Markov's Theorem on Quadratic Forms

Nadine Merk

April 9, 2020

1 Markov's Theorem

These notes will continue our discussion of Markov forms as started in the notes by Tiziana Busslinger. We will therefore assume familiarity with the content of [3].

In the following, all quadratic forms f considered are binary (i.e. in two variables) and indefinite, that is, take positive and negative values. A form $f(x,y) = \alpha x^2 + \beta xy + \gamma y^2$ is indefinite if and only if its discriminant

$$\delta(f) = \beta^2 - 4\alpha\gamma$$

is positive. The aim is to prove the following theorem (due to Markov [5]) about quadratic forms.

Theorem 1.1. *Let $f(x,y) = \alpha x^2 + \beta xy + \gamma y^2$ be a quadratic form with positive discriminant δ and real coefficients α, β and γ. If we set*

$$\mu = \inf(|f(x,y)|),$$

where the infimum is taken over all integers $(x,y) \neq (0,0)$, we obtain the following.

(a) The inequality $\mu > \frac{1}{3}\delta^{\frac{1}{2}}$ holds if and only if f is equivalent to a multiple of a Markov form.

(b) There are uncountably many quadratic forms, of which none is equivalent to a multiple of any other, such that equality $\mu = \frac{1}{3}\delta^{\frac{1}{2}}$ holds.

Note that the values δ and μ depend on f. If it is clear out of the context to which quadratic form δ and μ belong, we will refrain from writing $\delta(f)$ or $\mu(f)$, such as in the theorem.

The theorem tells us that there is a one-to-one correspondence between quadratic forms, whose infimum over all integral $(x,y) \neq (0,0)$ is bounded form below by $\frac{1}{3}\delta^{\frac{1}{2}}$, and multiples of Markov forms.

Let us for example consider forms of discriminant one. Then the theorem says that such a form typically takes values smaller or equal than $\frac{1}{3}$ (in absolute value) on integer pairs. Indeed, by part (a) there are only countably many forms of discriminant one with $\mu > \frac{1}{3}$ as there are countably many Markov forms. The number $\frac{1}{3}$ is sharp with this property as there are uncountably many forms of discriminant one with $\mu = \frac{1}{3}$ by part (b).

We will briefly recall the main definition of interest. Note that this can be found more thoroughly explained in either [3] or in [4, Ch. II, Sec. 3-4].

Let m, m_1, m_2 be positive integers with

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2, \tag{1}$$

where $m \geq \max(m_1, m_2)$. Such a solution is called *singular* if at least two of m, m_1 and m_2 are equal. Else the solution is called *non-singular*. Recall that there exist unique integers k and l such that

$$k \equiv \frac{m_2}{m_1} \equiv -\frac{m_1}{m_2} \mod m \quad \text{and} \quad k^2 + 1 = lm \tag{2}$$

hold with $0 \leq k < m$. Note that we have a similar statement for m_1 and m_2 in place of m, so that we obtain integers k_1, k_2 and l_1, l_2.

Definition 1.2. Let m be a solution of the Diophantine equation (1) as above. Then the *Markov form* F_m in the variables x and y is defined through the equation

$$mF_m(x,y) = mx^2 + (3m-2k)xy + (l-3k)y^2,$$

where k and l are integers as in (2).

Let us quickly look at some examples. If we consider the set of solutions $(m, m_1, m_2) = (1,1,1)$ of (1), we obtain the first Markov form

$$F_1(x,y) = x^2 + 3xy + y^2.$$

One can check that in this case we have $k = 0$ and $l = 1$. For the set of solutions $(m, m_1, m_2) = (2,1,1)$ we get the second Markov form

$$F_2(x,y) = x^2 + 2xy - y^2,$$

where $k = 1$ and $l = 1$ in this case. Note that $(1,1,1)$ and $(2,1,1)$ are the only singular solutions of (1).

2 Preliminary Results

2.1 Compactness and Isolation

We recall here results from [4, Ch. II, Sec. 2].

Lemma 2.1 (Compactness lemma). *For every integer $j \geq 1$ let*

$$f_j(x,y) = \alpha_j x^2 + \beta_j xy + \gamma_j y^2$$

be an indefinite quadratic form. Suppose that there are positive numbers K_1, K_2, K_3 and $j_0 \geq 1$ such that

$$K_1 \leq |\alpha_j| \leq K_2 \text{ and } |\beta_j| \leq K_3 |\alpha_j|$$

hold for every $j \geq j_0$. Furthermore, assume that the sequence of discriminants $(\delta(f_j))_j = (\beta_j^2 - 4\alpha_j\gamma_j)_j$ converges to $\delta_0 > 0$. Then there is a subsequence $(f_{j_k})_k$ that converges to an indefinite quadratic form f with discriminant δ_0.

By the above convergence statement, we mean that

$$\alpha_{j_k} \to \alpha, \quad \beta_{j_k} \to \beta, \quad \gamma_{j_k} \to \gamma$$

as $k \to \infty$, where $f(x,y) = \alpha x^2 + \beta xy + \gamma y^2$. Note that the existence of a convergent subsequence is a consequence of the fact that α_j, β_j and γ_j are bounded. The latter property follows from the boundedness of the discriminants, the α_j's and the β_j's. Furthermore, any limit must have discriminant δ_0 as $\delta(\cdot)$ is a continuous function in the coefficients of the binary forms. We refer to [4, Ch. II, Lemma 2] for a full proof.

Theorem 2.2 (Isolation theorem). *Let $f(x,y) = \alpha x^2 + \beta xy + \gamma y^2$ be a quadratic form with rational coefficients α, β, γ. Let*

$$\mu = \inf\{|f(x,y)| : (x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}\}$$

and suppose that the following assumptions are satisfied.

(a) The infimum μ is positive.

(b) The polynomial $f(x,1)$ has irrational roots ϕ_1, ϕ_2.

(c) There exists $(x,y) \in \mathbb{Z}^2$ with $f(x,y) = \mu$ and similarly for $-\mu$.

Then there exists $\mu' < \mu$ and $\varepsilon_0 > 0$ depending on the coefficients α, β, γ only with the following property. Suppose that $f^*(x, y)$ is another quadratic form and that α^* is the coefficient of x^2 and ϕ_1^*, ϕ_2^* are the roots of $f^*(x, 1)$. If

$$|\alpha - \alpha^*| < \varepsilon_0, \quad |\phi_1 - \phi_1^*| < \varepsilon_0 \quad \text{and} \quad |\phi_2 - \phi_2^*| < \varepsilon_0,$$

then there is some $(x_0, y_0) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ such that $|f^*(x_0, y_0)| < \mu'$ provided that f^* is not a multiple of f.

Proof. See [4, Ch. 2, Theorem 1]. □

Roughly speaking, the theorem says that any form f^* which is close to f must attain strictly smaller values on $\mathbb{Z}^2 \setminus \{(0,0)\}$ if f^* is not a multiple of f. The latter assumption is crucial as otherwise the infimum attained by $f^* = \lambda f$ would simply be $|\lambda|\mu$ which can be arbitrarily close to μ. We also remark that the assumption (c) rules out forms such as $x^2 - 3y^2$.

Example 2.3. Consider the quadratic form $f(x, y) = x^2 - 3y^2$. We claim that f does not satisfy condition (c) in Theorem 2.2. Suppose by contradiction that it satisfies part (c). Then there exist pairs (x_0, y_0) and (x_1, y_1) such that $x_0^2 - 3y_0^2 = \mu$ and $x_1^2 - 3y_1^2 = -\mu$. But then $x_0^2 + x_1^2 = 3(y_0^2 + y_1^2)$ so that 3 divides $x_0^2 + x_1^2$. The squares in $\mathbb{F}_3$ are 0 and 1 thus x_0^2 and x_1^2 need to be zero modulo 3. But then x_0 and x_1 are divisible by 3 as $\mathbb{F}_3$ is an integral domain. Writing $x_0 = 3\tilde{x}_0$ and $x_1 = 3\tilde{x}_1$ we obtain $3(\tilde{x}_0^2 + \tilde{x}_1^2) = y_0^2 + y_1^2$. Proceeding analogously with reversed roles, we see that y_0 and y_1 are also divisible by 3. In particular, $\frac{1}{3}(x_0, y_0)$ is integral and takes value $\frac{\mu}{3}$ which is impossible.

However, note that f satisfies the conditions (a) and (b) in the theorem. The roots of $f(x, 1)$ are $\pm\sqrt{3}$ so that (b) clearly holds. One can show that the condition in (a) follows from the fact that $\sqrt{3}$ is badly approximable (see [2] for this notion).

Lemma 2.4. *Let $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$ be a quadratic form. Suppose there exist coprime integers a and b such that $f(a, b) = \alpha' \neq 0$. Then there exist integers c and d with $ad - bc = 1$ such that*

$$f(ax + cy, bx + dy) = \alpha' x^2 + \beta' xy + \gamma' y^2$$

holds with $|\beta'| \leq |\alpha'|$.

If we suppose additionally that $\alpha' > 0$, then $f(x, y)$ is also equivalent to a form $\alpha' x^2 + \beta' xy + \gamma' y^2$ with $2\alpha' \leq \beta' \leq 3\alpha'$.

Proof. Suppose that a and b are coprime integers. Then there exist integers c' and d' such that $ad' - bc' = 1$ holds. Let us consider the form

$$f(ax + c'y, bx + d'y) = \alpha' x^2 + \beta'' xy + \gamma'' y^2 =: f_1(x, y)$$

for some coefficients β'' and γ''. Note that the x^2 coefficient of f_1 is indeed α' as $\alpha' = f_1(1, 0) = f(a, b)$. By a geometric argument one finds an integer n such that

$$|\beta'' - 2n\alpha'| \leq |\alpha'|$$

holds as $\alpha' \neq 0$. We set $c = c' + na$ and $d = d' + nb$ and one can check that the statement of the first part of the lemma is satisfied. Denote by $f'(x, y) = \alpha' x^2 + \beta' xy + \gamma' y^2$ the so-obtained form.

Suppose now that $\alpha' > 0$. If $\beta' \geq 0$ we have $0 \leq \beta' \leq \alpha'$ and hence

$$f'(x + y, y) = \alpha'(x + y)^2 + \beta'(x + y)y + \gamma' y^2 = \alpha' x^2 + (2\alpha' + \beta')xy + \gamma'' y^2$$

for some γ'' where $2\alpha' \leq 2\alpha' + \beta' \leq 3\alpha'$ by assumption on β'. If $\beta' < 0$ one can consider the form $f'(x + y, -y)$ and conclude similarly. □

2.2 Properties of Markov Forms

Lemma 2.5. *Let $F_m(x, y)$ be a Markov form. Then $F_m(x, y)$ is equivalent to $-F_m(x, y)$.*

Proof. One can check that the result is true for the Markov forms

$$F_1(x,y) = x^2 + 3xy + y^2 \quad \text{and} \quad F_2(x,y) = x^2 + 2xy - y^2$$

by verifying the equations

$$F_1(x+2y, -x-y) = -F_1(x,y) \quad \text{and} \quad F_2(y,-x) = -F_2(x,y).$$

Hence the statement is true for all singular solutions. We now want to show that

$$F_m(k_1x - l_1y, m_1x - k_1y) + F_m(x,y) = 0 \tag{3}$$

holds for a non-singular solution (m, m_1, m_2), where k_1 and l_1 are such that

$$k_1 \equiv \frac{m}{m_2} \equiv -\frac{m_2}{m} \mod m_1 \quad \text{and} \quad k_1^2 + 1 = l_1 m_2$$

with $0 \leq k_1 < m_1$. We will do this by showing that the left-hand side of equation (3) viewed as a quadratic polynomial in the variable $\frac{y}{x}$ has three distinct solutions and hence must be the zero polynomial.

We first use [3, Lemma 0.5] to see that $(x,y) = (1,0)$ and $(x,y) = (k_1, m_1)$ are solutions of (3). This is indeed true, as

$$F_m(k_1, m_1) = -1 \quad \text{and} \quad F_m(1,0) = 1,$$

where the first equation follows from [3, Lemma 0.5] and the second one always holds. This proves that $(1,0)$ is a solution of (3). On the other hand, we know that

$$k_1^2 - l_1 m_1 = 1 \quad \text{and} \quad m_1 k_1 - k_1 m_1 = 0,$$

where the first equality holds by definition of l_1. Hence, using again [3, Lemma 0.5], it follows that (k_1, m_1) is also a solution of (3).

By using [3, Lemma 0.4] we obtain additionally that $(x,y) = (k,m)$ is a solution of (3) since in this case we have

$$m_1 x - k_1 y = m_1 k - k_1 m = m_2$$

by [3, Lemma 0.4]. However, we also have

$$\begin{aligned} m_1(k_1x - l_1y) &= m_1(k_1k - l_1m) \\ &= m_1k_1k - m(k_1^2 + 1) \\ &= k_1m_2 - m \\ &= m_1k_2 - 3m_1m_2 \\ &= m_1(k_2 - 3m_2), \end{aligned}$$

where the second equality follows by the definition of l_1 and the following three equalities by [3, Lemma 0.4]. Hence, we obtain $k_1k - l_1m = k_2 - 3m_2$. Then we use [3, Lemma 0.5] one last time to see that (k,m) is indeed a solution of (3) and hence the lemma follows. □

Lemma 2.6. *Let $F_m(x,y)$ be a Markov form. Then we have the following estimate. For all integers $(x,y) \neq (0,0)$ we have*

$$|F_m(x,y)| \geq 1.$$

Proof. We set

$$\mu = \min\{|F_m(x,y)| : (x,y) \in \mathbb{Z}^2 \setminus \{0\}\}.$$

As mF_m has integral coefficients, the minimum indeed exists. Hence, there are integers x_0, y_0 with $\mu = |F_m(x_0,y_0)|$. Using Lemma 2.5 we can assume that

$$F_m(x_0, y_0) = \mu. \tag{4}$$

Recall from [3] that we have the relation

$$m^2 F_m(x,y) = \Phi_m(y,z) \tag{5}$$

where $z = mx - ky$ and $\Phi_m(y,z) = y^2 + 3myz + z^2$. Note that for any integral pair (y,z) an integral pair (x,y) with $z = mx - ky$ exists if and only if $z \equiv -ky \mod m$.

Let (x_0, y_0) be a solution of (4) and let $z_0 = mx_0 - ky_0$. If there is more than one solution of (4), we take the solution for which $|y_0| + |z_0| = |y_0| + |mx_0 - ky_0|$ is minimal.

- First, suppose that $y_0 z_0 < 0$ and $|y_0| < |z_0|$. Let $y_1 = 3my_0 + z_0$ and $z_1 = -y_0$. Thus, we have $z_1 \equiv -ky_1 \mod m$ as $z_0 \equiv -ky_0 \mod m$ and $k^2 = lm - 1 \equiv -1 \mod m$. Then

  $$\Phi_m(y_1,z_1) = (3my_0+z_0)^2 + 3m(3my_0+z_0)(-y_0) + y_0^2 = y_0^2 + 3my_0z_0 + z_0^2 = \Phi_m(y_0,z_0)$$

  and hence

  $$0 \le m^2\mu = m^2 F_m(x_0,y_0) = \Phi_m(y_0,z_0) = \Phi_m(z_1,y_1) = z_0y_1 + y_0^2$$

  where the last equality follows from the definition of Φ_m and y_1, z_1. In particular, (y_1, z_1) is a solution of (4) and $-y_0^2 \le z_0 y_1 < z_0^2$ where the second inequality follows from $y_0 z_0 < 0$. So $0 < \frac{-y_0}{z_0} \le y_1 < z_0$ which implies that $|y_1| < |z_0|$. Thus, we have $|y_1| + |z_1| < |y_0| + |z_0|$ as $|z_1| = |y_0|$. But this is a contradiction to the minimality of $|y_0| + |z_0|$.

- Similarly, the case $y_0 z_0 < 0$ and $|y_0| > |z_0|$ gives a contradiction.

- Note also that the case $y_0 = -z_0$ is not possible. Indeed, as $\Phi_m(y_0, -y_0) = -(3m-2)y_0^2 < 0$, but we only consider solutions of $F_m(x,y) = \mu$ which is non-negative.

Thus, we have $y_0 z_0 \ge 0$ or $y_0 = z_0$ but the former case includes the latter so we will assume henceforth that $y_0 z_0 \ge 0$. Let now $y_2 = z_0$ and $z_2 = -y_0$. Then we must have $z_2 \equiv -ky_2 \mod m$ as $k^2 \equiv -1 \mod m$ and (y_0, z_0) satisfies the analogous equation. We then consider

$$|\Phi_m(y_2,z_2)| = |y_0^2 + z_0^2 - 3my_0z_0| \le y_0^2 + z_0^2 + 3my_0z_0 = m^2\mu.$$

But since $\mu = \min\{|F_m(x,y)|\}$ we must have equality. As the triangle inequality applied to the absolute value of a difference of two positive numbers is always strict, we must have $y_0 = 0$ or $z_0 = 0$.

If $y_0 = 0$, then we have $m^2\mu = \Phi_m(0,z_0) = z_0^2 \ge m^2$ where the last inequality follows from $z_0 \equiv -ky_0 \equiv 0 \mod m$ which implies $m | z_0$. Hence, $\mu \ge 1$ in this case.

Similarly, one can show that $m^2\mu = y_0^2 \ge m^2$ in the case $z_0 = 0$. Hence, we also have $\mu \ge 1$. This concludes the proof. $\square$

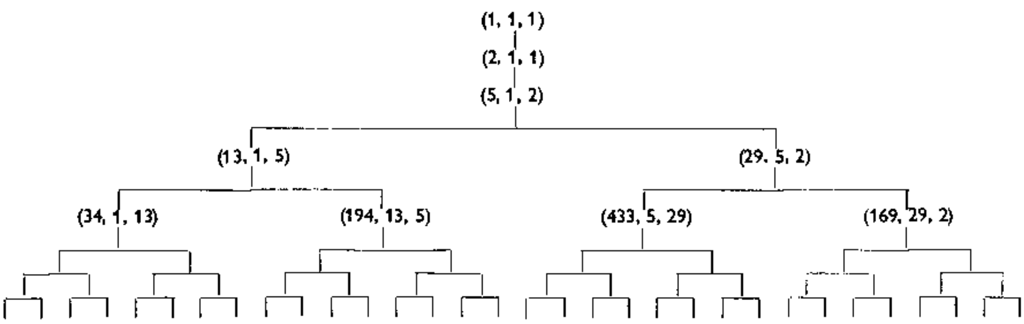

Figure 1: Markov tree of solutions of (1). Picture taken from [4].

2.3 Further Results

Lemma 2.7. *Let $f(x,y) = x^2 + \beta xy + \gamma y^2$ be a quadratic form with β and γ both real numbers. Suppose additionally that $f(k_1, m_1) \le -1$ and $f(k_2 - 3m_2, m_2) \le -1$, where $(m, k : m_1, k_1 : m_2, k_2)$ is an ordered Markov set. Then we have that*

$$\delta(f) \ge \delta(F_m).$$

We remark that $\delta(F_m) = 9 - \frac{4}{m^2}$ (which goes to 9 as $m \to \infty$).

Proof. Let $\Delta = \frac{1}{4}\delta(f)$ and $\Delta_m = \frac{1}{4}\delta(F_m)$ be such that we can write

$$f(x,y) = \left(x + \frac{1}{2}\beta y\right)^2 - \Delta y^2,$$
$$F(x,y) = \left(x + \frac{1}{2}\beta_m y\right)^2 - \Delta_m y^2$$

for every x and y. Hence, we are left to prove

$$\Delta \geq \Delta_m \tag{6}$$

by definition of Δ and Δ_m. By [3, Lemma 0.5] we have the inequality

$$f(x,y) \leq F_m(x,y) \tag{7}$$

for $(x,y) = (k_1, m_1)$ and $(x,y) = (k_1 - 3m_2, m_2)$. For such (x,y) we can thus rewrite equation (7) to obtain

$$\Delta - \Delta_m \geq \left(\frac{x}{y} + \frac{\beta}{2}\right)^2 - \left(\frac{x}{y} + \frac{\beta_m}{2}\right)^2.$$

We now consider two cases.

(1) If $\beta \geq \beta_m$, then equation (6) follows form above with $(x,y) = (k_1, m_1)$. Indeed, we then have

$$\Delta - \Delta_m \geq \left(\frac{k_1}{m_1} + \frac{\beta}{2}\right)^2 - \left(\frac{k_1}{m_1} + \frac{\beta_m}{2}\right)^2 \geq 0$$

since $\frac{k_1}{m_1} \geq 0$ and $\beta \geq \beta_m$.

(2) Suppose now that $\beta \leq \beta_m$ and apply (7) for $(x,y) = (k_2 - 3m_2, m_2)$ to obtain

$$\Delta - \Delta_m \geq \frac{\beta^2}{4} + \frac{3m_2 - k_2}{m_2}(\beta_m - \beta) - \frac{\beta_m^2}{4}.$$

However, we have

$$\frac{3m_2 - k_2}{m_2} \geq 2 > \frac{3m - k}{m} = \frac{\beta_m}{2}$$

so that

$$\Delta - \Delta_m \geq \frac{\beta^2}{4} + \frac{\beta_m}{2}(\beta_m - \beta) - \frac{\beta_m^2}{4} = \frac{1}{4}(\beta_m - \beta)^2 \geq 0$$

as $\beta_m - \beta \geq 0$. This concludes the proof.

□

Lemma 2.8. *Let $f(x,y) = x^2 + \beta xy + \gamma y^2$ be a quadratic form, where β and γ are real numbers. Assume that $f(k,m) \leq -1$ and $f(k - 3m, m) \leq -1$. Then we obtain the estimate*

$$\delta(f) \geq 9 + \frac{4}{m^2} > 9 \tag{8}$$

on the discriminant of f.

Proof. By [3, Lemma 0.5] we have that

$$f(x,y) \leq F_m(x,y) - 2$$

for $(x,y) = (k,m)$ and $(x,y) = (k - 3m, m)$. Then we can proceed similarly as in the proof of Lemma 2.7. □

Lemma 2.9. *We consider again the quadratic form $f(x,y) = x^2 + \beta xy + \gamma y^2$ with real coefficients β and γ that satisfy $2 \leq \beta \leq 3$ and $0 < \beta^2 - 4\gamma < 9$. If we suppose that $|f(x,y)| \geq 1$ for all integers $(x,y) \neq (0,0)$, then $f(x,y)$ is equivalent to a Markov form $F_m(x,y)$.*

For the proof and for later use we define two properties for integral $(x,y) \neq (0,0)$:

$$P_f(x,y) :\iff x^2 + \beta xy + \gamma y^2 \geq 1 \tag{9}$$

$$N_f(x,y) :\iff x^2 + \beta xy + \gamma y^2 \leq -1 \tag{10}$$

given an indefinite form f.

Proof. By assumption, for all integral $(x,y) \neq (0,0)$ either property $N_f(x,y)$ or property $P_f(x,y)$ holds.

First, we note that we have $N_f(1,-1)$. Indeed, as $P_f(1,-1)$ would mean $\gamma \geq \beta$, but this would contradict our assumptions $2 \leq \beta \leq 3$ and $\beta^2 - 4\gamma > 0$. Hence, $N_f(1,-1)$ holds, i.e. $-\beta + \gamma \leq -2$.

We now distinguish two cases:

- If $P_f(0,1)$ holds (meaning that $\gamma \geq 1$), then $\beta \leq 3$ as $\beta \geq \gamma + 2$ by the previous item. But we assumed that $2 \leq \beta \leq 3$ and thus $\beta = 3$. This implies that $\gamma \leq \beta - 2 \leq 1$ so that $\gamma = 1$. Overall, we obtain that $f(x,y) = x^2 + 3xy + y^2$ is the first Markov form.
- Otherwise, suppose that $N_f(0,1)$ holds (meaning that $\gamma \leq -1$). We then consider the integer pair $(x,y) = (-5,2)$ and suppose that property $P(-5,2)$ holds. Thus, $25 - 10\beta + 4\gamma \geq 1$ which implies that

  $$10\beta \leq 24 + 4\gamma \leq 20$$

  using $N_f(0,1)$. As $2 \leq \beta \leq 3$, this shows that $\beta = 2$. The above displayed inequality must thus be an equality so that $24 + 4\gamma = 20$ or in other words $\gamma = -1$. Overall, $f(x,y) = x^2 + 2xy - y^2$ is the second Markov form.

In the following we may thus assume that $N_f(0,1)$ and $N_f(-5,2)$ hold.

We now proceed iteratively by walking through the Markov tree and distingushing cases. The cases treated above corresponded to the first steps of the iteration (the singular solutions). Now let $(m,k;m_1,k_1;m_2,k_2)$ be an ordered Markov set with

$$N_f(k_1,m_1) \text{ and } N_f(k_2 - 3m_2, m_2). \tag{11}$$

We show that either f is a Markov form or (11) holds for a corresponding Markov set below (m,m_1,m_2) in the Markov tree (see Figure 1). To this end, we consider values $f(k,m)$ and $f(k-3m,m)$.

- If both $P_f(k,m)$ and $P_f(k-3m,m)$ hold, $f(x,y) = F_m(x,y)$ by [3, Lemma 0.5].
- Otherwise, at least one of the following two properties hold:
  - Both $N_f(k,m)$ and $N_f(k_2 - 3m_2, m_2)$ are true.
  - Both $N_f(k_1,m_1)$ and $N_f(k-3m,m)$ are true.

  Indeed, this follows from our assumption in (11). Both of the above cases correspond to our assumption in (11) for $(m'_1, k'_1; m, k; m_2, k_2)$ and $(m'_2, k'_2; m_1, k_1; m, k)$ respectively where (m'_1, m, m_2) and (m'_2, m_1, m) are just the vertices below (m, m_1, m_2) in the Markov tree (see Figure 1). We also note that by Lemma 2.8 not both of the above properties can hold.

We conclude from this iteration that $f(x,y)$ is a Markov form or that there exists a unique infinite sequence of Markov sets

$$M^{(j)} = (m^{(j)}, k^{(j)}; m_1^{(j)}, k_1^{(j)}; m_2^{(j)}, k_2^{(j)}) \tag{12}$$

for $j \in \mathbb{N}$ with $m^{(1)} < m^{(2)} < m^{(3)} < \ldots$ and with (11). If the latter were true, (11) together with Lemma 2.8 would imply that $\beta^2 - 4\gamma \geq 9$ as

$$\beta^2 - 4\gamma \geq 9 - 4(m^{(j)})^{-2} \to 9 \tag{13}$$

for $j \to \infty$ which would contradict our assumption on the discriminant of f. Hence, the lemma follows. □

Corollary 2.10. *Let $m > 2$ and $\tilde{m} > 2$ and suppose that $(\tilde{m}, \tilde{m}_1, \tilde{m}_2)$ is on the unique path in Figure 1 from $(1,1,1)$ to (m, m_1, m_2). Let $\tilde{M} = (\tilde{m}, \tilde{k}; \tilde{m}_1, \tilde{k}_1; \tilde{m}_2, \tilde{k}_2)$ be the Markov set for (m, m_1, m_2). Then the Markov form F_m satisfies (11) as in Lemma 2.9 for $\tilde{M}$, i.e. $N_{F_m}(\tilde{k}_1, \tilde{m}_1)$ and $N_{F_m}(\tilde{k}_2 - 3\tilde{m}_2, \tilde{m}_2)$ hold.*

Proof. Let $M = (m, k; m_1, k_1; m_2, k_2)$ be the Markov set corresponding to (m, m_1, m_2) and write $f = F_m$. Then f satisfies the conditions of Lemma 2.9: By Lemma 2.6 we have $|F_m(x,y)| \geq 1$ for all integral pairs $(x, y) \neq (0,0)$. Furthermore, $\delta(F_m) = 9 - 4m^{-2} < 9$ and the xy coefficient of F_m is between 2 and 3 as $0 \leq 2k \leq m$ implies

$$2 = \frac{3m - m}{m} \leq \frac{3m - 2k}{m} \leq \frac{3m}{m} = 3. \tag{14}$$

We are thus able to apply the iteration in the above proof of Lemma 2.9. At each vertex, the iteration either concludes and f is the Markov form at that vertex or it continues to a unique child of that vertex. Since $\delta(f) < 9$ the argument contradicting (12) still applies and the iteration for f must conclude at some vertex. This vertex must be (m, m_1, m_2). Hence, (11) must hold for any vertex visited by the iteration before (m, m_1, m_2) which is the statement of the lemma. □

Lemma 2.11. *There are uncountably many forms $f(x,y) = x^2 + \beta xy + \gamma y^2$ with $2 \leq \beta \leq 3$ and $\beta^2 - 4\gamma = 9$ such that the estimate*

$$|f(x,y)| \geq 1$$

holds for all integers $(x, y) \neq (0,0)$.

Proof. Let $\mathcal{M}$ be an infinite sequence of Markov sets $M^{(j)}$ for $j \in \mathbb{N}$ and

$$M^{(j)} = \left(m^{(j)}, k^{(j)}; m_1^{(j)}, k_1^{(j)}; m_2^{(j)}, k_2^{(j)}\right),$$

where $(m^{(j)}, m_1^{(j)}, m_2^{(j)})$ is

$$\begin{array}{ll} (1,1,1) & j = 1 \\ (2,1,1) & j = 2 \\ (5,1,2) & j = 3 \\ \vdots & \vdots \end{array}$$

and $(m^{(j+1)}, m_1^{(j+1)}, m_2^{(j+1)})$ for $j \geq 3$ is a solution below $(m^{(j)}, m_1^{(j)}, m_2^{(j)})$ (see Figure 1). Hence, the estimates $m^{(1)} < m^{(2)} < m^{(3)} < \ldots$ hold. Note that there are uncountably many of these sequences, since each sequence corresponds to a 0,1-sequence (and $\{0,1\}^{\mathbb{N}}$ is uncountable).

We want to show: each sequence corresponds to a distinct pair β, γ with the properties as in the lemma.

Let $F^{(j)}(x,y) = F_{m^{(j)}}(x,y) = x^2 + \beta^{(j)} xy + \gamma^{(j)} y^2$ for some real coeffcients $\beta^{(j)}, \gamma^{(j)}$. Then

$$\delta(F^{(j)}) = (\beta^{(j)})^2 - 4\gamma^{(j)} = 9 - 4(m^{(j)})^2 \to 9$$

when $j \to \infty$ as $m^{(j)} \to \infty$ when $j \to \infty$.

Now we use the Compactness Lemma 2.1 for these forms $F^{(j)}$. The lemma is indeed applicable as $2 \leq \beta^{(j)} \leq 3$ (see for instance (14)) and as $\delta(F^{(j)}) \to 9$ when $j \to \infty$. Thus, there is a subsequence $j_1 < j_2 < \ldots$ and β, γ real coefficients such that $\beta^{j_\ell} \to \beta$ and $\gamma^{j_\ell} \to \gamma$ for $\ell \to \infty$ and $\beta^2 - 4\gamma = 9$. In particular, $2 \leq \beta \leq 3$. We set $f(x,y) = x^2 + \beta xy + \gamma y^2$. We know that $|F^{(j_\ell)}(x,y)| \geq 1$ for all ℓ and all integral $(x,y) \neq (0,0)$. Hence,

$$|f(x,y)| = \lim_{\ell \to \infty} |F^{(j_\ell)}(x,y)| \geq 1$$

for all integral $(x,y) \neq (0,0)$.

It remains to show that the so-obtained limit forms are uniquely determined by the sequence they were constructed with. The following proof is largely inspired by the argument in Lemma 2.9. So suppose that $\mathcal{M} = (M^{(j)})_{j\in\mathbb{N}}$ and $\overline{\mathcal{M}} = (\overline{M}^{(j)})_{j\mathbb{N}}$ are two distinct sequences and that $f, \overline{f}$ are the respective corresponding forms constructed as above. Since $\mathcal{M}$ and $\overline{\mathcal{M}}$ are distinct, there exists a unique integer J with $M^{(j)} = \overline{M}^{(j)}$ for all $j \leq J$ and with $M^{(J+1)} \neq \overline{M}^{(J+1)}$. Let us write $M = M^{(J)} = (m, k; m_1, k_1; m_2, k_2)$ for simplicity. By the above, the properties $N_f(k_1, m_1)$, $N_f(k_2 - 3m_2)$, $N_{\overline{f}}(k_1, m_1)$, $N_{\overline{f}}(k_2 - 3m_2)$ hold. As in the proof of Lemma 2.9 either of the following two statements are true for $g = F_{m^{(j)}}$ or $g = F_{\overline{m}^{(j)}}$ when $j > J$:

(a) Both $N_g(k, m)$ and $N_g(k_2 - 3m_2, m_2)$ are true.

(b) Both $N_g(k_1, m_1)$ and $N_g(k - 3m, m)$ are true.

Which of these statements is true is determined by the child of M in the sequence $\mathcal{M}$ resp. $\overline{\mathcal{M}}$. But the children are distinct by choice of J as $M^{(J+1)} \neq \overline{M}^{(J+1)}$. So let us suppose without loss of generality that (a) is true for all $g = F_{m^{(j)}}$ and $j > J$ and that (b) is true for all $g = F_{\overline{m}^{(j)}}$ and $j > J$. Thus, we have

$$F_{m^{(j)}}(k, m) \leq -1 \text{ and } F_{m^{(j)}}(k_2 - 3m_2, m_2) \leq -1$$

which implies by taking limits for $j \to \infty$ that (a) holds for f. Analogously, (b) holds for $\overline{f}$. Since $\delta(f) = 9$, Lemma 2.8 implies that (b) cannot hold for f and hence f and $\overline{f}$ must be distinct. This concludes the proof. □

3 Proof of Markov's Theorem for Minima of Quadratic Forms

In this section we present a detailed proof of Theorem 1.1. However, for the sake of the reader we shall give a quick overview of the proof.

For the sufficient condition in (a) we use that the inequality $\mu(f') > \frac{1}{3}\delta(f')^{\frac{1}{2}}$ is invariant under multiples of f', where f' is any quadratic form. The concrete shape of a Markov form F_m allows us then to show the inequality first for F_m and hence for f.

The converse direction of (a) needs a bit more work. We will distinguish cases according to whether the infimum $\mu(f)$ is attained or not. In both cases we will use Lemma 2.4 to obtain that f is equivalent to a form f' whose coefficients are in some way better to work with.

The first case is more direct and can be found in all detail in the proof. In the case where the infimum is not attained, we will get a sequence $(f_n)_n$ of forms whose members are of the same shape as f'. The Compactness Lemma 2.1 then allows us to find a converging subsequence of $(f_n)_n$. We will then apply the Isolation Theorem 2.2 to the limit to conclude.

Lastly, part (b) will be a consequence of Lemma 2.11.

Proof of Theorem 1.1. Let $f(x,y) = \alpha x^2 + \beta xy + \gamma y^2$ be a quadratic form with positive discriminant $\beta^2 - 4\alpha\gamma$ and the fixed value μ as in Theorem 1.1.

(a) We will start by showing part (a) of the theorem. To do this, we will first prove that if f is equivalent to a multiple of a Markov form, then $\mu > \frac{1}{3}\delta^{\frac{1}{2}}$.

Let $F_m(x,y)$ be a Markov form such that f is equivalent to a multiple of F_m. Analogously as in the theorem we denote by

$$\mu(F_m) = \inf(|F(x,y)|)$$

the infimum over the absolute value of $F_m(x,y)$, where x and y are not both 0.

By Lemma 2.6 we have that $|F_m(x,y)| \geq 1$ for all x and y that are not both 0. Thus, $\mu(F_m) \geq 1$ follows. On the other hand, the discriminant of $F_m(x,y)$ given by

$$\delta(F_m) = \left(\frac{3m - 2k}{m}\right)^2 - 4\left(\frac{l - 3k}{m}\right),$$

which is strictly smaller than 9 as one can check by calculating and using properties of m and k as part of a Markov set. This yields $1 > \frac{1}{3}\delta(F_m)^{\frac{1}{2}}$ and we can conclude that $\mu(F_m) > \frac{1}{3}\delta(F_m)^{\frac{1}{2}}$.

Note that the inequality $\mu(f') > \frac{1}{3}\delta(f')^{\frac{1}{2}}$ is invariant under multiples of any quadratic form f'. Hence, the inequality $\mu(F_m) > \frac{1}{3}\delta(F_m)^{\frac{1}{2}}$ also holds for any multiple of F_m. In particular, for the multiple of F_m to which f is equivalent to. As the discriminant δ and the value of μ are invariant under equivalences of forms, the inequality follows also for f.

Let us now show the converse. Suppose that f is a quadratic form with positive discriminant δ that satisfies $\mu > \frac{1}{3}\delta^{\frac{1}{2}}$. We can assume without loss of generality that $\mu = 1$, else we simply replace f by $\mu^{-1}f$. Hence, we additionally have that $9 > \delta > 0$.

We have by assumption that $1 = \mu = \inf(|f(x,y)|)$. Thus, for all $\varepsilon > 0$ there exist integers a and c such that

$$1 \leq |f(a,c)| < 1 + \varepsilon.$$

Note that we can assume that a and c are coprime, else we would replace a and c by $(\gcd(a,c))^{-1}a$ respectively $(\gcd(a,c))^{-1}c$.

We then claim that for every $\varepsilon > 0$ either the form $f(x,y)$ or $-f(x,y)$ is equivalent to a form $f'(x,y) = \alpha' x^2 + \beta' xy + \gamma' y^2$, so that

$$1 \leq \alpha' < 1 + \varepsilon \quad \text{and} \quad 2\alpha' \leq \beta' \leq 3\alpha.$$

This is indeed true as the following observations show.

Since a and c are coprime, we can apply Lemma 2.4 to obtain a form $f'(x,y) = \alpha' x^2 + \beta' xy + \gamma' y^2$ that is equivalent to either $f(x,y)$ or $-f(x,y)$, depending on the sign of $f(a,c)$. On its coefficients the form f' satisfies the estimates

$$1 \leq \alpha' < 1 + \varepsilon \quad \text{and} \quad 2\alpha' \leq \beta' \leq 3\alpha',$$

where the first inequality on α' follows from $\mu(f') = \mu(f) = 1$, the second one on α' is a consequence of $\alpha' = f'(1,0) = |f(a,c)| < 1 + \varepsilon$ and lastly the inequalities on β' follow directly from Lemma 2.4. Hence, the claim follows.

We will now distinguish two cases.

(1) Suppose that the infimum is attained, that is there exist coprime integers a and c such that $1 = |f(a,c)|$. Using the claim we obtain a form $f'(x,y) = \alpha' x^2 + \beta^x y + \gamma y^2$ that is equivalent to either f or $-f$ with $2\alpha' \leq \beta' \leq 3\alpha'$. Note that f' is equivalent to f in the case $f(a,c) > 0$ and to $-f$ in the case $f(a,c) < 0$. Therefore, it follows that $\alpha' = f'(1,0) = 1$ in every of the two cases. Since f and $-f$ have the same discriminant it follows that $\delta(f') = \delta(f) = \delta(-f)$. Hence, all conditions of Lemma 2.9 apply to $f'(x,y)$. Thus $f'(x,y)$ is equivalent to a Markov form $F_m(x,y)$.
Since f' is equivalent to f or $-f$, it follows that either $f(x,y)$ or $-f(x,y)$ is also equivalent to $F_m(x,y)$. If the first case applies we are done. In the second case we use that $F_m(x,y)$ is equivalent to $-F_m(x,y)$ by Lemma 2.5, and therefore we are also done in the second case.

(2) Suppose now that the infimum is not attained. Let $n \geq 1$ be an integer. Using the claim on $\varepsilon_n = \frac{1}{n}$, we obtain an infinite sequence $(f_n)_n$ of quadratic forms given by

$$f_n(x,y) = \alpha_n x^2 + \beta_n xy + \gamma_n y^2,$$

where f_n is equivalent to either $f(x,y)$ or $-f(x,y)$ and satisfies $1 \leq \alpha_n < 1 + \varepsilon_n$, $2\alpha_n \leq \beta_n \leq 3\alpha_n$ and $\beta_n^2 - 4\alpha_n\gamma_n = \delta(f)$, where the latter equality follows from the same argument as in (1). Since $|f_n(x,y)| \geq 1$ holds for all integral $(x,y) \neq (0,0)$ by assumption, we also have $|f_n(x,y)| \geq 1$ for all non-zero integral (x,y).
We will now show that this sequence, or at least a subsequence, converges to a limit in the sense of the Compactness Lemma 2.1. To see this, we first note that $1 \leq \alpha_n < 1 + \varepsilon_n$ implies that $\alpha_n \to 1$ by our choice of ε_n. Using the Compactness Lemma 2.1 we can then suppose, by passing to a subsequence if necessary, that $(\beta_n)_n$ and $(\gamma_n)_n$ converge to limits β_0 respectively γ_0. We then consider the form

$$f_0(x,y) = x^2 + \beta_0 xy + \gamma_0 y^2.$$

Note that $|f_0(x,y)| = \lim_{n\to\infty} |f_n(x,y)| \geq 1$ as $n \to \infty$ for all integral $(x,y) \neq (0,0)$. Hence, one can check that all conditions of Lemma 2.9 apply and thus $f_0(x,y) = F_m(x,y)$ for a Markov form $F_m(x,y)$. However, we might not have that f_0 is equivalent to a f_n for some n. So we are not quite done yet.

Let us consider the roots Φ, θ of the polynomial $f_0(x,1)$ and the roots Φ_n, θ_n of the polynomial $f_n(x,1)$ for a positive integer n. Then we have

$$\Phi_n \to \Phi \quad \text{and} \quad \theta_n \to \theta$$

as $n \to \infty$. This is true because the roots Φ_n, θ_n are given by

$$\Phi_n, \theta_n = \frac{-\beta_n \pm \sqrt{\beta_n^2 - 4\gamma_n}}{2}.$$

If we use the convention that Φ_n is always the root with positive sign before the square root and θ_n the root with negative sign, we get the convergence of the roots since $(\beta_n)_n$ and $(\gamma_n)_n$ converge to β respectively γ.

We now want to apply the Isolation Theorem 2.2 to $F_m = f_0$. For this, note that F_m attains values -1 and 1 by [3, Lemma 0.5]. Furthermore, $F_m(x,1) = f_0(x,1)$ has only irrational roots as a rational root would yield a contraciction to $|f_0(x,y)| \geq 1$. Then we can apply the Isolation Theorem 2.2 to F_m and obtain $\mu' < \mu = 1$ and ε_0 as in the theorem. Then f_n for sufficiently large n will satisfy the estimates

$$|\Phi - \Phi_n| < \varepsilon_0 \quad \text{and} \quad |\theta - \theta_n| < \varepsilon_0$$

by convergence of the roots. On the other hand we have $|f_n(x,y)| \geq 1 > \mu'$. So we must have that f_n is a multiple of F_m and thus the statement follows.

(b) It is left to prove part (b) of the theorem. This will be fairly short compared to the proof of the first part as shows the following.

Under the assumption $\mu = 1$, we have to show that there are uncountably many, none a multiple of another, forms with discriminant 9. To prove the statement, note that for any given form f there are only countably many forms $f'(x,y) = f(ax+by, cx+dy)$, where a, b, c and d are integers. Hence, there are only countably many forms equivalent to f. Lemma 2.11 then yields the statement in part (b) and hence the theorem follows.

□

References

[1] M. Aigner. *Markov's theorem and 100 years of the Uniqueness Conjecture: a mathematical journey from irrational numbers to perfect matchings.* Springer, 2013.

[2] D. Akhmedov. *Badly approximable numbers.* Notes, 2020.

[3] T. Busslinger. *Markov's theorem on quadratic forms.* Notes, 2020.

[4] J.W.S. Cassels. *An introduction to Diophantine approximation.* Cambridge Tracts in Math., vol. 45, Cambridge Univ. Press, 1957.

[5] A.A. Markov. Sur les formes binaires indefinies, I. *Math. Ann.* 15 (1879), 281-309.