© Proceedings of the *11th Canadian Conference on Computational Geometry*
Vancouver (BC, Canada), August 15-18, 1999, pp. ?–?.

The periodicity of integral convex hulls for conics in $\mathbb{E}^2$

Helymar Balza-Gomez Dominique Michelucci Jean-Michel Moreau
LISSE / ENSM.SE*

Abstract

We present a method to construct the boundary of the *integral convex hull* of conics in the plane. This work may be related to a previous problem (constructing a circle or an ellipse by Bresenham's algorithm [3]), but is more general, complex and its solution involves strong arithmetic properties of the conics.

1 Introduction

Define the *integral convex hull* (*i.c.h.* in short) of a convex curve segment as the set of points with integral coordinates lying between the curve segment, the x-axis, and the two vertical lines through the endpoints of the curve segment. In this paper, we shall show that some transforms exist that leave invariant $\mathbb{Z}^2$ and the family of conics defined by:

$$\{(x,y) \in \mathbb{E}^2 \quad | \quad f(x,y) = ax^2 + bxy + cy^2 + dx + ey + f = 0\} \ , \quad (1)$$

where a, b, c are coprime integers ($\gcd(a,b,c) = 1$).

These transforms are then used to prove the periodicity of the boundary of the *i.c.h.* (noted $\mathcal{B}$ in the sequel) of the family of conics defined above (Section 2). Next, Section 3 presents applications of the method, and we conclude in Section 4.

*158 cours Fauriel, 42 023 St-Étienne, France. Email: {hbalza, micheluc, moreau}@emse.fr

2 Transformations

We wish to study transforms that leave conics globally invariant, and $\mathbb{Z}^2$. Such transforms T satisfy the two following conditions:

C_1 (*invariance*) :

$$(x\ y) = (x'\ y')T \Rightarrow f(x,y) = f(x',y')$$

C_2 (*unimodularity*) :

the coefficients of T are in $\mathbb{Z}$, and $\det T = +1$.

Note that, if T is unimodular, so is $T^k, k \in \mathbb{Z}$. Another important property is that unimodular transforms preserve convexity. The interested reader is referred to [4] for more details on unimodular transforms. We have the following general lemma:

Lemma 2.1 *Let Q be the matrix representation of a conic with $f(x,y)$ defined as above (i.e., $f(x,y) = (xy1)Q(xy1)^t$), and T be a transform. T leaves f invariant if and only if $TQT^t = Q$*

Proof Omitted. (See [1] for a detailed proof.)

2.1 The case of the parabola

Consider the parabola with equation (1), and $\Delta = b^2 - 4ac = 0$. We wish to find an unimodular transform T such that $TQT^t = Q$, where Q is the corresponding matrix. Let us suppose we work in homogeneous coordinates.

First, to simplify the equation, we need an unimodular system of coordinates O, I, J, with vector J

parallel to the symmetry axis of the parabola, *i.e.*, to the line:

$$y = \frac{-b}{2c}x = \frac{-2a}{b}x$$

Finally, in this system, defined by:

$$\begin{aligned} J &= (u = \frac{2c}{g}, v = \frac{-b}{g}) \text{ with } g = \gcd(2c, b) \\ I &= (s, t) \quad \text{with} \quad sv - tu = 1 \text{ (Bezout)}, \end{aligned}$$

the equation of the parabola becomes:

$$Y = \frac{AX^2 + BX + C}{M} \quad A, B, C \in \mathbb{Z},\ M \in \mathbb{N}^*,$$

and the matrix representation of the parabola is:

$$Q = \begin{pmatrix} A & 0 & B/2 \\ 0 & 0 & -M/2 \\ B/2 & -M/2 & C \end{pmatrix}.$$

In order to find the coefficients, we use the fact that the transform must leave the symmetry axis invariant. Hence, the transformation is such that:

$$\begin{aligned} &X = X' + x_0, \quad x_0 \in \mathbb{Z} \\ &Y = Y' + \alpha X' + y_0, \quad \alpha \in \mathbb{Z}, \quad y_0 \in \mathbb{Z} \end{aligned}$$

After substitution:

$$\begin{aligned} Y' &= \frac{1}{M}\big[AX'^2 + (2Ax_0 + B - \alpha M) \quad + \\ &\qquad (Ax_0^2 + Bx_0 + C - My_0)\big] \end{aligned}$$

Consequently:

$$\begin{aligned} &2Ax_0 = \alpha M \\ &Ax_0^2 + Bx_0 - My_0 = 0 \end{aligned}$$

A correct (although maybe not minimal) solution, is given by:

$$\begin{aligned} &x_0 = M\nu, \quad \alpha = 2At, \quad \nu \in \mathbb{Z} \\ &A(M\nu)^2 + B(M\nu) - My_0 = 0 \\ &\quad \Rightarrow \quad y_0 = AM\nu^2 + b\nu \end{aligned}$$

This leads to:

$$T_\nu = \begin{pmatrix} 1 & 2A\nu & 0 \\ 0 & 1 & 0 \\ M\nu & AM\nu^2 + B\nu & 1 \end{pmatrix}$$

where ν is an integer. (Note that $T_\nu = T_1^\nu$.)

In conclusion, since we have found a matrix T_ν such that: if $(x, y, 1)$ is a vertex of $\mathcal{B}$, then so is $(x, y, 1)T_\nu$, we have just proven that the integral convex hull of the parabola is periodic.

2.2 The case of the centered hyperbola

We shall first focus on the case of centered hyperbolæ, and then return to the general case in the next subsection. Starting from the matrix representation of the centered hyperbola:

$$\begin{aligned} &f(x, y) = ax^2 + bxy + cy^2 = m, \\ &\qquad \text{with} \quad m \in \mathbb{R}, \quad \Delta > 0, \quad \sqrt{\Delta} \notin \mathbb{N}: \\ &f(x, y) = (x\ y)Q(x\ y)^t, \\ &\qquad \text{with} \quad Q = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \end{aligned}$$

we compute the coefficients of the unimodular transform $T = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, satisfying conditions C_1 and C_2 above.

It is possible to show that computing the integral coefficients $A,\ B,\ C,\ D$ is equivalent to solving two Pell-Fermat equations with same discriminant $\Delta = b^2 - 4ac > 0$ (see [4]). The value for each coefficient is shown to depend on the value of $\Delta \bmod 4$, and two mutually exclusive cases are considered. As a consequence, thanks to the minimal solution $(u, v) \in \mathbb{N}^2$ of the above equations, we get

$$\begin{aligned} &\Delta \equiv 0 \bmod 4 \Rightarrow \\ &\qquad u^2 - \frac{\Delta}{4}v^2 = 1, \quad T = \begin{pmatrix} u - \frac{b}{2}v & av \\ -cv & u + \frac{b}{2}v \end{pmatrix} \\ &\Delta \equiv 1 \bmod 4 \Rightarrow \\ &\qquad u^2 - \Delta v^2 = 4, \quad T = \begin{pmatrix} \frac{u - bv}{2} & av \\ -cv & \frac{u + bv}{2} \end{pmatrix} \end{aligned}$$

Cases $\Delta \equiv 2$ or $3 \bmod 4$ are impossible. All transforms T^k $k \in \mathbb{Z}$, are unimodular and preserve the hyperbola. Conversely, all unimodular transforms leaving unchanged the hyperbola and $\mathbb{Z}^2$ are powers of T.

Remark: We could also consider extending *Condition* C_2 to $\det = \pm 1$, which fully translates unimodularity. However, in the case $\det = -1$, *Condition* C_1 is lost ($TQT^t = -Q, \quad \Rightarrow f(x', y') = -f(x, y)$). Still, the knowledge of the initial *i.c.h.*-boundary sequence on $f(x, y) = m$ allows to find all the *i.c.h.*-boundary sequences on $f(x, y) = -m$. The interested reader will find a more detailed analysis in [1].

Special cases and extensions

Note that in the special case where Δ is a squared integer (for example $xy = 1$), integral hulls have a finite number of vertices.

In the case of a non-centered hyperbola, the integral convex hull is not properly periodic, but only *quasi*-periodic.

2.3 The case of the ellipse

In this case, the discrimant in equation (1) is strictly negative. The transformation group is finite (and not infinite as was the case for the parabola and hyperbola), and the only transforms that may be considered are the trivial ones. For instance, the group of the ellipse defined by: $x^2 + xy + y^2 = m$ contains 12 transforms, and is generated by (say) $T = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, of order 6 (*i.e.*, $T^6 \equiv I$), and the symmetry $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

3 Applications and extensions

3.1 Construction of $\mathcal{B}$

Using the previous results, the integral convex hull of any parabola, or centered hyperbola is *periodic*: the whole integral convex hull is a repetition of a minimal "pattern", *i.e.*, sequence of points.

Let T be the associated transform of f:

- ▷ Apply T to line $Ox : y = 0 \rightsquigarrow D$
- ▷ The arc between D and Ox is a ''pattern'' of f
- ▷ Compute $D \cap f = I = (x_i, y_i)$
  - Compute $i.p._{(x \leq x_i)}$ the initial ''pattern'' of $\mathcal{B}$ $(O(k \log n))$
  - By applying T ,one goes from one point in the initial ''pattern'' $i.p._{(x \leq x_i)}$ to its equivalent in the next sequence, and so forth.

Figure 1: *Constructing the convex hull from the initial pattern. D and f are shown in Figure 2.*

One goes from one point in the initial *i.c.h.*-boundary to its equivalent in the next sequence by applying the associated transform of Section 2, and so forth. This operation is summarized in the algorithm of Figure 1.

The last problem is to compute all the points in the initial pattern. The outline of the method is as follows: we follow the curve, starting from any point on $\mathcal{B}$. We compute the next point of $\mathcal{B}$, using a technique akin to the continued fraction expansion of a real number, but tailored for this specific problem. And we repeat the process until we reach a point that is the image of the initial point under the associated transform. This process is detailed in [2], in which we are concerned with the the integral convex hull below straight-line segments and sections of biconvex curves. The algorithm presented there may be extended to any convex body (*cf.* [1]).

3.2 Integral convex hulls and factorization

Computing the integral convex hull for hyperbolæ defined by $xy = N$, $N \in \mathbb{N}$ yields the set of all integral couples p, q such that $pq = N$, and hence all the prime factors of N. In [2], the authors conjectured (using experimental evidence) that the boundary of

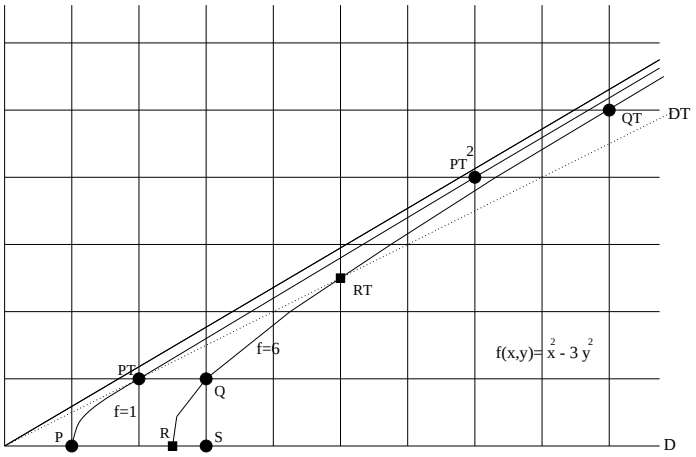

Figure 2: *Hyperbolæ* $f(x,y) = x^2 - 3y^2 = \delta$. *Cases* $\delta = 1$ *and* $\delta = 6$. *For* $\delta = 1$, $\{P\}$ *is the initial pattern,* $PT, PT^2 \ldots \in \mathcal{B}$ *For* $\delta = 6, \{S,Q\}$ *is the initial pattern.*

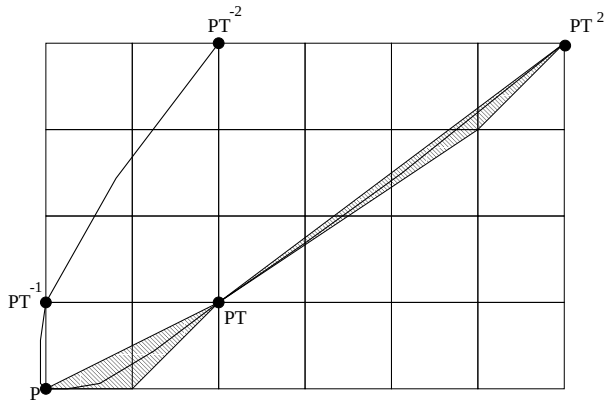

Figure 3: *Parabola* $x^2 + y^2 - 2xy - y = 0$, $\{P\}$ *is the initial pattern,* $PT^{-1}, PT^{-2}, \ldots, P, PT, PT^2, \ldots \in \mathcal{B}$. *Shaded triangles show* T *in action.*

the *i.c.h.* of the hyperbola contains about $N^{0.36}$ integral points. Hence, we now have a factorization algorithm with running time $O(N^{0.36} \log N)$, *i.e.*, slightly faster than the well-known brute-force algorithm testing all primes smaller than $\sqrt{N}$. In the case of a line segment s, computing the integral convex hull and counting the integer points on s both take $O(\log N)$ time, *i.e.*, a time proportional to the size of the data (length of minimum side in rectangular triangle with hypothenuse s). The algorithm for the construction of the *i.c.h.*-boundary for hyperlæ $xy = N$ is optimal (relatively to the output size). However, the algorithm that uses the *i.c.h.* to count the integral vertices on the hyperbola is not polynomial in the size of the data (the actual number of vertices). But this is quite correct: if a counting method existed that was polynomial in the size of the data, it would yield a polynomial method for factorization.

4 Conclusion

The algorithms we have presented in this paper have been coded in *Caml*. Indeed, they require the use of libraries for "big integers", as should be obvious from the nature of the solutions.

It is natural to want to extend the research presented in this paper to higher dimensions. It does not seem easy to generalize our results to quadrics. However, it may be possible to derive similar periodicity properties for certain cubic implicit surfaces. Such results are related to well-known number-theoretic properties.

We are also currently extending the 2D algorithm in [2] to compute 3D integer convex hulls.

References

[1] H. Balza-Gomez, D. Michelucci, and J-M. Moreau. On integral convex hulls. Technical report, LISSE-ENSM.SE, to appear.

[2] H. Balza-Gomez, D. Michelucci, and J.M. Moreau. Convex hulls of grid points below a line or a convex curve. In *Discrete Geometry for Computer Imagery, LNCS 1568*. Springer-Verlag, 1999.

[3] J.E. Bresenham. Algorithm for computer control of a digital plotter. *IBM System Journal*, 4:25–30, 1965.

[4] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1995.