Réduction de réseau (ENS 2002)[1]

$E = \mathbf{R}^2$ est muni de sa structure euclidienne canonique. Un *réseau* est une partie de E de la forme $G = \{\lambda\mathbf{u} + \mu\mathbf{v} \mid \lambda, \mu \in \mathbf{Z}\}$ où $(\mathbf{u}, \mathbf{v})$ est une base de E; $(\mathbf{u}, \mathbf{v})$ est alors appelée une *base* du réseau G.

1. *Analyser l'algorithme suivant:*

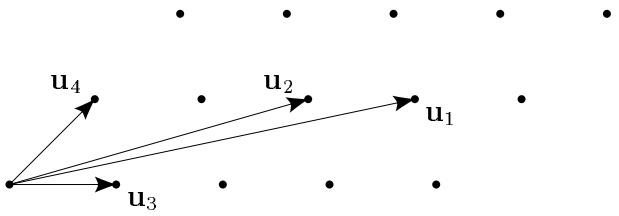
```
1  soit récursivement Gauss(u, v) =
2   (* (u, v) est une base d'un réseau G telle que ||u|| ⩾ ||v|| *)
3        q ← ⌊⟨v|u⟩/||v||² + 1/2⌋
4        w ← u − qv
5        si ||w|| ⩾ ||v|| alors
6             renvoyer (w, v)
7        sinon
8             renvoyer Gauss(v, w)
```

2. *Etudier le problème de trouver un point x' de G le plus proche d'un point donné x de E.*

Corrigé

1. En ligne 3, q est l'entier (ou l'un des deux entiers) le plus proche de $a = \langle\mathbf{v}|\mathbf{u}\rangle/\|\mathbf{v}\|^2$. Le vecteur $\mathbf{u} - a\mathbf{v}$ est la projection de $\mathbf{u}$ sur $\mathbf{v}^\perp$; c'est donc le vecteur de norme minimum de la droite $\mathbf{u} + \mathrm{Vect}(\mathbf{v})$. Le vecteur $\mathbf{w}$ défini ligne 4 est un vecteur de norme minimum de $G \cap (\mathbf{u} + \mathrm{Vect}(\mathbf{v}))$; en effet, si $\lambda \in \mathbf{Z}$, la quantité $\|\mathbf{u} - \lambda\mathbf{v}\|^2 = \mathbf{v}^2(\lambda - a)^2 + \mathbf{u}^2 - a^2\mathbf{v}^2$ est minimum pour $\lambda = q$.

Sur la figure suivante, $\mathbf{u}$, $\mathbf{v}$ et $\mathbf{w}$ sont appelés respectivement $\mathbf{u}_1$, $\mathbf{u}_2$ et $\mathbf{u}_3$.



L'algorithme termine. En effet, lors de l'appel récursif $Gauss(\mathbf{v}, \mathbf{w})$, la norme de $\mathbf{w}$ est $<$ à celle du vecteur $\mathbf{v}$ de l'appel principal $Gauss(\mathbf{u}, \mathbf{v})$; or tous les vecteurs considérés appartiennent au groupe discret G de sorte qu'un ensemble borné ne contient qu'un nombre fini de points de G. On vérifie que G est discret en notant que si $(\mathbf{u}, \mathbf{v})$ en est une base, alors $\| \ \| \geqslant kN$ où N est la norme euclidienne associée au produit scalaire sur E pour lequel $(\mathbf{u}, \mathbf{v})$ est une base orthonormale, donc, pour tout $\mathbf{x} = \lambda\mathbf{u} + \mu\mathbf{v} \in G \setminus \{0\}$, $\|\mathbf{x}\| \geqslant kN(\mathbf{x}) = k\sqrt{\lambda^2 + \mu^2} \geqslant k$.

Par exemple, sur la figure, $Gauss(\mathbf{u}_1, \mathbf{u}_2)$ donne lieu à l'appel récursif $Gauss(\mathbf{u}_2, \mathbf{u}_3)$ qui renvoie $(\mathbf{u}_4, \mathbf{u}_3)$.

Le couple $(\mathbf{u}, \mathbf{v})$ retourné par l'algorithme est une base de G et vérifie

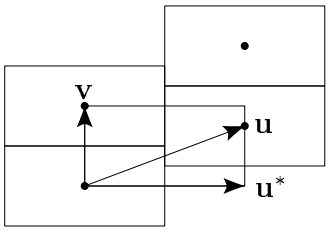
$$\|\mathbf{u}\| \geqslant \|\mathbf{v}\| \text{ et } \|\mathbf{u}\| = \min_{\lambda \in \mathbf{Z}} \|\mathbf{u} - \lambda\mathbf{v}\|.$$

1. D'après `http://pauillac.inria.fr/~quercia/papers/lll.tgz`

On en déduit que $|2\langle \mathbf{u}|\mathbf{v}\rangle| \leqslant \mathbf{v}^2$ puis que, pour tout $\mathbf{x} = \lambda\mathbf{u} + \mu\mathbf{v} \in G \setminus \{0\}$, $\mathbf{x}^2 = \lambda^2\mathbf{u}^2 + \mu^2\mathbf{v}^2 + 2\lambda\mu\langle \mathbf{u}|\mathbf{v}\rangle \geqslant (\lambda^2 + \mu^2 - |\lambda\mu|)\mathbf{v}^2 \geqslant \mathbf{v}^2$.

$\mathbf{v}$ est donc un vecteur non nul de G de norme minimum.

2. On utilise la base $(\mathbf{u}, \mathbf{v})$ trouvée par l'algorithme de Gauss. Soit $\mathbf{u}^*$ le projeté de $\mathbf{u}$ sur $\mathbf{v}^\perp$. Le rectangle R centré à l'origine et construit sur $(\mathbf{u}^*, \mathbf{v})$ pave l'espace E selon G; c.-à-d. que tout point x de E appartient à un translaté de R centré en un point de G. On en déduit la majoration $d^2(\mathbf{x}, G) \leqslant \frac{1}{4}\left(\mathbf{u}^{*2} + \mathbf{v}^2\right)$.



Or $\mathbf{u}^* = \mathbf{u} - \dfrac{\langle \mathbf{u}|\mathbf{v}\rangle}{\mathbf{v}^2}\mathbf{v}$; donc, à l'aide de $\|\mathbf{u}\| \geqslant \|\mathbf{v}\|$ et $|2\langle \mathbf{u}|\mathbf{v}\rangle| \leqslant \mathbf{v}^2$, il vient $\mathbf{u}^{*2} = \mathbf{u}^2 - \dfrac{\langle \mathbf{u}|\mathbf{v}\rangle^2}{\mathbf{v}^2} \geqslant \mathbf{v}^2 - \dfrac{\mathbf{v}^2}{4} = \dfrac{3}{4}\mathbf{v}^2$, puis $d^2(\mathbf{x}, G) \leqslant \dfrac{7}{12}u^{*2}$.

Soit maintenant $\mathbf{x} = \lambda\mathbf{u} + \mu\mathbf{v} \in E$; $\lambda, \mu \in \mathbf{R}$. Si $\mathbf{x}' = \lambda'\mathbf{u} + \mu'\mathbf{v}$ est un point de G le plus proche de $\mathbf{x}$, alors λ et λ' sont aussi les composantes de $\mathbf{x}$ et $\mathbf{x}'$ sur $\mathbf{u}^*$ dans la base orthogonale $(\mathbf{u}^*, \mathbf{v})$. Donc $(\lambda - \lambda')^2\mathbf{u}^{*2} \leqslant \|\mathbf{x} - \mathbf{x}'\|^2 \leqslant \dfrac{7}{12}u^{*2}$, puis $|\lambda - \lambda'| < 0,8$. Ou bien cette condition détermine λ', ou bien les seules valeurs possibles de λ' sont $\lfloor\lambda\rfloor$ ou $\lceil\lambda\rceil$. Pour chacune de ces valeurs de λ', il est alors facile de calculer le μ' optimal.