2) Explain geometrically why the area of the parallelogram is computed using $\det(F)$, where $F = [b_1\ b_2 \cdots]$

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

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

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

3)

Given:

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

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

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

Find:

Show $\det(F)$ divides (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

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

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 $\det(F)$ //

4)

Given:

A 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

$$L = F\underline{r} = G\underline{r}$$

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

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

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

We know $|L|$ is the volume of the parallelpiped 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 M from Gram-Schmidt process

Solution:

The Gram-Schmidt process can be written as

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

Thus

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

Write out a few steps

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

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

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

$$[b_1^* \quad b_2^* \quad \cdots \quad b_n^*] = \begin{bmatrix} 1 & u_{21} & u_{31} & \cdots & u_{i1} \\ 0 & 1 & u_{32} & & \vdots \\ \vdots & \vdots & \vdots & & \\ & & & & 1 \\ 0 & \cdots & & & \end{bmatrix}$$

6)

Given:

$F = F^* M$ where $F = [b_1\ b_2 \cdots b_n]^T$

$F^* = [b_1^*\ b_2^* \cdots b_n^*]^T$

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

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 Length

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

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

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

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

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

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

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 $j = 1$

$$|b_j|^2 \leq |b^*_j|^2 \quad //$$

8)

Given:

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

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

Find:

Prove the inequality (Hadamard's Inequality)

Solution:

Let $F = QR$ where Q is orthogonal ($[b^*] \forall\ i = 1, 2, \ldots n$)

R is upper triangular

Let q_j denote column of Q and f_j denote columns of F, and let r_{ij} denote entries of R. Thus

$$f_j = \sum_{i=1}^{j} r_{ij} q_i$$

Then we can say

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

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

Now we write

$$|\det(F)| = |\det(Q)|\,|\det(R)|$$

$$= 1 \left\| \prod_{j=1}^{n} r_{jj} \right\| \leq \prod_{j=1}^{n} \|f_j\|$$

Letting $f_j = b_j$ as in the problem statement

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

9)

Given:

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

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

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

$$\overset{(d)}{\geq} \min(\|b_1^*\|^2, \ldots, \|b_n^*\|^2)$$

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

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

$$= a_k^2 \langle b_k^*, b_k^* \rangle + \sum v_i^2 \langle b_k^*, b_k^* \rangle$$

$a_k \in \mathbb{Z}$ — Induced from L2 norm — $v_i \in \mathbb{R}$ — Induced

b)

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

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 $a_k^2 \geq 0$; removing this scalar only makes the value smaller. //

d)

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

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

15-A)

Given:

Theorem 1

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

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

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

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

Find:

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

$$\|b_i^*\|^2 \ge (3/4 - \mu_{i,i-1}^2) \|b_{i-1}^*\|^2$$

b) Show $\left(\frac{3}{4} - \mu_{i,i-1}^2\right) \|b_{i-1}^*\|^2 \ge \frac{1}{2} \|b_{i-1}^*\|^2$ for $1 < i \le n$

c) Show $\|b_i^*\|^2 \le 2^{i-j} \|b_j^*\|^2$ for $1 \le j \le i \le n$

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

Then show (5) is true

e) Put $j=1$ in (4) and take product over $i = 1, 2, \ldots, n$ to show (6) is true.

Solution:

a)

By definition a lattice is reduced if

$$|\mu_{ij}| \le 1/2 \quad 1 \le j < i \le n \tag{1}$$

$$\|b_i^* + \mu_{i,i-1} b_{i-1}^*\|^2 \ge \frac{3}{4} \|b_{i-1}^*\|^2 \tag{2}$$

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

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

$$\|b_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right)\|b_{i-1}\|^2 \quad //$$

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

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

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

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

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

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

$$\vdots$$

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

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

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

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

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

d) Hadamards inequality states

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

and has equality when the vectors are orthogonal! Therefore

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

$$b_i^* = b_i - \sum_{i=1}^{n} \mu_{ij} b_j^*$$

$$\|b_i^*\| = \|b_i\| - \sum_{i=1}^{n} \|\mu_{ij} b_j^*\|$$

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

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)

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

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

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

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

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

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

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

//

20 - 22)

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:

a)

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^*

$$\langle x, b_i^* \rangle = \sum_{j=1}^{n} r_j \langle b_j, b_i^* \rangle = \sum r_j' \langle b_j^*, b_i^* \rangle$$

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

b_j^* is orthogonal to all but b_i^*

$$\langle x, b_i^* \rangle = r_i \langle b_i, b_i^* \rangle = r_j' \langle b_j^*, b_j^* \rangle$$

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

0 — $b_i \perp b_k^*$ $\quad$ 1 $\quad$ 0

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) $x = \sum_{j=1}^{n} r_i' b_i^*$, 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.

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

23-24)

Given:

$$b_k' = b_k - r b_{k-1}$$

Find:

a) Show $\mu_{k,j}' = \mu_{k,j} - r\mu_{k-1,j}$ $\quad j = 1, 2, \ldots, k-1$
is the correct GS update

b) Show $\mu_{k,k-1}' = \mu_{k,k-1} - r \quad j = 1, 2, \ldots, k-1$
is the correct GS update, that ensures $|\mu_{k,k-1}| \leq 1/2$

Solution:

a) Lets try expanding b_k'

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

We are calculating b_k' with

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

This is not properly updating, so we simply can write

$$\mu_{ij}' = \mu_{k,i} - r\mu_{k-1,j} \quad \text{for } i = 1, 2, \ldots, k-1$$

b)

Writing

$$|\mu_{k,k-1}'| = \underbrace{|\mu_{k,k-1}|}_{\geq 1/2} - |r|$$

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