathcal{D}}$ として，$u \in A, u^\bullet \in B$ について the scaled grid problem を解き，least denominator exponent の昇順に $u$ を列挙する．
2. それぞれの解 $u$ について，
   (a) $\xi = 1 - u^\dagger u \in \mathbb{D}[\sqrt{2}]$ とおき，$n \in \mathbb{Z}$ と $l \geq 0$ が最小になるように $\xi^\bullet \xi = n/2^l$ と書く．
   (b) $n$ の素因数分解を計算する．$n \neq 0$ で素因数分解が見つからなければ，2(c) を飛ばして次の解 $u$ に進む．
   (c) $t^\dagger t = \xi$ を解く．もし解が存在すれば 3 に進み，そうでなければ次の解 $u$ に進む．
3. $$U = \begin{pmatrix} u & -t^\dagger \\ t^\dagger & u^\dagger \end{pmatrix} \tag{71}$$
   と定義し，$U$ と $U' = TUT^\dagger$ の Clifford+T circuit を計算する．より小さい T-count を持つ方を出力し，終了する．

$\mathcal{R}_\epsilon$ を含む楕円として，

$$E = \left\{ u \in \mathbb{R}^2 \;\middle|\; (u-z)^\top \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} \frac{4}{\epsilon^4} & 0 \\ 0 & \frac{1}{\epsilon^2} \end{pmatrix} \begin{pmatrix} x & y \\ -y & x \end{pmatrix} (u-z) \leq 1 \right\} \tag{72}$$

がとれる．ただし，$z = (x, y)^\top = (\cos(-\theta/2), \sin(-\theta/2))$.

## 7 参考文献


[1] gridsynth. https://www.mathstat.dal.ca/ selinger/newsynth/.

[2] Brett Giles and Peter Selinger. Remarks on matsumoto and amano's normal form for single-qubit clifford+t operators, 2019.

[3] Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. Fast and efficient exact synthesis of single qubit unitaries generated by clifford and t gates, 2013.

[4] Neil J. Ross and Peter Selinger. Optimal ancilla-free clifford+t approximation of z-rotations, 2016.

[5] Peter Selinger. Efficient clifford+t approximation of single-qubit operators, 2014.

[6] Peter Selinger and Neil J. Ross. Exact and approximate synthesis of quantum circuits. https://www.mathstat.dal.ca/ selinger/newsynth/, 2018.

[7] Shuntaro Yamamoto. quantum-programming/clifford-t-decomp. https://github.com/quantum-programming/clifford-T-decomp, 2024.

# A Lemma 2.7 の証明

**Lemma A.1** ([5, Lemma 17])**.** $\mathbb{R}$ 上の閉区間 $I=[I_l,I_r], J=[J_l,J_r]$ に対して, $\Delta_I \coloneqq I_r-I_l$, $\Delta_J \coloneqq J_r-J_l$ と定義する．このとき, $\Delta_I\Delta_J \geq (1+\sqrt{2})^2$ ならば, $|L_{\mathrm{ODGP}}(I,J)| \geq 1$ が成り立つ. つまり, $\Delta_I\Delta_J \geq (1+\sqrt{2})^2$ ならば，$I,J$ に対する one-dimensional grid problem の解が少なくとも一つ存在する．

*Proof.* 正の実数の組 $(\delta,\Delta)$ について，任意の $\xi,\eta\in\mathbb{R}$ に対して $|L_{\mathrm{ODGP}}([\xi,\xi+\delta],[\eta,\eta+\Delta])| \geq 1$ が成り立つとき，$(\delta,\Delta)$ は *coverage property* を持つと呼ぶ．$\delta\Delta \geq (1+\sqrt{2})^2$ ならば，$(\delta,\Delta)$ は coverage property を持つことを示せばよい.

(a) $(\delta,\Delta)$ は coverage property を持つとする．$\delta\leq\delta'$, $\Delta'\leq\Delta$ ならば，$(\delta',\Delta')$ も coverage property を持つ.
任意の $\xi,\eta\in\mathbb{R}$ に対して，$[\xi,\xi+\delta]\subseteq[\xi,\xi+\delta']$, $[\eta,\eta+\Delta]\subseteq[\eta,\eta+\Delta']$ より，

$$L_{\mathrm{ODGP}}([\xi,\xi+\delta],[\eta,\eta+\Delta]) \subseteq L_{\mathrm{ODGP}}([\xi,\xi+\delta'],[\eta,\eta+\Delta']) \tag{73}$$

が成り立つことより従う.

(b) $(\delta,\Delta)$ は coverage property を持つとする．このとき，$(\Delta,\delta)$ も coverage property を持つ.
任意の $\xi,\eta\in\mathbb{R}$ に対して，$\alpha\in L_{\mathrm{ODGP}}([\eta,\eta+\delta],[\xi,\xi+\Delta])$ ならば $\alpha^\bullet\in L_{\mathrm{ODGP}}([\xi,\xi+\Delta],[\eta,\eta+\delta])$ より従う.

(c) $(\delta,\Delta)$ は coverage property を持つとする．このとき，$(\lambda^{-1}\delta,\lambda\Delta)$, $(\lambda\delta,\lambda^{-1}\Delta)$ も coverage property を持つ.
Lemma 2.4 より，任意の $\xi,\eta\in\mathbb{R}$ に対して，

$$L_{\mathrm{ODGP}}([\lambda\xi,\lambda\xi+\delta],[-\lambda^{-1}\eta-\Delta,-\lambda^{-1}\eta]) = \lambda L_{\mathrm{ODGP}}([\xi,\xi+\lambda^{-1}\delta],[\eta,\eta+\lambda\Delta]), \tag{74}$$

$$L_{\mathrm{ODGP}}([\lambda^{-1}\xi,\lambda^{-1}\xi+\delta],[-\lambda\eta-\Delta,-\lambda\eta]) = \lambda^{-1} L_{\mathrm{ODGP}}([\xi,\xi+\lambda\delta],[\eta,\eta+\lambda^{-1}\Delta]) \tag{75}$$

が成り立つことより従う.

(d) $(\delta,\Delta)=(1+\sqrt{2},\sqrt{2})$ は coverage property を持つ.
$\xi,\eta\in\mathbb{R}$ を任意にとり，$a',b'\in\mathbb{R}$ を

$$a' = \frac{\xi+\eta+\Delta}{2}, \tag{76}$$

$$b' = \frac{\xi-\eta-\Delta}{2} \tag{77}$$

と定義する．このとき，$a'+b'=\xi$, $a'-b'=\eta+\Delta$ が成り立つことに留意する．$a_0,b_0\in\mathbb{Z}$ を

$$a_0-1 \leq a' < a_0, \tag{78}$$

$$(b_0-1)\sqrt{2} \leq b' < b_0\sqrt{2} \tag{79}$$

を満たすようにとり，$\alpha_0=a_0+b_0\sqrt{2}$, $\alpha_1=a_0+(b_0+1)\sqrt{2}$, $\alpha_1=(a_0-1)+b_0\sqrt{2}$ とおく．$\alpha_0$, $\alpha_1$, $\alpha_2$ のうち少なくとも一つは $[\xi,\xi+\delta]$ と $[\eta,\eta+\Delta]$ に対する解となることを示す.

- Case 1: $a_0-b_0\sqrt{2}\leq\eta+\Delta$ のとき,

$$\alpha_0 = a_0+b_0\sqrt{2} > a'+b' = \xi, \tag{80}$$

$$\alpha_0 = a_0 + b_0\sqrt{2} \le (a'+1) + (b'+\sqrt{2}) = \xi + \delta, \tag{81}$$
$$\alpha_0^\bullet = a_0 - b_0\sqrt{2} > a' - (b'+\sqrt{2}) = (\eta+\Delta) - \sqrt{2} = \eta, \tag{82}$$
$$\alpha_0^\bullet = a_0 - b_0\sqrt{2} \le \eta + \Delta \tag{83}$$

より，$\alpha_0 \in S_{\mathrm{ODGP}}([\xi, \xi+\delta], [\eta, \eta+\Delta])$.

- Case 2: $a_0 - b_0\sqrt{2} > \eta + \Delta$ かつ $a_0 + b_0\sqrt{2} \le \xi + 1$ のとき，

$$\alpha_1 = a_0 + (b_0+1)\sqrt{2} > a' + b' + \sqrt{2} = \xi + \sqrt{2} > \xi, \tag{84}$$
$$\alpha_1 = a_0 + (b_0+1)\sqrt{2} \le (\xi+1) + \sqrt{2} = \xi + \delta, \tag{85}$$
$$\alpha_1^\bullet = a_0 - (b_0+1)\sqrt{2} > (\eta+\Delta) - \sqrt{2} = \eta, \tag{86}$$
$$\alpha_1^\bullet = a_0 - (b_0+1)\sqrt{2} < (a'+1) - (b'+\sqrt{2}) = \eta + \Delta + 1 - \sqrt{2} = \eta + 1 < \eta + \Delta \tag{87}$$

より，$\alpha_1 \in S_{\mathrm{ODGP}}([\xi, \xi+\delta], [\eta, \eta+\Delta])$.

- Case 3: $a_0 - b_0\sqrt{2} > \eta + \Delta$ かつ $a_0 + b_0\sqrt{2} > \xi + 1$ のとき，

$$\alpha_2 = (a_0 - 1) + b_0\sqrt{2} > (\xi+1) - 1 = \xi, \tag{88}$$
$$\alpha_2 = (a_0 - 1) + b_0\sqrt{2} \le a' + (b'+\sqrt{2}) = \xi + \sqrt{2} < \xi + \delta, \tag{89}$$
$$\alpha_2^\bullet = (a_0 - 1) - b_0\sqrt{2} > (\eta+\Delta) - 1 = \eta + \sqrt{2} - 1 > \eta, \tag{90}$$
$$\alpha_2^\bullet = (a_0 - 1) - b_0\sqrt{2} \le a' - b' = \eta + \Delta \tag{91}$$

より，$\alpha_2 \in S_{\mathrm{ODGP}}([\xi, \xi+\delta], [\eta, \eta+\Delta])$.

図示: `https://www.desmos.com/calculator/fcg2cbrclh?lang=ja`

(e) $(\delta, \Delta) = (2+\sqrt{2}, 1)$ は coverage property を持つ．(b), (c), (d) より，$(\lambda\sqrt{2}, \lambda^{-1}(1+\sqrt{2}))$ も coverage property を持つことから従う．

(f) $\delta\Delta \ge (1+\sqrt{2})^2$ かつ $1 \le \delta < 1+\sqrt{2}$ ならば，$(\delta, \Delta)$ は coverage property を持つ．

- Case 1: $\delta > \sqrt{2}$ のとき，$\delta > \sqrt{2}$ かつ $\Delta > (1+\sqrt{2})^2/(1+\sqrt{2}) = 1+\sqrt{2}$. これらと (a), (b), (d) より，$(\delta, \Delta)$ は coverage property を持つ．
- Case 2: $\delta \le \sqrt{2}$ のとき，$\delta \ge 1$ かつ $\Delta \ge (1+\sqrt{2})^2/\sqrt{2} = 2 + 3\sqrt{2}/2 > 2 + \sqrt{2}$. これらと (a), (b), (e) より，$(\delta, \Delta)$ は coverage property を持つ．
- $\delta, \Delta > 0$, $\delta\Delta \ge (1+\sqrt{2})^2$ ならば，$(\delta, \Delta)$ は coverage property を持つ．
  $1 \le \lambda^{-m}\delta < \lambda = 1+\sqrt{2}$ を満たす $m \in \mathbb{Z}$ をとる．(f) より，$(\lambda^{-m}\delta, \lambda^m\Delta)$ は coverage property を持つ．これと (c) より，$(\delta, \Delta)$ も coverage property を持つ．

□

*Proof.* 微小量 $\epsilon > 0$ をとり，$N = \lfloor (1-\epsilon)\Delta_I\Delta_J/(1+\sqrt{2})^2 \rfloor$, $\eta_i = J_l + i\Delta_J/N$ $(i = 0, \dots, N)$, $J^{(i)} = [\eta_{i-1}, \eta_i - \epsilon\Delta_J/N]$ $(i = 1, \dots, N)$ とおく．$\{J^{(i)}\}_i$ は互いに素な閉区間列で，$J \supseteq \bigcup_{i=1}^N J^{(i)}$. したがって，

$$|S_{\mathrm{ODGP}}(I, J)| \ge \left| S_{\mathrm{ODGP}}(I, \bigcup_{i=1}^N J^{(i)}) \right| = \left| \bigcup_{i=1}^N S_{\mathrm{ODGP}}(I, J^{(i)}) \right| = \sum_{i=1}^N \left| S_{\mathrm{ODGP}}(I, J^{(i)}) \right| \tag{92}$$

が成り立つ．

$$\Delta_{J^{(i)}} = \left(\eta_i - \frac{\epsilon\Delta_J}{N}\right) - \eta_{i-1} = \frac{\Delta_J}{N} - \frac{\epsilon\Delta_J}{N} \ge (1-\epsilon)\Delta_J \cdot \left(\frac{(1-\epsilon)\Delta_I\Delta_J}{(1+\sqrt{2})^2}\right)^{-1} = \frac{(1+\sqrt{2})^2}{\Delta_I} \tag{93}$$

より，$\Delta_I \Delta_{J^{(i)}} \geq (1+\sqrt{2})^2$. よって，Lemma A.1 より，$\left|S_{\mathrm{ODGP}}(I, J^{(i)})\right| \geq 1$ であるから，$|S_{\mathrm{ODGP}}(I,J)|$ の下界について，

$$|S_{\mathrm{ODGP}}(I,J)| \geq N > (1-\epsilon)\Delta_I\Delta_J/(1+\sqrt{2})^2 - 1 \tag{94}$$

が得られる． □

**Lemma 2.7** ([4, Proposition 4.5] の補足)**.** $\mathbb{R}$ 上の閉区間 $I=[I_l, I_r], J=[J_l, J_r]$ に対して，$\Delta_I \coloneqq I_r - I_l$, $\Delta_J \coloneqq J_r - J_l$ と定義すると，$|S_{\mathrm{ODGP}}(I,J)| = \Omega(\Delta_I\Delta_J)$.

*Proof.* 微小量 $\epsilon > 0$ をとり，$N = \left\lfloor (1-\epsilon)\Delta_I\Delta_J/(1+\sqrt{2})^2 \right\rfloor$, $\eta_i = J_l + i\Delta_J/N$ $(i=0,\ldots,N)$, $J^{(i)} = [\eta_{i-1}, \eta_i - \epsilon\Delta_J/N]$ $(i=1,\ldots,N)$ とおく．$\left\{J^{(i)}\right\}_i$ は互いに素な閉区間列で，$J \supseteq \bigcup_{i=1}^N J^{(i)}$. したがって，

$$|S_{\mathrm{ODGP}}(I,J)| \geq \left|S_{\mathrm{ODGP}}(I, \bigcup_{i=1}^N J^{(i)})\right| = \left|\bigcup_{i=1}^N S_{\mathrm{ODGP}}(I, J^{(i)})\right| = \sum_{i=1}^N \left|S_{\mathrm{ODGP}}(I, J^{(i)})\right| \tag{95}$$

が成り立つ．

$$\Delta_{J^{(i)}} = \left(\eta_i - \frac{\epsilon\Delta_J}{N}\right) - \eta_{i-1} = \frac{\Delta_J}{N} - \frac{\epsilon\Delta_J}{N} \geq (1-\epsilon)\Delta_J \cdot \left(\frac{(1-\epsilon)\Delta_I\Delta_J}{(1+\sqrt{2})^2}\right)^{-1} = \frac{(1+\sqrt{2})^2}{\Delta_I} \tag{96}$$

より，$\Delta_I \Delta_{J^{(i)}} \geq (1+\sqrt{2})^2$. よって，Lemma A.1 より，$\left|S_{\mathrm{ODGP}}(I, J^{(i)})\right| \geq 1$ であるから，$|S_{\mathrm{ODGP}}(I,J)|$ の下界について，

$$|S_{\mathrm{ODGP}}(I,J)| \geq N > (1-\epsilon)\Delta_I\Delta_J/(1+\sqrt{2})^2 - 1 \tag{97}$$

が得られる． □

# B Theorem 3.12 の証明 [4, Appendix A]

ellipse $E = \left\{u \in \mathbb{R}^2 \;\middle|\; (u-p)^\dagger D(u-p) \leq 1\right\}$ を考える．$D$ は正定値対称行列より，$a, b, d \in \mathbb{R}$ を用いて，

$$D = \begin{pmatrix} a & b \\ b & d \end{pmatrix} \tag{98}$$

と書ける．このとき，$\mathrm{area}(E) = \pi/\sqrt{\det D}$, $\mathrm{area}(\mathrm{BBox}(E)) = 4\sqrt{ad}/\det D$. よって，

$$\mathrm{up}(E) = \frac{\mathrm{area}(E)}{\mathrm{area}(\mathrm{BBox}(E))} = \frac{\pi}{4}\sqrt{\frac{\det D}{ad}}. \tag{99}$$

したがって，$E$ の uprightness は平行移動，スカラー倍に関して不変である．よって，$\det D \neq 1$ のときは $D/\det D$ を考えるとすれば，$\det D = 1$ の場合に帰着できる．

$\det D = 1$ が成り立つとき，$b, e, z \in \mathbb{R}$ を用いて，

$$D = \begin{pmatrix} e\lambda^{-z} & b \\ b & e\lambda^z \end{pmatrix} \tag{100}$$

と書ける．ただし，$e > 0$, $e^2 = b^2 + 1$ である．このとき，$\mathrm{up}(E)$ は，

$$\mathrm{up}(E) = \frac{\pi}{4e} = \frac{\pi}{4\sqrt{b^2+1}} \tag{101}$$

と書ける．逆に，$\mathrm{up}(E) = M$ のとき，$b^2 = \pi^2/16M^2 - 1$ が成り立つことが分かる．

以降，$E_A, E_B \subseteq \mathbb{R}^2$ を ellipse として，$E_A$, $E_B$ を定義する実正定値対称行列をそれぞれ $D$, $\Delta$ とする．ただし，$\det D = \det \Delta = 1$ が満たされていると仮定する．このとき，行列の組 $(D, \Delta)$ を *state* と呼ぶ．$D$ と $\Delta$ は，$b, e, z \in \mathbb{R}$ と $\beta, \epsilon, \zeta \in \mathbb{R}$ を用いて，

$$D = \begin{pmatrix} e\lambda^{-z} & b \\ b & e\lambda^{z} \end{pmatrix}, \quad \Delta = \begin{pmatrix} \epsilon\lambda^{-\zeta} & \beta \\ \beta & \epsilon\lambda^{\zeta} \end{pmatrix} \tag{102}$$

と書ける．ただし，$e > 0$, $e^2 = b^2 + 1$, $\epsilon > 0$, $\epsilon^2 = \beta^2 + 1$ を満たす．

**Definition B.1** ([4, Definition A.1])**.** state $(D, \Delta)$ に対して，

$$\mathrm{Skew}(D) \coloneqq b^2, \quad \mathrm{Skew}(\Delta) \coloneqq \beta^2, \tag{103}$$

$$\mathrm{Bias}(D) \coloneqq \frac{e\lambda^{z}}{e\lambda^{-z}} = \lambda^{2z}, \quad \mathrm{Bias}(\Delta) \coloneqq \frac{\epsilon\lambda^{\zeta}}{\epsilon\lambda^{-\zeta}} = \lambda^{2\zeta}, \tag{104}$$

$$\mathrm{Skew}(D, \Delta) \coloneqq \mathrm{Skew}(D) + \mathrm{Skew}(\Delta) = b^2 + \beta^2, \tag{105}$$

$$\mathrm{Bias}(D, \Delta) \coloneqq \mathrm{Bias}(\Delta) / \mathrm{Bias}(D) = \lambda^{2(\zeta - z)} \tag{106}$$

と定義する．

**Remark B.2** ([4, Remark A.2])**.** state $(D, \Delta)$ が $b \geq 0$ を満たすとき，$-be \leq -b^2$ が成り立つ．実際，

$$e^2 = b^2 + 1 \Rightarrow e^2 \geq b^2 \Rightarrow e \geq b \Rightarrow -be \leq -b^2. \tag{107}$$

同様に，$b \leq 0$ を満たすとき，$be \leq -b^2$ が成り立つ．$\beta$ と $\epsilon$ に関しても，同様の式が成り立つ．

**Definition B.3** ([4, Definition A.3])**.** state $(D, \Delta)$ と grid operator $G$ に対して，

$$G \cdot (D, \Delta) \coloneqq ((G^{-1})^{\dagger} D G^{-1}, ((G^{\bullet})^{-1})^{\dagger} \Delta (G^{\bullet})^{-1}) \tag{108}$$

と定義する．

**Lemma B.4** ([4, Lemma A.4])**.** state $(D, \Delta)$ と中心 $p_A, p_B \in \mathbb{R}^2$ について，$E_A$ は中心 $p_A$ と行列 $D$ によって定義される ellipse，$E_B$ は中心 $p_B$ と行列 $\Delta$ によって定義される ellipse とする．$(D', \Delta') = G \cdot (D, \Delta)$ とすると，$G(A)$ は中心 $Gp_A$ と行列 $D'$ によって定義される ellipse，$G^{\bullet}(B)$ は中心 $G^{\bullet} p_B$ と行列 $\Delta'$ によって定義される ellipse である．

*Proof.*

$$\begin{aligned} G(A) &= \left\{ Gu \in \mathbb{R}^2 \;\middle|\; (u - p_A)^{\dagger} D (u - p_A) \leq 1 \right\} \\ &= \left\{ v \in \mathbb{R}^2 \;\middle|\; (G^{-1}v - p_A)^{\dagger} D (G^{-1}v - p_A) \leq 1 \right\} \\ &= \left\{ v \in \mathbb{R}^2 \;\middle|\; (v - Gp_A)^{\dagger} (G^{-1})^{\dagger} D G^{-1} (v - Gp_A) \leq 1 \right\} \\ &= \left\{ v \in \mathbb{R}^2 \;\middle|\; (v - Gp_A)^{\dagger} D' (v - Gp_A) \leq 1 \right\}. \end{aligned} \tag{109}$$

$G(B)$ についても同様. □

**Lemma B.5** (Step Lemma [4, Lemma A.5])**.** 任意の state $(D, \Delta)$ について，$\mathrm{Skew}(D, \Delta) \geq 15$ ならば，$\mathrm{Skew}(G \cdot (D, \Delta)) \leq 0.9\, \mathrm{Skew}(D, \Delta)$ を満たす special grid operator $G$ が存在する．更に，この $G$ は定数時間で計算可能である．

*Proof.* 証明略. □

**Theorem 3.12.** $E_A, E_B \subseteq \mathbb{R}^2$ を ellipse とする．このとき，$G(E_A)$ と $G^\bullet(E_B)$ が 1/6-upright であるような grid operator $G$ が存在する．更に，$E_A$ と $E_B$ が $M$-upright であるとき，この $G$ は $O(\log(1/M))$ 時間で計算できる．

*Proof.* $E_A$ は行列 $D$ によって定義され，$E_B$ は行列 $\Delta$ によって定義されるとする．$D \leftarrow D/\det D$, $\Delta \leftarrow \Delta/\det\Delta$ とすることで，$(D, \Delta)$ は state であると仮定してよい．Lemma B.5 を繰り返し用いることで，

$$\mathrm{Skew}(G_n G_{n-1} \cdots G_1 \cdot (D, \Delta)) \leq 15 \tag{110}$$

となるような special grid operator の列 $G_1, \ldots, G_n$ を得る．$G = G_n G_{n-1} \cdots G_1$, $(D', \Delta') = G \cdot (D, \Delta)$ とすると，$G$ は special grid operator であり，Lemma B.4 より，$G(A)$, $G^\bullet(B)$ はそれぞれ $D'$, $\Delta'$ によって定義される ellipse である．$b$, $\beta$ をそれぞれ $D'$, $\Delta'$ の非対角要素とすると，

$$b'^2 + \beta'^2 = \mathrm{Skew}(D', \Delta') = \mathrm{Skew}(G_n G_{n-1} \cdots G_1 \cdot (D, \Delta)) < 15 \tag{111}$$

より，$b'^2 \leq 15$ かつ $\beta'^2 \leq 15$ を得る．よって，

$$\mathrm{up}(G(A)) = \frac{\pi}{4\sqrt{b'^2+1}} \geq \frac{\pi}{4\sqrt{16}} > \frac{1}{6}, \quad \mathrm{up}(G^\bullet(B)) = \frac{\pi}{4\sqrt{\beta'^2+1}} \geq \frac{\pi}{4\sqrt{16}} > \frac{1}{6} \tag{112}$$

が成り立つ．

更に，Lemma B.5 を用いる度に Skew は 0.9 倍以下になるから，$n \leq \log_{0.9}(15/\mathrm{Skew}(D, \Delta)) + 1 = O(\log(\mathrm{Skew}(D, \Delta)))$ である．$b^2 \leq \pi^2/16M^2 - 1$, $\beta^2 \leq \pi^2/16M^2 - 1$ より，

$$\log(\mathrm{Skew}(D, \Delta)) \leq \log\left(\left(\pi^2/16M^2 - 1\right) + \left(\pi^2/16M^2 - 1\right)\right) = O(\log(1/M)). \tag{113}$$

よって，Lemma B.5 を用いる際の各ステップは定数時間であるから，全体での時間計算量は $O(\log(1/M))$ である． □