Number-theoretic methods in quantum information theory

Peter Selinger

Dalhousie University
Halifax, Canada

Thesis: Good algorithms come from good mathematics

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

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

- **New efficient synthesis algorithms** (ca. 2012):
  Algebraic number theory.

$$a + b\sqrt{2}.$$

Part I: Some number theory

Some number theory: Fermat's theorem on sums of two squares

Which integers can be written as a sum of two squares?

Some number theory: Fermat's theorem on sums of two squares

Which integers can be written as a sum of two squares?

Theorem. If $\mathfrak{n}$ and $\mathfrak{m}$ can each be written as a sum of two squares, then $\mathfrak{nm}$ can be written as a sum of two squares.

Some number theory: Fermat's theorem on sums of two squares

Which integers can be written as a sum of two squares?

Theorem. If n and m can each be written as a sum of two squares, then nm can be written as a sum of two squares.

Proof. This is easiest seen using complex numbers. Note that $a^2 + b^2 = (a + bi)(a - bi)$.

Therefore, n is a sum of two squares if and only if it can be written in the form $t^\dagger t$, for some Gaussian integer $t = a + bi \in \mathbb{Z}[i]$.

The claim follows because $nm = (t^\dagger t)(u^\dagger u) = (tu)^\dagger (tu)$. □

First lesson of number theory

We can learn more about the integers by moving to a larger ring, such as $\mathbb{Z}[\mathrm{i}]$.

Fermat's theorem on sums of two squares, continued

What about the converse?

Theorem. If nm can be written as a sum of two squares, and if n, m are relatively prime, and $n, m \geq 0$, then n and m can each be written as a sum of two squares.

Fermat's theorem on sums of two squares, continued

What about the converse?

Theorem. If nm can be written as a sum of two squares, and if n, m are relatively prime, and $n, m \geq 0$, then n and m can each be written as a sum of two squares.

Proof. Suppose $nm = a^2 + b^2 = (a + bi)(a - bi)$.

$\mathbb{Z}[i]$ is a Euclidean domain, so has greatest common divisors. Let $t = \gcd(n, a + bi)$ and $s = \gcd(m, a + bi)$ in $\mathbb{Z}[i]$.

An easy argument (using uniqueness of prime factorizations in $\mathbb{Z}[i]$) shows that $n = t^\dagger t$ and $m = s^\dagger s$. Hence both n and m can be written as a sum of two squares.

Second lesson of number theory

The fact that $\mathbb{Z}[\mathrm{i}]$ is a Euclidean domain, and in particular, the ability to take greatest common divisors and prime factorizations in $\mathbb{Z}[\mathrm{i}]$, is very helpful.

Definition. A ring is called a *Euclidean domain* if it is equipped with a notion of *division with remainder*. Specifically, such a ring must have:

1. A *Euclidean function*, i.e., a function f assigning a natural number to each ring element;

2. *Division with remainder*: For all a, b with $b \neq 0$, there exist q, r such that

$$a = bq + r$$

and $f(r) < f(b)$.

Main properties. In a Euclidean domain, the concepts of *divisor*, *greatest common divisor*, and *prime* make sense. The Euclidean algorithm can be used to compute greatest common divisors $d = \gcd(a, b)$, as well as x, y such that $d = xa + yb$. Euclidean domains satisfy unique prime factorization.

Fermat's theorem on sums of two squares, continued

By the previous theorems, it suffices to consider primes. Which primes can be written as a sum of two squares?

Obvious necessary condition: $p > 0$.

p		a^2+b^2
2	=	$1+1$
3	=	—
5	=	$1+4$
7	=	—
11	=	—
13	=	$4+9$
17	=	$1+16$
19	=	—
23	=	—
29	=	$4+25$

p		a^2+b^2
31	=	—
37	=	$1+36$
41	=	$16+25$
43	=	—
47	=	—
53	=	$4+49$
59	=	—
61	=	$25+36$
67	=	—
71	=	—

p		a^2+b^2
73	=	$9+64$
79	=	—
83	=	—
89	=	$25+64$
97	=	$16+81$
101	=	$1+100$
103	=	—
107	=	—
109	=	$9+100$
113	=	$49+64$

Fermat's theorem on sums of two squares, continued

By the previous theorems, it suffices to consider primes. Which primes can be written as a sum of two squares?

Obvious necessary condition: $p > 0$.

p		a^2+b^2	$p \pmod 4$
2	=	$1+1$	2
3	=	—	3
5	=	$1+4$	1
7	=	—	3
11	=	—	3
13	=	$4+9$	1
17	=	$1+16$	1
19	=	—	3
23	=	—	3
29	=	$4+25$	1

p		a^2+b^2	$p \pmod 4$
31	=	—	3
37	=	$36+1$	1
41	=	$25+16$	1
43	=	—	3
47	=	—	3
53	=	$49+4$	1
59	=	—	3
61	=	$36+25$	1
67	=	—	3
71	=	—	3

p		a^2+b^2	$p \pmod 4$
73	=	$9+64$	1
79	=	—	3
83	=	—	3
89	=	$25+64$	1
97	=	$16+81$	1
101	=	$1+100$	1
103	=	—	3
107	=	—	3
109	=	$9+100$	1
113	=	$49+64$	1

Fermat's theorem on sums of two squares, continued

Theorem. A positive odd prime p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$.

Proof. "$\Rightarrow$": $a^2 \equiv 0, 1 \pmod 4$, hence $a^2 + b^2 \equiv 0, 1, 2 \pmod 4$.

"$\Leftarrow$" Suppose p is a positive prime with $p \equiv 1 \pmod 4$.

(1) We can find $h \in \mathbb{Z}_p$ such that $h^2 = -1$. (This follows from Fermat's Little Theorem). W.l.o.g. $h < p/2$.

(2) Therefore, $h^2 + 1 = kp$, for some $k \in Z$. So kp can be written as a sum of two squares. It follows from the previous theorem that p can be written as a sum of two squares. $\square$

Moreover: There is an efficient algorithm to compute a, b.

Summary: Algorithm for $n = a^2 + b^2$

We shows that there exists an efficient (probabilistic) algorithm which,

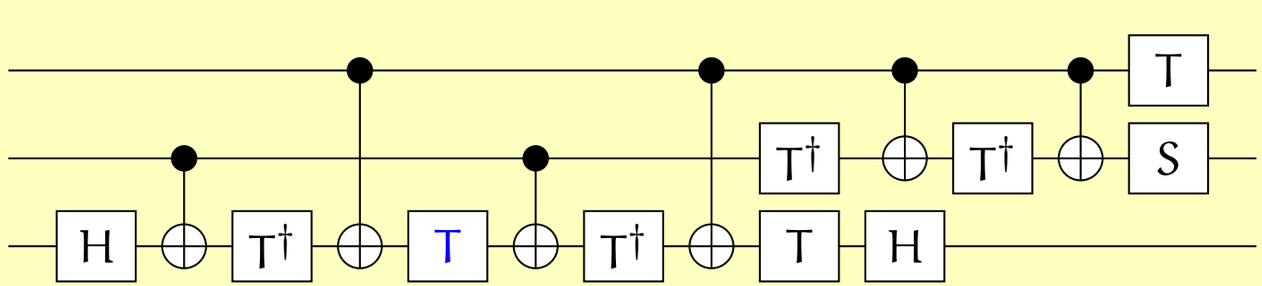
- **given** a number $n \in \mathbb{Z}$, and
- **given** a prime factorization of n,
- **decides** whether there exists $a, b \in \mathbb{Z}$ with $a^2 + b^2 = n$, and
- **computes** such a, b if they exist.

Part II: An algebraic characterization of Clifford+T circuits

Quantum circuits

Let $\mathcal{U}$ be the symmetric monoidal category of finite dimensional vector spaces and unitary maps. Since all morphisms are invertible, this is a groupoid.

The internal language for symmetric monoidal categories consists of linear string diagrams (no loops). These are more commonly known as *quantum circuits*.



There are uncountably many unitary operations. In quantum computing, we usually work with a fixed discrete *gate set*.

The Clifford groupoid

Definition. The *Clifford groupoid* is the smallest symmetric monoidal subcategory of $\mathcal{U}$ containing:

- The object $V = \mathbb{C}^2$;
- The maps $H, S : V \to V$, $\omega : I \to I$, and $CNot : V \otimes V \to V \otimes V$.

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

It also contains the Pauli $X = HSSH$, $Y = HSSHSS\omega^2$, and $Z = SS$ gates, among others.

Clifford gates are *not* universal for quantum computing; they can be efficiently simulated on a classical computer, using the *stabilizer formalism*.

However, Clifford gates can be very cheaply implemented under all practical error correction schemes (stabilizer codes and topological codes).

The Clifford+T groupoid

To get universal quantum computing, we need to add at least one non-Clifford gate. The gate most commonly used for this purpose is the T-gate:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

Reasons for singling out the T-gate:

- It is maximally noise tolerant among the non-Clifford gates. See [Buhrman-Cleve-Laurent-Linden-Schrijver-Unger].

- There are known fault-tolerant implementation of the T-gate in all important error correction schemes.

A necessary condition for being a Clifford+T operator

Let U be a Clifford+T operator on n qubits. Then the matrix entries of U are made up from integers, i, and $\frac{1}{\sqrt{2}}$ by multiplication and addition. In other words, every Clifford+T operator takes its matrix entries in the ring

$$\mathbb{Z}[\frac{1}{\sqrt{2}}, i] \quad = \quad \left\{ \quad \frac{1}{\sqrt{2}^k}(a + bi + c\sqrt{2} + di\sqrt{2}) \quad | \quad k \in \mathbb{N}; \quad a, b, c, d \in \mathbb{Z} \quad \right\}.$$

Proof: trivial, because it is true for the generators:

$$\mathrm{CNot} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \omega = \frac{1+i}{\sqrt{2}}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

Remarkably, the converse is also true

Theorem ([Giles, Selinger 2012], see also [Kliuchnikov, Maslov, Mosca 2012]).

Let U be an n-qubit unitary operator. Then U can be realized by a Clifford+T circuit (possibly with ancillas initialized and finalized in state $|0\rangle$) if and only if the entries of U are in $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$.

Moreover, one ancilla is always sufficient. If $\det U = 1$, no ancilla is necessary.

Example.

$$\frac{1}{\sqrt{2}^7}\begin{pmatrix} -3+4\sqrt{2}+(3+5\sqrt{2})\,i & 3+(-1+3\sqrt{2})\,i \\ -3-\sqrt{2}+(3-2\sqrt{2})\,i & 9-(1+3\sqrt{2})\,i \end{pmatrix}$$

$$= T\,H\,T\,S\,H\,T\,S\,H\,T\,H\,T\,S\,H\,T\,H\,T\,S\,H\,T\,H\,T\,S\,H\,T\,S\,S\,S\omega^7$$

Complexity: The Giles-Selinger algorithm produces $O(3^{2^n} nk)$ gates. This was improved to $O(4^n nk)$ by [Kliuchnikov 2013]. Here n is the number of qubits and k is the denominator exponent.

Description of the exact synthesis algorithm

Before we can describe the algorithm, we will need a fair amount of algebra. However, the basic idea is simple.

Recall from Gaussian elimination:

- A *row operation* on a matrix correspond to *left multiplication by an elementary matrix*.
- Therefore, if we can reduce a matrix U to the identity matrix by repeated application of row operations, we get

$$A_1 A_2 \cdots A_n U = I.$$

- If each A_i can be converted to a Clifford+T circuit, then U can be converted to a Clifford+T circuit.

We thus need to define suitable row operations, and show that any given U can be converted to the identity.

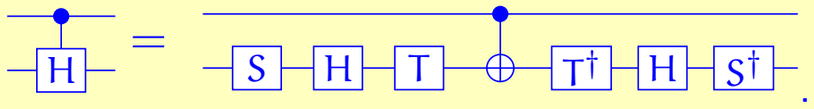
Row operations

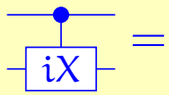
The row operations we will use are the following:

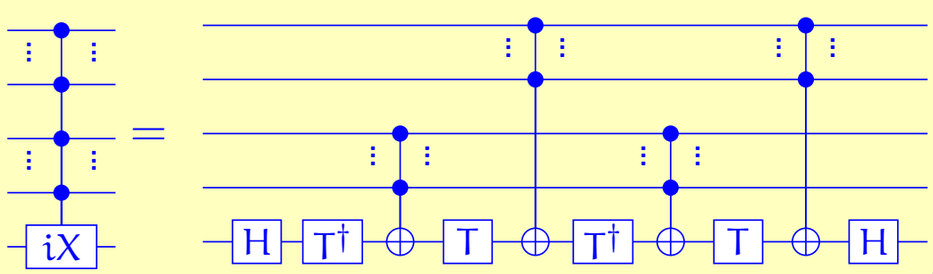
1. Multiply one row by ω ("shift");
2. Apply a Hadamard gate to a pair of rows ("reduce");
3. Exchange two rows ("swap").

$$\omega_{[j]} = \begin{array}{c} \\ \vdots \\ j \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccc} \cdots & j & \cdots \end{array} \\ \begin{pmatrix} I & & \\ & \omega & \\ & & I \end{pmatrix} \end{array}, \quad H_{[j,\ell]} = \begin{array}{c} \\ \vdots \\ j \\ \vdots \\ \ell \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccccc} \cdots & j & \cdots & \ell & \cdots \end{array} \\ \begin{pmatrix} I & & & & \\ & \frac{1}{\sqrt{2}} & & \frac{1}{\sqrt{2}} & \\ & & I & & \\ & \frac{1}{\sqrt{2}} & & \frac{-1}{\sqrt{2}} & \\ & & & & I \end{pmatrix} \end{array}, \quad X_{[j,\ell]} = \begin{array}{c} \\ \vdots \\ j \\ \vdots \\ \ell \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccccc} \cdots & j & \cdots & \ell & \cdots \end{array} \\ \begin{pmatrix} I & & & & \\ & 0 & & 1 & \\ & & I & & \\ & 1 & & 0 & \\ & & & & I \end{pmatrix} \end{array}.$$

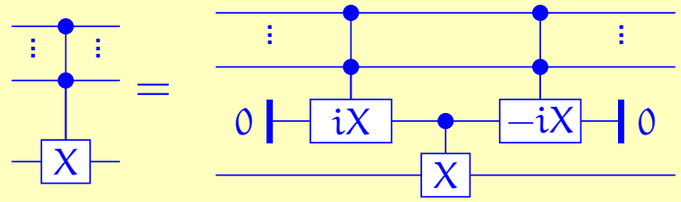
Each of these row operations can be easily represented as a Clifford+T circuit.



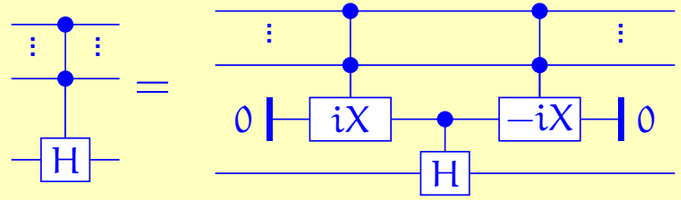




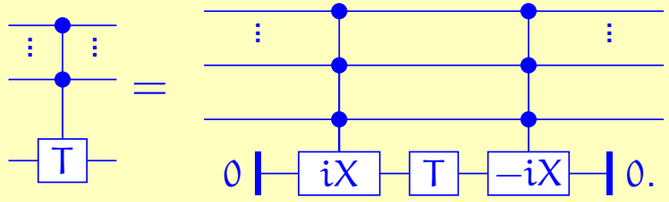
(a)



(b)



(c)



Some algebra

Definition. A complex number z is called *algebraic* if it is the root of some polynomial p with integer coefficients.

Example: $z = \sqrt{\frac{1}{2} + \sqrt{2}}$ is algebraic because

$$(z^2 - \frac{1}{2})^2 = 2,$$

or equivalently,

$$4z^4 - 4z^2 - 7 = 0.$$

Definition. A complex number z is an *algebraic integer* if it is the root of some *monic* polynomial p with integer coefficients. Monic means that the leading coefficient is 1.

Example: $w = \sqrt{1 + \sqrt{2}}$ is an algebraic integer, because

$$w^4 - 2w^2 - 1 = 0.$$

Examples

Field:	Ring of algebraic integers:	
$\mathbf{Q}$	$\mathbb{Z}$	(integers)
$\mathbf{Q}[\mathrm{i}]$	$\mathbb{Z}[\mathrm{i}]$	(Gaussian integers)
$\mathbf{Q}[\sqrt{2}]$	$\mathbb{Z}[\sqrt{2}]$	(quadratic integers of radicand 2)
$\mathbf{Q}[\sqrt{2},\mathrm{i}] = \mathbf{Q}[\omega]$	$\mathbb{Z}[\omega]$	(cyclotomic integers of degree 8)

Recall that $\omega = e^{i\pi/4}$.

We have $\omega = \frac{1+\mathrm{i}}{\sqrt{2}}$. Conversely, $\sqrt{2} = \omega + \omega^7$, $\mathrm{i} = \omega^2$. Thus $\mathbf{Q}[\sqrt{2},\mathrm{i}] = \mathbf{Q}[\omega]$.

Properties of algebraic numbers and algebraic integers

- The set of algebraic numbers is closed under addition, subtraction, multiplication, and division, i.e., it is a subfield of $\mathbb{C}$.

- The set of algebraic integers is closed under addition, subtraction, and multiplication, i.e., it is a subring of $\mathbb{C}$ (but not a field).

- Every rational number is algebraic; it is an algebraic integer iff it is an integer.

- If z is the root of a polynomial whose coefficients are algebraic numbers, then z is an algebraic number.

- If z is the root of a monic polynomial whose coefficients are algebraic integers, then z is an algebraic integer.

The automorphisms of $\mathbb{Z}[\omega]$

Because $\omega^4 = -1$, the elements of $\mathbb{Z}[\omega]$ can be uniquely written in the form

$$a\omega^3 + b\omega^2 + c\omega + d,$$

where $a, b, c, d \in \mathbb{Z}$.

The ring $\mathbb{Z}[\omega]$ has four automorphisms:

Complex conjugate. The automorphism $\dagger$ maps i to $-i$ and $\sqrt{2}$ to itself; equivalently, it maps ω to $-\omega^3$. Explicitly:

$$(a\omega^3 + b\omega^2 + c\omega + d)^\dagger = -c\omega^3 - b\omega^2 - a\omega + d.$$

Root-Two-conjugate. The automorphism $\bullet$ maps $\sqrt{2}$ to $-\sqrt{2}$ and i to itself; equivalently, it maps ω to $-\omega$. Explicitly:

$$(a\omega^3 + b\omega^2 + c\omega + d)^\bullet = -a\omega^3 + b\omega^2 - c\omega + d.$$

The other two automorphisms are $(-)^{\dagger\bullet} = (-)^{\bullet\dagger}$ and the identity.

Residues

Let $\mathbb{Z}_2$ be the ring of integers modulo 2. There is a unique ring homomorphism $\overline{(-)} : \mathbb{Z} \to \mathbb{Z}_2$, called the *parity map*: we have

$$\overline{a} = \begin{cases} 0 & \text{if } a \text{ is even,} \\ 1 & \text{if } a \text{ is odd.} \end{cases}$$

This induces a ring homomorphism $\rho : \mathbb{Z}[\omega] \to \mathbb{Z}_2[\omega]$, defined by

$$\rho(a\omega^3 + b\omega^2 + c\omega + d) = \overline{a}\omega^3 + \overline{b}\omega^2 + \overline{c}\omega + \overline{d}.$$

We call ρ the *residue map*, and we call $\rho(t)$ the *residue* of t.

Convention. For brevity, we write each residue $\overline{a}\omega^3 + \overline{b}\omega^2 + \overline{c}\omega + \overline{d}$ as a string of binary digits $\overline{a}\,\overline{b}\,\overline{c}\,\overline{d}$.

There are sixteen residues 0000, 0001, 0010, $\ldots$, 1111.

Dyadic fractions

Definition. The ring of *dyadic fractions* is $\mathbb{D} = \mathbb{Z}[\frac{1}{2}]$.

In other words, a dyadic fraction is a rational number of the form $\frac{a}{2^k}$, i.e., whose denominator is a power of 2.

The ring $\mathbb{D}[\omega]$ and denominator exponents

Recall that we are interested in matrices whose entries are in the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}, i]$. We have:

$$\mathbb{Z}[\frac{1}{\sqrt{2}}, i] = \mathbb{D}[\omega].$$

Its subring of algebraic integers is $\mathbb{Z}[\omega]$.

Each element t of $\mathbb{D}[\omega]$ can be written in the form

$$t = \frac{1}{\sqrt{2}^k}(a\omega^3 + b\omega^2 + c\omega + d),$$

where $a, b, c, d \in \mathbb{Z}$ and $k \in \mathbb{N}$. We say that k is a *denominator exponent* for t. The least such k is the *least denominator exponent* of t.

If k is a denominator exponent for t, then we define the k-*residue of* t to be the residue of $\sqrt{2}^k\, t$. Similarly for vectors and matrices.

Example

$$U = \frac{1}{\sqrt{2}^7}\begin{pmatrix} -3+4\sqrt{2}+(3+5\sqrt{2})\,i & 3+(-1+3\sqrt{2})\,i \\ -3-\sqrt{2}+(3-2\sqrt{2})\,i & 9-(1+3\sqrt{2})\,i \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}^7}\begin{pmatrix} \omega^3+3\omega^2+9\omega-3 & 3\omega^3-\omega^2+3\omega+3 \\ -\omega^3+3\omega^2-3\omega-3 & -3\omega^3-\omega^2-3\omega+9 \end{pmatrix}$$

A denominator exponent is 7. The 7-residue is

$$\begin{pmatrix} 1111 & 1111 \\ 1111 & 1111 \end{pmatrix}$$

But is this the least denominator exponent?

Example

$$U = \frac{1}{\sqrt{2}^7}\begin{pmatrix} -3+4\sqrt{2}+(3+5\sqrt{2})\,i & 3+(-1+3\sqrt{2})\,i \\ -3-\sqrt{2}+(3-2\sqrt{2})\,i & 9-(1+3\sqrt{2})\,i \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}^7}\begin{pmatrix} \omega^3+3\omega^2+9\omega-3 & 3\omega^3-\omega^2+3\omega+3 \\ -\omega^3+3\omega^2-3\omega-3 & -3\omega^3-\omega^2-3\omega+9 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}^6}\begin{pmatrix} 3\omega^3+5\omega^2+0\omega+4 & -2\omega^3+3\omega^2+\omega+0 \\ 3\omega^3-2\omega^2+0\omega-1 & -5\omega^3-3\omega^2+4\omega+0 \end{pmatrix}$$

The least denominator exponent is 6. The 6-residue is

$$\begin{pmatrix} 1100 & 0110 \\ 1001 & 1100 \end{pmatrix}$$

Operations on residues

At the heart of the exact synthesis algorithm are the following calculations on residues. For $t \in \mathbb{Z}[\omega]$, the residues of t, $\sqrt{2}\,t$, and $t^\dagger t$ are related as follows:

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$
0000	0000	0000
0001	1010	0001
0010	0101	0001
0011	1111	1010

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$
0100	1010	0001
0101	0000	0000
0110	1111	1010
0111	0101	0001

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$
1000	0101	0001
1001	1111	1010
1010	0000	0000
1011	1010	0001

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$
1100	1111	1010
1101	0101	0001
1110	1010	0001
1111	0000	0000

Operations on residues

At the heart of the exact synthesis algorithm are the following calculations on residues. For $t \in \mathbb{Z}[\omega]$, the residues of t, $\sqrt{2}\,t$, and $t^\dagger t$ are related as follows:

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$
0000	0000	0000
0001	1010	0001
0010	0101	0001
0011	1111	1010

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$
0100	1010	0001
0101	0000	0000
0110	1111	1010
0111	0101	0001

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$
1000	0101	0001
1001	1111	1010
1010	0000	0000
1011	1010	0001

$\rho(t)$	$\rho(\sqrt{2}\,t)$	$\rho(t^\dagger t)$
1100	1111	1010
1101	0101	0001
1110	1010	0001
1111	0000	0000

Lemma. For a residue x, the following are equivalent:

(a) x is reducible, i.e., of the form $\sqrt{2}\,y$;

(b) $x \in \{0000, 0101, 1010, 1111\}$;

(c) $\sqrt{2}\,x = 0000$;

(d) $x^\dagger x = 0000$.

For $k > 0$, the k-residues of one column satisfy

$$u_1^\dagger u_1 + \ldots + u_n^\dagger u_n = 2^k \equiv 0 \,(\mathrm{mod}\, 2) \tag{1}$$

From the table on the previous page:

- If $u^\dagger u = 0000$, then $u \in \{0000, 0101, 1010, 1111\}$.
- If $u^\dagger u = 1010$, then $u \in \{0011, 0110, 1100, 1001\}$.
- If $u^\dagger u = 0001$, then $u \in \{0001, 0010, 0100, 1000, \quad 0111, 1011, 1101, 1110\}$.

From (1), it follows that there are *an even number of each kind*.

On each such pair, by an appropriate sequence of "shift" and "reduce", we can decrease the denominator exponent.

By induction, the whole column can be reduced to denominator exponent 0, then to $(1, 0, \ldots, 0)$. By induction, the whole matrix can be reduced to I.

Summary: Algebraic characterization of the Clifford+T groupoid

We have proved:

Theorem. The Clifford+T groupoid consists precisely of the unitary $2^n \times 2^n$ matrices over the ring $\mathbb{D}[\omega]$.

Consequence: We can now use number-theoretic methods for solving circuit-theoretic problems. For example, as we will see in a later lecture, the *approximation problem* for circuits has been solved using such methods.

Gate complexity of exact synthesis

The Giles-Selinger exact synthesis algorithm produces $O(3^{2^n} nk)$ Clifford+T gates, where n is the number of qubits and k is the least denominator exponent.

Kliuchnikov improved this to $O(4^n nk)$.

It is unlikely that there will be an *optimal* algorithm for this problem, since the problem of finding minimal Clifford+T circuits is NP-hard.

However: Remarkably, for the case $n = 1$, there *does* exist an optimal solution. It was discovered by Matsumoto and Amano [2008].

Part III: Matsumoto-Amano normal forms

The Matsumoto-Amano normal form

Theorem [Matsumoto and Amano 2008]. Every Clifford+T operator U on a single qubit can be *uniquely* written of the form

$$U = (T \mid \epsilon)\,(HT \mid SHT)^*\,\mathcal{C},$$

where $\mathcal{C}$ is a Clifford operator.

Example.

$$U = T\,HT\,SHT\,SHT\,HT\,SHT\,HT\,SHT\,HT\,HT\,SHT\,SSS\omega^7$$

We can measure the "length" of an operator U in terms of its T-count; for example, the above U has T-count 11.

Theorem. Of all the possible single-qubit circuits for a given operator, the Matsumoto-Amano normal form has the smallest T-count.

Proof idea, Matsumoto and Amano normal form

Existence: By rewriting. Generators: S, H, T, ω. Rewrite rules:

$$\begin{aligned}
\mathrm{T}\ \mathrm{T} &\longrightarrow \mathrm{S} \\
\mathrm{S}\ \mathrm{T} &\longrightarrow \mathrm{T}\ \mathrm{S} \\
\omega\ \mathrm{T} &\longrightarrow \mathrm{T}\ \omega \\
\mathrm{H}\ \mathrm{HT} &\longrightarrow \mathrm{T} \\
\omega\ \mathrm{HT} &\longrightarrow \mathrm{HT}\ \omega \\
\mathrm{H}\ \mathrm{SHT} &\longrightarrow \mathrm{SHT}\ \mathrm{HSSH} \\
\mathrm{S}\ \mathrm{SHT} &\longrightarrow \mathrm{HT}\ \mathrm{HSSHS}\omega^7 \\
\omega\ \mathrm{SHT} &\longrightarrow \mathrm{SHT}\ \omega.
\end{aligned}$$

This terminates and leads to a normal form. It can be done efficiently (linear time).

Also, the rewriting rules do not increase T-count.

Proof idea, Matsumoto and Amano normal form

Uniqueness: Consider the Bloch sphere representation of the generators:

$$\hat{H} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \hat{S} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \hat{T} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix} \quad \hat{\omega} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Convert a Matsumoto-Amano normal form M to a Bloch sphere operator. The matrix entries are therefore in the ring $\mathbb{Z}[\sqrt{2}]$. Write it with least denominator exponent k:

$$\hat{M} = \frac{1}{\sqrt{2}^k} \begin{pmatrix} a + a'\sqrt{2} & b + b'\sqrt{2} & c + c'\sqrt{2} \\ d + d'\sqrt{2} & e + e'\sqrt{2} & f + f'\sqrt{2} \\ g + g'\sqrt{2} & h + h'\sqrt{2} & i + i'\sqrt{2} \end{pmatrix}$$

Consider the *parity matrix*

$$\begin{pmatrix} \overline{a} & \overline{b} & \overline{c} \\ \overline{d} & \overline{e} & \overline{f} \\ \overline{g} & \overline{h} & \overline{i} \end{pmatrix}$$

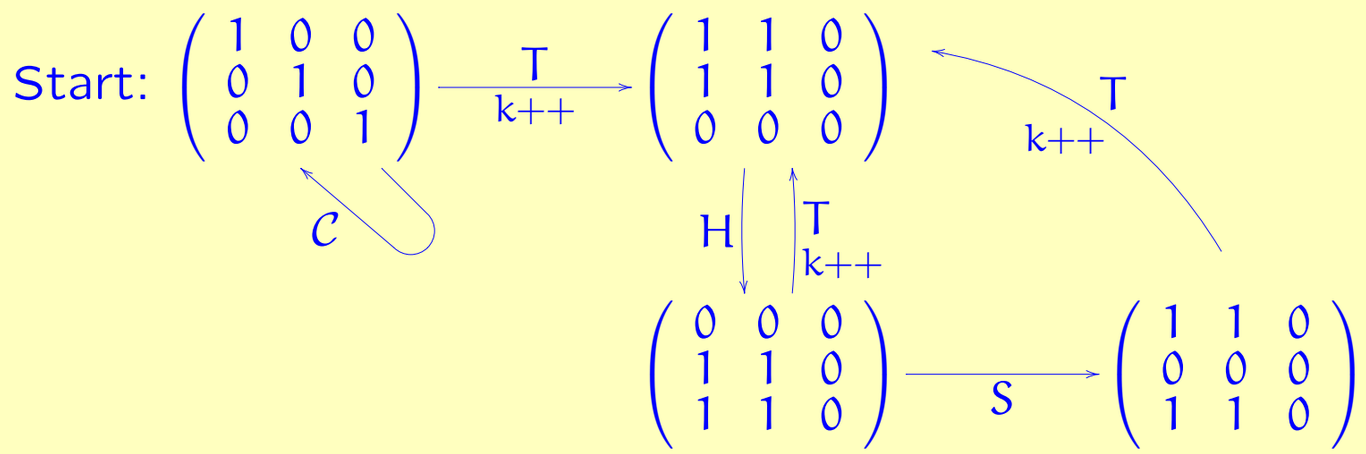
Uniqueness, continued

Lemma (by easy induction on normal form M):

- If M starts with HT, then $(\overline{a}, \overline{b}, \overline{c}) = (0, 0, 0)$ and $(\overline{d}, \overline{e}, \overline{f}) = (\overline{g}, \overline{h}, \overline{i}) \neq (0, 0, 0)$.
- If M starts with SHT, then $(\overline{d}, \overline{e}, \overline{f}) = (0, 0, 0)$ and $(\overline{a}, \overline{b}, \overline{c}) = (\overline{g}, \overline{h}, \overline{i}) \neq (0, 0, 0)$.
- If M starts with T, then $(\overline{g}, \overline{h}, \overline{i}) = (0, 0, 0)$ and $(\overline{a}, \overline{b}, \overline{c}) = (\overline{d}, \overline{e}, \overline{f}) \neq (0, 0, 0)$.
- If M is Clifford, then $(\overline{a}, \overline{b}, \overline{c}) \neq (\overline{d}, \overline{e}, \overline{f}) \neq (\overline{g}, \overline{h}, \overline{i}) \neq (\overline{a}, \overline{b}, \overline{c})$.

Moreover, each syllable HT, SHT, or T increases the denominator exponent k by exactly 1.

As a graph:



This shows the left action of Matsumoto-Amano normal forms on k-parities over $SO(3)$. All matrices are written modulo the right action of the Clifford group, i.e., modulo a permutation of the columns.

Counting normal forms

Theorem [Matsumoto and Amano 2008]. Every Clifford+T operator U on a single qubit can be *uniquely* written of the form

$$U = (T \mid \epsilon)\,(HT \mid SHT)^*\,\mathcal{C},$$

where $\mathcal{C}$ is a Clifford operator.

Corollary [Matsumoto and Amano 2008]. There are exactly

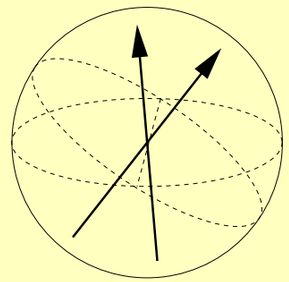
$$192 \cdot (3 \cdot 2^n - 2)$$

distinct Clifford+T operators of T-count $\leq n$.

Part IV: Approximation of unitary operators: geometric methods

The naïve method

Theorem. If A, B are two rotations by an irrational multiple of π, about two different axes, then A and B span a dense subgroup of $SO(3)$.



Proof. Obvious. Since the angle is irrational, operators of the form A^m can be used to approximate *any* angle of rotation about the given axis up to $\epsilon/3$. We can then use an operator of the form

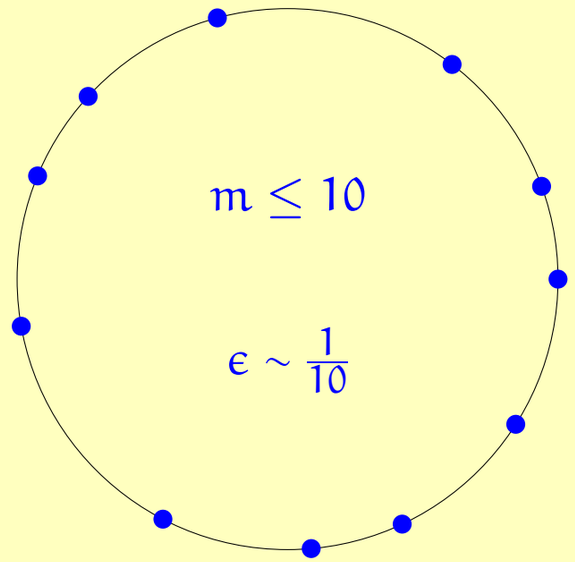
$$A^m B^p A^q$$

to approximate an (almost) arbitrary rotation up to ϵ.

How good is the naïve method?

Runtime: very efficient.

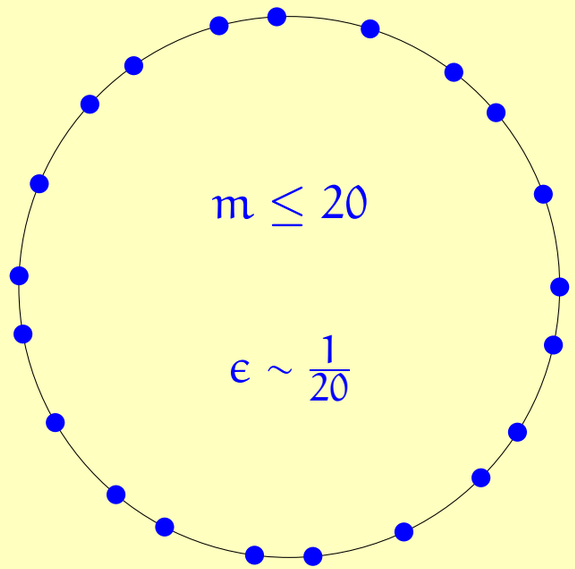
Gate count: How do m, p, and q scale with ϵ?



How good is the naïve method?

Runtime: very efficient.

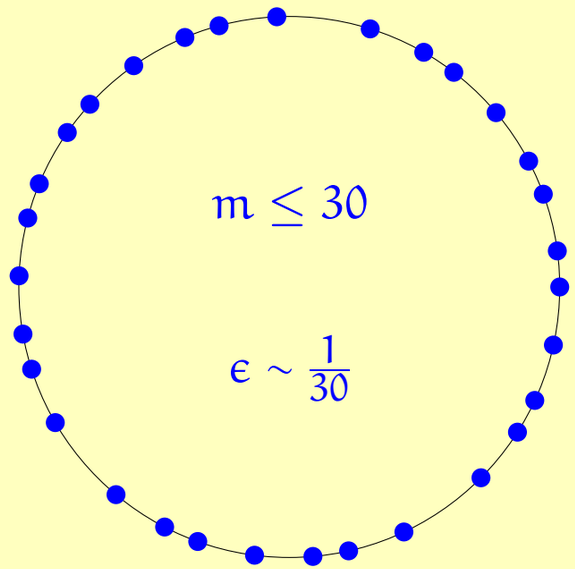
Gate count: How do m, p, and q scale with ϵ?



How good is the naïve method?

Runtime: very efficient.

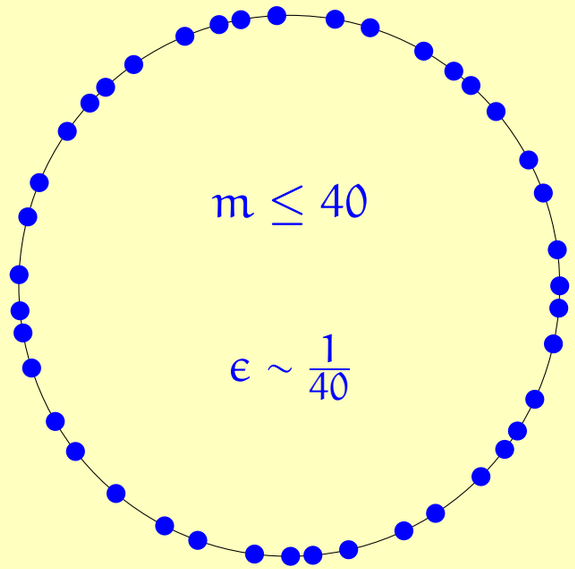
Gate count: How do m, p, and q scale with ϵ?



How good is the naïve method?

Runtime: very efficient.

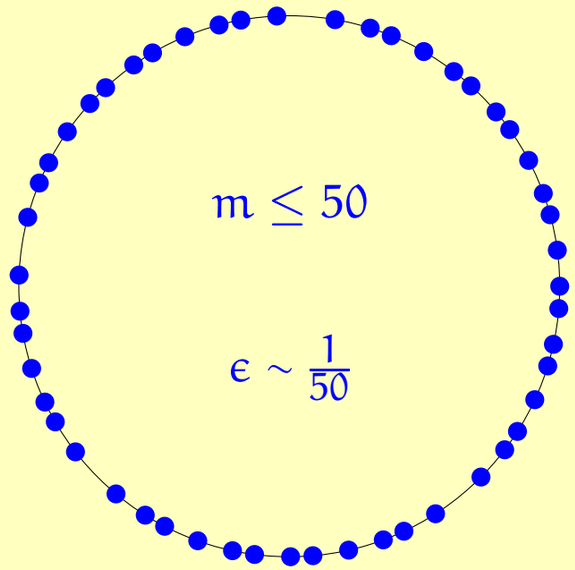
Gate count: How do m, p, and q scale with ϵ?



How good is the naïve method?

Runtime: very efficient.

Gate count: How do m, p, and q scale with ϵ?

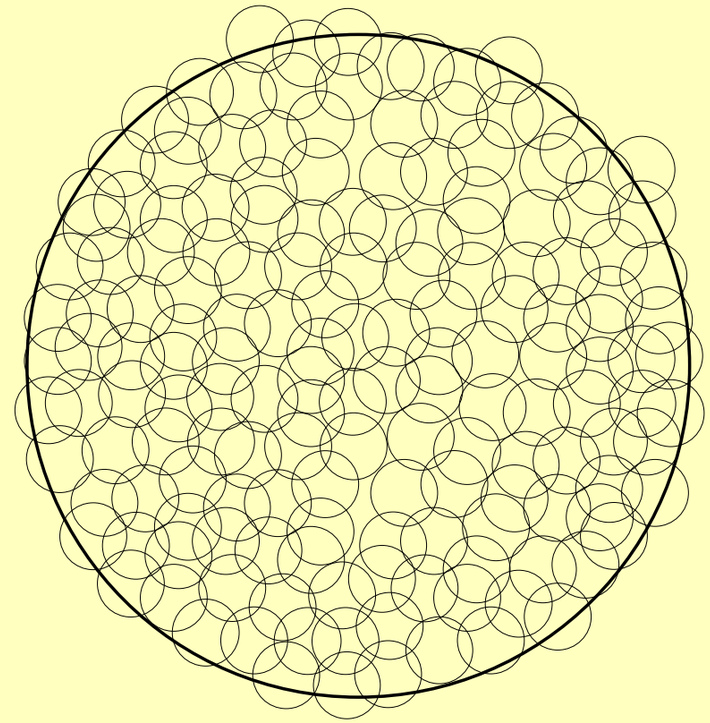


So the total number of gates is $n + m + q = O(1/\epsilon)$. How good is this?

Lower bounds

Another way to look at the approximation problem:

- $SO(3)$ is a 3-dimensional manifold.
- Therefore, the volume of an ϵ-ball is $O(\epsilon^3)$.
- Therefore, we need $O(1/\epsilon^3)$ ϵ-balls to cover $SO(3)$.
- Therefore, we need $O(1/\epsilon^3)$ distinct operators to approximate all unitaries up to ϵ.



Lower bounds, continued

- **Words of the form $A^*B^*A^*$.** There are $\leq n^3$ such words of length up to n. The information bound gives:

$$n^3 \geq \frac{C}{\epsilon^3} \quad \Rightarrow \quad n = \Omega(1/\epsilon).$$

  This is very redundant! Such words carry only $\log n$ bits of information.

Lower bounds, continued

- **Words of the form $A^*B^*A^*$.** There are $\leq n^3$ such words of length up to n. The information bound gives:

$$n^3 \geq \frac{C}{\epsilon^3} \quad \Rightarrow \quad n = \Omega(1/\epsilon).$$

  This is very redundant! Such words carry only $\log n$ bits of information.

- **Arbitrary words $(A|B)^*$.** There are $2^{n+1}-1$ words of length up to n. The information bound gives:

$$2^{n+1}-1 \geq \frac{C}{\epsilon^3} \quad \Rightarrow \quad n \geq 3\log_2(1/\epsilon) + K.$$

Lower bounds, continued

- **Words of the form $A^*B^*A^*$.** There are $\leq n^3$ such words of length up to n. The information bound gives:

$$n^3 \;\geq\; \frac{C}{\epsilon^3} \quad \Rightarrow \quad n \;=\; \Omega(1/\epsilon).$$

  This is very redundant! Such words carry only $\log n$ bits of information.

- **Arbitrary words $(A|B)^*$.** There are $2^{n+1}-1$ words of length up to n. The information bound gives:

$$2^{n+1}-1 \;\geq\; \frac{C}{\epsilon^3} \quad \Rightarrow \quad n \;\geq\; 3\log_2(1/\epsilon) + K.$$

- **Matsumoto-Amano normal forms.** Up to a phase, there are $24\cdot(3\cdot 2^n - 2)$ Clifford+T operators of T-count $\leq n$. The information bound gives:

$$24\cdot(3\cdot 2^n - 2) \;\geq\; \frac{C}{\epsilon^3} \quad \Rightarrow \quad n \;\geq\; 3\log_2(1/\epsilon) + K.$$

The Solovay-Kitaev algorithm in a nutshell

Basic observation:

If $\|A - A'\|, \|B - B'\| = O(\epsilon)$, then $\|ABA^{-1}B^{-1} - A'B'A'^{-1}B'^{-1}\| = O(\epsilon^{1.5})$.

Rough strategy for approximating U up to $\epsilon^{1.5}$:

- Find C approximating U up to ϵ.
- Write UC^{-1} in the form $A'B'A'^{-1}B'^{-1}$.
- Find A, B approximating A', B' up to ϵ.
- Then $ABA^{-1}B^{-1}C$ approximates U up to $\epsilon^{1.5}$.

This gives a *recursive* procedure for approximating U up to ϵ, $\epsilon^{1.5}$, $\epsilon^{1.5^2}$, $\epsilon^{1.5^3}$, ...

Gate complexity of Solovay-Kitaev

While $ABA^{-1}B^{-1}C$ is less redundant than $A^*B^*A^*$, it is still redundant.

Each recursive step multiplies the accuracy (in digits) by 1.5, and multiplies the gate count by 5.

Thus, the gate count is d^c, where $d = \log(1/\epsilon)$ is the accuracy (in digits), and $c = \log 5 / \log 1.5 \approx 3.96$.

$$\text{Gate count} = O(\log^{3.96}(1/\epsilon)).$$

Compare with the information-theoretic lower bound:

$$\text{Gate count} = O(\log(1/\epsilon)).$$

Gate complexity, in numbers.

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

Part V: Grid problems

Neil J. Ross and Peter Selinger

The ring $\mathbb{Z}[\sqrt{2}]$

Consider the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

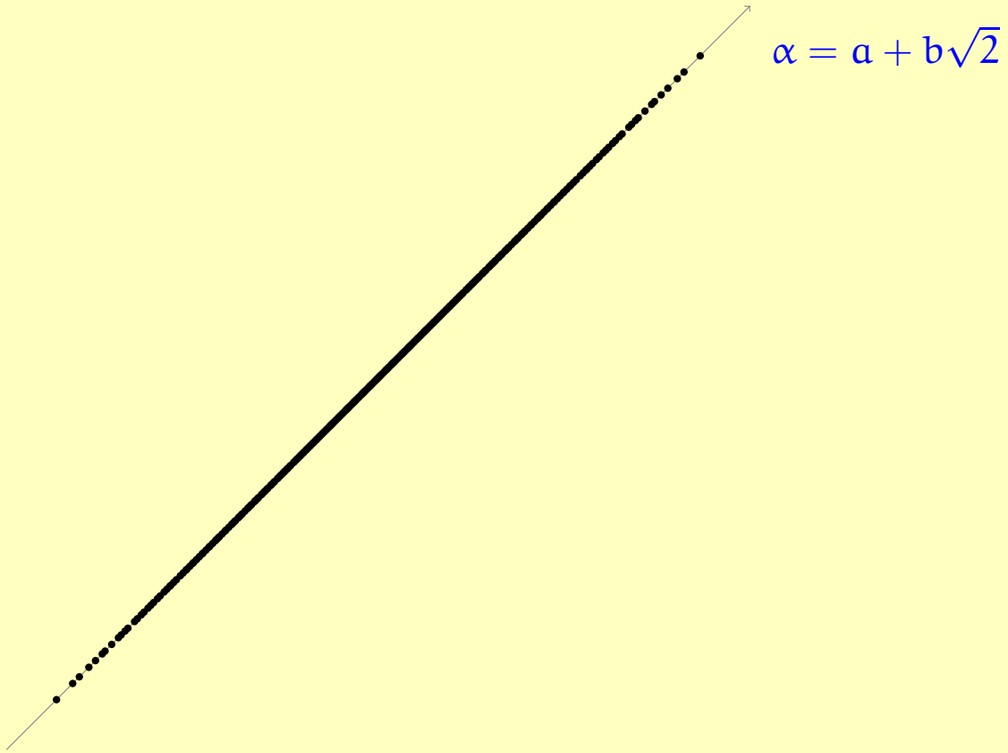
It has an automorphism (*"conjugation"*): $(a + b\sqrt{2})^\bullet = a - b\sqrt{2}$. Automorphism properties:

$$\begin{aligned} (\alpha + \beta)^\bullet &= \alpha^\bullet + \beta^\bullet \\ (\alpha - \beta)^\bullet &= \alpha^\bullet - \beta^\bullet \\ (\alpha\beta)^\bullet &= \alpha^\bullet\beta^\bullet \end{aligned}$$

Note that $\alpha^\bullet\alpha = a^2 - 2b^2$ is an integer, called the *norm* of α.

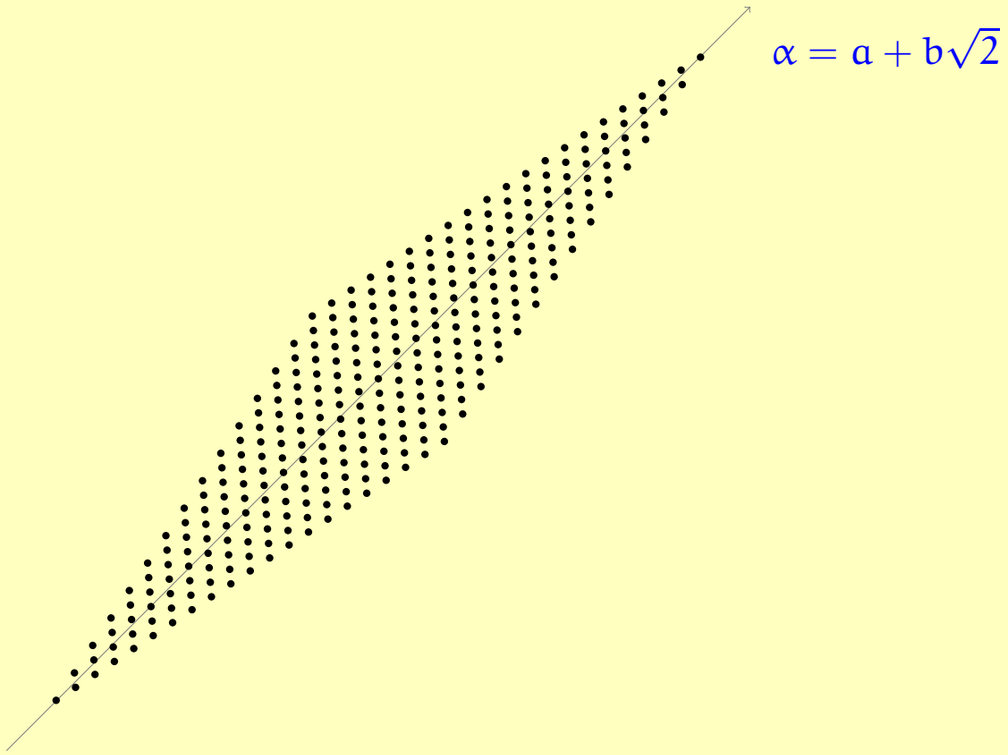
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



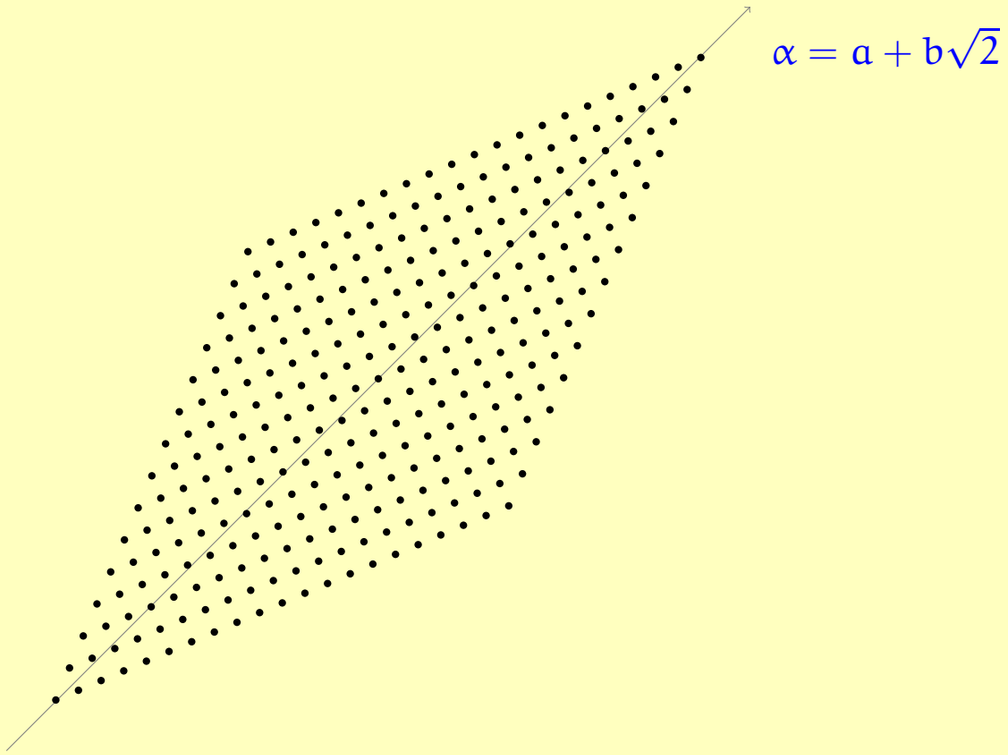
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



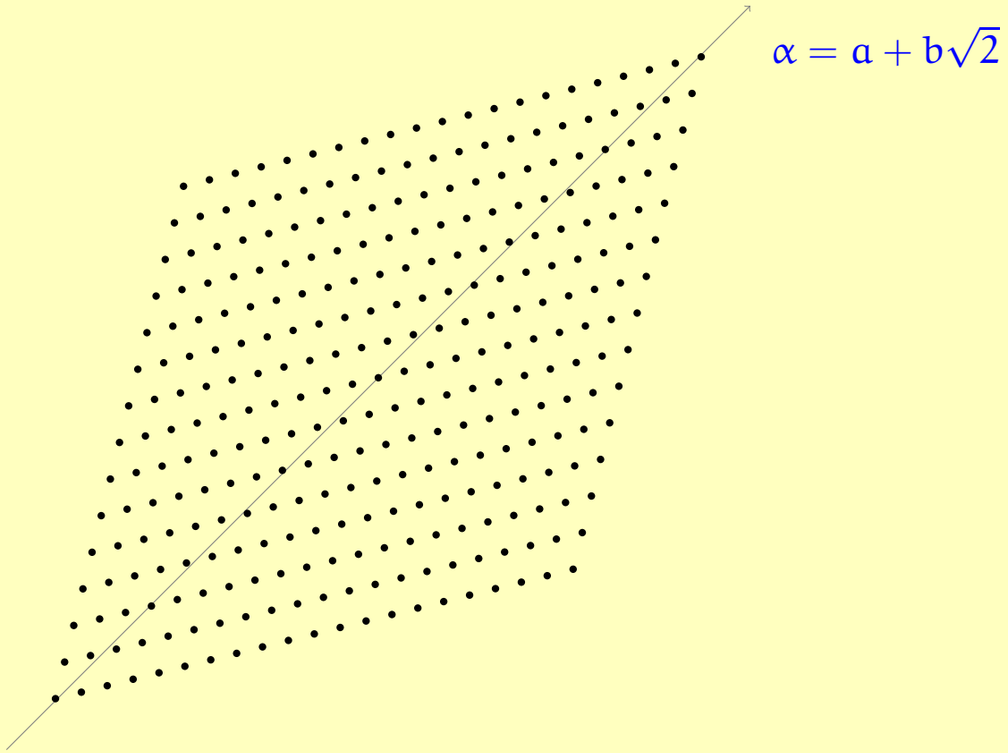
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



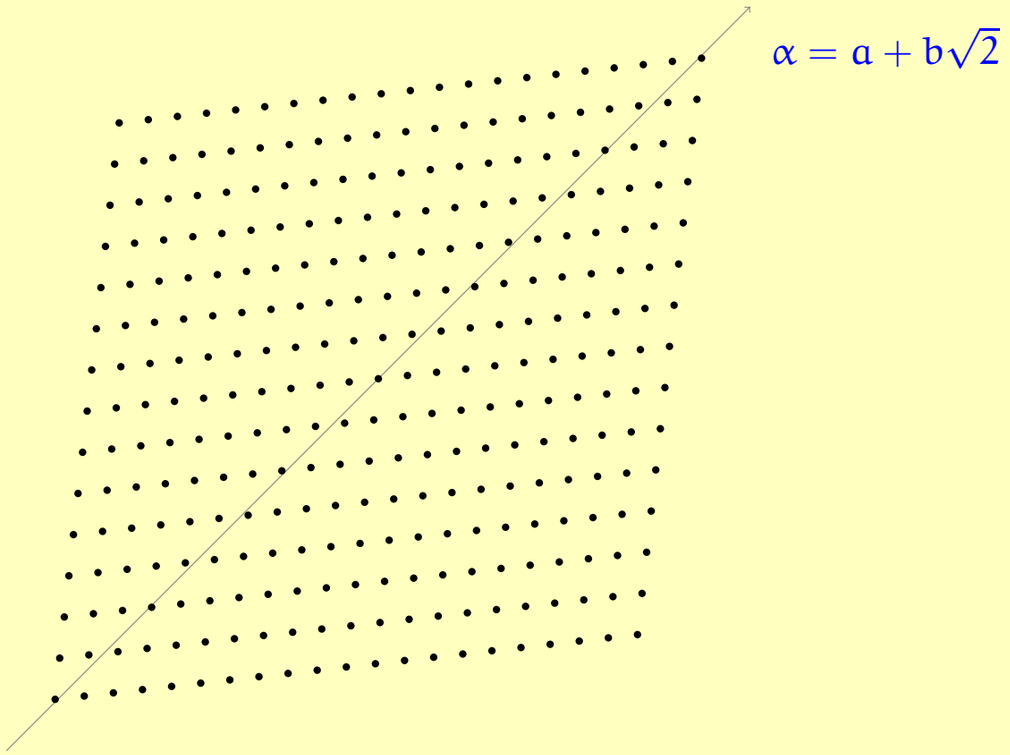
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



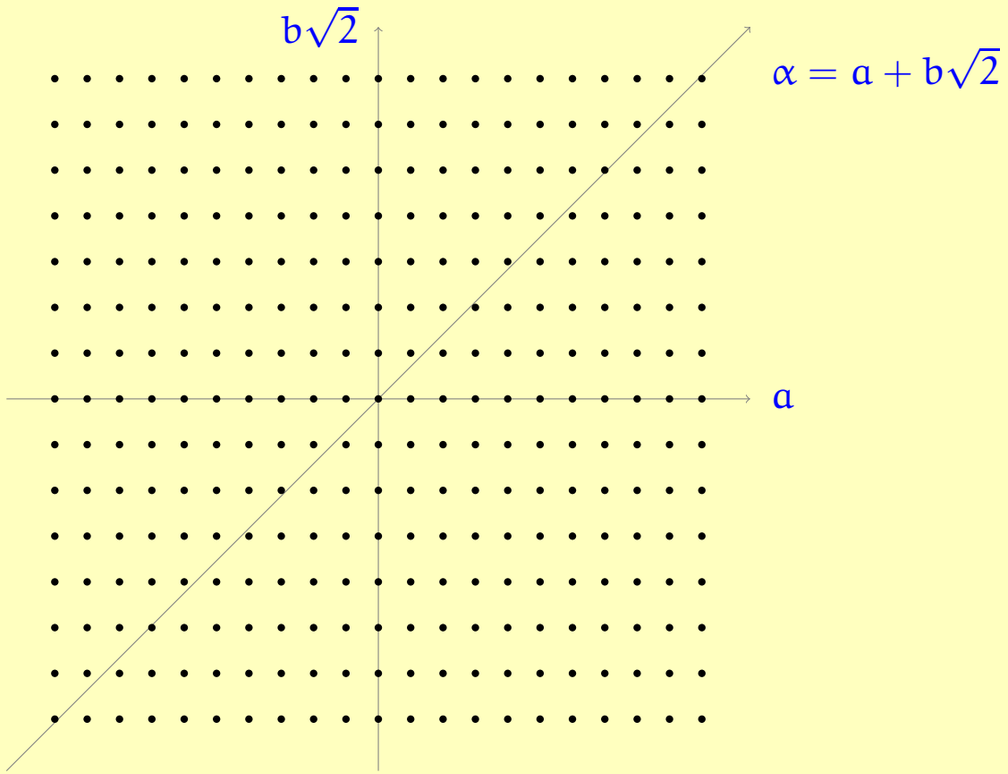
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



Dense or discrete?

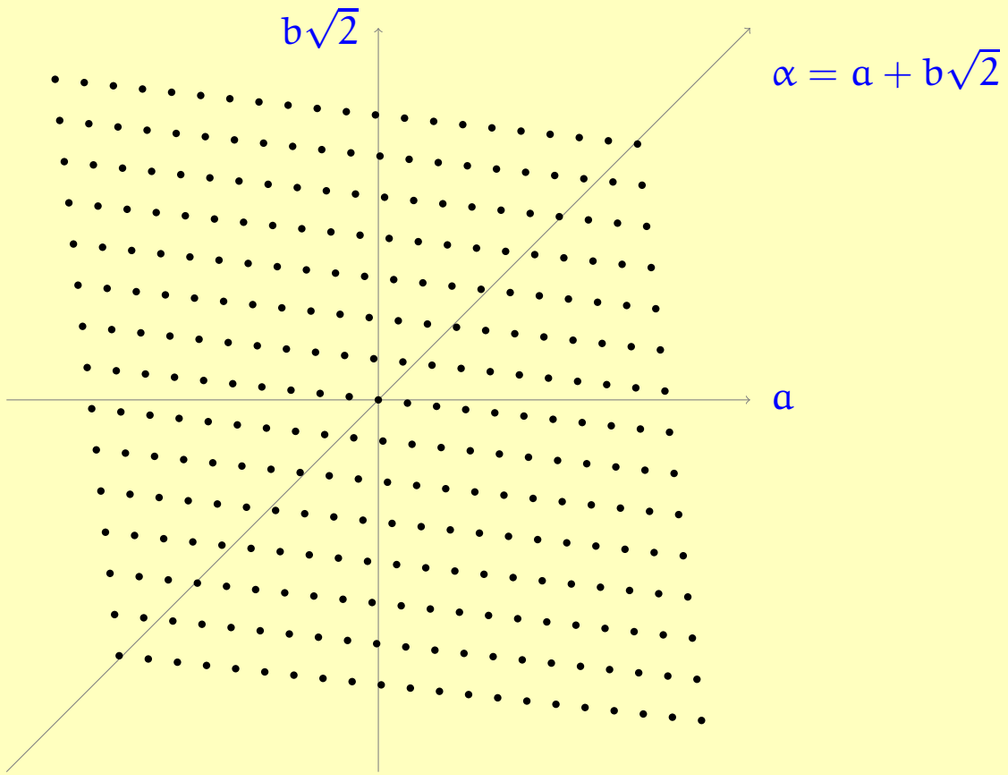
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

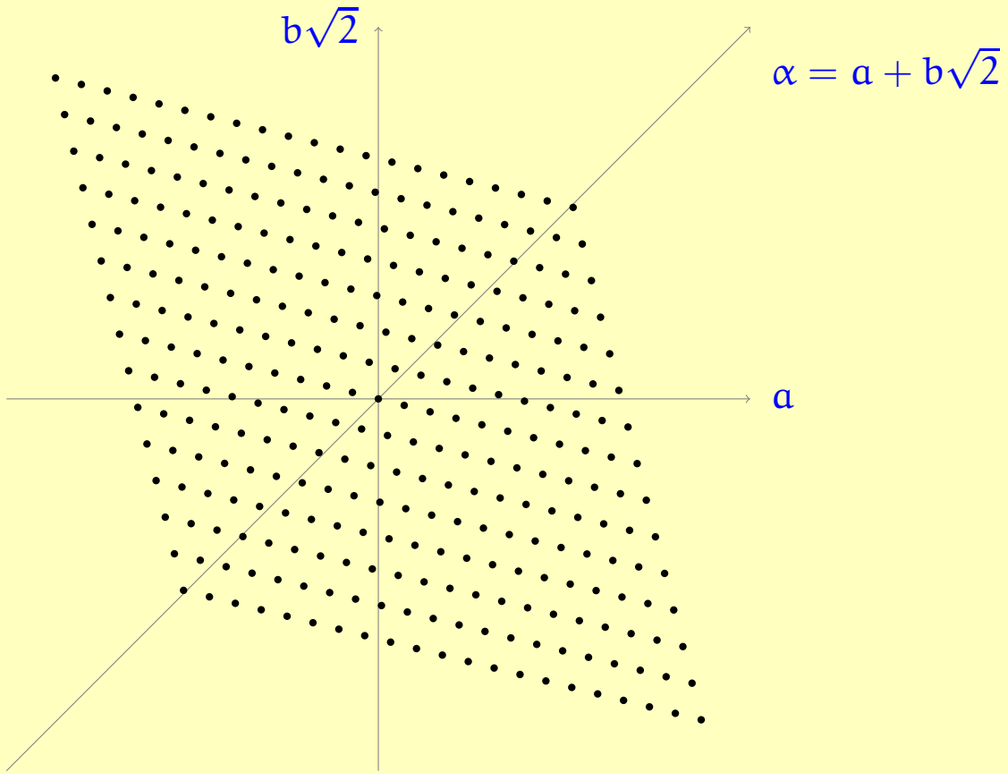
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

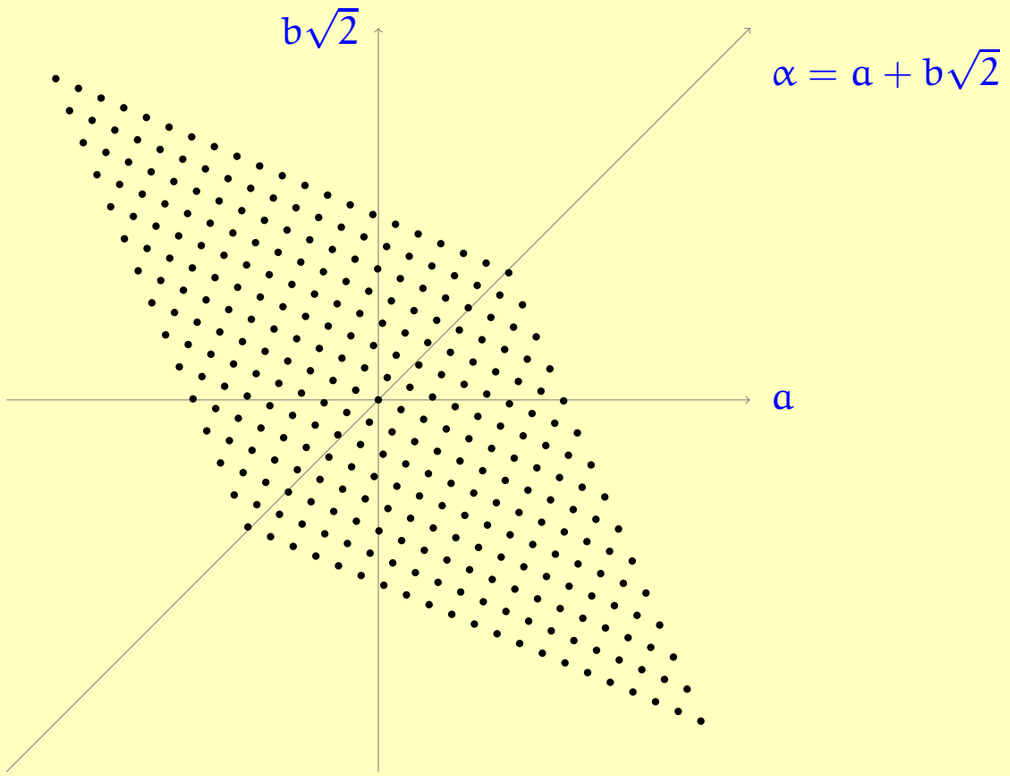
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

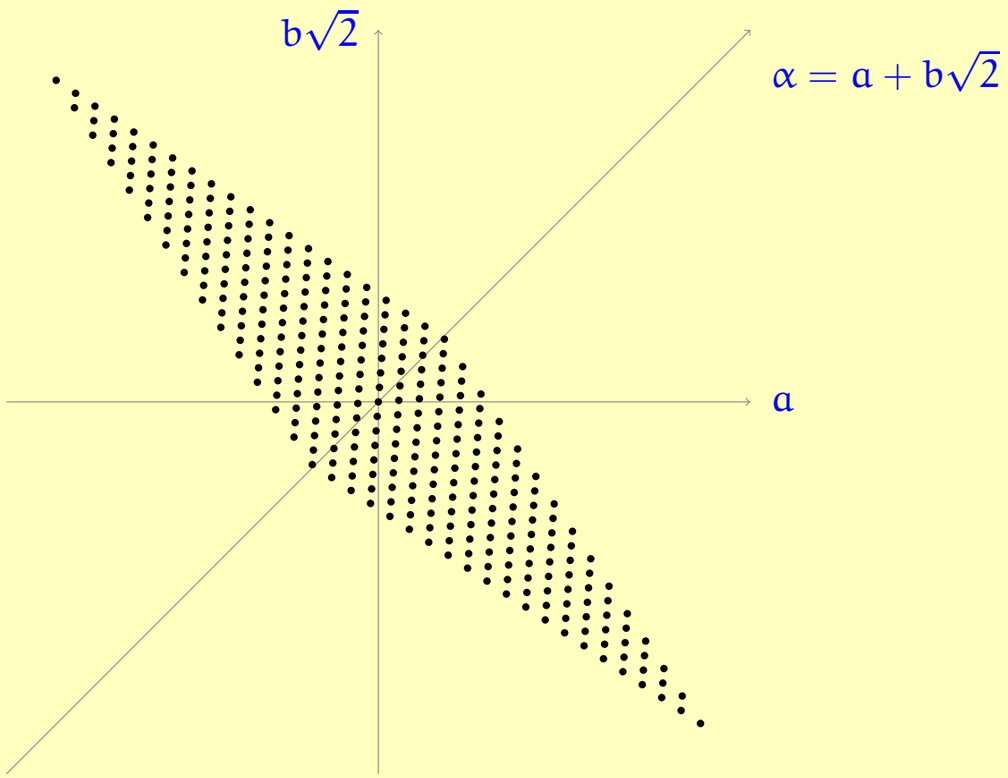
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

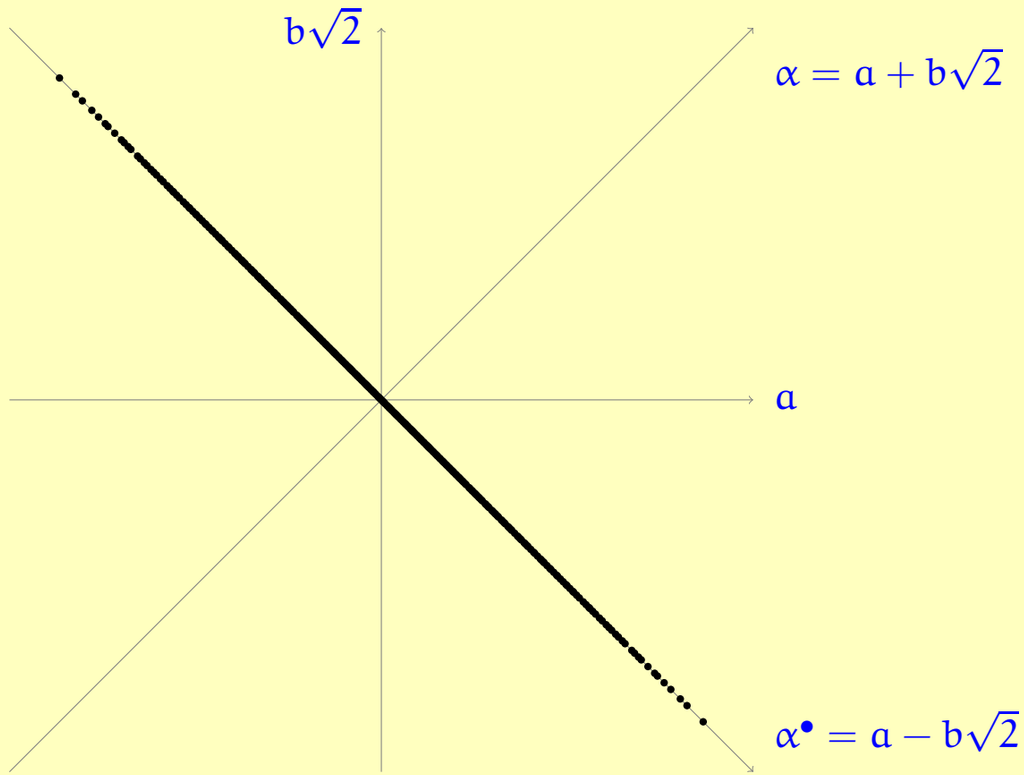
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

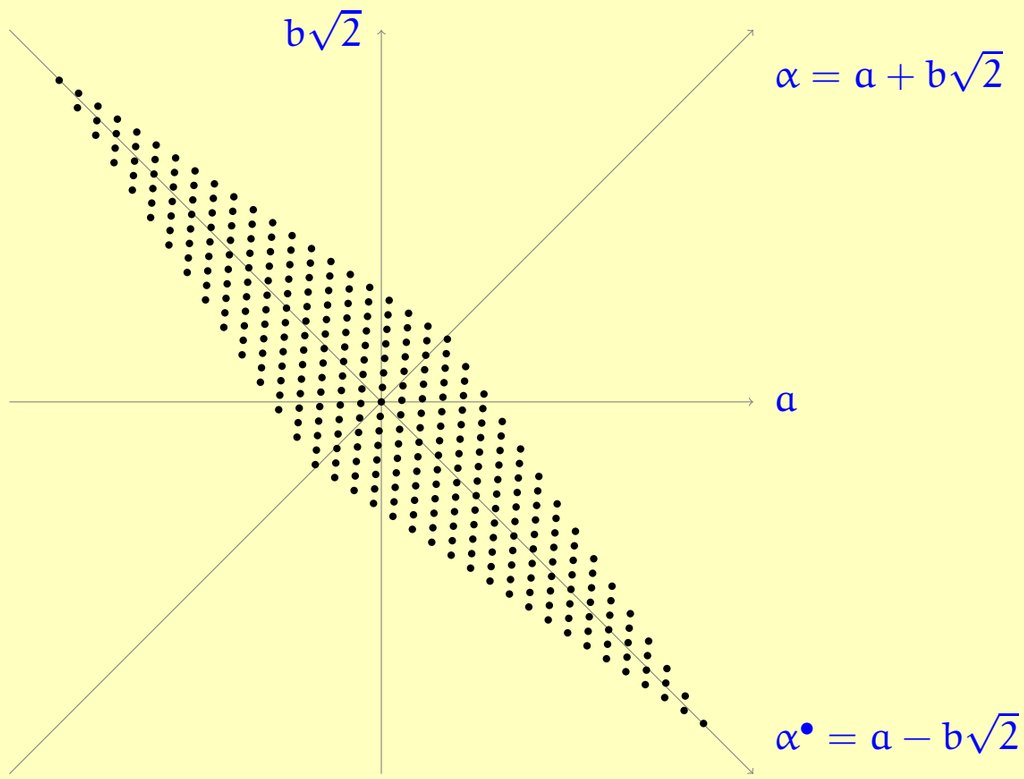
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

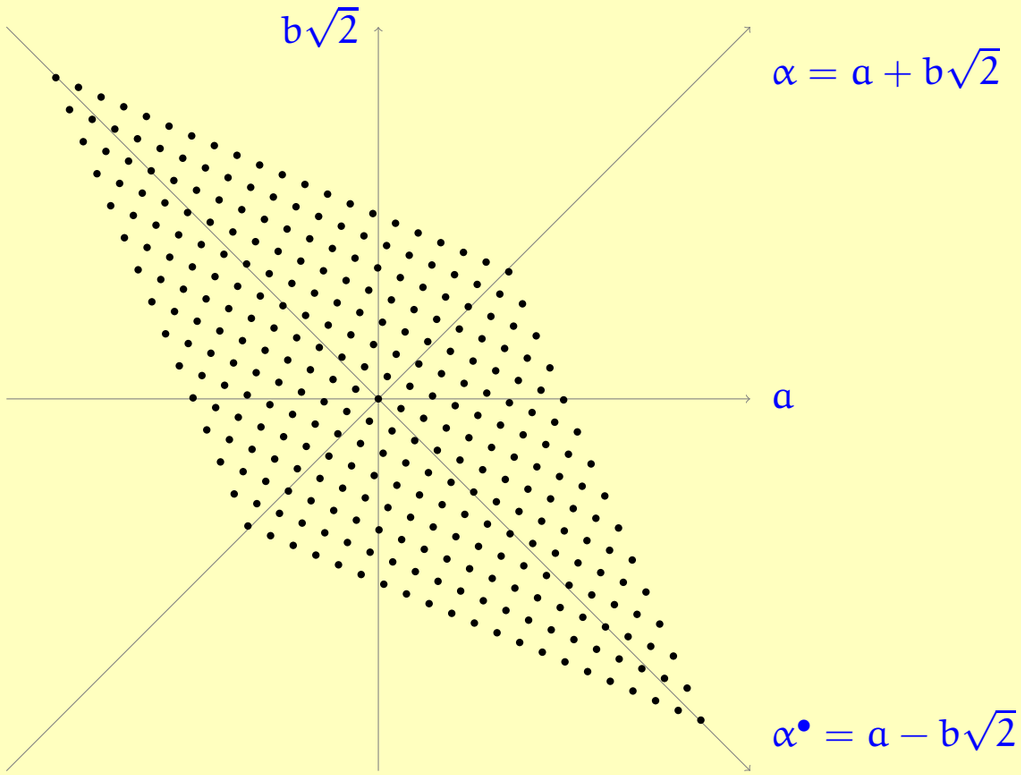
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

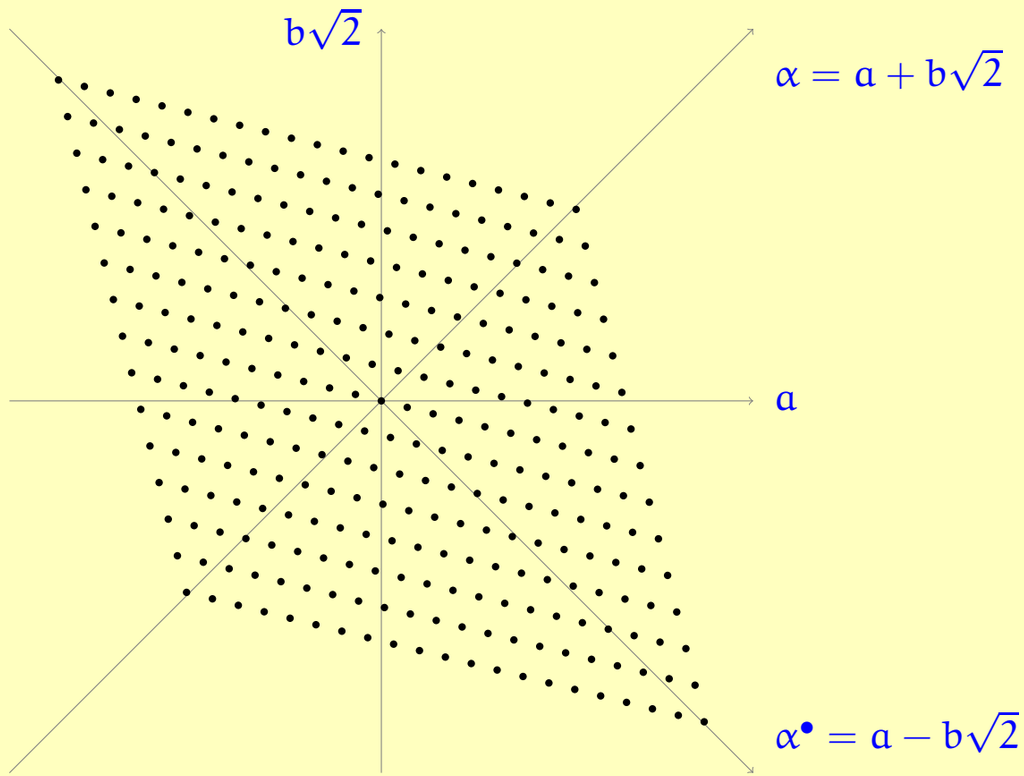
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

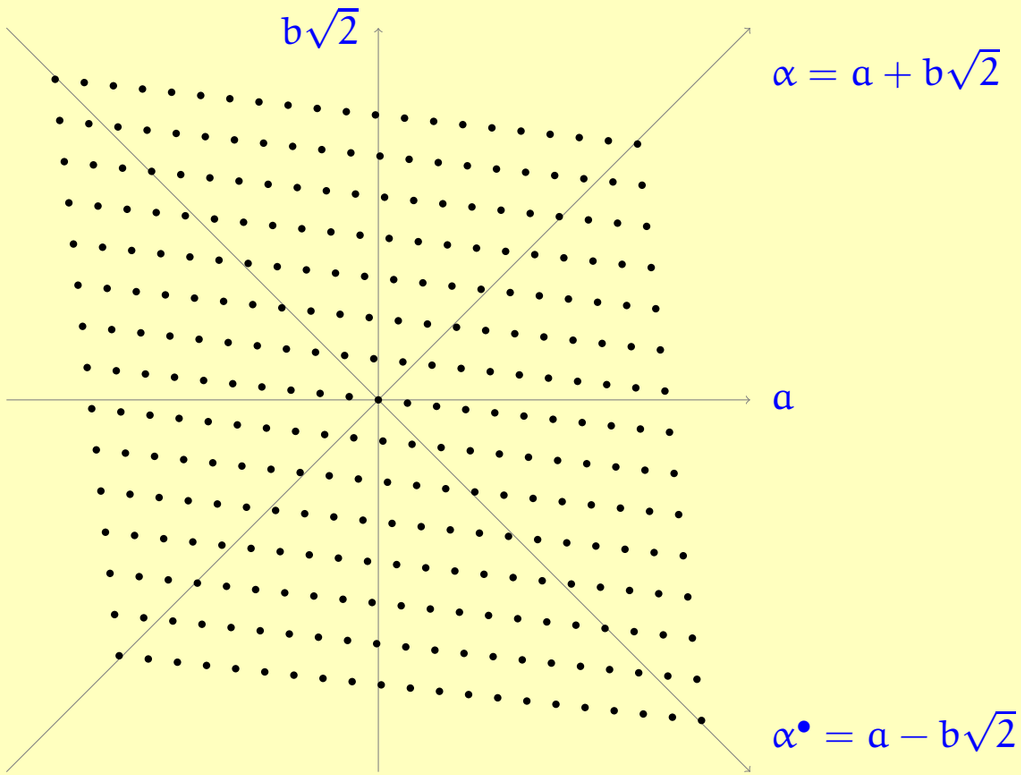
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

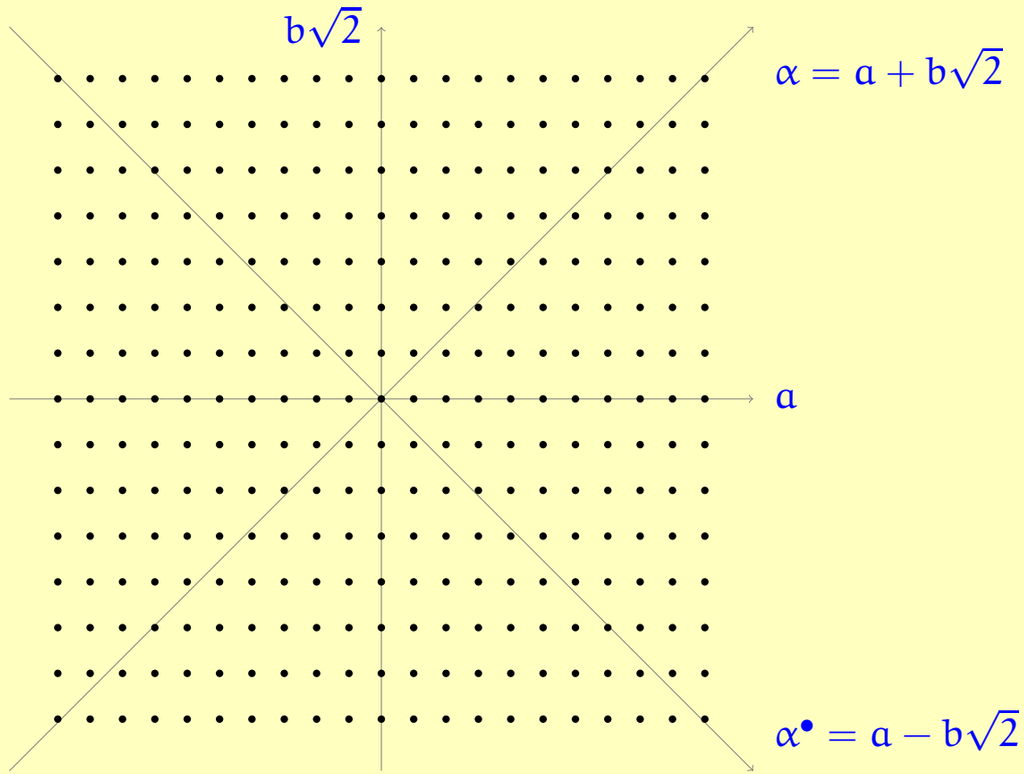
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.

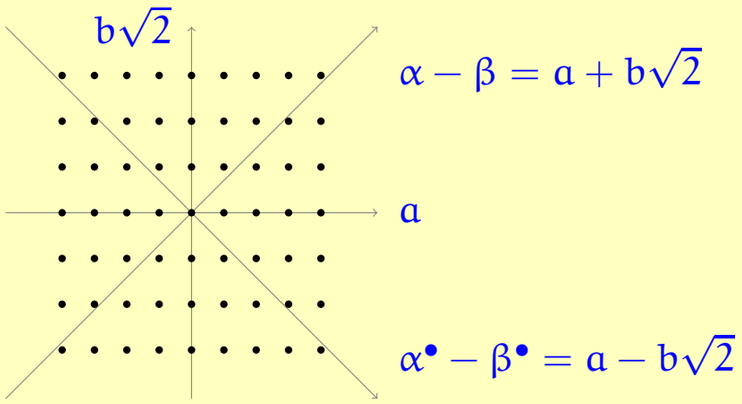


But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

The automorphism "$\bullet$"

The function $\alpha \mapsto \alpha^\bullet$ is *extremely non-continuous*. In fact, it can never happen that $|\alpha - \beta|$ and $|\alpha^\bullet - \beta^\bullet|$ are small at the same time (unless $\alpha = \beta$).

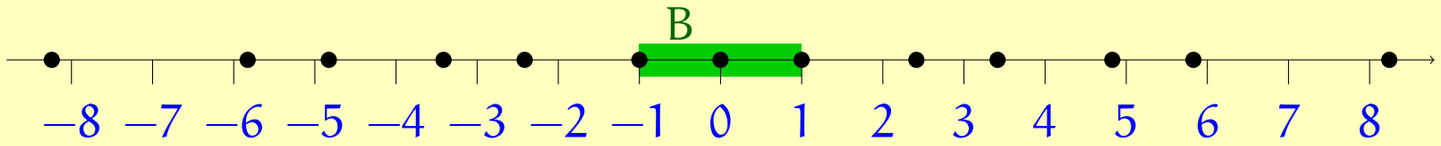
Proof: let $\alpha - \beta = a + b\sqrt{2}$. Then $|\alpha - \beta| \cdot |\alpha^\bullet - \beta^\bullet| = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$, which is an integer.



1-dimensional grid problems

Definition. Let B be a set of real numbers. The *grid* for B is the set

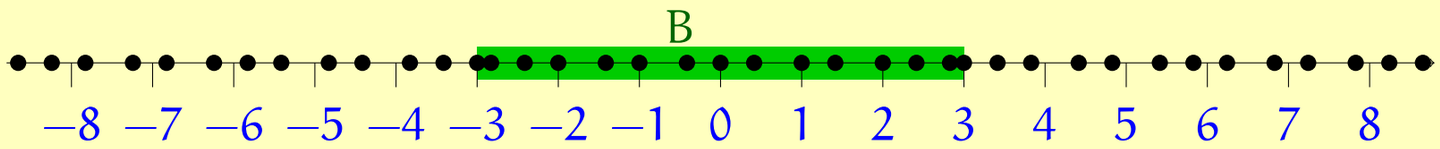
$$\mathsf{grid}(B) = \{\alpha \in \mathbb{Z}[\sqrt{2}] \mid \alpha^\bullet \in B\}.$$



1-dimensional grid problems

Definition. Let B be a set of real numbers. The *grid* for B is the set

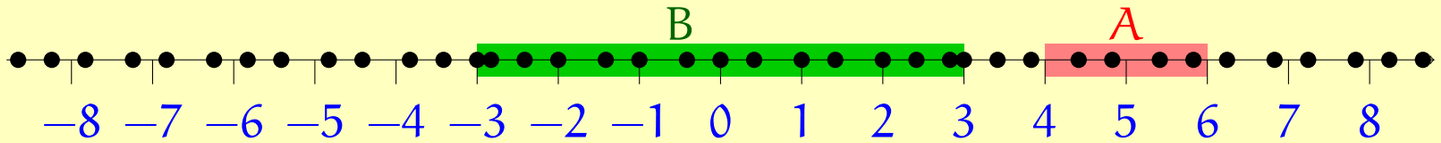
$$\mathrm{grid}(B) = \{\alpha \in \mathbb{Z}[\sqrt{2}] \mid \alpha^\bullet \in B\}.$$



1-dimensional grid problems

Definition. Let B be a set of real numbers. The *grid* for B is the set

$$\mathsf{grid}(\mathrm{B}) = \{\alpha \in \mathbb{Z}[\sqrt{2}] \mid \alpha^\bullet \in \mathrm{B}\}.$$



Given finite intervals A and B of the real numbers, the *1-dimensional grid problem* is to find $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that

$$\alpha \in \mathrm{A} \quad \text{and} \quad \alpha^\bullet \in \mathrm{B}.$$

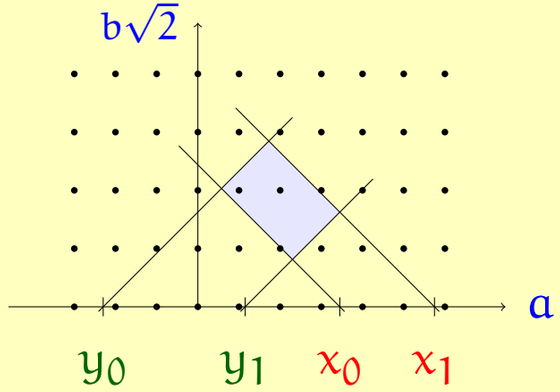
1-dimensional grid problems

Given finite intervals A and B of the real numbers, the *1-dimensional grid problem* is to find $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that

$$\alpha \in A \quad \text{and} \quad \alpha^\bullet \in B.$$

Equivalently, find $a, b \in \mathbb{Z}$ such that:

$$a + b\sqrt{2} \in A \quad \text{and} \quad a - b\sqrt{2} \in B.$$

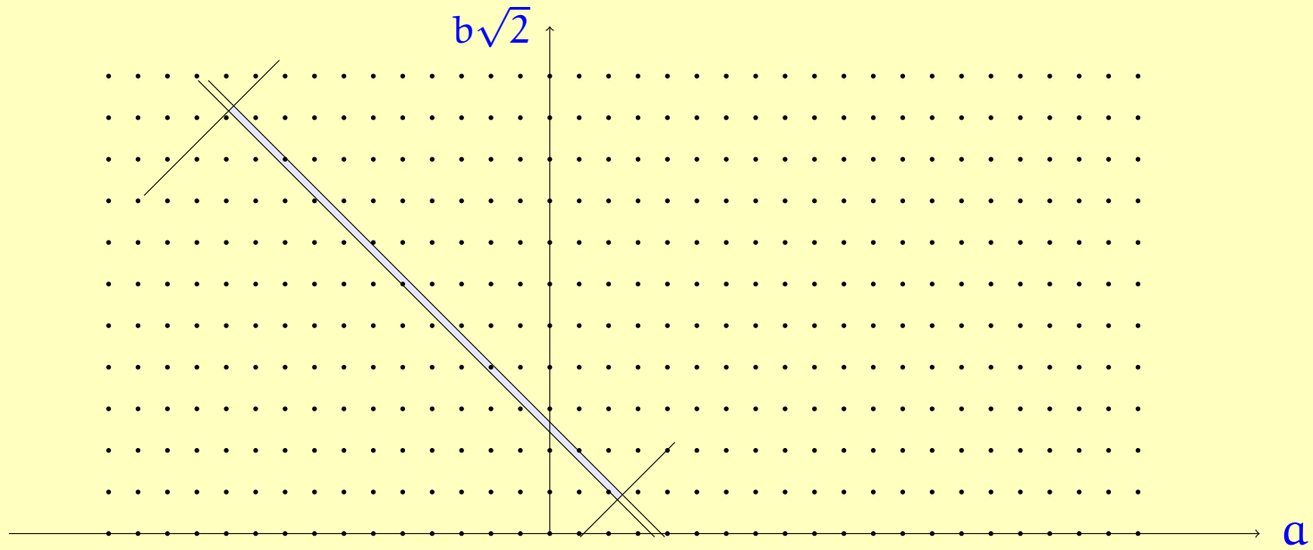


$A = [x0, x1], \quad B = [y0, y1]$

It is clear that there will be solutions when $|A|$ and $|B|$ are large. The number of solutions is $O(|A| \cdot |B|)$ in that case.

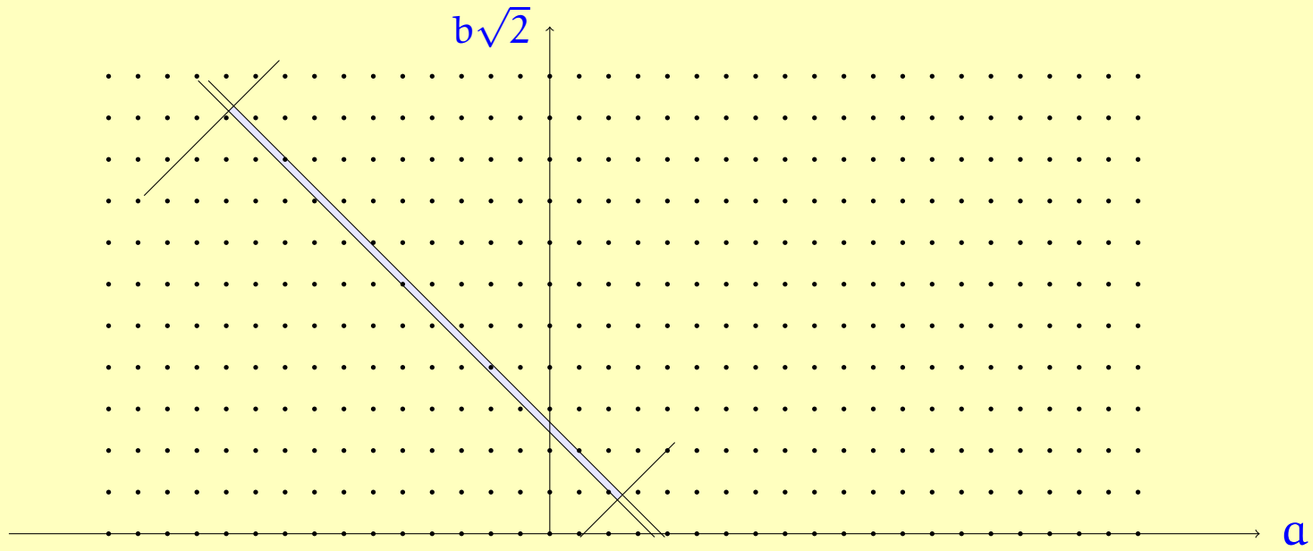
The problematic case: long and skinny

Suppose $|\mathcal{A}|$ is tiny and $|\mathcal{B}|$ is large, so that we end up with a long and skinny rectangle:



The problematic case: long and skinny

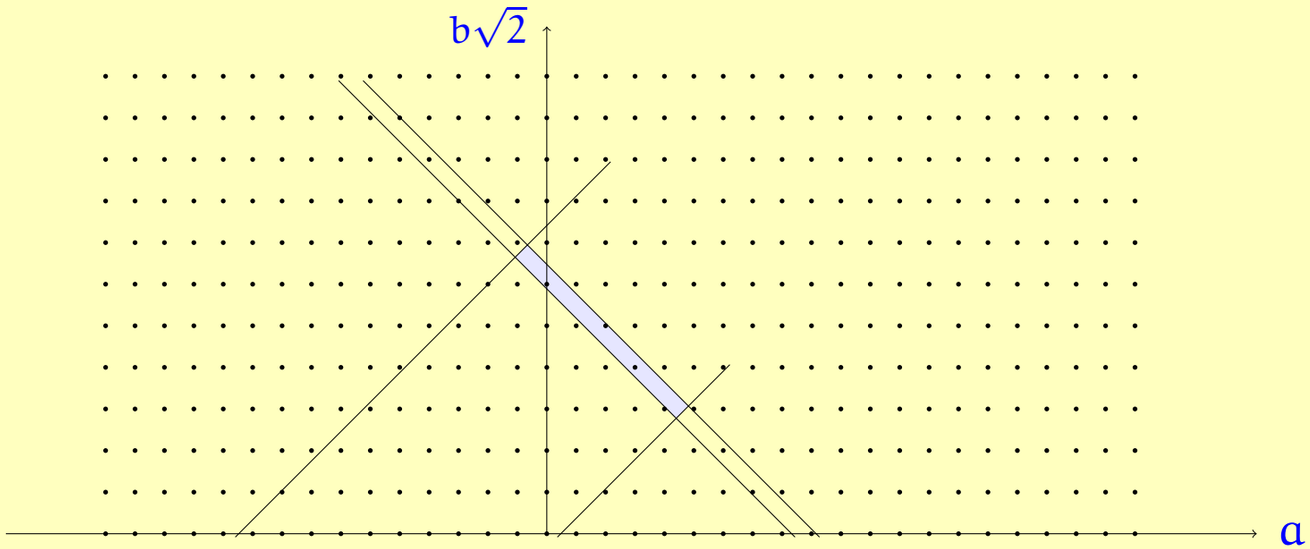
Suppose $|\mathcal{A}|$ is tiny and $|\mathcal{B}|$ is large, so that we end up with a long and skinny rectangle:



Solution: *scaling*. $\lambda = 1+\sqrt{2}$ is a unit of the ring $\mathbb{Z}[\sqrt{2}]$, with $\lambda^{-1} = \sqrt{2}-1$. So multiplication by λ maps the grid to itself. So we can equivalently consider the problem for $\lambda^n\mathcal{A}$ and $\lambda^{\bullet n}\mathcal{B}$, which takes us back to the "fat" case.

The problematic case: long and skinny

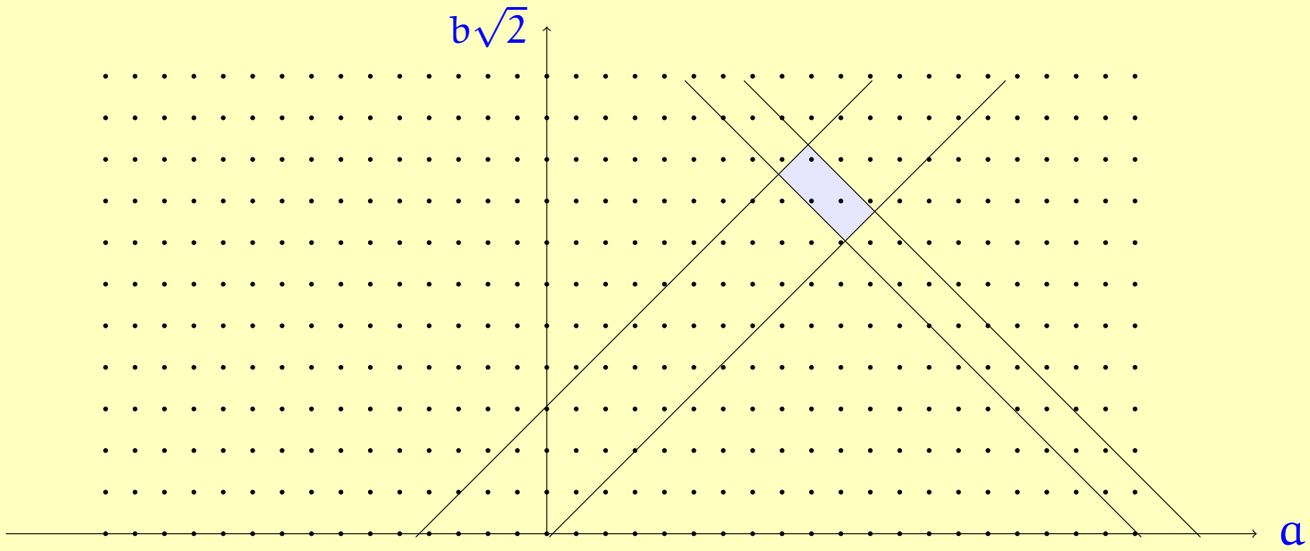
Suppose $|\mathcal{A}|$ is tiny and $|\mathcal{B}|$ is large, so that we end up with a long and skinny rectangle:



Solution: *scaling*. $\lambda = 1 + \sqrt{2}$ is a unit of the ring $\mathbb{Z}[\sqrt{2}]$, with $\lambda^{-1} = \sqrt{2} - 1$. So multiplication by λ maps the grid to itself. So we can equivalently consider the problem for $\lambda^n \mathcal{A}$ and $\lambda^{\bullet^n} \mathcal{B}$, which takes us back to the "fat" case.

The problematic case: long and skinny

Suppose $|\mathcal{A}|$ is tiny and $|\mathcal{B}|$ is large, so that we end up with a long and skinny rectangle:



Solution: *scaling*. $\lambda = 1 + \sqrt{2}$ is a unit of the ring $\mathbb{Z}[\sqrt{2}]$, with $\lambda^{-1} = \sqrt{2} - 1$. So multiplication by λ maps the grid to itself. So we can equivalently consider the problem for $\lambda^{n}\mathcal{A}$ and $\lambda^{\bullet n}\mathcal{B}$, which takes us back to the "fat" case.

Solution of 1-dimensional grid problems

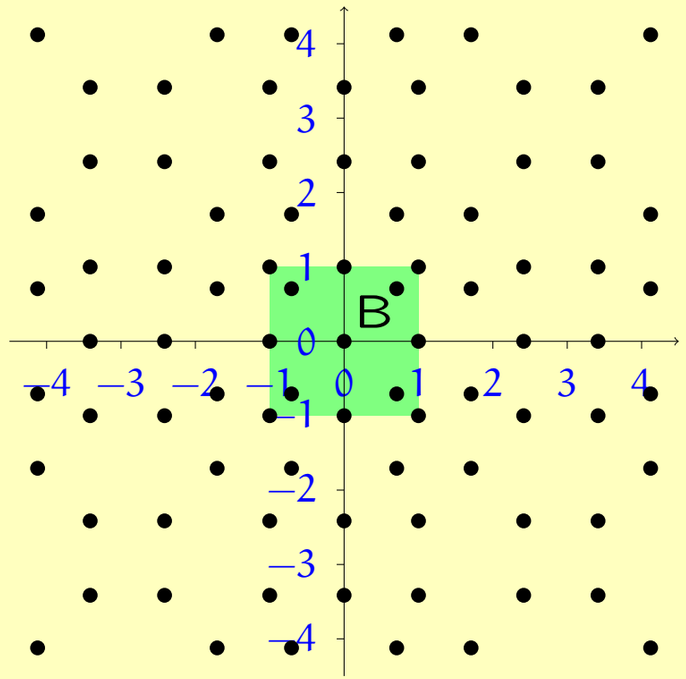
Theorem. Let A and B be finite real intervals. There exists an efficient algorithm that enumerates all solutions of the grid problem for A and B.

2-dimensional grid problems

Consider the ring $\mathbb{Z}[\omega]$, where $\omega = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}$. $\mathbb{Z}[\omega]$ is a subset of the complex numbers, which we can identify with the Euclidean plane $\mathbb{R}^2$.

Definition. Let B be a bounded convex subset of the plane. Just as in the 1-dimensional case, the *grid* for B is the set

$$\mathsf{grid}(B) = \{\alpha \in \mathbb{Z}[\omega] \mid \alpha^\bullet \in B\}.$$

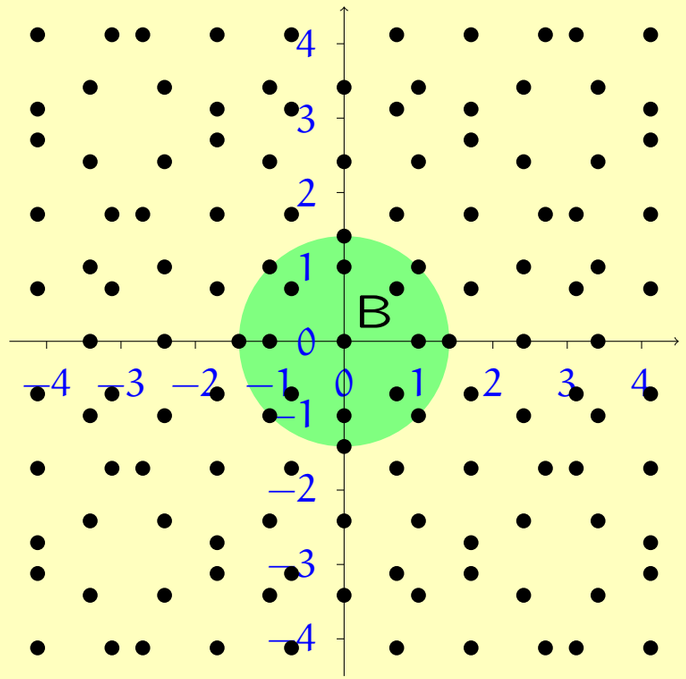


2-dimensional grid problems

Consider the ring $\mathbb{Z}[\omega]$, where $\omega = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}$. $\mathbb{Z}[\omega]$ is a subset of the complex numbers, which we can identify with the Euclidean plane $\mathbb{R}^2$.

Definition. Let B be a bounded convex subset of the plane. Just as in the 1-dimensional case, the *grid* for B is the set

$$\mathsf{grid}(B) = \{\alpha \in \mathbb{Z}[\omega] \mid \alpha^\bullet \in B\}.$$

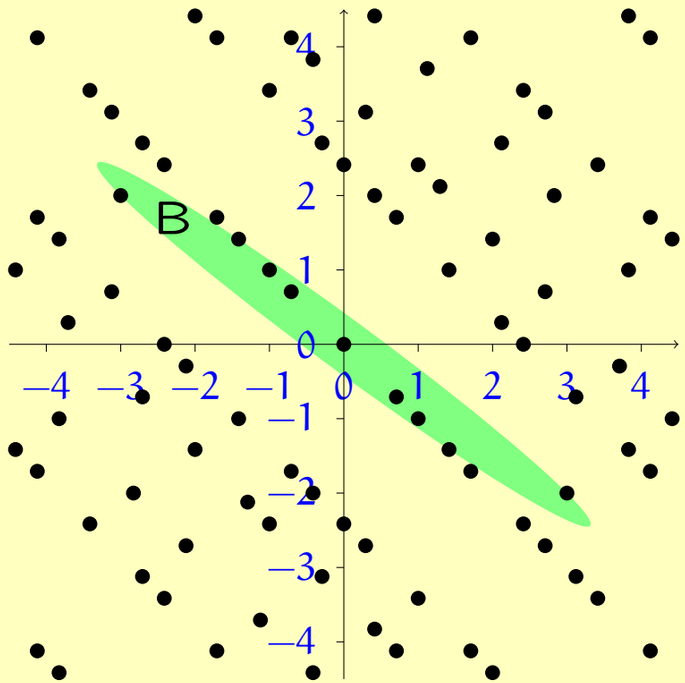


2-dimensional grid problems

Consider the ring $\mathbb{Z}[\omega]$, where $\omega = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}$. $\mathbb{Z}[\omega]$ is a subset of the complex numbers, which we can identify with the Euclidean plane $\mathbb{R}^2$.

Definition. Let B be a bounded convex subset of the plane. Just as in the 1-dimensional case, the *grid* for B is the set

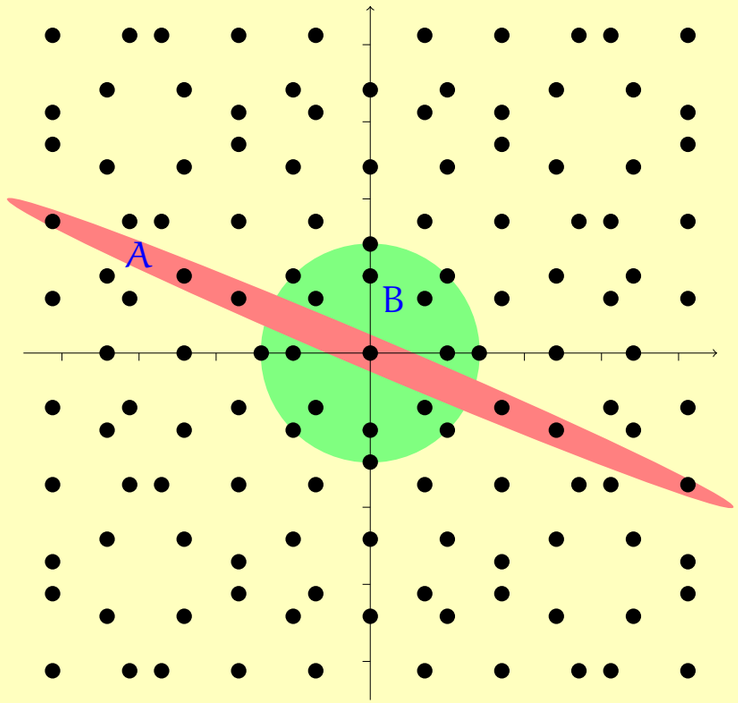
$$\mathsf{grid}(B) = \{\alpha \in \mathbb{Z}[\omega] \mid \alpha^\bullet \in B\}.$$



2-dimensional grid problems

Given bounded convex subsets $\mathcal{A}$ and $\mathcal{B}$ of the plane, the *2-dimensional grid problem* is to find $u \in \mathbb{Z}[\omega]$ such that

$$u \in \mathcal{A} \quad \text{and} \quad u^\bullet \in \mathcal{B}.$$

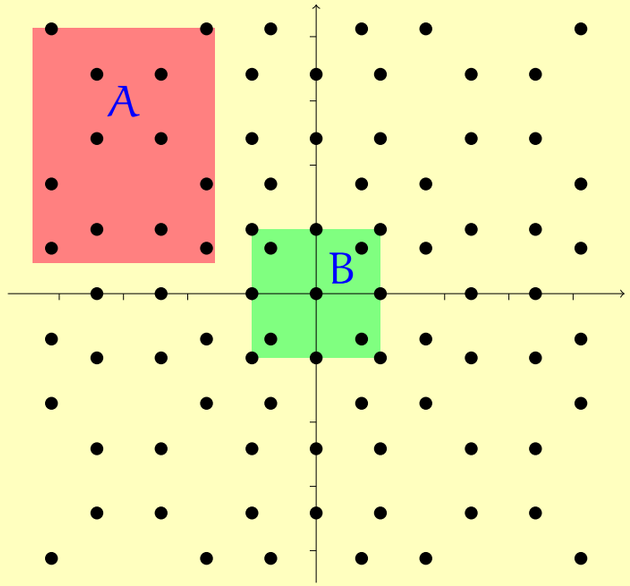


The easiest case: upright rectangles

If $A = A_x \times A_y$ and $B = B_x \times B_y$, the problem reduces to two 1-dimensional problems:

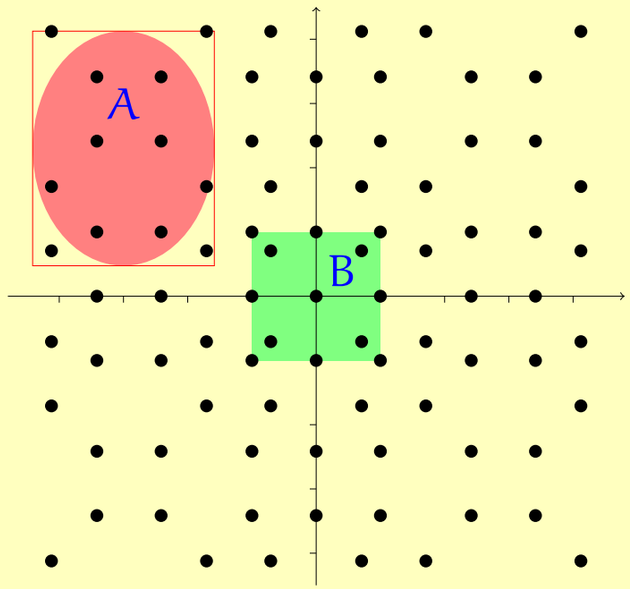
$$\alpha \in A_x, \quad \alpha^\bullet \in B_x \quad \text{and} \quad \beta \in A_y, \quad \beta^\bullet \in B_y,$$

where $u = \alpha + i\beta \in \mathbb{Z}[\omega]$. (This means $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ or $\alpha, \beta \in \mathbb{Z}[\sqrt{2}] + 1/\sqrt{2}$).



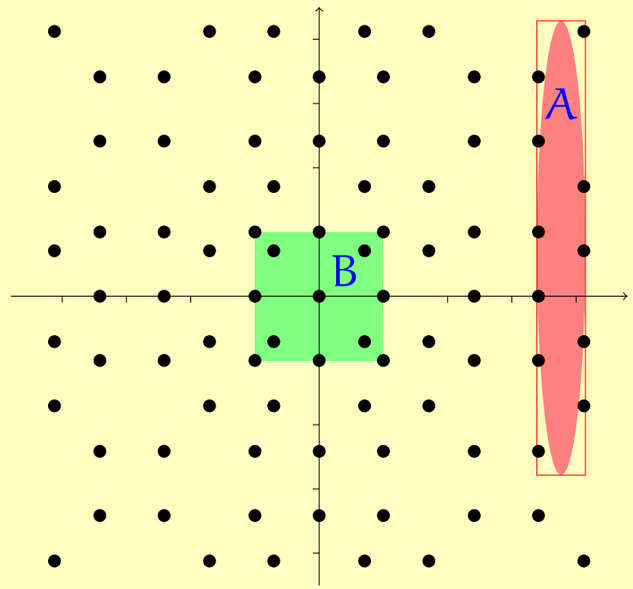
Also easy: upright sets

The *uprightness* of a set A is the ratio of its area to the area of its bounding box. If A and B are upright, the grid problem reduces to that of rectangles.



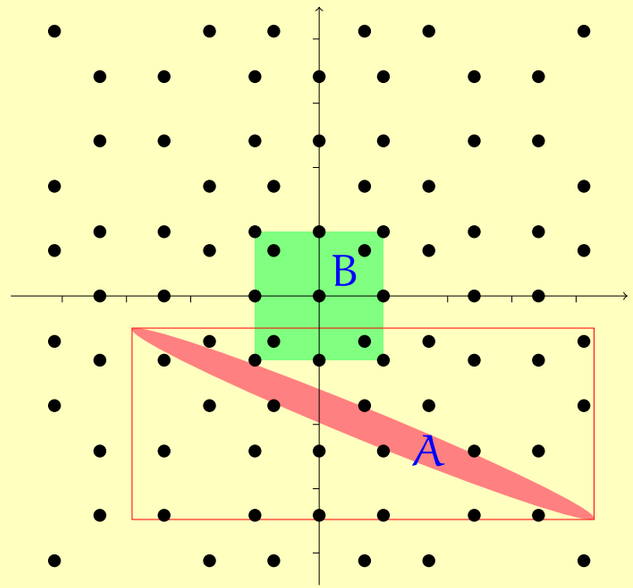
Also easy: upright sets

The *uprightness* of a set A is the ratio of its area to the area of its bounding box. If A and B are upright, the grid problem reduces to that of rectangles.



The hardest case: long and skinny, not upright

Convex sets that are not upright are long and skinny. In this case, finding grid points is a priori a hard problem.



Our solution: grid operators

A linear operator $G : \mathbb{R}^2 \to \mathbb{R}^2$ is called a *grid operator* if $G(Z[\omega]) = Z[\omega]$.

Some useful grid operators:

$$\mathbf{R} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \quad \mathbf{A} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{bmatrix}$$

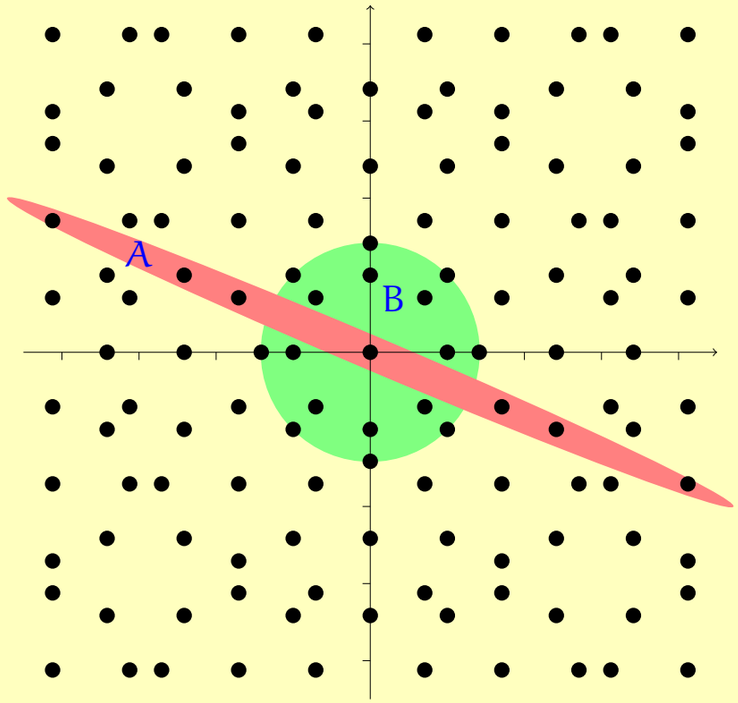
$$\mathbf{K} = \frac{1}{\sqrt{2}} \begin{bmatrix} -\lambda^{-1} & -1 \\ \lambda & 1 \end{bmatrix} \quad \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Proposition. Let G be a grid operator. Then the grid problem for A and B is equivalent to the grid problem for $G(A)$ and $G^\bullet(B)$.

Proof: obvious, because $\alpha \in A$ iff $G(\alpha) \in G(A)$, and $\alpha^\bullet \in B$ iff $G(\alpha)^\bullet \in G^\bullet(B)$.

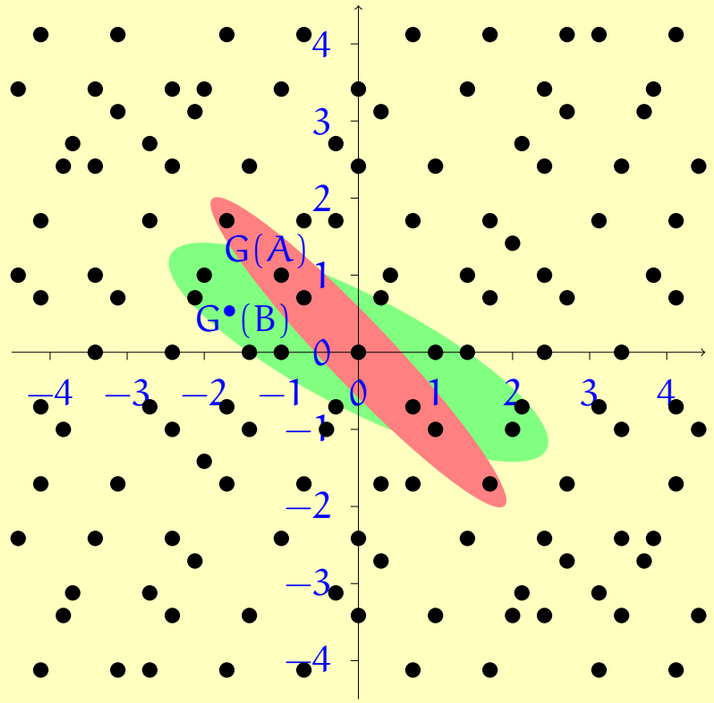
Effect of a grid operator

$$\mathbf{B} = \begin{bmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{bmatrix} \quad \mathbf{B}^{\bullet} = \begin{bmatrix} 1 & -\sqrt{2} \\ 0 & 1 \end{bmatrix}$$



Effect of a grid operator

$$\mathbf{B} = \begin{bmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{bmatrix} \quad \mathbf{B}^{\bullet} = \begin{bmatrix} 1 & -\sqrt{2} \\ 0 & 1 \end{bmatrix}$$



Demo

Solution of 2-dimensional grid problems

Main Theorem. Let $\mathcal{A}$ and $\mathcal{B}$ be bounded convex sets with non-empty interior. Then there exists a grid operator G such that $G(\mathcal{A})$ and $G^\bullet(\mathcal{B})$ are $1/15$-upright.

Moreover, if $\mathcal{A}$ and $\mathcal{B}$ are M-upright, then G can be efficiently computed in $O(\log(1/M))$ steps.

Corollary (Solution of 2-dimensional grid problems). Let $\mathcal{A}$ and $\mathcal{B}$ be bounded convex sets with non-empty interior. There exists an efficient algorithm that enumerates all solutions of the grid problem for $\mathcal{A}$ and $\mathcal{B}$.

Part VI: An algorithm for optimal Clifford+T approximations

Recall: Exact synthesis for single-qubit Clifford+T operators

Definition. The *Clifford+T group* on one qubit is generated by the Hadamard gate H, the phase gate S, the scalar $\omega = e^{i\pi/4}$, and the T- or $\pi/8$-gate:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \omega = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}.$$

Theorem (Matsumoto and Amano). *Every Clifford+T operator* $U : \mathbb{C}^2 \to \mathbb{C}^2$ *can be uniquely written of the form*

$$U = (T \mid \epsilon)\,(HT \mid SHT)^*\,\mathcal{C}.$$

Theorem (Kliuchnikov, Maslov, Mosca). *A unitary operator* $U = \begin{pmatrix} u & v \\ t & s \end{pmatrix}$ *is a Clifford+T operator if and only if* $u, v, t, s \in \frac{1}{\sqrt{2}^k}\mathbb{Z}[\omega]$.

Moreover, if $\det U = 1$, then the T-count of the resulting operator is equal to $2k-2$.

The approximate synthesis problem

Problem. Given an operator $U \in SU(2)$ and $\epsilon > 0$, find a Clifford+T operator U' of small T-count, such that $\|U' - U\| \leq \epsilon$.

Naïve idea

Given

$$U = \begin{pmatrix} u & v \\ t & s \end{pmatrix},$$

first approximate u, v, t, s up to ϵ in $\mathbb{D}[\omega]$, then use exact synthesis to convert

$$U' = \begin{pmatrix} u' & v' \\ t' & s' \end{pmatrix}$$

to a circuit.

This does not work: U' is not unitary!

The approximate synthesis problem

Problem. Given an operator $U \in SU(2)$ and $\epsilon > 0$, find a Clifford+T operator U' of small T-count, such that $\|U' - U\| \leq \epsilon$.

Basic construction

We will approximate a z-rotation

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

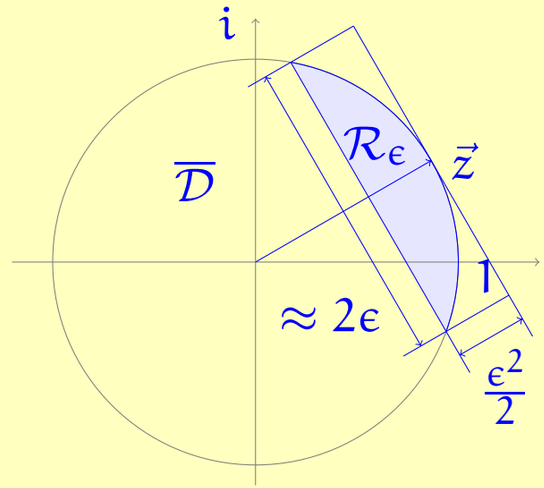
by a matrix of the form

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

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

Observation. The error is a function of u (and not of t). Indeed, setting $z = e^{-i\theta/2}$ and $u' = \frac{u}{\sqrt{2}^k}$, we have

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



The problem then reduces to:

(1) Finding $u \in \mathbb{Z}[\omega]$ such that $\frac{u}{\sqrt{2}^k} \in \mathcal{R}_\epsilon$, with small k;

(2) Solving the Diophantine equation $t^\dagger t + u^\dagger u = 2^k$.

Diophantine equations are computationally easy (if we can factor)

Consider a Diophantine equation of the form

$$\mathfrak{t}^\dagger \mathfrak{t} = \xi \tag{2}$$

where $\xi \in \mathbb{Z}[\sqrt{2}]$ is given and $\mathfrak{t} \in \mathbb{Z}[\omega]$ is unknown.

Necessary condition. The equation (2) has a solution only if $\xi \geq 0$ and $\xi^\bullet \geq 0$.

Theorem. There exists a probabilistic polynomial time algorithm which decides whether the equation (2) has a solution or not, and produces the solution if there is one, *provided that the algorithm is given the prime factorization of* $\mathfrak{n} = \xi^\bullet \xi$.

This is okay, because factoring random numbers is not as hard as worst-case numbers.

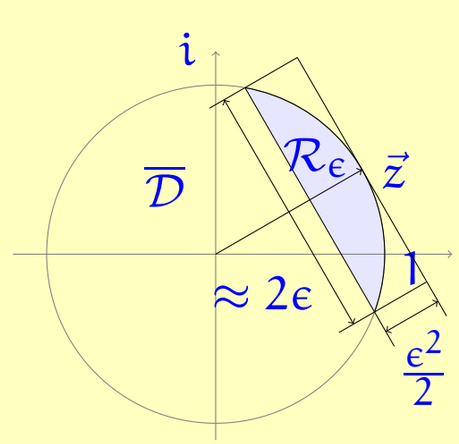
Proof. Exactly like Fermat's theorem on sums of two squares, except we replace the Euclidean domains $\mathbb{Z}$ and $\mathbb{Z}[\mathfrak{i}]$ by $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\omega]$.

The candidate selection problem

The only remaining problem is to find suitable u. Note that $\xi^\bullet = (2^k - u^\dagger u)^\bullet \geq 0$ iff $u^\bullet/\sqrt{2}^k$ is in the unit disk.

Candidate selection problem. Find $k \in \mathbb{N}$ and $u \in \mathbb{Z}[\omega]$ such that

1. $u/\sqrt{2}^k$ is in the epsilon-region $\mathcal{R}_\epsilon$;
2. $u^\bullet/\sqrt{2}^k$ is in the unit disk;



But this is a 2-dimensional grid problem, so can be solved efficiently.

Algorithm 1

(1) For all $k \in \mathbb{N}$, enumerate all $u \in \mathbb{Z}[\omega]$ such that $u/\sqrt{2}^k \in \mathcal{R}_\epsilon$ and $u^\bullet/\sqrt{2}^k \in \overline{\mathcal{D}}$.

(2) For each u:
  (a) Compute $\xi = 2^k - u^\dagger u$ and $n = \xi^\bullet \xi$.
  (b) Attempt to find a prime factorization of n.
  (c) If a prime factorization is found, attempt to solve the equation $t^\dagger t = \xi$.

(3) When step (2) succeeds, output U.

Results

- In the presence of a factoring oracle (e.g., a quantum computer), Algorithm 1 is *optimal* in an absolute sense: it finds the solution with the smallest possible T-count whatsoever, for the given θ and ϵ.

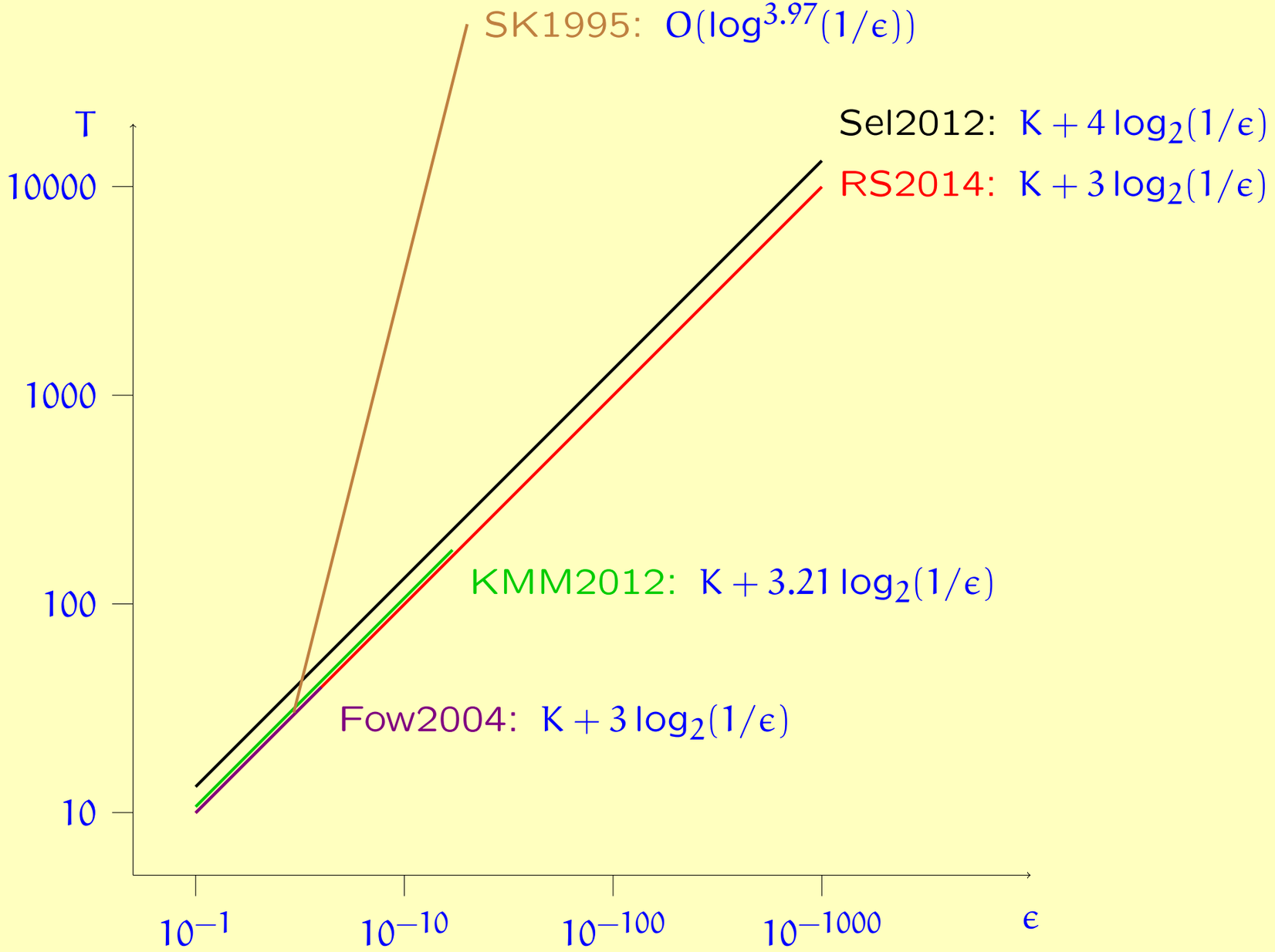
- In the absence of a factoring oracle, Algorithm 1 is *nearly optimal*: it yields T-counts of $m + O(\log(\log(1/\epsilon)))$, where m is the second-to-optimal T-count.

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

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

Experimental results

ϵ	T-count	T-bound	Actual error	Runtime	Candidates	Time/Cand.
10^{-10}	102	≥ 102	$0.91180 \cdot 10^{-10}$	0.0190s	3.0	0.0064s
10^{-20}	200	≥ 198	$0.87670 \cdot 10^{-20}$	0.0433s	7.0	0.0061s
10^{-30}	298	≥ 298	$0.99836 \cdot 10^{-30}$	0.0600s	7.0	0.0085s
10^{-40}	402	≥ 400	$0.77378 \cdot 10^{-40}$	0.0976s	11.7	0.0084s
10^{-50}	500	≥ 500	$0.82008 \cdot 10^{-50}$	0.1353s	20.3	0.0067s
10^{-60}	602	≥ 596	$0.61151 \cdot 10^{-60}$	0.1548s	16.0	0.0097s
10^{-70}	702	≥ 698	$0.40936 \cdot 10^{-70}$	0.1931s	20.9	0.0093s
10^{-80}	804	≥ 794	$0.92372 \cdot 10^{-80}$	0.2402s	27.2	0.0088s
10^{-90}	898	≥ 898	$0.96607 \cdot 10^{-90}$	0.2696s	22.2	0.0121s
10^{-100}	1000	≥ 998	$0.78879 \cdot 10^{-100}$	0.3443s	31.2	0.0110s
10^{-200}	1998	≥ 1994	$0.73266 \cdot 10^{-200}$	1.1423s	62.3	0.0183s
10^{-500}	4990	≥ 4986	$0.67156 \cdot 10^{-500}$	8.6509s	170.4	0.0508s
10^{-1000}	9974	≥ 9966	$0.80457 \cdot 10^{-1000}$	47.9300s	270.4	0.1773s
10^{-2000}	19942	≥ 19934	$0.88272 \cdot 10^{-2000}$	383.1024s	556.7	0.6881s


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

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

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

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

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

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

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

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

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

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

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

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

The end.