4005-898 Independent Study

Chapter 8: Basis Reduction

Alexander Lange

March 22, 2012

PROBLEM 8.1. *Give a complete proof of Lemma 8.1: U solves $AU = B$ if and only if U solves*

$$\begin{bmatrix} I & \vec{0} \\ A & -B \end{bmatrix} \begin{bmatrix} U \\ 1 \end{bmatrix} = \begin{bmatrix} U \\ \vec{0} \end{bmatrix}$$

Solution. Let A be an m by n matrix and $B = [b_1\ b_2 \ldots b_m]^T$

(a) *Claim:* If $U = [u_1\ u_2 \ldots u_n]^T$ such that $AU = B$, then $\left[\begin{smallmatrix} I & \vec{0} \\ A & -B \end{smallmatrix}\right] \left[\begin{smallmatrix} U \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} U \\ \vec{0} \end{smallmatrix}\right]$
Proof: Since $AU = B$, we know that

$$\begin{aligned} a_{11}u_1 + a_{12}u_2 + \cdots + a_{1n}u_n &= b_1 \\ a_{21}u_1 + a_{22}u_2 + \cdots + a_{2n}u_n &= b_2 \\ &\vdots \\ a_{m1}u_1 + a_{m2}u_2 + \cdots + a_{mn}u_n &= b_m \end{aligned}$$

The first n rows of $\left[\begin{smallmatrix} I & \vec{0} \\ A & -B \end{smallmatrix}\right]$ make up $[\ I\ \ \vec{0}\ ]$ and clearly,

$$\begin{bmatrix} I & \vec{0} \end{bmatrix} \begin{bmatrix} U \\ 1 \end{bmatrix} = U.$$

The last m rows make up $[\ A\ \ -B\ ]$, so

$$\begin{aligned} \begin{bmatrix} A & -B \end{bmatrix} \begin{bmatrix} U \\ 1 \end{bmatrix} &= \begin{bmatrix} (a_{11}u_1 + a_{12}u_2 + \cdots + a_{1n}u_n) - b_1 \\ (a_{21}u_1 + a_{22}u_2 + \cdots + a_{2n}u_n) - b_2 \\ \vdots \\ (a_{m1}u_1 + a_{m2}u_2 + \cdots + a_{mn}u_n) - b_m \end{bmatrix} \\ &= \begin{bmatrix} b_1 - b_1 \\ b_2 - b_2 \\ \vdots \\ b_m - b_m \end{bmatrix} \\ &= \vec{0} \end{aligned}$$

Therefore, $\left[\begin{smallmatrix} I & \vec{0} \\ A & -B \end{smallmatrix}\right] \left[\begin{smallmatrix} U \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} U \\ \vec{0} \end{smallmatrix}\right]$.

(b) *Claim:* If $U = [u_1\ u_2 \dots u_n]^T$ such that $\left[\begin{smallmatrix} I & \vec{0} \\ A & -B \end{smallmatrix}\right]\left[\begin{smallmatrix} U \\ 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} U \\ \vec{0} \end{smallmatrix}\right]$, then $AU = B$.
Proof: Very similar to part (a), but in reverse.

PROBLEM 8.2. *Which of the following are in the lattice* $\mathcal{L} = \mathsf{span}_{\mathbb{Z}}(B)$ *where*

$$B = \begin{bmatrix} 1 & -2 \\ 3 & 1 \end{bmatrix}$$

Solution. Let $\vec{b_1} = [1, 3]$ and $\vec{b_2} = [-2, 1]$ (the columns of B). The following vectors are in $\mathcal{L}$

- $5\vec{b_1} + 3\vec{b_2} = [-1, 18] \implies [-1, 18] \in \mathcal{L}$
- $4\vec{b_1} = [4, 12] \implies [4, 12] \in \mathcal{L}$
- $3\vec{b_1} + \vec{b_2} = [1, 10] \implies [1, 10] \in \mathcal{L}$
- $-3\vec{b_1} + 2\vec{b_2} = [1, -11] \implies [1, -11] \in \mathcal{L}$

PROBLEM 8.3. *Compute* $\mathsf{wt}(M)$ *and* $\mathsf{vol}(\mathcal{L})$ *with* $M = \left[\begin{smallmatrix} 1 & -2 \\ 3 & 1 \end{smallmatrix}\right]$ *and verify Hadamard's inequality for this lattice.*

Solution. We first apply Gram-Schmidt to M. Since there's only two vectors ($\vec{b_1}$ and $\vec{b_2}$), we know $\vec{b_1^*} = \vec{b_1}$ and we only need to compute $\vec{b_2^*}$

$$\vec{b_2^*} = \vec{b_2} - \frac{\vec{b_1} \cdot \vec{b_2}}{\vec{b_1} \cdot \vec{b_1}} \vec{b_1} = \begin{bmatrix} -2 \\ 1 \end{bmatrix} - \frac{1}{10} \begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} -\frac{21}{10} \\ \frac{7}{10} \end{bmatrix}$$

We can then compute $\mathsf{wt}(M)$ and $\mathsf{vol}(\mathcal{L})$

$$\begin{aligned} \mathsf{wt}(M) &= \|\vec{b_1}\| \cdot \|\vec{b_2}\| \\ &= \sqrt{10} \cdot \sqrt{5} \\ &= 5\sqrt{2} \end{aligned}$$

$$\begin{aligned} \mathsf{vol}(\mathcal{L}) &= \|\vec{b_1^*}\| \cdot \|\vec{b_2^*}\| \\ &= \sqrt{10} \cdot \sqrt{\frac{21^2 + 7^2}{10^2}} \\ &= 7 \end{aligned}$$

Since $\sqrt{2} \approx 1.4142 > 7/5 = 1.4$, we know that $\mathsf{wt}(M) > \mathsf{vol}(\mathcal{L})$, which agrees with *Hadamard's inequality.*

PROBLEM 8.5. *Using the Gram-Schmidt algorithm, work out the orthogonal basis for the lattice spanned by*

$$M = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Solution. Let $\vec{b_1} = [1, 1, 1]$, $\vec{b_2} = [1, 0, 1]$ and $\vec{b_3} = [2, 1, 0]$. Then $\vec{b_1^*} = \vec{b_1}$,

$$\begin{aligned} \vec{b_2^*} &= \vec{b_2} - \frac{\vec{b_1^*} \cdot \vec{b_2}}{\vec{b_1^*} \cdot \vec{b_1^*}} \vec{b_1^*} \\ &= [1, 0, 1] - \tfrac{2}{3}[1, 1, 1] \\ &= [\tfrac{1}{3}, -\tfrac{2}{3}, \tfrac{1}{3}] \end{aligned}$$

$$\begin{aligned} \vec{b_3^*} &= \vec{b_3} - \frac{\vec{b_1^*} \cdot \vec{b_3}}{\vec{b_1^*} \cdot \vec{b_1^*}} \vec{b_1^*} - \frac{\vec{b_2^*} \cdot \vec{b_3}}{\vec{b_2^*} \cdot \vec{b_2^*}} \vec{b_2^*} \\ &= [2, 1, 0] - \tfrac{3}{3}[1, 1, 1] - 0[\tfrac{1}{3}, -\tfrac{2}{3}, \tfrac{1}{3}] \\ &= [1, 0, -1] \end{aligned}$$

We can now compute $\mathsf{wt}(M) = \|\vec{b_1}\| \cdot \|\vec{b_2}\| \cdot \|\vec{b_3}\| = \sqrt{30}$ and $\mathsf{vol}(\mathcal{L}) = \|\vec{b_1^*}\| \cdot \|\vec{b_2^*}\| \cdot \|\vec{b_3^*}\| = 2$. Clearly, $\mathsf{wt}(M) > \mathsf{vol}(\mathcal{L})$.

PROBLEM 8.6. *Consider the matrix*

$$M = \begin{bmatrix} 0 & 2 & 3 & 1 \\ 1 & 0 & -1 & 5 \\ 2 & -2 & 2 & 0 \\ 2 & 2 & 0 & -2 \end{bmatrix}$$

(a) Show that M is a reduced matrix (b) Verify the inequalities of a reduced matrix hold for M

Solution. We let $\vec{b_1} = [0, 1, 2, 2]$, $\vec{b_2} = [2, 0, -2, 2]$, $\vec{b_3} = [3, -1, 2, 0]$ and $\vec{b_4} = [1, 5, 0, -2]$. We then run $\textsc{GramSchmidt}(\vec{b_1}, \vec{b_2}, \vec{b_3}, \vec{b_4})$ and obtain $\vec{b_1^*} = [0, 1, 2, 2]$, $\vec{b_2^*} = [2, 0, -2, 2]$, $\vec{b_3^*} = [2.6667, -1.3333, 1.6667, -1]$ and $\vec{b_4^*} = [1.7544, 4.6784, -0.2924, -2.0468]$.

(a) In order to show that M is a reduced basis, we first need all $|\alpha_{i,j}| < \frac{1}{2}$ for all $i < j$. These values can be represented as an upper triangular matrix with all zeros in the diagonal:

$$\alpha = \begin{bmatrix} & 0 & 0.3333 & 0.1111 \\ & & 0.1667 & -0.1667 \\ & & & -0.1579 \\ 0 & & & \end{bmatrix}$$

Clearly, the absolute value of the six appropriate entries of α are all less than $\frac{1}{2}$.

Next, we need to show that for all $j = 1, 2, \ldots, n-1$,

$$\|\vec{b^*_{j+1}} + \alpha_{j,j+1}\vec{b^*_j}\|^2 \geq \frac{3}{4}\|\vec{b^*_j}\|^2$$

$$\begin{array}{ll} j = 1, & \|\vec{b^*_2} + \alpha_{1,2}\vec{b^*_1}\|^2 = 12, \quad \frac{3}{4}\|\vec{b^*_1}\|^2 = \frac{3}{4} \cdot 9 \\ j = 2, & \|\vec{b^*_3} + \alpha_{2,3}\vec{b^*_2}\|^2 = 13, \quad \frac{3}{4}\|\vec{b^*_2}\|^2 = \frac{3}{4} \cdot 12 \\ j = 3, & \|\vec{b^*_4} + \alpha_{3,4}\vec{b^*_3}\|^2 = 29.556, \quad \frac{3}{4}\|\vec{b^*_3}\|^2 = \frac{3}{4} \cdot 12.6679 \end{array}$$

(b) Next we need to show the following two results:

(1) $\|\vec{b_1}\| \leq 2^{(n-1)/4}\mathsf{vol}(\mathcal{L})^{1/n}$

(2) $\mathsf{wt}(M) \leq 2^{n(n-1)/4}\mathsf{vol}(\mathcal{L})$

We compute $\mathsf{wt}(M) = \sqrt{9 \cdot 12 \cdot 14 \cdot 30} \approx 212.9789$ and $\mathsf{vol}(\mathcal{L}) \approx 199.9999$. Then $\|\vec{b_1}\| = 3$ and $2^{3/4}\mathsf{vol}(\mathcal{L})^{1/4} = 6.3246$ which implies (1) is true. We compute $2^3\mathsf{vol}(\mathcal{L}) = 1599.9996$ which shows (2) to be true.