1. Solutions

1 (1) En dimension 1, l'algorithm projette la cible orthogonalement sur la droite générée par un (nécessairement plus court) vecteur du réseau. Le plus proche vecteur est obtenu en arrondissant la coordonnée du projeté au plus proche entier.

(2) Puisque $(b_1, \dots, b_n)$ est une base de l'espace ambiant, on peut écrire $t = \sum t_i b_i = \sum_i \lceil t_i \rfloor b_i + \sum_i \{t_i\} b_i = s + e$, avec e dans le domaine fondamental (recentré) défini par les b_i. Ici, $\{t\}$ désigne la partie fractionnaire "recentrée", c'est-à-dire le réel $t - \lceil t \rfloor \in [1/2, 1/2)$, négatif si $t \geq \lfloor t \rfloor + 1/2$ et positif si $t < \lfloor t \rfloor + 1/2$. On peut donc écrire $\|s - t\| = \|e\| \leq \sum_i |\{t_i\}| \cdot \|b_i\|$ par l'inégalité triangulaire, et le résultat suit.

(3) On peut procéder par récurrence. C'est vrai en dimension 1 d'après la première question, alors supposons que c'est vrai en dimension $n-1$. Ecrivons $t = \tilde{t} + t_n b_n$, avec $\tilde{t} \in \mathrm{Vect}_{\mathbb{R}}(b_1, \dots, b_{n-1})$ et $t_n \in \mathbb{R}$, et de la même manière $s = \tilde{s} + \lceil t_n \rfloor b_n$ avec $\tilde{s} \in \mathcal{L}(b_1, \dots, b_{n-1})$. Soit $u = \tilde{u} + u_n b_n$ un autre vecteur de $\mathcal{L}$. Par Pythagore, on a $\|t - u\|^2 = \|\tilde{t} - \tilde{u}\|^2 + (t_n - u_n)^2 \cdot \|b_n\|^2$. L'hypothèse de récurrence donne que le premier terme de la somme est plus grand que $\|\tilde{t} - \tilde{s}\|^2$, et par définition du plus proche entier, $|t_n - u_n| \geq |t_n - \lceil t_n \rfloor|$. De nouveau par Pythagore, on conclut que $\|t - u\| \geq \|t - s\|$, ce qu'on voulait.

2 (1) Comme $V_{i+1} = V_i \perp \mathbb{R} \cdot b_{i+1}^*$, on peut écrire $\mathbf{t} = t_{i+1} b_{i+1}^* + v$ avec $v \in V_i$ et $t_i \in \mathbb{R}$. Si $z = \sum_{j \leq i+1} z_j b_j \in \mathcal{L}(b_1, \dots, b_{i+1})$, notons que $V_i + z = V_i + z_{i+1} b_{i+1}$, et il suffit donc de regarder les translatés entiers de V_i le long de b_{i+1}. On a alors par translation et propriétés des projections orthogonales

$$\begin{aligned} d(t, V_i + z_{i+1} b_{i+1}) = d(t - z_{i+1} b_{i+1}, V_i) &= \|\pi_{\mathbb{R} b_{i+1}^*}(t - z_{i+1} b_{i+1})\| \\ &= \frac{|\langle t - z_{i+1} b_{i+1}, b_{i+1}^* \rangle|}{\|b_{i+1}^*\|} \\ &= |t_{i+1} - z_{i+1}| \cdot \|b_{i+1}^*\|, \end{aligned}$$

la dernière ligne venant de l'orthogonalité de b_{i+1}^* avec V_i. C'est donc bien $\lceil t_{i+1} \rfloor b_{i+1}$ qui donne l'hyperplan le plus proche de t parmi les translatés de V_i le long de b_{i+1}.

(2) Bien qu'on trouve l'hyperplan le plus proche de la cible à chaque étape, il est tout à fait possible que cet hyperplan ne contienne pas le plus proche vecteur du réseau. Il faut donc distinguer ces deux cas lorsqu'on étudie l'algorithme.

(3) Il s'agit justement du cas où l'algorithme ne prend pas le bon hyperplan. La question précédente impliquant que $d(t, V_i + y) \leq \|b_{i+1}^*\|/2$, on a donc nécessairement $\|t - u\| > \|b_{i+1}^*\|/2$.

(4) C'est le bon cas pour la qualité, mais le cas plus compliqué pour la preuve. Un dessin permet de se rendre compte de l'instance de dimension plus basse qui est intéressante. Soit t' la projection orthogonale de t sur l'hyperplan affine $V_i + y$. Par orthogonalité, on a $\|t - u\|^2 = \|t - t'\|^2 + \|t' - u\|^2$, ce qui implique que u est un vecteur de $\mathcal{L}$ le plus proche de $t' \in V_i + y$. De manière équivalente, $s - y$ est un plus proche vecteur de $t' - y \in V_i$: on a réduit la dimension de 1.

(5) Dans l'esprit de l'exercice précédent, il s'agit en fait de montrer que $e = e_1$ est dans le domaine fondamental recentré associé aux $\widetilde{b_i}$. Notons qu'à chaque étape de l'algorithme, on a $s + e_i = t$, et montrons qu'à chaque étape,

$$\left| \frac{\langle e_i, b_j^* \rangle}{\|b_j^*\|^2} \right| \leq \frac{1}{2}, \text{ si } j \geq i.$$

Notons $t = \sum_i t_i b_i^*$, de sorte que $e_n = t - \lceil t_n \rfloor b_n$. En utilisant la définition des Gram-Schmidt, et la notation du cours μ_{ij}, on peut alors écrire

$$\begin{aligned} e_n &= \sum_{i=1}^{n} t_i b_i^* - \lceil t_n \rfloor \cdot (b_n^* + \sum_{i=1}^{n-1} \mu_{ni} b_i^*) \\ &= \sum_{i=1}^{n-1} (t_i - \mu_{ni}) b_i^* + (t_n - \lceil t_n \rfloor) b_n^*, \end{aligned}$$

et on a bien $|t_n - \lceil t_n \rfloor| \leq \frac{1}{2}$. Supposons maintenant que la propriété est vraie pour e_{i+1}. Par construction des Gram-Schmidt, b_i est orthogonal à b_j^* pour tout $j > i$, et donc soustraire un multiple de b_i à un vecteur n'agit pas sur ses dernières $n - i + 1$ coordonnées dans la base des b_i^*. Autrement dit, avec $e_i = e_{i+1} - c_i b_i$, on sait que $\langle e_i, b_j^* \rangle = \langle e_{i+1}, b_j^* \rangle$ si $j > i$, et on observe ensuire que

$$\langle e_i, b_i^* \rangle = \langle e_{i+1}, b_i^* \rangle - c_i \|b_i^*\|^2.$$

On obtient l'inégalité attendue par définition des c_i. L'algorithme renvoie donc $e = \sum_i e_i b_i^*$ avec $|e_i| < 1/2$, et il vient $\|e\|^2 \leq \frac{1}{4} \sum_i \|b_i^*\|^2$ par orthogonalité, ce qui conclut.

(6) Les propriétés des bases réduites donnent que $\frac{1}{2}\|b_i^*\|^2 \leq \|b_{i+1}^*\|^2$, qu'on étend en $\|b_j^*\|^2 \leq 2^{i-j}\|b_i^*\|^2$ pour $1 \leq j < i \leq n$. Donc, si Nearest Plane se trompe d'hyperplan dans V_{i+1}, alors il renvoie $s \in V_{i+1}$ tel que

$$\|t - s\|^2 \leq \frac{\|b_{i+1}^*\|^2}{4} \cdot \sum_{j=1}^{i+1} 2^{i+1-j} \leq 2^{i-1} \cdot \|b_{i+1}^*\|^2.$$

(7) D'après la question (3), on a alors $\|b_{i+1}^*\| \leq 2d(t, \mathcal{L})$, ce qui donne le résultat.

(8) On commence donc par réduire la base avec LLL, en temps polynomial, puis on utilise Nearest Plane. A l'étape i, ou bien l'hyperplan choisi contient le plus proche vecteur u, ou bien non. Dans le second cas, on a gagné d'après la question (6). Dans le premier cas, la question (4) nous ramène à une instance $t' - y$ dans $\mathcal{L}(b_1, \ldots, b_i)$, et on rappelle que $u - y$ est aussi un plus proche vecteur de $t' - y$ dans $\mathcal{L}(b_1, \ldots, b_i)$. Supposons par récurrence que Nearest Plane nous renvoie s' tel que $\|t' - y - s'\| \leq 2^{i/2} \cdot \|t' - u\|$. L'algorithme construit ensuite $s = s' + y$, ce qui nous permet d'écrire

$$\begin{aligned} \|s - t\|^2 = \|s' + y - t\|^2 &= \|s' + y - t'\|^2 + \|t - t'\|^2 \\ &\leq 2^i \|t' - u\|^2 + \|t - t'\|^2, \end{aligned} \tag{1}$$

où la deuxième inégalité s'obtient par orthogonalité et la seconde par hypothèse de récurrence. On a vu à la question (4) que lorsque $u \in V_i + y$, alors $\|t - u\|^2 = \|t' - u\|^2 + \|t - t'\|^2$, donc chaque terme de la somme de droite est plus petit que le terme de gauche. On en déduit dans (1) que $\|t - s\|^2 \leq (2^i + 1) \cdot d(t, \mathcal{L})$, ce qui donne le résultat annoncé.