STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1959 - 008

Geometric deduction of Markov's minimal forms

C.G. Lekkerkerker

Lecture held at Amsterdam on April 25, 1959

1959

ZW 1959-008

Geometric deduction of Markov's minimal forms

by

C.G. Lekkerkerker

Lecture held at Amsterdam on April 25, 1959

1. In the following we shall consider indefinite binary quadratic forms. Such forms have the shape

$$q = q(x) = \alpha x_1^2 + \beta x_1 x_2 + \gamma x_2^2 \qquad (\alpha, \beta, \gamma \text{ real});$$

and have positive discriminant

$$d = d(q) = \beta^2 - 4\alpha\gamma .$$

In this report we shall be concerned with the lower bound of $|q(x)|$ for integral $x_1, x_2 \neq 0, 0$.

We shall denote points with integral coordinates by $u=(u_1,u_2)$, $v=(v_1,v_2)$, etc. In particular, we shall write $o=(0,0)$. For given q, we put

(1) $$\mu(q) = \inf_{u \neq o} |q(u)| .$$

Further, we shall call two forms q,q' equivalent, and write $q \sim q'$, if there is an integral unimodular transformation

$$x \rightarrow Ux = (u_{11}x_1 + u_{12}x_2, u_{21}x_1 + u_{22}x_2)$$

such that $q(Ux)=q'(x)$. Next, we shall write $q \approx q'$ if q is equivalent with a multiple $\sigma q'$ of q'. The following relations are trivial:

(2) $$\mu(q) = \mu(q') \text{ and } d(q) = d(q') \text{ if } q \sim q'$$

(3) $$\mu(q)/\sqrt{d(q)} = \mu(q')/\sqrt{d(q')} \quad \text{if} \quad q \approx q'.$$

The theorem of Markov, which we shall state below and for which we intend to give a geometric proof, gives detailed information concerning the quantity $\mu(q)/\sqrt{d(q)}$.

The geometry can be brought in as follows. Let S be the two-dimensional domain

(4) $$S : |x_1 x_2| < 1,$$

bounded by the two orthogonal hyperbolas $x_1x_2=\pm 1$, and let Y denote the lattice of points u in the plane with integral coordinates. The domain S is left invariant under the hyperbolic rotations

(5) $$T : x_1' = \tau x_1 , \quad x_2' = \tau^{-1} x_2 \quad (\tau \neq 0 \text{ and real})$$

and under the reflections with respect to the coordinate axes and the lines $x_1=\pm x_2$.

Further, if we subject Y to a nonsingular linear transformation

$$x \rightarrow Ax = (a_{11}x_1+a_{12}x_2, a_{21}x_1+a_{22}x_2),$$

then we get a general plane lattice Λ consisting of the points Au $(u \in Y)$ enz. It is generated by the two points Ae, Af, where $e=(1,0)$ and $f=(0,1)$, and has determinant

$$d(\Lambda) = |\det A| .$$

Now consider an arbitrary form $q(x)$. It can be written as the product of two linear factors, say

(6) $$q(x) = (a_{11}x_1+a_{12}x_2)(a_{21}x_1+a_{22}x_2);$$

if A is the matrix (a_{ij}) and $\overline{q}$ denotes the special form $\overline{q}(x)=x_1x_2$, then (6) reads

(6') $$q(x) = \overline{q}(Ax).$$

Suppose that $\mu(q)$ has a positive value μ. Then, by (1) and (6), each point $x\neq o$ of the form Au satisfies $|x_1x_2| \geqslant \mu$, i.e. the lattice $\Lambda = AY$, where A satisfies (6'), has no point $\neq 0$ in $\sqrt{\mu}\, S$. With the usual terminology, we say that Λ is admissible for $\sqrt{\mu}\, S$. More precisely, we have

(7) $$\inf_{x\neq o, x\in\Lambda} |x_1x_2| = \mu ,$$

where $\mu = \mu(q)$, $\Lambda = AY$, $q(x)=\overline{q}(Ax)$, so that Λ is admissible for $\sqrt{\mu}\, S$, but no longer for $\sqrt{\mu'}\, S$ as $\mu' \mu$.

We may denote the square root of the left hand member of (7) by

(8) $$\mu(\Lambda) = \mu(S, \Lambda) = \inf_{x\neq o, x\in\Lambda} |x_1x_2|^{\frac{1}{2}} .$$

We further note that the form (6) has discriminant $(\det A)^2$. Then, for the lattice Λ considered above,

(9) $$\mu(\Lambda) = \sqrt{\mu(q)}\ , \quad d(\Lambda) = \sqrt{d(q)}.$$

There is a correspondence between forms q and lattices Λ. It can be expressed by

(10) $$q(x) = \overline{q}(Ax)\ , \quad \Lambda = A\Upsilon\ .$$

But this correspondence is not one-to-one. On the other hand, any two lattices $A\Upsilon$ and $AU\Upsilon$ are identical, since $\Upsilon = U\Upsilon$. Thus, equivalent forms correspond with the same lattice. On the other hand, the form $\overline{q}$ is left invariant under all hyperbolic rotations T (which means that q(x) and $q(A^{-1}TAx)$ are identical for all T). The corresponding lattices are $\Lambda = A\Upsilon$, $\Lambda' = TA\Upsilon$. Such lattices are obtained from each other by means of a hyperbolic rotation of the plane, and one has the formulas (similar to (2)):

(11) $$\mu(\Lambda) = \mu(\Lambda') \text{ and } d(\Lambda) = d(\Lambda') \text{ if } \Lambda' = T\Lambda\ .$$

The right form of the correspondence between forms and lattices is given in our case by

(12) $$\{q_U\}_U \leftrightarrow \{\Omega^{\varepsilon} T\Lambda\}_T \qquad (\varepsilon = 0, 1),$$

where q and Λ are connected by (10) and q_U means the form q(Ux).

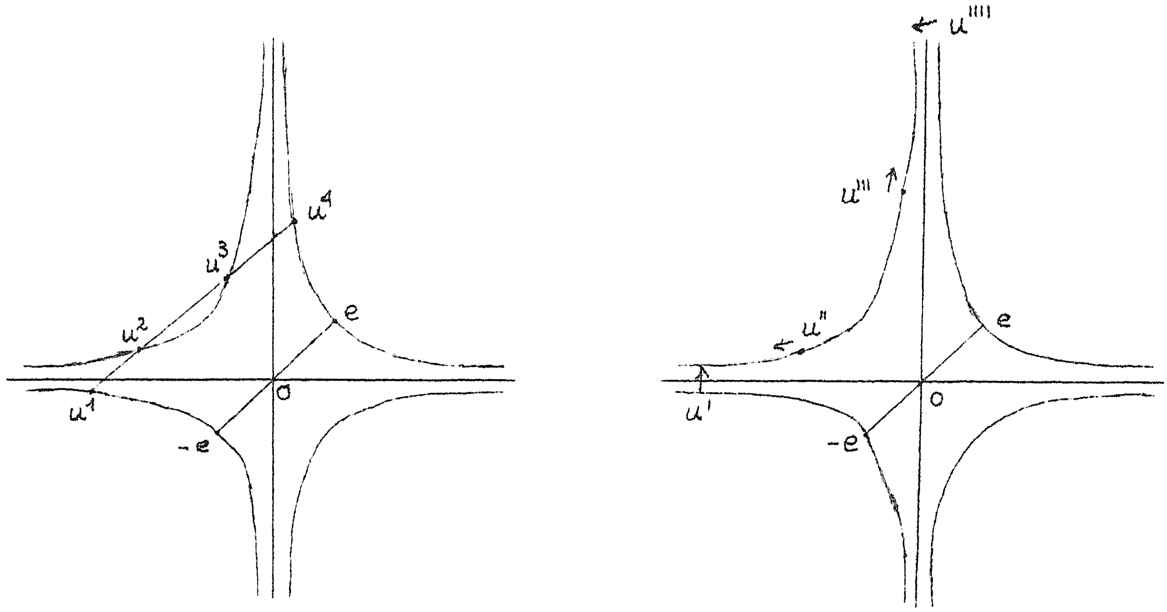
2. We proceed to find all lattices Λ with

(13) $$\mu(S, \Lambda) = 1\ , \qquad d(\Lambda) < 3.$$

Let B denote the boundary of S, and let B_1, B_2, B_3 be the parts of B in the 1st,2nd,3rd quadrant respectively. Let x^0 be the point (1,1) on B_1. We shall first determine the lattices Λ satisfying (13) and <u>having a point on the boundary B</u>. It is no restriction to suppose that $x^0 \varepsilon \Lambda$; then Λ has a basis $\{e, f\}$, with

(14) $$e = x^0.$$

A generic point u_1e+u_2f of Λ may be denoted by $u=(u_1,u_2)$; accordingly, from now on coordinates will always be taken with respect to a (suitably chosen) basis $\{x^0, f\}$ of Λ. The lattice Λ is determined completely if we know three points e,u,v of Λ on the boundary B; likewise, the corresponding quadratic form q is determined uniquely by its values in e,u,v. We now construct a certain denumerable set of lattices and then prove that these lattices are all admissible and give all lattices satisfying our conditions. We repeat that we always take $e=x^0$.



The first lattice, say $\Lambda_1=A_1Y$, is such that $u^2=(-2,1)\in B_2$ and $u^3=(-1,1)\in B_2$. Put

$$(15)\qquad q_1(x) = \det(x,V_0x), \quad \text{where} \quad V_0 = \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}.$$

Then $q_1(u) = 1,-1,-1$ for $u=e,u^2,u^3$ respectively, and so $\overline{q}(A_1x)=q_1(x)$. For arbitrary A, we have

$$(16)\qquad \det(Ax,Ay) = \det A \cdot \det(x,y).$$

Hence, $q_1(V_0x) = q_1(x)$, i.e. V_0 is an automorphism of $q_1(x)$. Hence, $u^1=-V_0^{-1}e=(-3,1)$ lies on B_3 and $u^4=V_0e=(0,1)$ lies on B_1.

The second lattice, say $\Lambda_2=A_2Y$, is obtained from Λ_1 by moving u^2 along B_2 until u^4 reaches B_2. Put

$$(17)\qquad q_2(x) = \tfrac{1}{2}\det(x,U_0x), \text{ where } U_0 = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}.$$

Then $q_2(u) = 1,-1,-1$ for $u=e,u^2,u^4$, and so $\overline{q}(A_2x)=q_2(x)$. Further, U_0 is an automorphism of $q_2(x)$, so that $-U_0^{-1}e=(-5,2)$ lies on B_3 and $U_0e=(1,2)$ lies on B_1. As is easily verified, the matrices U_0, V_0 satisfy the following relation, which will be important in the sequel:

$$(18)\qquad U_0V_0 = V_0KU_0, \quad \text{with } K=\begin{pmatrix} -1 & 6 \\ 0 & -1 \end{pmatrix}.$$

The third lattice, say $\Lambda_3 = A_3 Y$, has the points $u^4 = V_0 e = (0,1)$ and $-U_0^{-1}e = (-5,2)$ on B_2. We put

$$q_5(x) = \frac{1}{5}\det(x, U_0 V_0 x). \tag{19}$$

We have $q_5(e)=1$. By repeated application of (16) and (18) and by using $Ke=-e$ we find that $q_5(V_0 e) = q_5(-U_0^{-1}e) = -q_5(e) = -1$. So $\overline{q}(A_3 x) = q_5(x)$. Further, $U_0 V_0$ is an automorphism of $q_5(x)$. So we find that Λ_3 has a.o. the following four points on B:

$$u' = -(U_0 V_0)^{-1}e, \quad u'' = -U_0^{-1}e, \quad u''' = U_0 V_0 e. \tag{20}$$

These points are connected with each other by

$$V_0 u' = u'', \quad U_0 V_0 u'' = u''', \quad U_0 u''' = u''''. \tag{21}$$

The above procedure can be continued indefinitely. It should be noted that Λ_1 and Λ_2 are symmetric with respect to the bisectrices of the axes, but not Λ_3. So from Λ_3 we can obtain two different lattices, for which respectively u', u''' and u'', u'''' lie on B_2. We now introduce the following notations.

- $\mathfrak{M}$: set of pairs of integral matrices (U,V) such that
  - a) $(U_0, V_0) \in \mathfrak{M}$
  - b) if $(U,V) \in \mathfrak{M}$, then $(UV, V) \in \mathfrak{M}$ and $(U, UV) \in \mathfrak{M}$
- $|\mathfrak{M}|$: set of matrices in $\mathfrak{M}$
- $\Lambda(U,V)$: lattice through x^0 with $-U^{-1}e \in B_2$ and $Ve \in B_2$
- $\mathcal{L}$: set of the lattices $\Lambda_1, \Lambda_2, \Lambda(U,V)$ $((U,V) \in \mathfrak{M})$
- $q(U,V;x)$: form q with $q(e)=1$, $q(-U^{-1}e) = q(Ve) = -1$
- $I = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $L = \begin{pmatrix}1 & -3\\ 0 & 1\end{pmatrix}$ (so that $K = -L^2$) .

Then, if (U,V) is a pair of $\mathfrak{M}$ and W is an arbitrary matrix of $|\mathfrak{M}|$, the following seven properties hold:

I $UV = VKU$

II $(WL)^2 = -I$

III $q(U,V;x) = \frac{1}{m}\det(x, Wx)$, where $W = (w_{ij}) = UV$ and $m = w_{21}$

IV $q(U,V;x)$ is invariant under the transformation UV and is transformed into $-q(U,V;x)$ by VL

V $\Lambda(U,V)$ has four points u', u'', u''', u'''' on B_3, B_2, B_2, B_1 respectively, such that

(22) $$UVu' = -e,\ Uu'' = -e,\ Ve = u''',\ UVe = u'''',$$

(23) $$Vu' = u'',\ UVu'' = u''',\ Uu''' = u''''$$

VI W has the form $\begin{pmatrix} k & 1 \\ m & 3m-k \end{pmatrix}$, so that the corresponding form $\frac{1}{m}\det(x,Wx) = \frac{1}{m}\{mx_1^2+(3m-2k)x_1x_2-lx_2^2\} = q_m(x)$, say, has discriminant $d_m = d(q_m) = 9-4m^{-2}$

VII the lattices in $\mathcal{L}$ are admissible for S.

Proof. Properties I and II are easily proved by induction.

Property III can be verified as follows:

$$\det(e,We) = m,$$
$$\det(U^{-1}e, UVU^{-1}e) = \det(U^{-1}e, VKe) = -\det(e,UVe) = -m,$$
$$\det(Ve, UVVe) = \det(e, KUVe) = -m.$$

The first clause in IV is a consequence of III and the second one is proved as follows:

$$\det(VLx, UVVLx) = \det(VLx, -VL^2UVLx) = \det(x, -LUVLx)$$
$$= \det(UVx, -(UVL)^2x) = \det(UVx, x) = -\det(x, UVx).$$

Property V is proved by induction as follows. We saw already that V holds for $\Lambda_3 = \Lambda(U,V)$. Suppose V holds for $\Lambda(U,V)$, and consider $\Lambda(UV,V)$. Let $v^{(i)}$ $(1 \leq i \leq 4)$ be the points with

$$UVVv' = -e,\ UVv'' = -e,\ Ve = v''',\ UVVe = v''''.$$

Then $v'' = u'$, $v''' = u'''$, and so

$$Vv' = -(UV)^{-1}e = v'',\ UVVv'' = UVVu' = UVu'' = u''' = v''',$$
$$UVv''' = UVVe = v''''.$$

Further, by IV and the proof of III, the $v^{(i)}$ lie on B. Hence V holds for $\Lambda(UV,V)$. Similarly for (U,UV).

As for the proof of VI, let $W=UV$ and let the $u^{(i)}$ be given by (22). By II, $(WL)^2e = -e$ or $LWLe = -W^{-1}e$, i.e. $Lu'''' = u'$. Now $u'''' = We$ has second coordinate $w_{21} = m$, and so u'''' has the form (k,m). Then $u' = Lu'''' = (k-3m, m)$. Then, since $u'''' = We$ and $u' = W^{-1}e$, W has the form stated. Since $\det W = 1$, we have

(24) $$k^2+1 = m(3k-1).$$

Finally, $d_m = m^{-2}\{(3m-2k)^2+4lm\} = 9-4m^{-2}$. Property VI also holds for $W = U_0, V_0$.

Property VII = lemma 10 in [2], chapter II; the proof is based on IV and VI.

It is now easy to prove the following

Theorem 1. The lattices Λ satisfying (13) and passing through x^0 are just given by the lattices in $\mathcal{L}$.

Proof. Let Λ be such a lattice. Let G_1 be the set of points outside S lying in the 1st or 3rd quadrant, and let G_2 denote the set of points outside S in the 2nd quadrant. We may suppose that (-2,1) and (-1,1) belong to G_2 (see the figure). If (-3,1) and (0,1) belong to G_1, then necessarily $\Lambda = \Lambda_1$. If not, then for reasons of symmetry we may suppose that $(0,1) \in G_2$. Then necessarily $\Lambda = \Lambda_2$, if $(-5,2) \in G_1$ and $(1,2) \in G_1$ (see figure). If not, then we may suppose that $(-5,2) \in G_2$. Then $-U_0^{-1}e$ and $V_0 e$ lie in G_2.

We now use the following property, which is geometrically clear: if Λ satisfies our conditions, if $u^{(i)}$ are defined by (22) and if u'', u''' lie in G_2 and u', u'''' in G_1, then necessarily $\Lambda = \Lambda(U,V)$. Suppose that, for some pair $(U,V) \in \mathfrak{M}$,

$$(25) \qquad -U^{-1}e \in G_2 , \quad Ve \in G_2 .$$

Then there are four possibilities:

a) $-(UV)^{-1}e$, $UVe \in G_1$; then $\Lambda = \Lambda(U,V)$

b) $-(UV)^{-1}e, \in G_2$; then (25) holds for the pair (UV,V)

c) $UVe \in G_2$; then (25) holds for the pair (U,UV)

d) $-(UV)^{-1}$, $UVe \in G_2$; it is easy to prove that in this case $d(\Lambda) > 3$.

We now note that $d_m = 9-4m^{-2}$ and that m is a positive integer increasing for each step. It follows that after finitely many steps the possibility a) occurs, since $d(\Lambda) < 3$. This proves theorem 1.

In order to solve our problem completely we must consider lattices which do not have a point on B. But here we have the following

Lemma. Each lattice satisfying (13) has points on B.

The proof of this lemma may be sketched as follows. Let Λ be any lattice with $\mu(S, \Lambda) = 1$, which does not have any point on the boundary. Then there is a sequence of points $x^r (r=1,2,\ldots)$ of with $|\overline{q}(x^r)| \to 1$. Suppose $\overline{q}(x^r) \to 1$. By applying suitable hyperbolic rotations T_r we get a sequence of lattices $\Lambda_r = T_r\Lambda$ with $\mu(S, \Lambda_r)=1$ $(r=1,2,\ldots)$, $\Lambda_r \ni y^r$, $y^r \to x^0$. A suitable subsequence of the sequence $\{\Lambda_r\}$ converges to some lattice $\overline{\Lambda}$. This lattice $\overline{\Lambda}$ contains the point x^0 and has determinant $d(\overline{\Lambda})=d(\Lambda)$. Further, each point of $\overline{\Lambda}$ is the limit of a point of Λ_r and so $\overline{\Lambda}$ is admissible for S. Hence, by theorem 1, if Λ satisfies (13), then $\overline{\Lambda}$ belongs to the set $\mathcal{L}$. Finally, using the corresponding automorphism W, one can find a neighbourhood N of $\overline{\Lambda}$ and a positive number δ with the following property:

(26) if $\Lambda' \in N$ and Λ' is not homothetic with $\overline{\Lambda}$, then

$$\mu(S, \Lambda') < 1 - \delta$$

(see theorem I in [2], chapter II). This contradicts the properties of the Λ_r, and so proves the lemma.

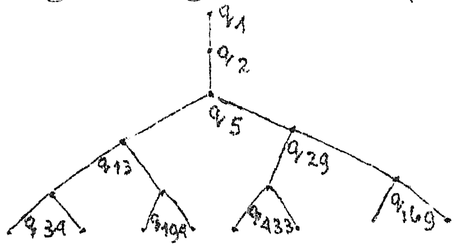
The lattices Λ in $\mathcal{L}$ have points on B_1 as well as B_2. Hence theorem 1 and the lemma together give the following

Theorem 2. Each lattice Λ' with $\mu(S, \Lambda')=1$, $d(\Lambda') < 3$ is of the form $\Lambda' = T\Lambda$, where T is a hyperbolic rotation of S and $\Lambda \in \mathcal{L}$.

This theorem can immediately be put in the following arithmetic form:

Theorem 2'. Let $q=q(x)$ be an indefinite binary quadratic form, of discriminant d. Then $\mu(q) > \frac{1}{3}\sqrt{d}$, if and only if $q \approx q_m = \frac{1}{m}\det(x, Wx)$ for some $W \in |\mathfrak{M}|$ $(m=w_{21})$. Further, $\mu(q) = \sqrt{d/d_m}$, with $d_m = 9-4m^{-2}$, if $q \approx q_m$.

The pairs (U,V), hence also the forms q_m, can be represented by a genealogical tree (see figure). The numbers m associated with three matrices U,V,W=UV, say m_1, m_2, m, satisfy the famous equation of Markov:



(27) $m_1^2 + m_2^2 + m^2 = 3m_1m_2m$.

This relation is easily proved by induction. Cohn deduces it from property I and a general relation for the traces of 2 x 2-matrices. As is well known, one can deduce from theorem 2' a corresponding theorem for the approximation of inationals by rationals.

Final remark. Probably the method of this report can be extended to the more general domain $-1 < x_1x_2 < k$ (k a positive integer).

However, even the second minimum of this region is not yet known (see [4]).

References

[1] A.A. Markoff, Sur les formes quadratiques binaires indéfinies, Math. Annalen 15, 381-409 (1880)

[2] J.W.S. Cassels, An introduction to diophantine approximation, Cambridge 1957

[3] H. Cohn, Approach to Markoff's minimal forms through modular functions, Annals Math. 61, 1-12 (1955)

[4] D.B. Sawyer, The minimum of indefinite binary quadratic forms, Journ. London Math. Soc. 28, 387-394 (1953).