

LLL

2)

Explain geometrically why the area of the parallelogram is computed using $\det(S)$, where $S = [\underline{a} \underline{b}]$

Solution:

The area of a parallelogram spanned by vectors \underline{a} and \underline{b} is the magnitude of $\underline{a} \times \underline{b}$. The cross product can be written as the determinant

$$\underline{a} \times \underline{b} = \begin{vmatrix} i & j & k \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}$$

a_3 and b_3 are 0 so we get

$$\underline{a} \times \underline{b} = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} k$$

Thus, the area of a parallelogram is the absolute value of the // determinant.

3)
Given:

- L_1 and L_2 are lattices generated by (g_1, g_2, \dots, g_n) and (b_1, b_2, \dots, b_n) respectively.

- $L_1 \subset L_2$.

- Let

$$G = [g_1, g_2, \dots, g_n]$$

$$F = [b_1, b_2, \dots, b_n]$$

Find:

Show $\det(F)$ divides $\det(G)$, i.e. $\frac{\det(G)}{\det(F)} \in \mathbb{Z}$

Solution:

We have shown that $\det(G)$ represents the area of the parallelogram spanned by the vectors in G . If

$$L_1 \subset L_2$$

we know $L = \sum_{i=1}^n \mathbb{Z} b_i$ so we write

$$L_1 = \sum_{i=1}^n \mathbb{Z} g_i \quad L_2 = \sum_{i=1}^k \mathbb{Z} b_i \quad \text{where } n > k$$

$$\text{Therefore } \frac{\det(G)}{\det(F)} = \frac{|L_1|}{|L_2|} = \frac{\left| \sum_{i=1}^n \mathbb{Z} g_i \right|}{\left| \sum_{i=1}^k \mathbb{Z} b_i \right|}$$

Therefore $\det(G)$ is divisible by $\det(F)$

17

11

4)

Given:

 \Rightarrow lattice may have more than one basis set.

Find:

- If F and G are matrices of basis vectors, then

$$|\det(F)| = |\det(G)|$$

- Check that is true for

$$b_1 = \begin{bmatrix} 10 \\ 2 \end{bmatrix} \quad b_2 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} \quad g_1 = \begin{bmatrix} 2 \\ 3 \end{bmatrix} \quad g_2 = \begin{bmatrix} 8 \\ -1 \end{bmatrix}$$

Solution:

Let the lattice L be formed by

$$L = F\Gamma = G\Gamma$$

where $\underline{\Gamma} = [r_1 \ r_2 \ \dots \ r_n]$ s.t. $r_i \in \mathbb{Z}$ and

$$F = [b_1 \ b_2 \ \dots \ b_n]$$

$$G = [g_1 \ g_2 \ \dots \ g_n]$$

We know $|L|$ is the volume of the parallelepiped span. Thus

$$|L| = |\det(F)| = |\det(G)| //$$

$$b = \begin{bmatrix} 10 & 12 \\ 2 & 5 \end{bmatrix} \quad |\det(b)| = |10 \cdot 5 - 12 \cdot 2| = 26 //$$

$$g = \begin{bmatrix} 2 & 8 \\ 3 & -1 \end{bmatrix} = |2(-1) - 8 \cdot 3| = 26 //$$

5)

Demonstrate an understanding of the structure of matrix H from Gram-Schmidt process

Solution:

The Gram-Schmidt process can be written as

$$b_i^* = b_i - \sum_{j=1}^{i-1} u_{ij} b_j^* \quad u_{ij} = \frac{\langle b_i, b_j^* \rangle}{\|b_j^*\|^2}$$

Thus

$$b_i = b_i^* + \sum_{j=1}^{i-1} u_{ij} b_j^* \Rightarrow F = F^* H$$

Write out a few steps

$$b_1 = b_1^* + \sum_{j=1}^0 u_{1j} b_j^* = b_1^*$$

$$b_2 = b_2^* + \sum_{j=1}^1 u_{2j} b_j^* = b_2 + u_{21} b_1$$

When each b_i is a column of F . Writing this out we see the pattern

$$[b_1^* \ b_2^* \ \dots \ b_n^*] = \begin{bmatrix} 1 & u_{11} & u_{12} & \dots & u_{1n} \\ 0 & 1 & u_{22} & & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & \ddots & \ddots & & \end{bmatrix}$$



6)

Given:

$$f = f^* M \text{ where } f = [b_1 \ b_2 \ \dots \ b_n]$$

$$f^* = [b_1^* \ b_2^* \ \dots \ b_n^*]^T$$

$$M = \begin{bmatrix} 1 & m_{21} & m_{31} & \cdots & m_{n1} \\ 0 & 1 & m_{32} & \cdots & m_{n2} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & & & & m_{n-1} \\ 0 & & & & 1 \end{bmatrix}$$

Find:

Show $\det(f) = \det(f^*)$

Solution:

The change of basis is a similarity transform, thus

f and f^* are similar

A property of similar matrices is that they share the same determinant. Therefore, $\det(f) = \det(f^*)$

7)

Show that $\|b_i^*\| \leq \|b_i\|$

Solution:

From GSP and let $| \cdot |$ denote Euclidean Lengths

$$\|b_i\|^2 = \|b_i^*\|^2 + \sum_{j=1}^{i-1} u_{ij}^2 \|b_j^*\|^2$$

The paper specifies that a basis is reduced if $|u_{ij}| \leq \frac{1}{2}$
 for $1 \leq j \leq i \leq n$. Thus

$$\|b_i\|^2 = \|b_i^*\|^2 + \sum_{j=1}^{i-1} \frac{1}{4} \|b_j^*\|^2 \quad (1)$$

It was also shown that

$$\|b_i^* + u_{i,i-1} b_{i-1}^*\|^2 \geq \frac{3}{4} \|b_{i-1}^*\|^2 \quad \text{for } 1 \leq i \leq n$$

Rewriting we find

$$\begin{aligned} \|b_i^*\| &= \sqrt{\frac{3}{4} \|b_{i-1}^*\|^2 - \|u_{i,i-1} b_{i-1}^*\|^2} \\ &= \left(\frac{3}{4} - u_{i,i-1}^2 \right)^{1/2} \|b_{i-1}^*\| \geq \frac{1}{2} \|b_{i-1}^*\| \end{aligned}$$

by induction

$$\|b_j^*\|^2 \leq 2^{i-j} \|b_i^*\|^2 \quad \text{for } 1 \leq j \leq i \leq n$$

Using this lets go back to (1)

$$\|b_i\|^2 \leq \|b_i^*\|^2 + \sum_{j=1}^{i-1} \frac{1}{4} (2^{i-j}) \|b_j^*\|^2$$

$$= \left(1 + \frac{1}{4}(2^i - 2)\right) |b_i^*|^2$$

$$\Rightarrow |b_i|^2 \leq 2^{i-1} |b_i^*|^2$$

By the literature it follows that

$$|b_j|^2 \leq 2^{j-1} |b_j^*|^2 \leq 2^{i-1} |b_i^*|^2$$

if $j = i$

$$|b_i|^2 \leq |b_i^*|^2 //$$



8)

Given:

Let F be a matrix with column vectors $b_1 - b_n$. Then

$$|\det(F)| \leq \|b_1\| \cdots \|b_n\|.$$

Find:

Poss the inequality (Hadamard's Inequality)

Solution:

Let $F = QR$ where Q is orthogonal $[b_i^*]^T i = 1, 2, \dots, n$)

R is upper triangular

Let q_i denote column of RQ and f_i denote columns of F , and let r_{ij} denote entries of R . Thus

$$f_i = \sum_{j=1}^n r_{ij} q_i$$

Then we can say

$$\|f_j\|^2 = \sum_{i=1}^n |r_{ij}|^2 \|q_i\|^2 \geq |r_{jj}|^2$$

$$\Rightarrow \|f_j\|^2 \geq |r_{jj}|^2$$

Now we write

$$\begin{aligned} |\det(F)| &= |\det(Q)| |\det(R)| \\ &= 1 \prod_{j=1}^n |r_{jj}| = \prod_{j=1}^n \|f_j\| \end{aligned}$$

Letting $f_j = b_j$ as in the problem statement

$$|\det(F)| \leq \prod_{i=1}^n \|b_i\| //$$

9)

Given:

$$\|b\|^2 \stackrel{(a)}{=} a_k^2 \langle b_k^*, b_k^* \rangle + \sum_{i=1}^{k-1} v_i^2 \langle b_i^*, b_i^* \rangle$$

$$\stackrel{(b)}{\geq} a_k^2 \|b_k^*\|^2$$

$$\stackrel{(c)}{\geq} \|b_k^*\|^2$$

$$\stackrel{(d)}{=} \min(\|b_1^*\|^2, \dots, \|b_n^*\|^2)$$

Find:

Justify equality (a) and inequalities (b), (c), (d).

Solution

$$(a) b = \sum_{i=1}^n a_i \sum_{j=1}^i u_{ij} b_j^* = a_k b_k^* + \sum_{i=1}^{k-1} v_i b_i^*$$

Therefore

$$\|b\|^2 = \|a_k\|^2 \|b_k^*\|^2 + \sum_{i=1}^{k-1} \|v_i\|^2 \|b_i^*\|^2$$

$$= a_k^2 \langle b_k^*, b_k^* \rangle + \sum_{i=1}^{k-1} v_i^2 \langle b_i^*, b_i^* \rangle$$

$a_k \in \mathbb{Z}$
Induced
from
 L_2 -norm

$v_i \in \mathbb{R}$
Induced

b)

$$\|b\|^2 \geq a_k^2 \|b_k^*\|^2 + 0$$

Dropped terms, therefore $\|b\|^2$
must be greater. $0 \geq 0$ because
we are taking the norm, removing
0 will only make the value
smaller.

c)

$$\geq \|b_k^*\|^2$$

Similarly $\partial \kappa^2 \geq 0$, removing this scalar only makes the value smaller. //

d)

$$\geq \min(\|b_1^*\|^2, \dots, \|b_n^*\|^2)$$

Any norm in $\|b_k^*\|^2$ must be as large as the smallest



15-19)

Given:

Theorem 1

Let b_1, \dots, b_n be a reduced basis for lattice L and let b_1^*, \dots, b_n^* be a Gram-Schmidt basis. Then,

$$\|b_j\|^2 \leq 2^{i-1} \|b_i^*\|^2 \quad \text{for } 1 \leq j \leq i \leq n$$

$$|L| \leq \prod_{i=1}^n \|b_i\| \leq 2^{n(n-1)/4} |L|$$

$$\|b_i\| \leq 2^{(n-1)/4} |L|^{1/n}$$

Find:

a) Show $\{b_1, \dots, b_n\}$ and $\{b_1^*, \dots, b_n^*\}$ that

$$\|b_i^*\|^2 \geq (\frac{3}{4} - M_{i-1}^2) \|b_{i-1}^*\|^2$$

b) Show $(\frac{3}{4} - M_{i-1}^2) \|b_{i-1}^*\|^2 = \frac{1}{4} \|b_{i-1}^*\|^2$ for $1 < i \leq n$

c) Show $\|b_i^*\|^2 = 2^{i-1} \|b_i^*\|^2$ for $1 \leq i \leq n$

d) Show $|L| = |\det[b_1^*, b_2^*, \dots, b_n^*]| = \prod_{i=1}^n \|b_i^*\|$

Then show (c) is true

e) Put $j=1$ in (4) and take product over $i=1, 2, \dots, n$
to show (b) is true.

Solution:

(1) By definition a lattice is reduced if

$$|M_{ij}| \leq \frac{1}{2} \quad 1 \leq j < i \leq n$$

$$\|b_i^* + M_{i-1} b_{i-1}^*\|^2 \geq \frac{3}{4} \|b_{i-1}^*\|^2$$

(1)

(2)

If we rewrite (a) as $\epsilon \in \mathbb{R}$

$$\|b_i^*\|^2 \geq \frac{3}{4} \|b_{i-1}^*\|^2 - \|u_{i-1}, b_{i-1}^*\|^2$$

$$\|b_i^*\|^2 = \left(\frac{3}{4} - u_{i-1}^2\right) \|b_{i-1}^*\|^2$$

b) $|u_{i-1}| \leq \frac{1}{2}$, so let us use its max value of $\frac{1}{2}$

$$\|b_i^*\|^2 = \left(\frac{3}{4} - \frac{1}{4}\right) \|b_{i-1}^*\|^2 = \frac{1}{2} \|b_{i-1}^*\|^2$$

c) Let $1 \leq j \leq i \leq n$

$$2\|b_j^*\|^2 \geq \|b_{j-1}^*\|^2$$

$$\|b_{j-1}^*\|^2 \geq \frac{1}{2} \|b_{j-2}^*\|^2$$

$$\|b_{j-2}^*\|^2 \geq \frac{1}{2} \|b_{j-3}^*\|^2$$

⋮

$$\|b_{j+1}^*\|^2 \geq \frac{1}{2} \|b_j^*\|^2$$

Using what is to the left, lets progress downward plugging variables

$$2\|b_i^*\|^2 \geq \|b_{i-1}^*\|^2 \geq \frac{1}{2} \|b_{i-2}^*\|^2$$

$$\text{but } \|b_{i-2}^*\|^2 \geq \frac{1}{2} \|b_{i-3}^*\|^2, \text{ so}$$

$$2\|b_i^*\|^2 \geq \frac{1}{2} \frac{1}{2} \|b_{i-3}^*\|^2$$

Recursively moving down we find

$$2\|b_i^*\|^2 \geq \left(\frac{1}{2}\right)^{i-j-1} \|b_j^*\|^2$$

Thus,

$$2^{i-j} \|b_i^*\|^2 \geq \|b_j^*\|^2$$

d) Hadamards inequality states

$$\det(L) \leq \prod_{i=1}^n \|b_i\|$$

and has equality when the vectors are orthogonal! Therefore

$$\|L\| = \prod_{i=1}^n \|d_i^*\|$$

$$b_i^* = b_i - \sum_{j=1}^n M_{ij} b_j^*$$

$$\|b_i^*\| = \|b_i\| - \sum_{j=1}^n \|M_{ij} b_j^*\|$$

$$\|b_i^*\| \leq \|b_i\|$$

Let $i=j$ and using the previous proof

$$\|b_i\|^2 \leq 2^{i-1} \|b_i^*\|^2$$

$$\|b_i\| \leq 2^{\frac{i-1}{2}} \|b_i^*\|$$

Substitute into (3)

$$|L| \leq \prod_{i=1}^n \|b_i\|^2 \leq \prod_{i=1}^n 2^{\frac{i-1}{2}} \|b_i^*\|^2$$

$$= \underbrace{\prod_{i=1}^n \left(2^{\frac{i-1}{2}}\right)}_{\text{Look at this for a moment}} |L|$$

$$(2^0)(2^{\frac{1}{2}}) \cdots (2^{\frac{n-1}{2}}) = 2^{0+1+\dots+\frac{n-1}{2}} = 2^{\frac{n(n-1)}{4}}$$

$$\text{This comes from } \sum_{i=1}^n i = \frac{n(n+1)}{2}$$

We can then rewrite the equation as

$$|L| \leq 2^{\frac{n(n-1)}{4}} |L|$$



e) Set $j=1$ in (4) from paper

$$\|b_1\|^2 \leq 2^{i-1} \|b_i^*\|^2$$

$$\|b_1\| \leq 2^{\frac{i-1}{2}} \|b_i^*\|$$

Apply $\prod_{i=1}^n$ operator on both sides

$$\prod_{i=1}^n \|b_i\| = \prod_{i=1}^n 2^{\frac{i-1}{2}} \|b_i^*\| = 2^{\frac{n(n-1)}{4}} |L|$$

$$\|b_1\|^n \leq 2^{\frac{n(n-1)}{4}} |L|$$

$$\|b_1\| \leq 2^{\frac{(n-1)}{4}} |L|^{1/4}$$



Given: Theorem 2

Find:

a) Why does $r_i = r'_i$

b) Explain why $\|x\|^2 \geq r_i'^2 \|b_i^*\|^2 \geq \|b_i^*\|^2$

c) Using (4) from literature, explain why (7) from the literature is true.

Solution:

b)
Write

$$x = \sum_{j=1}^n r_j b_j = \sum_{j=1}^n r'_j b_j^*$$

Take the inner product of x with b_i^*

$$\langle x, b_i^* \rangle = \underbrace{\sum_{j=1}^n r_j}_{\text{Note that } b_j \text{ can be}} \langle b_i, b_i^* \rangle = \underbrace{\sum_{j=1}^n r'_j}_{b_j^* \text{ is orthogonal to all}} \langle b_j^*, b_i^* \rangle$$

Note that b_j can be written in terms as a linear combination of b_j^* terms. Therefore, $b_j \perp b_i + j = 1 - n$ and $j \neq i$.

b_j^* is orthogonal to all b_i^*

$$\langle x, b_i^* \rangle = r_i \underbrace{\langle b_i, b_i^* \rangle}_{\text{and } j \neq i} = r'_i \langle b_i^*, b_i^* \rangle$$

$$b_i^* = b_i - \underbrace{\sum_{k=1}^{i-1} \langle b_i, b_k^* \rangle}_{0} b_k^*, \quad b_i = b_i^* + \underbrace{\sum_{k=1}^{i-1} \langle b_i, b_k^* \rangle}_{1} b_k^*$$

So we are left with $b_i = b_i^*$

Rewriting $\langle x, b_i^* \rangle$

$$r_i \langle b_i^*, b_i^* \rangle = r'_i \langle b_i^*, b_i^* \rangle$$

$$r_i = r'_i //$$

b) $x = \sum_{j=1}^n r_j b_j^*$, so $x \geq r_i b_i^*$ and $\|x\|^2 \geq r_i'^2 \|b_i^*\|^2$

$r_i'^2 \in \mathbb{R}^+$, so dropping only makes the value smaller.

$$\Rightarrow \|x\|^2 \geq \|b_i^*\|^2 //$$

c) setting $j=1$ in (4) from the paper

$$\|b_i\|^2 \leq 2^{i-1} \|b_i^*\|^2 \leq 2^{m-i} \|b_i^*\|^2 \leq 2^{n-i} \|x\|^2 //$$

23-24)

Given:

$$b_k^* = b_k - r b_{k-1}$$

Find:

a) Show $m_{k,j}^* = m_{k,j} - r m_{k-1,j}$ $j=1, 2, \dots, k-1$
is the correct GS update

b) Show $m_{k,k-1}^* = m_{k,k-1} - r$ $j=1, 2, \dots, k-1$
is the correct GS update that ensures $|m_{k,k-1}| \leq \frac{1}{2}$

Solution:

a) Let's try expanding b_k^*

$$b_k^* + \sum_{j=1}^{k-1} m_{ij} b_j^* - r \left(b_{k-1}^* + \sum_{j=1}^{k-2} m_{ij} b_j^* \right)$$

We are calculating b_k^* with

$$\sum_{j=1}^{k-1} m_{ij} b_j^* - \sum_{j=1}^{k-2} (r m_{ij}) b_j^*$$

This is not properly updating, so we simply can write

$$m_{ij}^* = m_{k,i} - r m_{k-1,i} \quad \text{for } i=1, 2, \dots, k-1$$

b)

Writing

$$|m_{k,k-1}| = |m_{k,k-1} - 1| r \\ \sim \\ > \frac{1}{2}$$

Because $|m_{k,k-1}| > \frac{1}{2}$ and r is the integer closest to $m_{k,k-1}$ then
 $|m_{k,k-1}| \leq \frac{1}{2}$. //

LLL

Alexander Brown

March 12, 2023

1 1

1.1 Question

Write a MATLAB program that will plot a lattice in the interval [0,40] on the x axis and [0,20] on the y axis.

1.2 Solution

```
b1 = [10;2];
b2 = [12;5];
b = [b1 b2];
plattice(b, "one")
```

Output is shown in Figure 1.

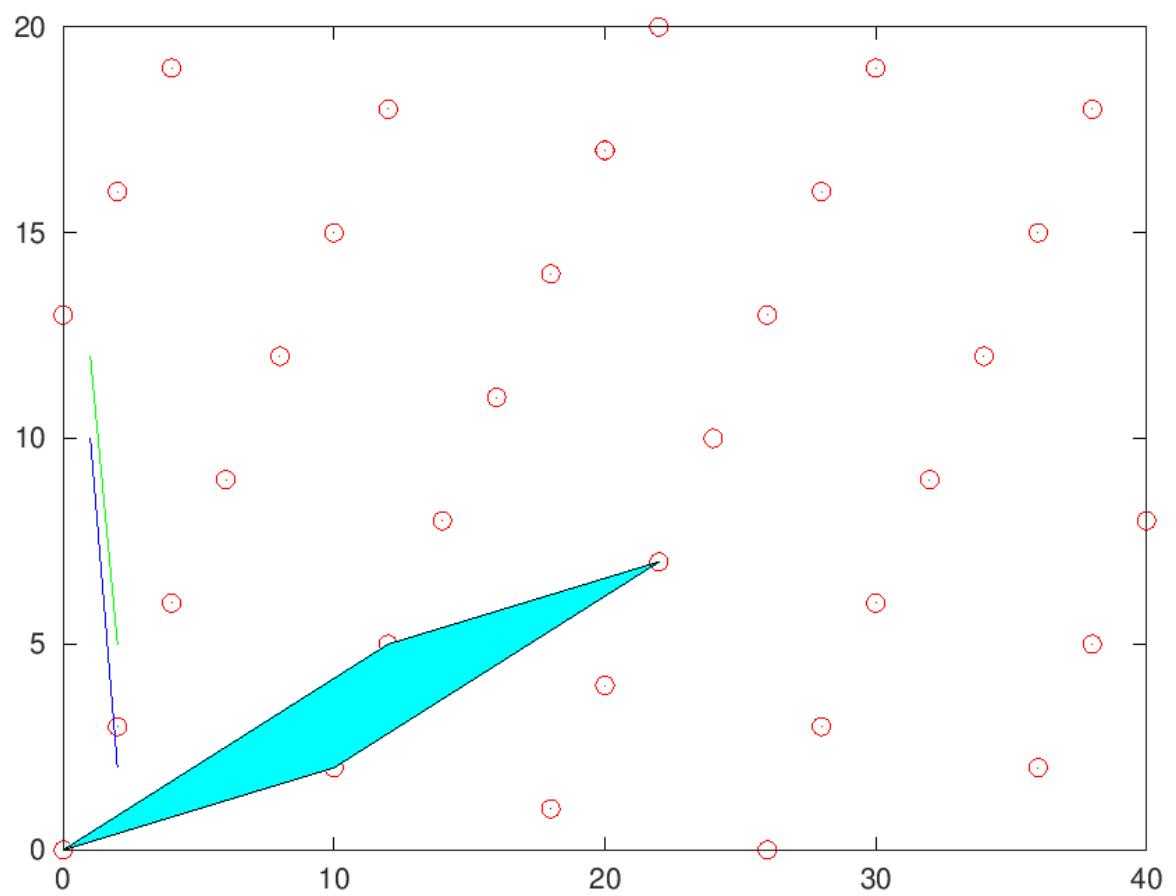


Figure 1: Plot of lattice

2 11

2.1 Question

For the basis vectors

$$b1 = \begin{bmatrix} 12 \\ 2 \end{bmatrix} b2 = \begin{bmatrix} 13 \\ 4 \end{bmatrix} \quad (1)$$

verify that the reduced basis vectors are

$$b1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix} b2 = \begin{bmatrix} 9 \\ -4 \end{bmatrix} \quad (2)$$

2.2 Solution

```
b1 = [12;2];
b2 = [13;4];
b = [b1 b2];
LLL(b,true);
```

$$\begin{array}{cc} 1 & 9 \\ 2 & -4 \end{array}$$

Output is shown in Figure 2

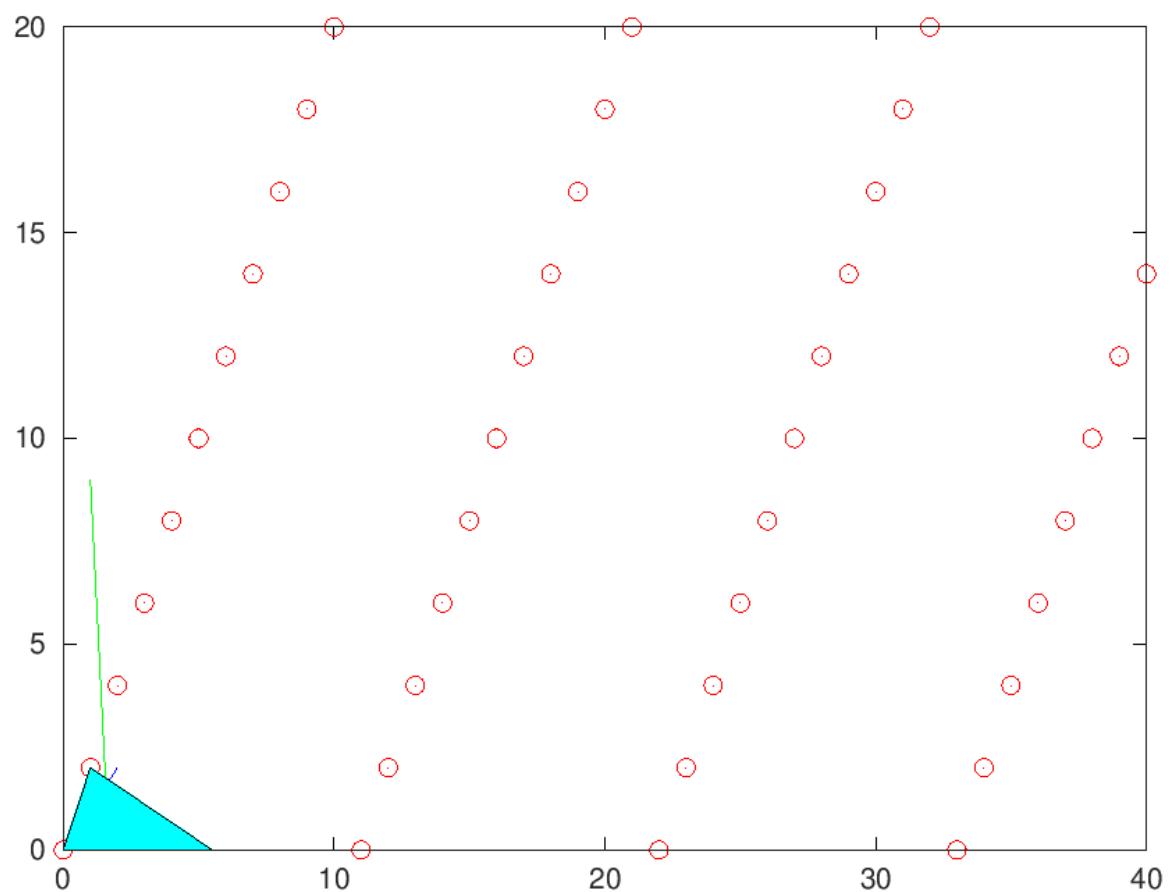


Figure 2: Plot of reduced lattice

3 12

3.1 Question

$$B = \begin{bmatrix} 1 & -1 & 2 \\ 1 & 0 & 5 \\ 1 & 2 & 6 \end{bmatrix} \quad (3)$$

verify that the reduced basis vectors are

$$B = \begin{bmatrix} 0 & 1 & -2 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \quad (4)$$

3.2 Solution

```
B = [1, -1, 3;
      1, 0, 5;
      1, 2, 6];

LLL(B, false);
```

$$\begin{array}{ccc} 0 & 1 & -2 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{array}$$

4 13

4.1 Question

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -366 & -385 & -392 & -401 & -422 & -437 & 1215 \end{bmatrix} \quad (5)$$

verify that the short vector

$$b1 = [0 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0] \quad (6)$$

is obtained.

4.2 Solution

```
B = [1, 0, 0, 0, 0, 0, 0;
      0, 1, 0, 0, 0, 0, 0;
```

```
0 , 0 , 1 , 0 , 0 , 0 ;  
0 , 0 , 0 , 1 , 0 , 0 ;  
0 , 0 , 0 , 0 , 1 , 0 ;  
0 , 0 , 0 , 0 , 0 , 1 ;  
-366 , -385 , -392 , -401 , -422 , -437 , 1215]
```

```
LLL(B, false);
```

```
0 0 1 0 -2 0 5  
0 1 0 2 1 1 2  
1 1 1 -1 1 -1 2  
1 0 -1 1 -1 -1 0  
1 0 1 0 -1 2 -1  
0 1 1 1 -1 -1 -4  
0 1 -1 -1 0 1 1
```

5 14

5.1 Question

5.2 Solution

The result from `hackerman.m` is "]".

```
hackerman
```

```
]
```