MAS400: Solutions 7

1. Calculate the Gram–Schmidt orthogonalisations of the following.

   (a) $\{(1,1,1),(1,2,3),(1,4,9)\}$.

   (b) $\{(1,2,0),(0,1,2),(2,0,1)\}$.

(a) $v_1^* := v_1 = (1,1,1)$;
$v_2^* := v_2 - \frac{v_2 \cdot v_1^*}{v_1^* \cdot v_1^*} v_1^* = (1,2,3) - \frac{6}{3}(1,1,1) = (-1,0,1)$;
$v_3^* := v_3 - \frac{v_3 \cdot v_2^*}{v_2^* \cdot v_2^*} v_2^* - \frac{v_3 \cdot v_1^*}{v_1^* \cdot v_1^*} v_1^* = (1,4,9) - \frac{8}{2}(-1,0,1) - \frac{14}{3}(1,1,1) = (\frac{1}{3}, -\frac{2}{3}, \frac{1}{3})$.

(b) $v_1^* := v_1 = (1,2,0)$;
$v_2^* := v_2 - \frac{v_2 \cdot v_1^*}{v_1^* \cdot v_1^*} v_1^* = (0,1,2) - \frac{2}{5}(1,2,0) = (-\frac{2}{5}, \frac{1}{5}, 2)$;
$v_3^* := v_3 - \frac{v_3 \cdot v_2^*}{v_2^* \cdot v_2^*} v_2^* - \frac{v_3 \cdot v_1^*}{v_1^* \cdot v_1^*} v_1^* = (2,0,1) - \frac{6/5}{21/5}(-\frac{2}{5}, \frac{1}{5}, 2) - \frac{2}{5}(1,2,0) = (2,0,1) - \frac{2}{7}(-\frac{2}{5}, \frac{1}{5}, 2) - \frac{2}{5}(1,2,0) = (\frac{12}{7}, -\frac{6}{7}, \frac{3}{7})$.

2. Calculate using `BasisReduction` (LLL-)reduced bases for the following lattices.

   (a) $\Lambda_1 = \langle (3,-5),(7,-11) \rangle_{\mathbb{Z}}$.

   (b) $\Lambda_2 = \langle (12,2),(13,4) \rangle_{\mathbb{Z}}$.

   (c) $\Lambda_3 = \langle (1,1,1),(1,1,-1),(1,-1,1) \rangle_{\mathbb{Z}}$.

In the first two questions, the for-loops only operate when $i = 2$, and the only changes that occur then are $m := \text{Round}(\mu_{21})$; $w_2 := w_2 - m w_1$ and $\mu_{21} := \mu_{21} - m\mu_{11} = \mu_{21} - m$.

(a) We let $w_1 = (3,-5)$ and $w_2 = (7,-11)$, and the GSO is $w_1^* = (3,-5)$ and $w_2^* = (7,-11) - \frac{76}{34}(3,-5) = (\frac{5}{17}, \frac{3}{17})$ with $\mu_{21} = \frac{38}{17}$. The first trip through the for-loops gives $m := \text{Round}(\frac{38}{17}) = 2$, $w_2 = w_2 - 2w_1 = (1,-1)$, $\mu_{21} = \mu_{21} - 2 = \frac{4}{17}$. Now $|w_1^*|^2 = 34 > 2|w_2^*|^2 = 2(\frac{34}{17^2}) = \frac{4}{17}$.
Thus the if-loop gives $w_1 = (1,-1)$, $w_2 = (3,-5)$, $w_1^* = (1,-1)$, $w_2^* = (3,-5) - \frac{8}{2}(1,-1) = (-1,-1)$, $\mu_{21} = 4$, and $i = 1$. When $i = 1$ the for-loops do nothing, and the if-loop increments i to 2. Now we get $m := \text{Round}(4) = 4$, $w_2 = w_2 - 4w_1 = (-1,-1)$, $\mu_{21} = \mu_{21} - 4 = 0$. Now $|w_1^*|^2 = 2 \leqslant 2|w_2^*|^2 = 4$. Therefore we are done and the reduced basis is $((1,-1),(-1,-1))$.

(b) We let $w_1 = (12, 2)$ and $w_2 = (13, 4)$, and the GSO is $w_1^* = (12, 2)$ and $w_2^* = (13, 4) - \frac{164}{185}(12, 2) = (\frac{437}{185}, \frac{412}{185})$ with $\mu_{21} = \frac{164}{185}$. The first trip through the for-loops gives $m := \text{Round}(\frac{164}{185}) = 1$, $w_2 = w_2 - w_1 = (1, 2)$, $\mu_{21} = \mu_{21} - 1 = -\frac{21}{185}$. Now $|w_1^*|^2 = 148 > 18 > 2|w_2^*|^2$ (since $|\frac{437}{185}|, |\frac{412}{185}| < 3$).

Thus the if-loop gives $w_1 = (1, 2)$, $w_2 = (12, 2)$, $w_1^* = (1, 2)$, $w_2^* = (12, 2) - \frac{16}{5}(1, 2) = (\frac{44}{5}, \frac{-22}{5})$, $\mu_{21} = \frac{16}{5}$, and $i = 1$. When $i = 1$ the for-loops do nothing, and the if-loop increments i to 2. Now we get $m := \text{Round}(\frac{16}{5}) = 3$, $w_2 = w_2 - 3w_1 = (9, -4)$, $\mu_{21} = \mu_{21} - 3 = \frac{1}{5}$. Now $|w_1^*|^2 = 5 \leqslant 2|w_2^*|^2 = 2(\frac{484}{5})$. Therefore we are done and the reduced basis is $((1, 2), (9, -4))$.

(c) We let $w_1 = (1, 1, 1)$, $w_2 = (1, 1, -1)$, $w_3 = (1, -1, 1)$. The GSO is $w_1^* = (1, 1, 1)$, $w_2^* = (1, 1, -1) - \frac{1}{3}(1, 1, 1) = (\frac{2}{3}, \frac{2}{3}, -\frac{4}{3})$ and $w_3^* = (1, -1, 1) - \frac{-4/3}{8/3}(\frac{2}{3}, \frac{2}{3}, -\frac{4}{3}) - \frac{1}{3}(1, 1, 1) = (1, -1, 0)$. The matrix (μ_{ij}) is:

$$(\mu_{ij}) = \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{3} & 1 & 0 \\ \frac{-1}{2} & \frac{1}{3} & 1 \end{pmatrix}.$$

Now $\text{Round}(\mu_{ij}) = 0$ whenever $i < j$, and so the for-loops of `BasisReduction` will not be the first part of the algorithm to alter the w_i, w_i^* or μ_{ij}. But $|w_1|^2 = 3$, $|w_2^*|^2 = \frac{8}{3}$ and $|w_3^*|^2 = 2$, and we have $|w_1^*|^2 \leqslant 2|w_2^*|^2$ and $|w_2^*|^2 \leqslant 2|w_3^*|^2$. So the if-loop in `BasisReduction` will not perform the initial change of the w_i, w_i^* or μ_{ij}, and will simply increment the counter i. Therefore the reduced basis is $((1, 1, 1), (1, 1, -1), (1, -1, 1))$.