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.a

1.2 Solution

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

Output is shown in Figure 1.

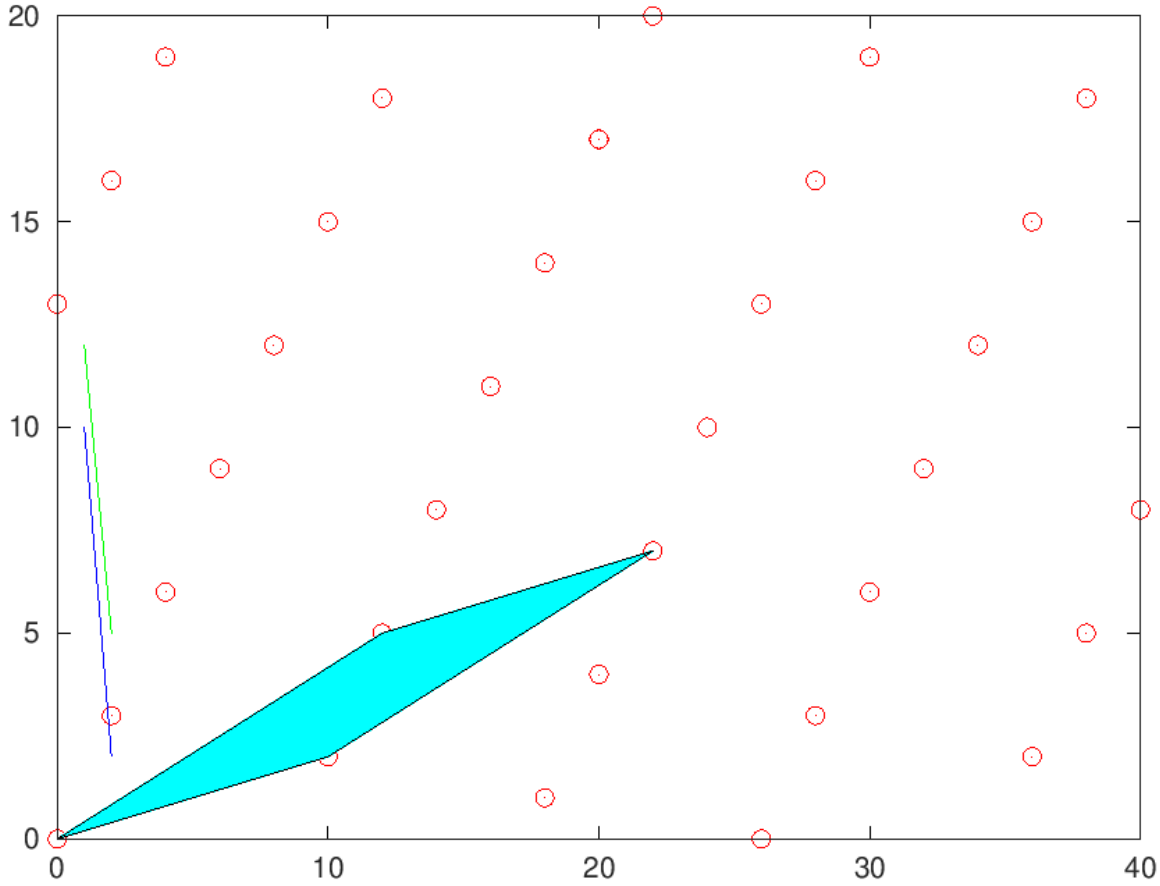

Figure 1: Plot of lattice

2 11

2.1 Question

For the basis vectors

$$b1 = \begin{bmatrix} 12 \\ 2 \end{bmatrix} b2 = \begin{bmatrix} 13 \\ 4 \end{bmatrix} \tag{1}$$

verify that the reduced basis vectors are

$$b1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix} b2 = \begin{bmatrix} 9 \\ -4 \end{bmatrix} \tag{2}$$

2.2 Solution

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

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

Output is shown in Figure 2

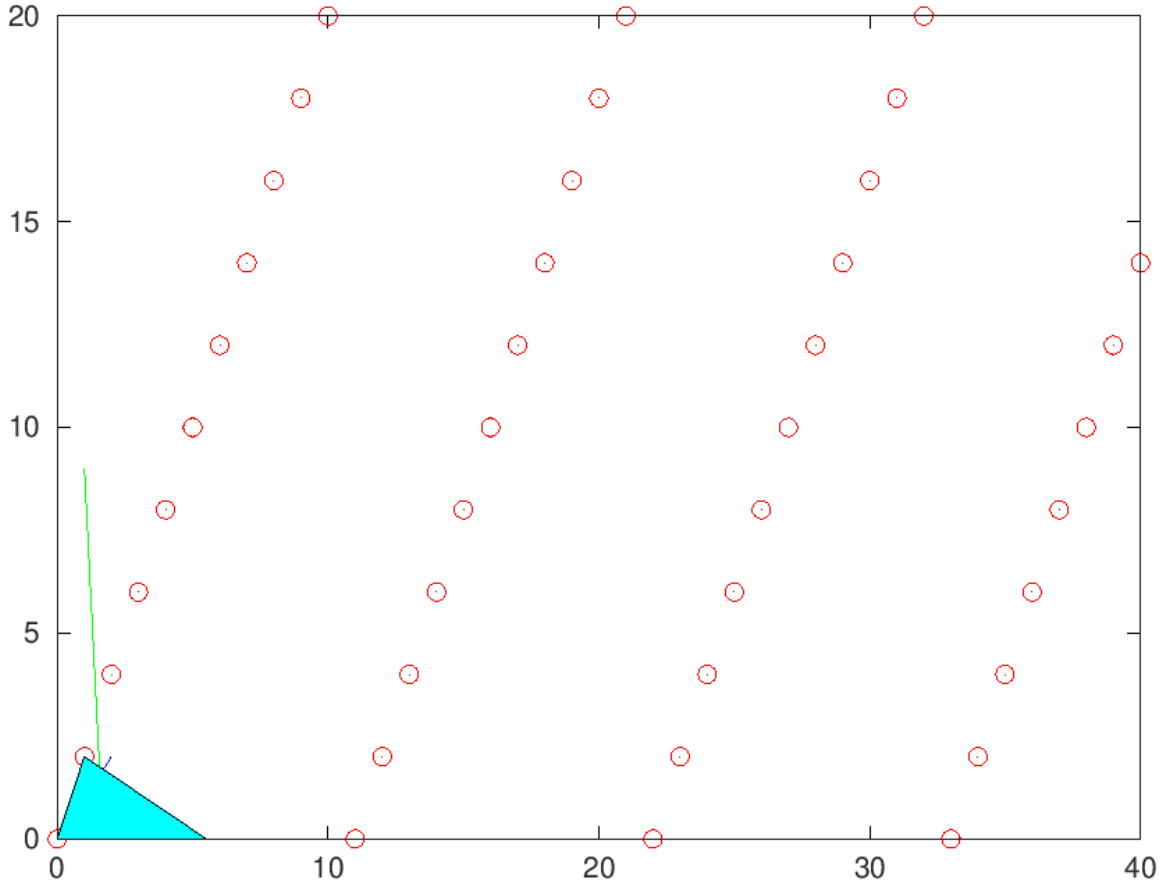

Figure 2: Plot of reduced lattice

3 12

3.1 Question

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

verify that the reduced basis vectors are

$$B = \begin{bmatrix} 0 & 1 & -2 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \tag{4}$$

3.2 Solution

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

LLL(B,false);
```

$$\begin{matrix} 0 & 1 & -2 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{matrix}$$

4 13

4.1 Question

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

verify that the short vector

$$b1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \tag{6}$$

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 , 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]

LLL(B,false);
```

$$\begin{array}{ccccccc} 0 & 0 & 1 & 0 & -2 & 0 & 5 \\ 0 & 1 & 0 & 2 & 1 & 1 & 2 \\ 1 & 1 & 1 & -1 & 1 & -1 & 2 \\ 1 & 0 & -1 & 1 & -1 & -1 & 0 \\ 1 & 0 & 1 & 0 & -1 & 2 & -1 \\ 0 & 1 & 1 & 1 & -1 & -1 & -4 \\ 0 & 1 & -1 & -1 & 0 & 1 & 1 \end{array}$$

5 14

5.1 Question

5.2 Solution

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

```
hackerman


]
```