

MATHÉMATIQUES

GÉOMÉTRIE ET ORDINATEURS (I) DROITES, CERCLES, PARABOLES

Jean-Pierre REVEILLÈS
LLAIC1, Université d'Auvergne
jprev@llaic.u-clermont1.fr

1 – Géométrie et virgule flottante

L'ARITHMÉTIQUE flottante des ordinateurs a été essentiellement mise au point pour traiter des problèmes relevant de l'analyse. Dans ce système de calcul qui n'utilise qu'un nombre fini de nombres décimaux, les équations usuelles ou comparaisons n'ont plus de sens et sont généralement remplacées par des *inéquations*.

Si cette modification s'adapte malgré tout assez bien à l'analyse numérique, c'est parce que cette discipline dispose de nombreux théorèmes de continuité donnant des approximations aussi bonnes qu'on veut des grandeurs désirées : limites de suites, valeurs d'intégrales, extréma, zéros de fonctions, solutions d'équations différentielles ou aux dérivées partielles.

Mais si l'arithmétique flottante n'est pas une gêne insurmontable pour l'analyse numérique, elle en est une en géométrie ou en algèbre. La factorisation des polynômes, par exemple, n'est pas un phénomène continu : une petite perturbation peut changer complètement le résultat. C'est aussi le cas en géométrie : même si une surface est une entité régulière, la topologie de ses sections peut changer brutalement quand on *traverse* une valeur critique. Connaître un plan de section approximativement peut être inacceptable dans certaines applications en CAO (conception assistée par ordinateur) et en FAO (fabrication assistée par ordinateur)

par exemple. Des questions apparemment simples posent déjà des problèmes (alignement de 3 points, appartenance d'un point à une droite, calcul du rang d'une famille de vecteurs) et sont impossibles à traiter dans le système de calcul à virgule flottante.

Les difficultés de ce type sont à l'origine de nombreux travaux destinés à construire d'autres systèmes de calcul. Malheureusement la nature *finitiste* des ordinateurs rend cette tâche insurmontable malgré les prolongements de travaux historiques précurseurs, (en particulier la *Théorie des Corps* de David Hilbert), qui ont abouti à l'avènement du calcul formel et de la théorie de la démonstration automatique. Bien que ces théories, appuyées par l'algorithmique algébrique des *bases de Gröbner* aient contribué à rapprocher la géométrie et l'informatique, cette forme de discrétisation de la géométrie est très éloignée des discrétisations provoquées par les appareils d'acquisition ou d'affichage. Elles n'évacuent pas le souhait d'un système adapté aux nombreuses discrétisations de la géométrie provoquées par l'emploi des ordinateurs.

2 – Géométrie discrète ou numérique

Un très grand nombre de disciplines scientifiques ont besoin de traiter des concepts géométriques par le biais de l'ordinateur : CAO, modélisation géométrique, géométrie algorithmique, analyse, traitement et synthèse d'images, imagerie médicale, systèmes périphériques, parallélisme. Même si cette obligation apparaît sous des formes très diverses, les difficultés ou les impasses rencontrées dues à l'arithmétique flottante sont très souvent irrémédiables : incohérences, pertes d'information, plantages. Les résoudre suppose d'examiner leur traduction effective dans le système de calcul numérique employé. Réparer l'arithmétique flottante est une tâche insurmontable (et se heurtant à des résultats d'indécidabilité connus des informaticiens), si l'on veut obtenir une géométrie numérique générale analogue à l'analyse du même nom.

Les efforts des chercheurs intéressés dans le traitement de notions géométriques en machine se regroupent en deux courants essentiels : le courant pragmatique du *tout-voxel* et le courant théorique de la *construction des théories discrètes*. Pour les premiers des discrétisations assez fines de la réalité produisent des ensembles finis de données (pixels, voxels) auxquels les ordinateurs, eux aussi finis, s'adaptent de manière évidente, (cf [3], [9]). Cette approche est souvent inévitable si l'on doit traiter les données numériques fournies par des appareils de mesures : caméras CDD, scanners, etc. Elle a malheureusement l'inconvénient de nécessiter des ressources machine importantes pour traiter le volume colossal de

données engendrées, bien que les progrès technologiques constants permettent de considérer cette voie comme praticable dans un futur proche pour quelques applications.

Par contre un très grand nombre d'applications resteront toujours hors de portée de cette approche *tout voxel*, ce qui a conduit les *constructivistes* de cette communauté, à la suite des pionniers tels que Rosenfeld, Earnshaw, Bresenham, Bruckstein, Kong etc., (cf [1], [10], [14], [15], [16]), qui ont posé les premiers jalons de la *topologie discrète*, à essayer plutôt de dégager des résultats mathématiques généraux valables pour des objets discrets judicieusement définis. Des développements parallèles dans d'autres branches des mathématiques devraient aboutir à la constitution de véritables théories discrètes, la géométrie étant la plus attendue.

Ces constructivistes observent que les discrétisations données par la plupart des appareils d'acquisition sont des sous-ensembles bornés de \mathbb{Z} , \mathbb{Z}^2 , \mathbb{Z}^3 (voire \mathbb{Z}^4) assez *réguliers* dont il est assez tentant d'étudier les structures. La tentation est d'autant plus grande qu'on constate qu'ils interviennent par ailleurs : en physique dans la description de la matière cristallisée ou en mathématique (géométrie des nombres, convexité, optimisation entière entre autres). Il n'est pas déraisonnable d'essayer de dégager les propriétés *géométriques* de ces ensembles qui soient les plus proches de celles des ensembles continus. Quelques éléments de cette *géométrie discrète* sont présentés dans cet article. Pour traiter simultanément les aspects théoriques et numériques, deux piliers traditionnels de la géométrie sont modifiés : les équations sont abandonnées au profit des inéquations et les espaces euclidiens continus sont remplacé par les espaces discrets \mathbb{Z}^n . Par conséquent les objets fondamentaux de cette géométrie sont définis à l'aide d'*inéquations diophantiennes* (voir [4], [5], [12], [13]). Précisons que les inéquations de la géométrie discrète n'assurent pas à priori le contrôle des erreurs de calcul, comme c'est le cas en analyse numérique, mais celui de la topologie des objets introduits. Il est en effet indispensable que ceux-ci possèdent assez de points pour devenir *connexes* au sens des nouvelles topologies discrètes. C'est le choix du cadre arithmétique dans lequel est placée cette géométrie qui permet d'effectuer des *traitements numériques exacts*.

L'étude des versions discrètes des droites, plans, variétés, etc. définis dans \mathbb{Z}^n requiert l'emploi d'outils mathématiques classiques : arithmétique, groupes, équations et inéquations diophantiennes, combinatoire, optimisation entière. Les applications pratiques, qui sont la motivation de cette nouvelle approche de la géométrie, reçoivent une attention toute particulière, ce qui nécessite aussi d'aborder les questions *d'algorithmique*

et de *complexité* qui lui sont liées. On est donc conduit à prolonger certains travaux mathématiques comme ceux de Minkowski, Gauss, Hilbert, Klein, (en particulier à adapter le fameux *Programme d'Erlangen* de ce dernier) etc. mais aussi, de manière paradoxale, l'algorithme d'Euclide ainsi que ses versions plus récentes : fractions continues, bases de groupes etc. (voir les ouvrages [7], [8], [11], [17] pour ces notions classiques). Mais la notion classique certainement la plus utile pour cette théorie est l'interprétation géométrique du *théorème de Bézout* qui s'avère très fructueuse.

Ce premier article montre comment quelques résultats classiques de mathématique interviennent naturellement dans l'étude des propriétés d'objets discrets tels que droites, cercles et sphères. Il illustre également l'usage que l'on peut faire de ces nouvelles propriétés tant dans la pratique (les codes Maple de plusieurs algorithmes sont joints), que dans la compréhension de questions théoriques. Les objets discrets étudiés dans cette partie sont presque tous de dimension 2. Les sphères discrètes, introduites pour prolonger de manière évidente une propriété des cercles discrets, donnent un aperçu des objets de dimension 3 qui seront examinés dans la deuxième partie.

3 – Droites discrètes définition et reconnaissance

La simplicité de la ligne droite euclidienne disparaît totalement dès qu'on la discrétise. Reste-t-il d'ailleurs une notion mathématique digne d'intérêt après discrétisation ? Un objet discret analogue, ayant lui aussi un rôle fondamental, existe-t-il pour la géométrie discrète ? Dans le cas de la discrétisation du plan euclidien par le groupe \mathbb{Z}^2 , ce qui rend compte d'un très grand nombre de discrétisations pratiques, une définition raisonnable de ce qu'est une *droite discrète* s'énonce comme suit.

Définition 1. — Soient a, b, μ et $\omega \geq 0$ des entiers où a et b sont premiers entre eux. On appelle *droite discrète de vecteur normal* (a, b) , de *borne inférieure* μ et d'*épaisseur arithmétique* ω l'ensemble des points entiers (x, y) solutions de la double inéquation

$$(1) \quad \mu \leq ax + by < \mu + \omega.$$

Cette *droite*, notée $\mathcal{D}(a, b, \mu, \omega)$, n'est que l'ensemble des points entiers de la bande semi-ouverte définie par les droites usuelles d'équations $ax + by = \mu$ et $ax + by = \mu + \omega$. Les points entiers de la première droite appartiennent à $\mathcal{D}(a, b, \mu, \omega)$, ceux de la deuxième en étant exclus.

Il est commode d'appeler *pointillé* une droite discrète d'épaisseur arithmétique égale à 1, c'est à dire l'ensemble des solutions d'une équation diophantienne $ax + by = \mu$; on dit alors que μ est l'indice du pointillé. Le vecteur (u, v) tel que $au + bv = 1$ et $0 \leq u < |b|$ est appelé le *vecteur*

de Bézout du pointillé $ax + by = \mu$. La translation de ce pointillé selon son vecteur de Bézout donne le pointillé $ax + by = \mu + 1$, appelé *suivant* du pointillé d'indice μ . De nombreuses propriétés des droites et plans discrets sont contenues dans les références [4] et [12].

En pratique la représentation graphique d'une droite euclidienne sur un écran discret, fait souvent appel à de tels ensembles de points. Le cas particulier où $\omega = \max(|a|, |b|)$ — dit cas *naïf* — joue un rôle privilégié car les droites discrètes associées définissent une bijection de \mathbb{Z} dans lui-même. Ces dernières peuvent également être définies comme l'ensemble des points entiers les plus proches d'une droite euclidienne donnée. Cette propriété caractéristique des droites naïves explique bien leur intérêt, dès que de bonnes approximations discrètes des droites euclidiennes sont requises, mais s'avère insuffisante pour construire une théorie géométrique.

La notion précédente se généralise immédiatement au cas des hyperplans discrets définis par une double inéquation :

$$(2) \quad \mu \leq \vec{a} \cdot \vec{x} < \mu + \omega$$

où \vec{a} et \vec{x} sont deux vecteurs (entiers) de \mathbb{Z}^n , les entiers ω et μ étant comme ci-dessus.

Pour étayer un peu l'avantage de la définition (1) nous allons nous intéresser à un *problème inverse* discret à savoir celui de *retrouver les quatre paramètres d'une droite discrète à partir des coordonnées entières de certains de ses points*. De nombreux dispositifs digitaux transforment des droites, des plans ou des hyperplans en structures discrètes telles que celles définies par (2) ou par des inéquations diophantiennes plus générales. Retrouver les caractéristiques géométriques à partir des données discrètes est donc un problème pratique important. Reconnaître des segments de droites discrètes permet immédiatement de *polygonaliser* les courbes discrètes, ce qui est à l'origine de nombreuses applications pratiques (cf [4], [6]). On pourrait être tenté de croire que le problème précédent est très particulier et que les discrétisations données par l'instrumentation actuelle sont beaucoup plus générales. C'est partiellement vrai car bien que ces discrétisations portent sur des fonctions très souvent non-linéaires elles sont néanmoins suffisamment différentiables pour que ces discrétisations soient localement du type (2). Reconnaître des hyperplans locaux permet donc de trouver les gradients de ces fonctions.

Ce type de problème pourrait être abordé par la programmation linéaire entière mais il donnerait des calculs lourds et peut éclairants. Il est plus pertinent de chercher des algorithmes de nature géométrique fondés sur la structure même des objets considérés. Le reste du paragraphe sera

consacré au cas particulier des segments discrets naïfs ; on se rapportera à [4] pour des résultats sur la reconnaissance des plans discrets.

Plus précisément étant donné l'ensemble S des points entiers de \mathbb{Z}^2 situés sur le segment OM d'une droite discrète naïve $\mu \leq ax + by < \mu + b$ reconnue où l'on suppose $0 < -a < b$, et où 0 désigne l'origine des coordonnées et $M = (x, y)$, il s'agit de savoir si l'adjonction du point $N_1 = (x + 1, y)$ ou du point $N_2 = (x + 1, y + 1)$ forme encore avec OM un segment de droite discrète ou non, avec éventuellement changement de paramètres. Comme la pente $-a/b$ de la droite discrète supportant S est comprise entre 0 et 1 et comme l'épaisseur arithmétique ω est égale à b , la correspondance f qui définit y à partir de x est fonctionnelle de \mathbb{Z} dans \mathbb{Z} et est ici déterminée par $f : x \mapsto -\lfloor \frac{ax - \mu}{b} \rfloor$. L'observation des droites conduit à montrer que

$$\forall x \quad (0 \leq f(x + 1) - f(x) \leq 1).$$

Ceci implique que les deux positions possible de N pour incrémenter le segment S sont N_1 ou N_2 .

Le segment discret S ci-dessus contient au moins un point (x_0, y_0) vérifiant l'égalité $ax_0 + by_0 = \mu$ et au moins un point (x_1, y_1) vérifiant l'égalité $ax_1 + by_1 = \mu + b - 1$. On désigne par P le point de S d'abscisse minimale vérifiant l'équation $ax + by = \mu$ et par Q celui d'abscisse minimale vérifiant $ax + by = \mu + b - 1$; on dit que P (resp. Q) est le point d'appui inférieur (resp. supérieur) principal du segment S .

Posons $N = (x', y')$, on vérifie facilement le résultat suivant.

Théorème 1. — Soient la droite naïve $\mu \leq ax + by < \mu + b$ et $r = ax' + by'$, alors si

- $\mu \leq r < \mu + b$ l'ensemble $S \cup \{N\}$ est un segment de la droite discrète $\mathcal{D}(a, b, \mu, b)$, i.e. les caractéristiques sont les mêmes,
- $r = \mu - 1$ ou $r = \mu + b$, l'ensemble $S \cup \{N\}$ est un segment de la droite discrète $\mathcal{D}(a', b', \mu', b')$ avec un nouveau point d'appui supérieur principal Q' défini par $OQ' = ON + (-b, a + 1)$ et de nouvelles caractéristiques $(b', -a') = PN$ si $r = \mu - 1$ et $OP' = ON + (-b, a - 1)$, $(b', -a') = QN$ si $r = \mu + b$.
- $r < \mu - 1$ ou $r > \mu + b$, l'ensemble $S \cup \{N\}$ ne peut pas former un segment de droite discrète.

Dans le cas où $N = (x + 1, y)$ et $r = \mu - 1$, la nouvelle direction de la droite portant $S \cup \{N\}$ est celle du segment PN , i.e. on a $(b', -a') = PN$, et $\mu' = a'x_P + b'y_P$. On a un résultat analogue avec Q à la place de P si $N = (x + 1, y + 1)$. Plus précisément $(b', -a') = QN$ et $\mu' = a'x_Q + b'(y_Q - 1) + 1$. Chaque fois que la direction du segment change, l'un des deux points d'appui principaux se déplace : c'est le point d'appui

supérieur principal, noté Q , dans le premier cas, le point d'appui inférieur dans le deuxième.

Rappelons que le 4-voisinage d'un point $P = (x, y)$ de \mathbb{Z}^2 est l'ensemble des points $\{(x+1, y), (x, y+1), (x-1, y), (x, y-1)\}$. De même le 8-voisinage de P est l'ensemble $\{(x+1, y), (x+1, y+1), (x, y+1), (x-1, y), (x-1, y+1), (x-1, y-1), (x, y-1), (x+1, y-1)\}$. Une suite de points P_1, P_2, \dots, P_n de \mathbb{Z}^2 est une courbe 8-connexe si $\forall i \in [1, n-1]$, P_i et P_{i+1} sont 8-voisins, c'est-à-dire si chaque point appartient au 8-voisinage du point qui le suit dans l'énumération de 1 à n ; on a une définition analogue pour les courbes 4-connexes. Une partie A de \mathbb{Z}^2 est dite 8-connexe si deux points quelconques de A peuvent être reliés par une courbe discrète 8-connexe; une définition équivalente peut être donnée pour les parties 4-connexes. La figure 1 donne un exemple de chacun de ces types de courbe.

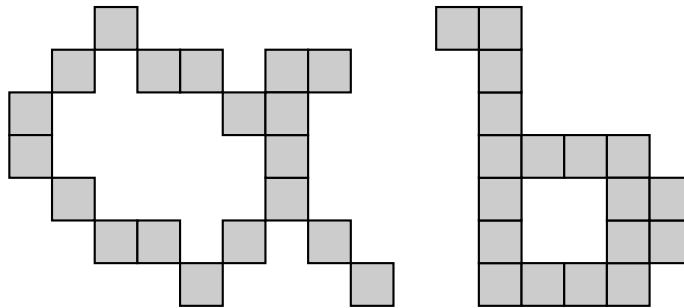


Figure 1. — La connexité des courbes discrètes

On en déduit facilement l'algorithme incrémental suivant de reconnaissance d'un segment discret, noté *Incr*, utilisé dans la procédure *Reco* donnée ci-dessous. Celle-ci peut servir à *polygonaliser* une courbe discrète 8-connexe à partir d'un point quelconque. On observe que, contrairement à ce qui se passe dans le continu, toute courbe *connexe* tracée sur un écran d'ordinateur est formée d'une suite de segments de droites discrètes; c'est donc toujours une ligne *polygonale*. En particulier elle est paramétrisable. Par contre il n'existe pas de polygonalisation canonique.

Il utilise la fonction booléenne *Incr* qui prend la valeur *vrai* si le segment discret défini par les variables globales a, b, x_P, y_P, x_Q, y_Q peut être prolongé par le point N .

```
Incr:=proc(N)
local d, r, mu:
global a, b, x, y:
```

```

mu := a * xP + b * yP;
r := a * N[1] + b * N[2];
d := evalb(r ≥ mu - 1 and r ≤ mu + b);
if d then
  if r = mu - 1 then
    xQ := N[1] - b; yQ := N[2] + a + 1;
    a := yP - N[2]; b := N[1] - xP;
  elif r = mu + b then
    xP := N[1] - b; yQ := N[2] + a - 1;
    a := yQ - N[2]; b := N[1] - xQ
  fi
fi;
end;

```

La procédure *Reco* analyse une courbe discrète 8-connexe et rend les paramètres du premier segment discret rencontré.

```

Reco:=proc(C)
local i, d;
global a, b, x, y;
a := 0; b := 1;
x[P] := C[1][1]; y[P] := C[1][2];
x[Q] := C[1][1]; y[Q] := C[1][1];
i := 2;
while i < nops(C) and Incr(C[i]) = 'true'
do i := i + 1 od;
[a, b, x[P], y[P], x[Q], y[Q]]
end;

```

4 – Enveloppe convexe des cercles discrets

La plupart des applications concrètes nécessitant un calcul d'enveloppe convexe de points peuvent se contenter d'un résultat *approximatif* résultant de l'imperfection des données et des erreurs de calculs causés par l'arithmétique flottante. L'exécution des algorithmes classiques de convexité dans ce système de calcul ne peut pas donner le résultat de manière certaine et il n'est pas possible de corriger ce défaut en augmentant la précision puisque le *nombre de sommets* de l'enveloppe n'est pas une fonction continue du rayon du cercle. Si l'on s'intéresse à l'obtention exacte de cette structure, il est indispensable de disposer d'algorithmes fonctionnant sur d'autres principes.

Ce problème va être traité en *effectuant uniquement des calculs arithmétiques, donc exacts, sur les coordonnées entières des points donnés.*

Cercles et sphères discrets sont définis de manière analogue aux droites ou plans discrets précédents, c'est-à-dire comme l'ensemble des points entiers respectivement contenus dans une couronne euclidienne circulaire ou sphérique de rayons extrêmes $R - \frac{1}{2}$ et $R + \frac{1}{2}$, où R est entier. On désignera par \mathcal{C}_R et \mathcal{S}_R le cercle et la sphère discrets ainsi définis.

Traitons d'abord le cas des cercles discrets. L'algorithme en pseudo-code suivant donne la partie du bord 8-connexe de \mathcal{C}_R contenue dans l'octant $0 \leq x \leq y$. On obtient le tracé complet par les symétries évidentes. La procédure $point(x, y)$ affiche un point en coordonnées (x, y) .

```

 $x = 0; y = R; temp = R^2 + R$ 
répéter
   $point(x, y);$ 
   $temp = temp + 2x + 1;$ 
   $x = x + 1;$ 
  si  $temp \geq R^2 + R + 1$ 
    alors
       $temp = temp - 2y + 1; y = y - 1$ 
    fin si
jusqu'à  $x \geq y$ 

```

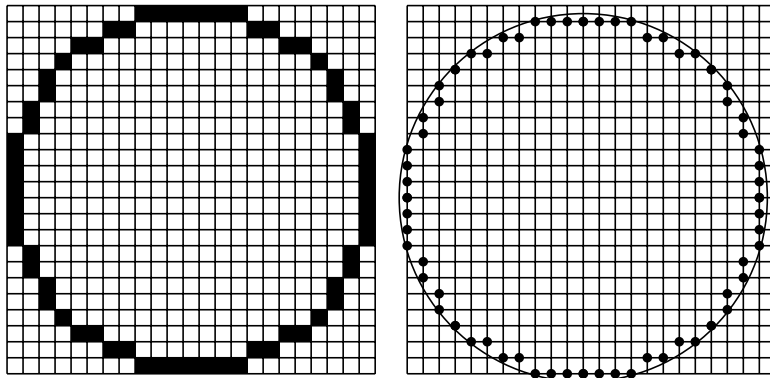


Figure 2. — Le cercle discret de rayon 11

Plusieurs types d'algorithmes robustes peuvent être développés pour des ensembles de points tels que \mathcal{C}_R . Ici nous allons montrer qu'il y a là encore une structure arithmétique sous-jacente à cette géométrie, celle-ci étant contenue dans les propriétés bézoutiennes du réseau \mathbb{Z}^2 ; (les références [8] et [17] présentent les aspects théoriques et concrets des ces notions).

Plus précisément si M et N sont deux points de \mathcal{C}_R , nous allons montrer qu'il est possible de caractériser arithmétiquement les cordes MN qui appartiennent à l'enveloppe convexe réelle de \mathcal{C}_R .

On désigne par $\{\frac{\mu}{\nu}\}_\rho$ le *plus petit reste* de la division euclidienne de l'entier μ par l'entier ν , i.e. l'unique entier ε vérifiant $-\frac{1}{2}\nu \leq \varepsilon < \frac{1}{2}\nu$ pour lequel il existe un quotient entier θ vérifiant

$$\mu = \nu\theta + \varepsilon.$$

Nous nous intéressons aux cordes extrémales d'un cercle discret. Commençons par observer un exemple avec le cercle discret \mathcal{C}_R de rayon 25. Considérons les pointillés associés à la direction d'une corde MN du cercle discret \mathcal{C}_R d'extrémités M et N comme sur la figure 4 ainsi que ceux de la direction orthogonale.

Les coordonnées des points M et N étant respectivement $(5, 25)$ et $(11, 23)$, la corde MN représentée sur la figure 4 est une partie du pointillé d'équation $x + 3y = 80$. Pour des raisons évidentes on dira que celui d'équation $x + 3y = 81$ est le pointillé *suivant* MN . On voit que la corde MN est une arête de l'enveloppe convexe du cercle discret de rayon 25 si et seulement si tous les points de son pointillé suivant sont extérieurs au cercle de rayon $25 + \frac{1}{2}$, ce qui est bien le cas sur cet exemple. Il faut remarquer que la droite euclidienne contenant le pointillé suivant peut fort bien couper le cercle euclidien limite de rayon $R + \frac{1}{2}$.

Ceci se généralise dans le théorème 1 qui suit.

Théorème 1. — Soit $M = (x, y)$ un point de \mathcal{C}_R et $\nu = (b, -a)$ une direction entière de vecteur de Bézout (u, v) , tel que $au + bv = 1$ et $0 \leq u < b$. Soit $r = \left\{ \frac{(ax+by+1)(bu-av)}{a^2+b^2} \right\}_\rho$, où l'indice ρ désigne un calcul modulaire au plus petit reste. Alors la corde définie par M et ν est extrémale pour l'enveloppe convexe de \mathcal{C}_R si et seulement si on a

$$r^2 > (a^2 + b^2)\left(R + \frac{1}{2}\right)^2 - (ax + by + 1)^2.$$

Démonstration — Elle résultera des lemmes 1 et 2 qui suivent appliqués aux pointillés associés à la direction entière (a, b) , avec $\text{pgcd}(a, b) = 1$. On observe que ceux-ci sont équidistants et que la distance qui les sépare est égale à $(a^2 + b^2)^{-\frac{1}{2}}$ et qu'on passe d'un pointillé au suivant par une translation du vecteur de Bézout $(v, -u)$ où $au + bv = 1$ et $0 \leq u < b$ (n'importe quel vecteur de Bézout ferait l'affaire, mais celui que la contrainte portant sur u détermine a le mérite d'être petit).

Remarque. — Les pointillés considérés ci-dessus sont *orthogonaux* au vecteur (a, b) ; le vecteur $(b, -a)$ les dirige.

On a un résultat analogue pour la direction orthogonale $(b, -a)$ dont la distance entre pointillés est encore $(a^2 + b^2)^{-\frac{1}{2}}$ et le vecteur de Bézout est égal à (u, v) .

Il est clair que l'indice du pointillé associé à la direction (a, b) passant par le point $(b, -a)$ est égal à $a^2 + b^2$.

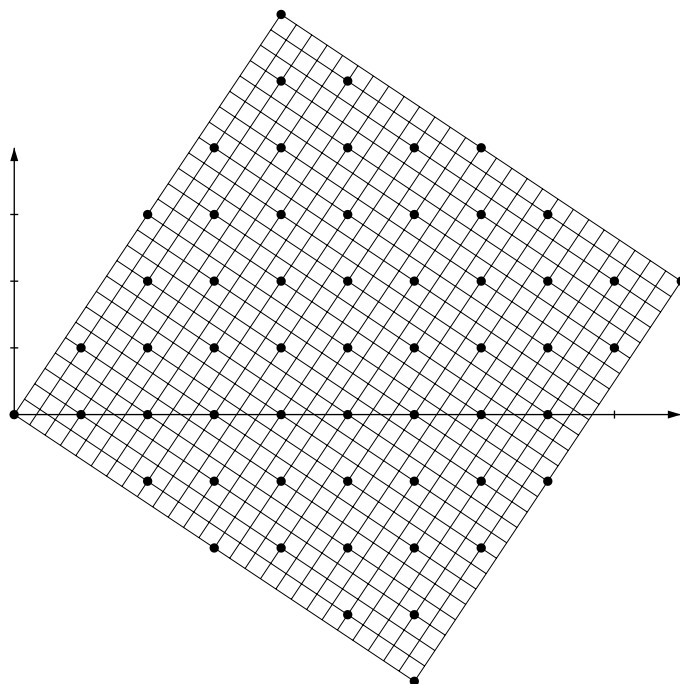


Figure 3. — Les pointillés associés à la direction $(2, 3)$; les points noirs sont les points entiers de \mathbb{Z}^2 .

Les pointillés simultanément associés aux deux directions orthogonales (a, b) et $(b, -a)$ produisent un système de coordonnées engendré par la base rationnelle $\mathcal{B} = \left(\left(\frac{b}{a^2 + b^2}, \frac{-a}{a^2 + b^2} \right), \left(\frac{a}{a^2 + b^2}, \frac{b}{a^2 + b^2} \right) \right)$.

Le point entier de coordonnées (x, y) a encore des coordonnées entières dans cette base : $(bx - ay, ax + by)$; et réciproquement le point de coordonnées (k, l) dans la base \mathcal{B} possède des coordonnées $\frac{1}{a^2 + b^2}(bk + al, -ak + bl)$ dans la base canonique de \mathbb{R}^2 . Pour compléter ces évidences, remarquons qu'un point de coordonnées (k, l) dans \mathcal{B} est toujours rationnel; il est entier ssi

$$\begin{cases} bk + al & \equiv 0 \pmod{a^2 + b^2} \\ -ak + bl & \equiv 0 \pmod{a^2 + b^2} \end{cases}$$

Le lemme suivant est géométriquement évident :

Lemme 1. — Une corde MN du cercle discret \mathcal{C}_R appartient à l'enveloppe convexe de cet ensemble ssi son pointillé suivant est extérieur au cercle euclidien de rayon $R + \frac{1}{2}$.

Nous pouvons caractériser arithmétiquement les cordes extrémales de l'enveloppe convexe. Rappelons que si m et n sont deux entiers, avec $n > 0$ et si r est le reste de la division euclidienne usuelle de m par n alors le reste de la division au plus petit reste de m par n est celui des deux nombres r et $n - r$ ayant la plus petite valeur absolue. On le désignera par $\left\{ \frac{m}{n} \right\}_\rho$.

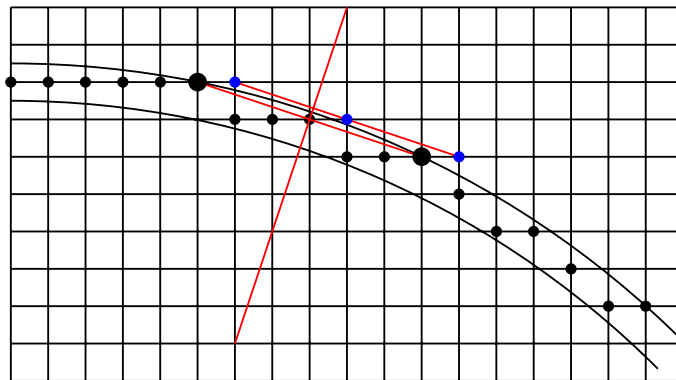


Figure 4. — Une corde et son pointillé de Bézout
 $R = 25$, $M = (5, 25)$, $(a, b) = (1, 3)$, $(u, v) = (1, 0)$

Le vecteur entier (a, b) (et réduit, i.e. $\text{pgcd}(a, b) = 1$) est orthogonal à la corde MN . Soient u et v les coefficients de Bézout tels que $au + bv = 1$ et désignons par x et y les coordonnées du point M . Soit r l'entier défini par

$$r = \left\{ \frac{(ax + by + 1)(bu - av)}{a^2 + b^2} \right\}_\rho.$$

Observons le pointillé suivant MN .

Lemme 2. — Soit un point (X, Y) appartenant au pointillé d'équation $aX + bY = ax + by + 1$ qui suit celui portant MN . Si $K = (s, t)$ est le point de ce pointillé qui est le plus proche de la droite dirigée par le vecteur (a, b) alors on a $bs - at = r$.

Ce lemme exprime l'indice de K relatif à la direction (a, b) à l'aide de l'arithmétique de a et b . Sur la figure 4 précédente K est le point de coordonnées $(9, 24)$, son indice relatif à la direction $(1, 3)$ s'évalue avec

la forme $3x - y$, il vaut donc $r = 3.9 - 24 = 3$. Comme $a = 1$ et $b = 3$ on a $u = 1, v = 0$. Le lemme 2 dit que cette valeur r s'obtient aussi à partir de $M = (5, 25)$ en calculant $(3-0)(5+3.25+1) \pmod{10}$ soit $243 \pmod{10}$, qui donne également 3 évalué au plus petit reste. Le lemme donne de l'information sur le point K sans en connaître ses coordonnées ; c'est son intérêt.

Connaissant la distance entre les pointillés, qui est $(a^2 + b^2)^{-\frac{1}{2}}$, on déduit du lemme 2 que la distance de K à la perpendiculaire à MN passant par l'origine d'équation $y = \frac{b}{a}x$, vaut $r(a^2 + b^2)^{-\frac{1}{2}}$. Mais la distance de l'origine au pointillé passant par K et dirigé par $(b, -a)$ (le suivant de MN) est $(ax + by + 1)(a^2 + b^2)^{-\frac{1}{2}}$. Nous pouvons donc calculer le carré de la distance OK :

Par conséquent le pointillé successeur de MN est à l'extérieur du cercle euclidien de rayon $R + \frac{1}{2}$ ssi on a

$$(1) \quad (ax + by + 1)^2 + r^2 > (a^2 + b^2)\left(R + \frac{1}{2}\right)^2$$

C'est la caractérisation d'extrémalité de la corde MN dans l'enveloppe convexe de \mathcal{C}_R .

La démonstration du lemme 2 revient à calculer les coordonnées de K dans la base \mathcal{B} et à remarquer qu'elles valent $(r, ax + by + 1)$. Seule l'expression de r en fonction des données mérite d'être explicitée. Considérons les pointillés associés à la direction $(b, -a)$, qui est celle de la corde MN . Le vecteur de Bézout (u, v) appartient au pointillé d'indice 1 de cette famille, i.e. $au + bv = 1$. Toujours dans cette famille le point K a pour indice $ax + by + 1$, puisque K appartient au pointillé suivant celui de $M = (x, y)$. Donc le point L de coordonnées $(ax + by + 1)(u, v)$ est également sur le même pointillé que K . On évalue alors l'indice de L dans le système de pointillés orthogonaux aux précédents, c'est-à-dire la valeur de la forme $bx - ay$ en L . Cet indice vaut $(ax + by + 1)(bu - av)$. Mais l'indice du vecteur $(b, -a)$ pour cette dernière forme étant $a^2 + b^2$, le quotient de la division euclidienne de l'indice de L par $a^2 + b^2$ donne le nombre de points entiers du pointillé de K parallèle à MN situés entre L et la droite $y = \frac{b}{a}x$. Si q est ce quotient le point $L - q(u, v)$ est la solution de l'équation diophantienne $aX + bY = ax + by + 1$ ayant la plus petite valeur $bX - aY$ positive possible. Le reste pris au sens de la division au plus petit reste donne bien l'indice $bX - aY$ du point K le plus proche de la droite $y = \frac{b}{a}x$. On pourrait également faire le raisonnement à partir

d'autres points L possibles comme $L = M + (u, v) = (x + u, y + v)$. Dans ce cas la valeur de r s'évaluerait par le reste

$$r = \left\{ \frac{b(x + u) - a(y + v)}{a^2 + b^2} \right\}_\rho$$

mais la condition (1) resterait inchangée.

Il reste à montrer que si le pointillé suivant de MN ne possède pas de points dans \mathcal{C}_R , les pointillés d'indice supérieur n'en ont pas non plus.

Il suffit de considérer les solutions de $a(X - x) + b(Y - y) = 0$, de $a(X - x) + b(Y - y) = 1$ et $a(X - x) + b(Y - y) = 2$ qui satisfont aussi $x \leq X < x + b$. S'il existait une solution $M_2 = (x_2, y_2)$ de $a(X - x) + b(Y - y) = 2$ vérifiant aussi $x \leq X < x + b$ avec $M_2 \in \mathcal{C}_R$ et aucune solution du système $a(X - x) + b(Y - y) = 1, x \leq X < x + b$ dans \mathcal{C}_R . Mais ce dernier a une solution unique, soit $M_1 = (x_1, y_1)$. Par linéarité on aurait aussi l'identité $(x_0, y_0) + 2(x_1 - x_0, y_1 - y_0) = (x_2, y_2)$, ce qui signifie que le point M_1 est le milieu du segment MM_2 . Par convexité M_1 devrait appartenir à \mathcal{C}_R , ce qui est une contradiction.

Cet exemple montre comment on peut rendre les algorithmes géométriques classiques *robustes* i.e. exacts, quand leurs données sont entières.

5 – Enveloppe convexe des paraboles discrètes

Regardons le cas simple où cette conique est discrétisée par l'ensemble des points entiers (x, y) qui satisfont aux inéquations

$$(2) \quad 0 \leq ay - x^2 < a,$$

a étant également un entier positif.

On constate facilement que la structure de cette courbe discrète, que l'on désignera par \mathcal{P} , c'est-à-dire ses paliers, correspond bijectivement aux séquences montantes de la suite des *résidus quadratiques* $x^2 \pmod{a}$ elle-même périodique et de période a .

Cette parabole admet la représentation paramétrique entière :

$$(1) \quad x \mapsto \left[\frac{x^2}{a} \right] + 1.$$

Bien que la parabole définie par $-a < ay - x^2 \leq 0$ admette la paramétrisation plus simple définie par $\left[\frac{x^2}{a} \right]$, celle que nous avons choisie en (2) s'avèrera plus maniable dans les calculs ultérieurs.

Le résultat suivant caractérise arithmétiquement les arêtes de l'enveloppe convexe de la parabole discrète \mathcal{P} .

Théorème 2. — Soit $M = (x, y)$ un point de \mathcal{P} et $\nu = (\alpha, \beta)$ un vecteur entier issu de M de vecteur de Bézout (u, v) . On pose $k = \beta x - \alpha y$ et

$$r = \left\{ \frac{2(k+1)u\alpha - a\beta}{2\alpha^2} \right\}_\rho$$

où ρ indique un calcul au plus petit reste. Alors la corde définie par M et ν est une arête de l'enveloppe convexe de \mathcal{P} si et seulement si on a

$$r^2 > a^2\beta^2 - 4ax\alpha\beta + 4ay\alpha^2 - 4a\alpha.$$

Ce critère assure que le segment d'origine M et d'extrémité $M + \ell\nu$, pour ℓ convenable, est une arête de l'enveloppe convexe de \mathcal{P} . Une formule simple pour ℓ sera donnée plus loin. Dans ce qui suit nous supposons $x \geq 0$ et $0 \leq \beta < \alpha$, c'est-à-dire que nous travaillons sur la partie de \mathcal{P} définie par $0 \leq X \leq a/2$. La démarche suit à peu de chose près les principes mis en évidence dans le cas du cercle discret.

Démonstration — Désignons par $\nu' = (u, v)$ le vecteur de Bézout du vecteur $\nu = (\alpha, \beta)$; il satisfait à l'équation

$$(4) \quad \beta u - \alpha v = 1,$$

et on peut supposer $0 \leq v < u < \alpha$. Rappelons que le rationnel $\frac{v}{u}$ est l'avant-dernière réduite de la fraction continue associée à $\frac{\beta}{\alpha}$ et qu'on l'obtient rapidement par l'algorithme dit d'Euclide-Blankinship (cf [2], [17]).

L'expression du critère cherché utilise essentiellement deux cordes de la parabole euclidienne $Y = \frac{X^2}{a}$ notée (p) :

- celle passant par M et dirigée par le vecteur ν , d'équation

$$(5) \quad \beta X - \alpha Y = k,$$

avec $k = \beta x - \alpha y \geq 0$,

- ainsi que la corde définie par la droite d'équation

$$(2) \quad \beta X - \alpha Y = k + 1.$$

La deuxième est appelée *corde de Bézout* de la corde (5); les abscisses x_1, x_2 des points d'intersection de (6) avec (p) sont données par l'équation

$$(7) \quad X^2 - \frac{a\beta}{\alpha}X + \frac{a(k+1)}{\alpha} = 0.$$

On en déduit immédiatement que l'on a

$$(x_2 - x_1)^2 = \frac{a^2\beta^2}{\alpha^2} - 4\frac{(k+1)a}{\alpha}.$$

On obtient de la même manière

$$(y_2 - y_1)^2 = \frac{a\beta^2}{\alpha^2} \left(\frac{a\beta^2}{\alpha^2} - 4 \frac{(k+1)}{\alpha} \right).$$

Cherchons maintenant le *point entier* de la corde de Bézout le plus proche du milieu I de cette corde. Si P est un point entier quelconque de la corde, comme ceux-ci sont distants de $(\alpha^2 + \beta^2)^{\frac{1}{2}}$, il est facile d'en déduire le point cherché.

Un point tel que P est facile à obtenir, il suffit de multiplier le vecteur ν' par $k+1$, i.e. de poser $P = (k+1)(u, v)$. Calculons la longueur du segment IP , les coordonnées de I se déduisant facilement des coefficients de l'équation (7) : $I = (a\beta/2\alpha, (a\beta^2 - 2(k+1)\alpha)/2\alpha^2)$, on a

$$(8) \quad IP = \left(\frac{2(k+1)u\alpha - a\beta}{2\alpha^2} \right) (\alpha^2 + \beta^2)^{\frac{1}{2}}.$$

Cette expression permet de trouver, en utilisant le *plus petit reste* de $2(k+1)\alpha u - a\beta$ modulo $2\alpha^2$, noté

$$r = \left\{ \frac{2(k+1)\alpha u - a\beta}{2\alpha^2} \right\}_\rho$$

comme précédemment pour le cercle discret.

Plus précisément nous savons que le point entier C le plus proche de I est défini par $IC = \pm \frac{r}{2\alpha^2}(\alpha, \beta)$.

On aboutit à la condition cherchée en écrivant que la valeur absolue de la première composante $|IP_x|$ est supérieure à $|x_2 - x_1|$, ou ce qui est équivalent en prenant les carrés :

$$r^2 > a^2\beta^2 - 4(k+1)a\alpha.$$

En remplaçant k par sa valeur on a

$$r^2 > a^2\beta^2 - 4ax\alpha\beta + 4ay\alpha^2 - 4a\alpha,$$

qui est bien la condition annoncée.

L'entier ℓ mentionné plus haut s'exprime comme partie entière :

$$\ell = \left[\frac{2(k+1)\alpha u - a\beta}{2\alpha^2} \right].$$

Il est tel que le segment d'extrémités M et $M + \ell\nu$ est une arête de l'enveloppe convexe de \mathcal{P} si le théorème est satisfait.

6 – Enveloppe convexe des sphères discrètes

Le traitement numérique de la géométrie se complique avec l'augmentation de la dimension. Il est important de localiser la source des difficultés. Mais ce n'est pas parce que le but avoué d'une discipline est de produire des applications, comme c'est le cas pour la géométrie discrète, qu'elle pourra éviter de se heurter à des difficultés d'ordre théorique.

Ce paragraphe montre que la généralisation naturelle du théorème 1 aux sphères discrètes fait intervenir *la réduction des bases des groupes* \mathbb{Z}^3 . L'exemple retenu a le mérite, à notre avis, de donner un sens géométrique à des questions souvent considérées comme abstraites lorsqu'elles sont abordées sous un angle strictement algébrique. Si ce cas peut être traité directement il n'évacue toutefois pas, dans les dimensions supérieures, le recours à la théorie complète considérée comme assez sophistiquée.

La sphère discrète \mathcal{S}_R considérée est formée des points frontière de la boule discrète définie par l'inéquation $x^2 + y^2 + z^2 < (R + \frac{1}{2})^2$.

L'algorithme suivant construit les points de la sphère discrète \mathcal{S}_R qui satisfont aux inégalités $0 \leq x \leq y \leq z$, ce qui donne un $48 - i\grave{e}me$ de la sphère complète. Leur projection sur le plan xOy est le quart d'ellipse $x^2 + 2y^2 < (R + \frac{1}{2})^2, x \geq 0, y \geq 0$. La variable tmp_e permet de construire le bord de cette ellipse en suivant le point courant de coordonnées (x, y_e) de manière incrémentale.

```

 $x = 0; y = 0; z = 0; tmp = R^2 + R$ 
 $y_e = [R\sqrt{(2)}/2]; tmp_e = tmp;$ 
pour  $x = 0$  à  $R$  faire
  pour  $y = 0$  à  $y_e$  faire
     $point(x, y, z);$ 
     $tmp = tmp + 2y + 1;$ 
     $y = y + 1;$ 
    si  $tmp \geq R^2 + R + 1$ 
      alors
         $tmp = tmp - 2z + 1; z = z - 1$ 
      fin si
    fin pour
   $tmp_e = tmp_e + 2x + 1$ 
  si  $tmp_e \geq R^2$ 
    alors
       $tmp_e = tmp_e - 4y_e + 2;$ 
       $y_e = y_e - 1$ 
    fin si
  fin pour

```

Soient $M = (x, y, z)$ un point de \mathcal{S}_R et $\nu = (\alpha, \beta, \gamma)$, $\nu' = (\alpha', \beta', \gamma')$ deux directions entières. Le produit vectoriel $\nu \wedge \nu'$ donne le vecteur normal à la face définie par M et les deux directions ν et ν' , noté $n = (a, b, c)$. Cette fois notre problème nécessite l'étude des deux cercles d'intersection définis par les plans $aX + bY + cZ = k$ et $aX + bY + cZ = k + 1$, où $k = ax + by + cz$, avec la sphère euclidienne $X^2 + Y^2 + Z^2 = (R + \frac{1}{2})^2$. La partie essentielle du travail consiste à calculer la distance du point I d'intersection de la droite dirigée par $n = (a, b, c)$ et du plan $aX + bY + cZ = k + 1$, de coordonnées

$$I = (k + 1)(a^2 + b^2 + c^2)^{-1}(a, b, c),$$

aux éléments du réseau entier d'équation

$$aX + bY + cZ = k + 1.$$

Nous avons vu à propos des procédures présentées dans ce paragraphe comment évaluer cette distance qui sera notée r comme dans les deux cas précédents; on a aussi le résultat suivant.

Théorème 3. — *La face définie par le point M et les deux vecteurs ν et ν' , est une face de l'enveloppe convexe de \mathcal{S}_R si et seulement si on a*

$$r^2 > (R + \frac{1}{2})^2 - \frac{(ax + by + cz + 1)^2}{a^2 + b^2 + c^2}.$$

La généralisation du théorème 1 aux sphères discrètes nécessite donc de savoir trouver le point d'un sous-groupe G de rang 2, de \mathbb{Z}^3 , le plus proche d'un point (rationnel) donné du plan euclidien défini par G . Ce problème suppose lui-même que l'on sache trouver la *base minimale* d'un groupe tel que G . Ces questions sont traitées dans la partie II de l'article (à paraître dans la *Gazette*).

Dans notre cas le groupe G est défini par une équation diophantienne

$$ax + by + cz = 0,$$

il s'agira donc de déterminer la base minimale du sous-groupe G de \mathbb{Z}^3 orthogonal à la direction entière (a, b, c) normale à la face testée.

Bibliographie

- [1] BRESENHAM (J.). — *Algorithm for computer control of a digital plotter*. IBM System Journal, 1965, vol. 4, pp. 25-30.
- [2] BLANKINSHIP W.A. — *A new version of the Euclidean algorithm*. Amer. Math. monthly, pp. 742-745, 1963.
- [3] COHEN (D.) ET KAUFMAN (A.E.). — *Fundamentals of surface voxelisation*, CVGIP-GMIP, 57 (6), v. 95, pp. 453-461.
- [4] I. DEBLED-RENNESON. — *Etude et reconnaissance des droites et plans discrets*. Thèse, Université Louis Pasteur, Strasbourg, France, déc. 1995.

- [5] DEBLED (I.) ET REVEILLÈS (J.-P.) — *A New Approach to Digital Planes*. — Vision Geometry III, (R.A. Melter, A.Y. Wu eds.), Boston 1994, pp. 12–21, SPIE vol. 2356.
- [6] DEBLED (I.) ET REVEILLÈS (J.P.) — *A linear algorithm for the segmentation of discrete curves*. — In Parallel Image Analysis and applications. Series in Machine Perception artificial intelligence, Vol. 19 pp. 73-100, World Scientific 1996, ISBN 981-02-2476-1
- [7] ERDÖS (P.), GRUBER (P.M.) ET HAMMER (J.). — *Lattice points*. Longman Scientific & Technical. 1989.
- [8] HARDY (G.H.) ET WRIGHT (E.M.) — *An introduction to the theory of number*, fifth edition, Oxford Sc. Pub., 1989.
- [9] KAUFMAN (A.E.). — *Volume synthesis*. 6th International Workshop, Discrete Geometry for Computer Imagery 96, Lyon, France, November 1996. Lecture Notes in Computer Science, Springer Verlag.
- [10] KONG (T.I.) ET ROSENFELD (A.) . — *Digital Topology : Introduction and survey* — Computer Vision, Graphics and Image Processing 48, pp. 352-393, 1989.
- [11] LANG (S.) . — *Algebra*, 3rd edition. Addison-Wesley. 1994.
- [12] REVEILLÈS (J.-P.). — *Géométrie discrète, calcul en nombres entiers et algorithmique*, —Thèse d'État, Strasbourg, 1991.
- [13] REVEILLÈS J.-P. ET YAACOUB (J.). — *MAT Operator for contour extraction*. *Journal of Electronic Imaging*,
- [14] ROSENFELD (A.). — *Picture processing by computer*, Acad. press, N.-Y. 1969.
- [15] ROSENFELD (A.). — *Picture Languages*, Acad. press, N.-Y. 1979.
- [16] ROSENFELD (A.). — *Digital straight lines segments*, I.E.E.E. Trans. on Computers, t. 23, 12, 1974, p. 1264-1369.
- [17] SEROUL (R.). — *Math-info. Informatique pour mathématiciens*. Collection *ii*a, InterEditions 1995.