Formes quadratiques unimodulaires réduites en petite dimension

Denis SIMON
LMNO - UMR 6139 Université de Caen – France
Campus II – Boulevard Mal Juin
BP 5186 – 14032 Caen Cedex
Courriel :simon@math.unicaen.fr

11 mai 2005

Résumé

Dans un précédent article ([2]), nous avons donné un algorithme pour la réduction des formes quadratiques entières indéfinies. Nous montrons ici que la qualité de cette réduction est meilleure que celle annoncée. En particulier, nous montrons que l'algorithme réduit complètement les formes quadratiques unimodulaires de dimension $n \leqslant 7$, et qu'il permet de résoudre toutes les équations quadratiques unimodulaires de dimension $n \leqslant 9$.

Dans [2], nous avons proposé un algorithme très proche de l'algorithme LLL (voir [1, §2.6]), pour la réduction des formes quadratiques entières indéfinies. Nous avons vu que cet algorithme pouvait servir pour la résolution des équations quadratiques unimodulaires en dimension $n \leqslant 6$. La résolution dans le cas unimodulaire en dimension $n = 3$ nous avait permis de résoudre le cas non unimodulaire en dimension $n = 3$.

Notre objectif, dans cette note, est de montrer que l'algorithme de [2] permet en réalité de résoudre les équations quadratiques unimodulaires en dimension $n \leqslant 9$: nous montrons cela avec les théorèmes 5 et 6. Pour cela, nous allons dresser la liste complète des sorties possibles de l'algorithme. Cette amélioration nous permettra, dans un prochain article ([3]), de donner un algorithme efficace pour la résolution de toutes les équations quadratiques, de déterminant quelconque, et de dimension $n \geqslant 4$.

Notations : On note $S_n(\mathbb{Z})$ l'ensemble des matrices carrées symétriques d'ordre n, à coeffcients dans $\mathbb{Z}$. Soit $Q \in S_n(\mathbb{Z})$, on note $d = d(Q) = (d_1, \ldots, d_n)$ le n-uplet formé des mineurs d'ordre $1, \ldots, n$ extraits dans le coin en haut à gauche de Q : $d_k = \det((Q_{i,j})_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant k})$. Par convention, on note $d_0 = 1$. En particulier, on a $d_k \in \mathbb{Z}$ pour tout k, et $d_n = \det Q$. Lorsque les d_k sont non nuls, on note $\mathbf{b}^{*2} = (\mathbf{b}_1^{*2}, \ldots, \mathbf{b}_n^{*2}) = \left(\frac{d_1}{d_0}, \ldots, \frac{d_n}{d_{n-1}}\right)$. Les coefficients $\mathbf{b}_k^{*2}$ sont exactement les coefficients diagonaux de l'orthogonalisée de Gram-Schmidt de Q. Ces notations sont identiques à celles utilisées dans [1, §2.6] et [2]. On remarque que lorsque Q est définie positive (resp. négative), les coefficients $\mathbf{b}_k^{*2}$ sont tous positifs (resp. négatifs). Lorsque

Q est indéfinie, de signature (r, s), il y en a r qui sont positifs, et s négatifs. On note alors $\mid d \mid = (\mid d_1 \mid, \ldots, \mid d_n \mid)$, et $\mid \mathbf{b}^{*2} \mid = (\mid \mathbf{b}_1^{*2} \mid, \ldots, \mid \mathbf{b}_n^{*2} \mid)$.

1 Bornes sur $\mid d \mid$ à la sorite de l'algorithme

L'algorithme 1.3 de [2], permet la réduction des formes quadratiques entières indéfinies, et la qualité de sa sortie est donnée par le résultat suivant :

Théorème 1 *Soit $Q \in S_n(\mathbb{Z})$ de déterminant $d_n \neq 0$. En appliquant l'algorithme 1.3 de [2], avec un paramètre réel c, $\frac{1}{4} < c < 1$, on trouve soit un zéro de Q, soit un changement de base de $\mathbb{Z}^n$ tel que, dans la nouvelle base, on ait pour tout entier k, $1 < k \leqslant n$,*

$$\mid \mathbf{b}_{k-1}^{*2} \mid \leqslant \gamma \mid \mathbf{b}_k^{*2} \mid \tag{1}$$

et

$$1 \leqslant \mid \mathbf{b}_1^{*2} \mid^n \leqslant \gamma^{n(n-1)/2} \mid d_n \mid \tag{2}$$

avec $\gamma = \left(c - \frac{1}{4}\right)^{-1} > \frac{4}{3}$. Si, de plus, Q est indéfinie, on a

$$1 \leqslant \mid \mathbf{b}_1^{*2} \mid^n \leqslant \frac{3}{4}\gamma^{n(n-1)/2} \mid d_n \mid . \tag{3}$$

La dernière relation était prouvée de la manière suivante : si Q est indéfinie, alors il existe au moins un entier k, $1 < k \leqslant n$, tel que $\mathbf{b}_{k-1}^{*2}$ et $\mathbf{b}_k^{*2}$ soient de signes opposés. Dans ce cas, on avait montré dans [2] l'inégalité

$$\mid \mathbf{b}_{k-1}^{*2} \mid \leqslant \mid \mathbf{b}_k^{*2} \mid . \tag{4}$$

On peut traduire les inégalités du théorème 1 en fonction des entiers d_k, en particulier

$$d_{k-1}^2 \leqslant \gamma \mid d_k d_{k-2} \mid \tag{5}$$

Pour les applications données dans [2], ces inégalités étaient suffisantes, mais ici, il nous en faut davantage. En particulier, on veut des bornes pour $d_1, d_2, \ldots, d_{n-1}$.

Proposition 2 *Dans les conditions identiques à celles du théorème 1, on pose, pour tout entier k, $0 \leqslant k \leqslant n$, $c_k = \gamma^{k(k-n)/2} \mid d_k \mid\mid d_n \mid^{-k/n}$. La suite $\log c_k$ est convexe, et elle vérifie $c_k \leqslant 1$ pour tout $0 \leqslant k \leqslant n$.*

Preuve : L'inégalité (5) s'écrit $c_k^2 \leqslant c_{k-1}c_{k+1}$, ce qui signifie que $\log c_k$ est une suite convexe. De plus, par définition, on a $c_0 = c_n = 1$, donc par convexité, on obtient $c_k^n \leqslant c_0^{n-k} c_n^k \leqslant 1$. ■

Corollaire 3 *Si c, n et d_n sont fixés, il n'existe qu'un nombre fini de valeurs possibles pour le n–uplet $\mid d \mid$ correspondant à la sortie de l'algorithme 1.3 de [2]. Ces n–uplets satisfont*

$$\mid d_k \mid \leqslant \gamma^{k(n-k)/2} \mid d_n \mid^{k/n} \tag{6}$$

Preuve : L'inégalité (6) est la traduction directe de $c_k \leqslant 1$. Comme les d_k sont des entiers, ceci montre déjà qu'il n'y a qu'un nombre fini de possibilités pour $\mid d \mid$. Parmi ces possibilités, il faut encore supprimer celles qui ne satisfont pas les inégalités (5). ■

Pour illustrer ce corollaire, nous allons dresser la liste de tous les n–uplets $\mid d \mid$ satisfaisant les relations (5) et (6), dans le cas unimodulaire ($\mid d_n \mid = 1$), et pour les dimensions n comprises entre 2 et 9. Ces listes s'obtiennent rapidement avec un petit programme sur ordinateur. Nous indiquons la valeur utilisée pour le paramètre c.

Pour $n \leqslant 5$, on trouve

$$\begin{array}{llll} n=2 & (c>1/2) & \mid d \mid = (1,1) \\ n=3 & (c>3/4) & \mid d \mid = (1,1,1) \\ n=4 & (c>3/4) & \mid d \mid = (1,1,1,1) \\ n=5 & (c>11/12) & \mid d \mid = (1,1,1,1,1) \end{array}$$

Ces valeurs numériques signifient que l'algorithme de réduction des formes quadratiques définies ou indéfinies permet toujours, soit de trouver un zéro des formes quadratiques unimodulaires, soit de les réduire à une forme diagonale à coefficients ± 1. Pour $n \leqslant 5$, ces résultats sont la traduction directe du théorème 1.6 de [2], avec des meilleures valeurs du paramètre c. La diminution de la valeur de c augmente la rapidité de l'algorithme.

Pour $n = 6$, et $c > 11/12$, on trouve encore $\mid d \mid = (1,1,1,1,1,1)$. Ceci prouve que le théorème 1.8 de [2] est encore vrai sans supposer que la forme soit indéfinie. De plus la valeur du paramètre c est diminuée.

Pour $n = 7$ et $c > 11/12$, on trouve $\mid d \mid \in \{(1,1,1,1,1,1,1), (2,3,4,4,3,2,1)\}$.

Pour $n = 8$ et $c > 193/196$, on trouve

$$\begin{array}{ll} \mid d \mid \in \{ & (1,1,1,1,1,1,1,1), (1,2,3,4,4,3,2,1), \\ & (2,3,4,4,3,2,1,1), (2,3,4,4,4,3,2,1)\}. \end{array}$$

Enfin, pour $n = 9$ et $c > 193/196$, on trouve

$$\begin{array}{ll} \mid d \mid \in \{ & (1,1,1,1,1,1,1,1,1), (1,1,2,3,4,4,3,2,1), (1,2,3,4,4,3,2,1,1), \\ & (1,2,3,4,4,4,3,2,1), (2,3,4,4,3,2,1,1,1), (2,3,4,4,4,3,2,1,1), \\ & (2,3,4,4,4,4,3,2,1), (2,3,4,5,5,4,3,2,1), (2,4,6,7,7,6,4,2,1), \\ & (2,4,6,8,8,6,4,2,1)\}. \end{array}$$

On pourrait dresser des listes semblables pour $n = 10, 11, \ldots$ mais leur taille augmente assez rapidement.

2 Existence de formes quadratiques ayant un d donné

Dans cette partie, nous nous donnons un n–uplet fixé $d = (d_1, \ldots, d_n)$ d'entiers non nuls, et nous cherchons à construire les matrices $Q \in S_n(\mathbb{Z})$ telles que $d(Q) = d$. Il existe en général une infinité de telles matrices. Si U est une matrice $n \times n$ triangulaire supérieure à coefficients diagonaux ègaux à 1, la matrice $Q' = U^t Q U$ vérifie encore $d(Q') = d(Q)$. Modulo cette transformation, il n'existe qu'un nombre fini de $Q \in$

$S_n(\mathbb{Z})$ satisfaisant $d(Q) = d$. Nous donnons ici un algorithme récursif pour toutes les déterminer.

Si $n = 1$, une seule matrice convient : $Q = (d_1)$. Supposons maintenant que l'on sache construire toutes les matrices $Q' \in S_{n-1}(\mathbb{Z})$ vérifiant $d(Q') = (d_1, \ldots, d_{n-1})$. Pour chacune des matrices Q' de cette liste, on fait les opérations suivantes :

On considère les coefficients $Q_{1,n}, \ldots, Q_{n,n}$ comme des inconnues. Le vecteur $v = (Q_{1,n}, \ldots, Q_{n-1,n})^t$ n'est défini que modulo Q' (en effet, si on applique à Q un changement de base triangulaire supérieur, le vecteur v est transformé en $Q'X + v$, où X est un vecteur arbitraire à coefficients entiers). En considérant la forme normale d'Hermite de Q', on voit alors qu'il suffit de tester $\mid \det Q' \mid = \mid d_{n-1} \mid$ valeurs pour le vecteur v. Parmi ces $\mid d_{n-1} \mid$ valeurs, on ne garde que celles pour lesquelles l'équation $\det Q = d_n$ donne une valeur entière pour $Q_{n,n}$. Comme cette équation est linéaire en $Q_{n,n}$ de coefficient dominant $d_{n-1} \neq 0$, cela donne au plus une valeur de $Q_{n,n}$ pour chaque valeur de v.

Cet algorithme montre qu'il existe au plus $\mid \prod_{i<n} d_i \mid$ matrices Q (modulo les transformations triangulaires définies plus haut) satisfaisant $d(Q) = d$. En appliquant cet algorithme, on obtient par exemple le résultat suivant :

Lemme 4 *Il n'existe pas de $Q \in S_5(\mathbb{Z})$ telle que $d(Q) = (2, 3, 4, 4, 3)$.*

3 Énoncé des résultats

Théorème 5 *Soit n un entier, $2 \leqslant n \leqslant 7$. Soit $Q \in S_n(\mathbb{Z})$ de déterminant $d_n \neq 0$. En appliquant l'algorithme 1.3 de [2], avec un paramètre réel c, $\frac{11}{12} < c < 1$, on trouve soit un zéro de Q, soit un changement de base de $\mathbb{Z}^n$ tel que, dans la nouvelle base, Q soit diagonale à coefficients ± 1.*

Preuve : Si $n \leqslant 5$, on retrouve les résultats de [2]. Le cas $n = 6$ a été montré dans la partie 1. Si $n = 7$, d'après la partie 1, il suffit de prouver que l'on ne peut pas terminer avec $\mid d(Q) \mid = (2, 3, 4, 4, 3, 2, 1)$. Supposons que l'on termine avec une telle matrice. Alors, on a $\mid \mathbf{b}^{*2} \mid = (2, \frac{3}{2}, \frac{4}{3}, 1, \frac{3}{4}, \frac{2}{3}, \frac{1}{2})$. Comme ces valeurs sont strictement décroissantes, la relation (4) montre que Q est définie. Quitte à considérer $-Q$, on peut toujours supposer qu'elle est définie positive, et donc $d(Q) = (2, 3, 4, 4, 3, 2, 1)$. En extrayant le premier bloc 5×5 de Q, on aurait alors une matrice $Q' \in S_5(\mathbb{Z})$ qui contredirait le lemme 4. ■

Théorème 6 *Soit n un entier, $2 \leqslant n \leqslant 9$. Soit $Q \in S_n(\mathbb{Z})$ de déterminant $d_n \neq 0$. On suppose que Q est indéfinie. Si l'algorithme 1.3 de [2], appliqué à Q avec un paramètre réel c, $\frac{193}{196} < c < 1$, ne trouve pas de zéro de Q, alors il trouve une base $\mathbf{b}_1, \ldots, \mathbf{b}_n$ ayant la propriété suivante :*

Il existe un zéro de Q parmi les vecteurs $\mathbf{b}_i^* + \mathbf{b}_j^*$, où $(\mathbf{b}_i^*)$ est la base de Gram-Schmidt associée à la base $(\mathbf{b}_i)$.

Preuve : Supposons que l'on n'ait pas trouvé de zéro de Q. Notons encore Q la matrice dans la nouvelle base. Nous avons choisi les notations de telle sorte que l'on ait $\mathbf{b}_i^{*t} Q \mathbf{b}_i^* = \mathbf{b}_i^{*2}$. Il suffit donc de montrer que pour cette matrice réduite Q, le n–uplet

$\mathbf{b}^{*2}$ contient deux coefficients opposés. Si $n \leqslant 7$, alors d'après le théorème 5, on a $|\ \mathbf{b}^{*2}\ | = (1, \dots 1)$. Or, Q est indéfinie, donc $\mathbf{b}^{*2}$ contient au moins un changement de signe, d'où le résultat. Supposons que $n = 8$. D'après la partie 1, et le lemme 4, on a $|\ d\ | \in \{(1,1,1,1,1,1,1,1), (2,3,4,4,4,3,2,1)\}$. Dans le premier cas, la conclusion est immédiate. Dans le deuxième cas, on a $|\ \mathbf{b}^{*2}\ | = (2, \frac{3}{2}, \frac{4}{3}, 1, 1, \frac{3}{4}, \frac{2}{3}, \frac{1}{2})$. Or, Q est indéfinie, et l'inégalité (4) montre que $\mathbf{b}^{*2} = \pm(2, \frac{3}{2}, \frac{4}{3}, 1, -1, -\frac{3}{4}, -\frac{2}{3}, -\frac{1}{2})$. Mais alors $\mathbf{b}_4^* + \mathbf{b}_5^*$ est un zéro de Q. On traite tous les cas de la dimension $n = 9$ de la même manière. ■

Références

[1] H. Cohen : *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math. **138**, Third corrected printing, Springer–Verlag (1996).

[2] D. Simon : *Solving quadratic equations using reduced unimodular quadratic forms*, Math. Comp., vol 74 no 251 (2005), 1531–1543.

[3] D. Simon : *Quadratic equations in dimension* 4, 5*, and more*, préprint (2005).