Archimedean Quadratic Modules

A Decision Procedure in Dimension Two

Dissertation

zur Erlangung des akademischen Grades

des Doktors der Naturwissenschaften

am Fachbereich Mathematik und Statistik

der Universität Konstanz

Maria Eugênia Canto Cabral

Tag der mündlichen Prüfung: 10. Januar 2005

Erster Referent: Prof. Dr. Alexander Prestel (Konstanz)

Zweiter Referent: Prof. Dr. Claus Scheiderer (Konstanz)

Maria Eugênia Canto Cabral
Fachbereich Mathematik und Statistik
Universität Konstanz
78457 Konstanz
Deutschland

maria.cabral@uni-konstanz.de

Zusammenfassung

Es seien A der Polynomring in n Variablen über $\mathbb{R}$ und $h_1, \ldots, h_m \in A$. Wir bezeichnen mit ΣA^2 die Menge aller endlichen Summen von Quadraten des Ringes A.

1991 bewies Schmüdgen den folgenden Satz: Wenn die semialgebraische Menge $W(h) := \{a \in \mathbb{R}^n | \quad h_i(a) \geq 0 \text{ für } i = 1, \ldots, m\}$ kompakt ist, dann gilt

$$\forall f \in A : f > 0 \text{ auf } W(h) \Rightarrow f \in \sum_{\nu_i \in \{0,1\}} h_1^{\nu_1} \cdots h_m^{\nu_m} \Sigma A^2.$$

2001 bewiesen Jacobi und Prestel unter der selben Voraussetzung ein abstraktes Kriterium dafür, wann die folgende stärkere Implikation gilt:

$$\forall f \in A : f > 0 \text{ auf } W(h) \Rightarrow f \in \Sigma A^2 + h_1 \Sigma A^2 + \cdots + h_m \Sigma A^2 \tag{1}$$

Als Korollar erhält man: Für $n = 1$ und m beliebig, als auch für n beliebig und $m = 2$ gilt (1). Bereits für den Fall $n = 2$ gibt es Beispiele von Polynomen $h_1, \ldots, h_m \in A$ mit $W(h)$ kompakt, für die (1) nicht gilt.

In der folgenden Arbeit präsentieren wir ein effektives algorithmisches Verfahren für den Fall $n = 2$, welches uns zu entscheiden erlaubt, wann (1) gilt.

Das Verfahren basiert auf einer Reduktion der gemäß Jacobi und Prestel durchzuführenden Tests, die schon für $n > 2$ aufgrund der komplizierteren Bewertungstheorie nicht mehr möglich ist. In der Tat ist es für $n > 2$ unbekannt, ob die Frage, wann (1) gilt, überhaupt entscheidbar ist oder nicht.

Abstract

Let A be the polynomial ring in n Variables over $\mathbb{R}$ and $h_1, \ldots, h_m \in A$. We will denote by ΣA^2 the set of all finite sums of squares of the ring A.

In 1991 Schmüdgen proved the following theorem: If the semialgebraic set $W(h) := \{a \in \mathbb{R}^n | \quad h_i(a) \geq 0 \text{ for } i = 1, \ldots, m\}$ is compact, then

$$\forall f \in A : f > 0 \text{ in } W(h) \Rightarrow f \in \sum_{\nu_i \in \{0,1\}} h_1^{\nu_1} \cdots h_m^{\nu_m} \Sigma A^2.$$

In 2001 Jacobi and Prestel proved under the same assumption an abstract criterion for the following stronger condition to hold:

$$\forall f \in A : f > 0 \text{ in } W(h) \Rightarrow f \in \Sigma A^2 + h_1 \Sigma A^2 + \cdots + h_m \Sigma A^2 \tag{2}$$

As a corollary one obtains: For $n = 1$ and arbitrary m, (2) holds, as well as for n arbitrary and $m = 2$. Already for the case $n = 2$ there exist examples of polynomials $h_1, \ldots, h_m \in A$ with $W(h)$ compact for which (2) does not hold.

In the following work we present an algorithmic procedure for the case $n = 2$, which enable us to decide when (2) holds.

The procedure is based on a reduction of the tests to be done according to Jacobi and Prestel which is already for $n > 2$ no longer possible, because of the more complicated valuation theory. In fact, for $n > 2$, it is unknown, if the question when (2) holds is decidable or not.

Danksagung

Zuallererst möchte ich mich bei Prof. Dr. Alexander Prestel ganz herzlich bedanken. Ohne seine Betreuung wäre diese Arbeit nicht zustande gekommen.

Den Arbeitskollegen Markus Schweighofer und Karim Johannes Becher bin ich ebenfalls sehr dankbar.

Bei meiner Großmutter Madalena Canto und der Freundin Luziânia Pinheiro möchte ich mich für die emotionale Unterstützung bedanken, sowie bei meinen Freunden aus Winterthur (insbesondere Gorete Newton).

Contents

Chapter 1

Introduction

Let $h_1, \ldots, h_m$ be polynomials in n variables with real coefficients. The semialgebraic set defined by $h_1, \ldots, h_m$, and denoted by $W(h)$, is the subset of the $\mathbb{R}^n$ where all the polynomials $h_1, \ldots, h_m$ are nonnegative. Let A be the polynomial ring $\mathbb{R}[X_1, \ldots, X_n]$. The interest on Archimedean quadratic modules comes from questions related to the characterization of the polynomials in A that are strictly positive on the set $W(h)$. These characterization is very important for example in Optimization.

In 1991 Schmüdgen proved that for $W(h)$ compact we have: for all $f \in A$, if $f > 0$ on $W(h)$ necessarily

$$f \in \sum_{\nu_i \in \{0,1\}} h_1^{\nu_1} \ldots h_m^{\nu_m} \sum A^2,$$

where $\sum A^2$ denote the set of finite sums of squares in A.

For applications if we have a conciser representation much better. So, a natural question is, assuming that $W(h)$ is compact, when is it possible to discard the products in the representation above.

Thus, one would like to know when holds the following stronger implication:

$$\forall f \in A : f > 0 \text{ on } W(h) \Rightarrow f \in \sum A^2 + h_1 \sum A^2 + \cdots + h_m \sum A^2. \quad (1.1)$$

Let $M(h) := \sum A^2 + h_1 \sum A^2 + \cdots + h_m \sum A^2$. This subset of the ring A contains the element 1, is closed under addition and closed under multiplication by squares. If in addition $-1 \notin M(h)$, then M(h) is called a *quadratic module* of the ring A. A quadratic module $M \subset A$ is *Archimedean* if for every $f \in A$ there is a $N \in \mathbb{N}$ with $N - f \in M$.

Thomas Jacobi proved in his PhD-thesis that if $M(h)$ is a quadratic module, then the following are equivalent:

(a) $W(h)$ is compact and for all $f \in \mathbb{R}[X_1, \ldots, X_n]$: $f > 0$ on $W(h)$ implies $f \in M(h)$;

(b) M(h) is Archimedean.

The proof that (a) implies (b) is trivial if one knows the Theorem 2.3 below. The other implication is a consequence of the Representation Theorem for quadratic modules (T.Jacobi).

Thus, in order to answer the question above, one has to investigate when $M(h)$ is Archimedean. The Jacobi-Prestel Criterion stated below gives an abstract characterization of the polynomials $h_1, \ldots, h_m$ for which the module $M(h)$ is Archimedean.

Let $h_1, \ldots, h_m \in A$, $W(h)$ and $M(h)$ as above. For a real prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$ we define $F_{\mathfrak{p}} := Quot(A/\mathfrak{p})$ and $\Re_\infty(\mathfrak{p})$ to be the set of residually real valuations v on $F_{\mathfrak{p}}$ for which $v(X_i + \mathfrak{p}) < 0$ for some $i = 1, \ldots, n$.

Jacobi-Prestel Criterion. *Suppose that $W(h)$ is compact and $M(h)$ is a quadratic module. Then the following facts are equivalent:*

(a) $M(h)$ is Archimedean;

(b) For every real prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$ and for every valuation $v \in \Re_\infty(\mathfrak{p})$ the regular part of the quadratic form

$$\langle 1, h_1 + \mathfrak{p}, \ldots, h_m + \mathfrak{p} \rangle$$

is weakly isotropic over the Henselization of $F_{\mathfrak{p}}$ with respect to the valuation v.

As an important corollary of the Jacobi-Prestel Criterion one has: when the semialgebraic set $W(h)$ is defined only by two polynomials, then $M(h)$ is Archimedean. This is also true for only one indeterminate and an arbitrary number of polynomials. For the case $n = 2$ there are examples of both situations, Archimedean and not Archimedean modules.

In this Thesis, for the case $n = 2$, the Jacobi-Prestel Criterion will be transformed in an effective algorithm, which permits to test if the module $M(h)$ is Archimedean or not.

Chapter 2

Preliminaries

The notation of this work is mainly taken from [PD]. This applies in particular to the valuation theory used here.

The main goal of this chapter is to prove some results that will be useful later, specially the Characterization Theorem of Jacobi-Prestel, which will be very important for the algorithmic procedure that will be described in the next chapters.

In what follows A will always denote the polynomial ring $\mathbb{R}[X_1, \ldots, X_n]$. The set of polynomials which are a square of the ring A, i. e., the elements $f \in A$ such that $f = a^2$ for some $a \in A$, will be denoted by A^2. The set of all finite sums of squares will be denoted by $\sum A^2$.

For polynomials $h_1, \ldots, h_m \in A$ one defines the following sets:

$$W(h) := W(h_1, \ldots, h_m) := \{a \in \mathbb{R}^n | \quad h_i(a) \geq 0 \text{ for } i = 1, \ldots, m\} \quad ;$$

$$M(h) := M(h_1, \ldots, h_m) := \sum A^2 + h_1 \sum A^2 + \cdots + h_m \sum A^2.$$

Definition 2.1. A subset $M \subset A$ is called a *quadratic module* if it has the following properties : $1 \in M$, $M + M \subset M$, $A^2.M \subset M$ and $-1 \notin M$. A quadratic module $M \subset A$ is said to be *Archimedean* if for every $f \in A$ there is an $N \in \mathbb{N}$ such that $N - f \in A$.

Remark 2.2. (i) $M(h)$ is a quadratic module if, and only if, $-1 \notin M(h)$.

(ii) $W(h) \neq \emptyset$ implies that $M(h)$ is a quadratic module. The converse is not true. For an example of $W(h) = \emptyset$ and $-1 \notin M(h)$ see [PD], exercise 5.5.7.

(iii) Note that if $M(h)$ is Archimedean, then the semialgebraic set $W(h)$ is necessarily compact.

The next theorem says that in order to verify that a quadratic module $M \subset A$ is Archimedean it is sufficient to check the condition above only for the polynomial $\sum_{i=1}^n X_i^2$, instead of all elements $f \in A$.

Theorem 2.3. *Let M be a quadratic module of the ring A. Then*

$$M \quad is \quad Archimedean \Leftrightarrow N - \sum_{i=1}^{n} X_i^2 \quad \in \quad M \quad for \quad some \quad N \in \mathbb{N}.$$

Proof: ($\Rightarrow$) Follows immediately from the definition.
($\Leftarrow$) Let $f := N - \sum_{i=1}^n X_i^2$. By the hypothesis $f \in M$. Therefore, for each $i = 1, \ldots, n$,

$$(N + \frac{1}{4}) \pm X_i = (\frac{1}{2} \pm X_i)^2 + f + \sum_{j \neq i} X_i^2 \quad \in \quad \sum A^2 + f \sum A^2 \subset M.$$

Thus for every $a \in \mathbb{R} \cup \{X_1, \ldots, X_n\}$ there exists an $m \in \mathbb{N}$ with $m \pm a \in M$. Now, using induction on the complexity of elements of the ring A, suppose that for $g, h \in A$ there are $r, s \in \mathbb{N}$ such that $r \pm g \in M$ and $s \pm h \in M$. Then $(r+s) \pm (g+h) \in M$ and, as the set $\sum A^2 + f \sum A^2$ is closed under multiplication, follows that

$$3rs - gh = (r + g)(s - h) + r(s + h) + s(r - g) \quad \in \quad \sum A^2 + f \sum A^2$$

and therefore $3rs - gh \in M$. Similarly one obtains $3rs + gh \in M$.

$\square$

Example 2.4. Let $h_i = X_i$ for $i = 1, \ldots, n$ and $h_{n+1} = 1 - \sum_{i=1}^n X_i$ and consider $M = M(h)$. Thus for every $i = 1, \ldots, n$ one has

$$1 - X_i = (1 - \sum_{i=1}^{n} X_i) + \sum_{j \neq i} X_j \in M.$$

Trivially $1 + X_i \in M$. Consequently for all $a \in \mathbb{R} \cup \{X_1, \ldots, X_n\}$ there exists an $m \in \mathbb{N}$ such that $m \pm a \in M$. Thus, it follows from the proof of the theorem 2.3 that $M(h)$ is Archimedean. Or explicitly :

$$n - \sum_{i=1}^{n} X_i^2 = \sum_{i=1}^{n} \frac{1}{2}(1 + X_i)^2(1 - X_i) + \frac{1}{2}(1 - X_i)^2(1 + X_i) \in M.$$

Definition 2.5. A *semiordering* of the ring A is a quadratic module $S \subset A$ with the additional properties: $S \cup -S = A$ and $S \cap -S$ is a prime ideal of A.

Theorem 2.6. *Let $h_1, \ldots, h_m \in A$ and suppose that $M(h)$ is a quadratic module. Then the following are equivalent:*

(i) $M(h)$ is Archimedean;

(ii) Every semiordering S of A which contains $M(h)$ is Archimedean.

For a proof of this theorem see ([PD], pg. 119).

Example 2.7. Suppose that $n \geq 2$. Let $h_i = X_i - \frac{1}{2}$ for $i = 1, \ldots, n$ and $h_{n+1} = 1 - \prod_{i=1}^n X_i$. In this case, $W(h)$ is compact but the quadratic module $M(h)$ is not Archimedean. There is a semiordering of $\mathbb{R}(X_1, \ldots, X_n)$ containing $M(h)$ such that for all $N \in \mathbb{N}$ one has $N - \sum X_i^2 \in -S$. (See [PD], Example 6.1.2).

The next theorem provides a connection between Archimedeanness and weak isotropy of quadratic forms. In order to state it, one needs some definitions.

A prime ideal $\mathfrak{p}$ of A is said to be *real* if the quotient ring $A/\mathfrak{p}$ is a real ring. The quotient field of the integral domain $A/\mathfrak{p}$ will be denoted by $F_{\mathfrak{p}}$. For a diagonal quadratic form $\langle a_1, \ldots, a_m \rangle$ over a field K the form obtained from this one by discarding all zeros of the diagonal entries is called its *regular part* and will be denoted by $\langle a_1, \ldots, a_m \rangle^*$.

In what follows we will consider the canonical residue homomorphism

$$\bar{\ }: A \twoheadrightarrow A/\mathfrak{p}.$$

Theorem 2.8. *Let $h_1, \ldots, h_m$ be polynomials in A such that the set $M(h)$ is a quadratic module. The following are equivalent:*

(1) The module $M(h)$ is Archimedean ;

(2) There is an $N \in \mathbb{N}$ such that $N - \sum_{i=1}^n X_i^2 \in S \setminus -S$ for all semiorderings S of A which contain $M(h)$;

(3) There is an $N \in \mathbb{N}$ such that for all real prime ideals $\mathfrak{p}$ of A the regular quadratic form $\left\langle 1, -\overline{(N - \sum_{i=1}^n X_i^2)}, \bar{h}_1, \ldots, \bar{h}_s \right\rangle^*$ is weakly isotropic over the field $F_{\mathfrak{p}}$.

For the proof of this Theorem we need the following result:

Weak Positivstellensatz. *Suppose M is a quadratic module of A, and $f \in A$. Then the following are equivalent:*

(i) $f \in S \backslash -S$ *for all semiorderings S of A that contain M;*

(ii) $\sigma f = 1 + m$, *for some $\sigma \in \sum A^2$ and some $m \in M$.*

Proof: $(i) \Rightarrow (ii)$: Suppose $f \sum A^2 \cap (1 + M) = \emptyset$. Then $M' := M - f \sum A^2$ is a quadratic module. Choose a maximal quadratic module S containing M', by Zorn's lemma. Then S is a semiordering with $M \subseteq S$, by [PD], Proposition 5.1.4. Then $f \notin S \backslash -S$, since $-f \in S$.
$(ii) \Rightarrow (i)$: Let S be a semiordering of A which contains M. For $m \in M$ we have $1 + m \in S \backslash -S$, otherwise $-1 \in S$. Therefore $\sigma f = 1 + m$ yields $\sigma f \in S \backslash -S$. Hence $f \in S \backslash -S$.

□

Now we are able to prove Theorem 2.8.

Proof of Theorem 2.8: $(1) \Rightarrow (2)$: By definition there is an $N' \in \mathbb{N}$ such that $N' - \sum X_i^2 \in M(h)$. Thus $1 + N' - \sum X_i^2 \in M(h)$ and therefore $1 + N' - \sum X_i^2 \in S$ for every semiordering S of A which contains $M(h)$. If $1 + N' - \sum X_i^2 = -a$, for some $a \in S$, then -1 will be in S, contradicting the fact that S is a semiordering. Thus $1 + N' - \sum X_i^2 \in S \backslash -S$.

$(2) \Rightarrow (3)$: Let $f := N - \sum_{i=1}^n X_i^2$. By the weak Positivstellensatz there is a $\sigma \in \sum A^2$ with $\sigma f \in 1 + M$. Thus there are $\sigma_0, \dots, \sigma_s \in \sum A^2$ such that

$$0 = -\sigma f + 1 + \sigma_0 + \sigma_1 h_1 + \cdots + \sigma_s h_m.$$

Therefore, passing to the quotient ring $A/\mathfrak{p}$ we obtain that $\langle 1, -\bar{f}, \bar{h}_1, \dots, \bar{h}_s \rangle^*$ is weakly isotropic over the field $F_{\mathfrak{p}}$.

$(3) \Rightarrow (2)$: First observe that if a regular quadratic form $\langle a_1, \dots, a_m \rangle$ is weakly isotropic over a field K, then it is indefinite with respect to all semiorderings of K. In fact, if $\sum_i \sigma_i a_i = 0$ for some $\sigma_i \in \sum K^2$ not all zero, say $\sigma_j \neq 0$, then $-a_j = \sum_{i \neq j} \frac{\sigma_i}{\sigma_j} a_i$. Consequently, $a_j \in -S$ if $a_i \in S$ for all $i \neq j$. Let S be a semiordering of A which contains $M(h)$ and let $\mathfrak{p} := S \cap -S$. Then $\bar{S}$ is a semiordering of $\bar{A} := A/\mathfrak{p}$ with $\bar{S} \cap -\bar{S} = \{0\}$. Thus the ideal $\mathfrak{p}$ is real and $\bar{S}$ extends to a semiordering of $F_{\mathfrak{p}}$. By the hypothesis the form $\langle 1, -\bar{f}, \bar{h}_1, \dots, \bar{h}_s \rangle^*$ is weakly isotropic over the field $F_{\mathfrak{p}}$, where $f := N - \sum_{i=1}^n X_i^2$. Since each $h_i \in M(h) \subset S$, we have $\bar{h_1}, \dots, \bar{h_m} \in \bar{S}$. Thus $\bar{f} \in \bar{S} \backslash \{0\}$. Hence $f \in S \backslash -S$.

$(2) \Rightarrow (1)$: By theorem 2.3 every semiordering S of A containing $M(h)$ is Archimedean. So by theorem 2.6, it follows that $M(h)$ is Archimedean too.

□

A very important result which will be useful to prove the Characterization Theorem is the Local-Global Principle for Weak Isotropy, which was proved independently by Bröcker and Prestel in 1974 (for a proof see, for example, [Pr1]).

Theorem 2.9 (Local-Global Principle of Bröcker-Prestel). *Let K be a real field and ρ a quadratic form over K. If ρ is indefinite with respect to every Archimedean ordering of K and weakly isotropic over all henselizations of K with respect to every non-trivial residually real valuations, then ρ is weakly isotropic over K.*

The goal of this work is to present an algorithm to verify whether the quadratic module $M(h)$ is Archimedean or not. By Theorem 2.8, the problem is then reduced to test the weak isotropy of a quadratic form over a real field. The Local-Global Principle above suggests to check this condition over Henselian fields. However, for real Henselian fields one can test the weak isotropy on its residue field. This is the claim of the next proposition. To state it one needs to define the residue forms.

Definition 2.10. Let $\rho = \langle a_1, \ldots, a_m \rangle$ be a regular quadratic form over K (of characteristic $\neq 2$) and v a valuation of K with $v(K^\times) =: \Gamma$. Write $\rho \cong \rho^{(1)} \perp \cdots \perp \rho^{(t)}$ with $\rho^{(i)} := \langle a_{i1}, \ldots, a_{ir_i} \rangle$ obtained from ρ by grouping the entries with the same value modulo 2Γ. Choose $1 = c_1, \ldots, c_t \in K^\times$ such that $v(c_i)$ represents the class $v(a_{ij}) + 2\Gamma$. Take $b_{ij} \in K^\times$ with $a_{ij} c_i^{-1} b_{ij}^2 \in \mathcal{O}_v^\times$. The forms $\overline{\rho_{(i)}} := \left\langle \ldots, \overline{c_i^{-1} a_{ij} b_{ij}^2}, \ldots \right\rangle_{1 \leq j \leq r_i}$ are called *v-residue forms* of ρ.

Proposition 2.11. *Let (K, v) be a Henselian field such that the residue field K_v is real and char(K_v)$\neq 2$. Let $\rho = \langle a_1, \ldots, a_m \rangle$ be a regular quadratic form over K. Then , ρ is isotropic (resp., weakly isotropic) over K if, and only if, at least one of the residue forms $\overline{\rho_{(i)}}$ is isotropic (resp., weakly isotropic) over K_v.*

Proof: ($\Rightarrow$) There exists $\sigma_{ij} \in K$ not all zero such that

$$0 = \sum_{i,j} a_{ij} \sigma_{ij}^2.$$

Choose indices k and l such that $v(a_{kl}\sigma_{kl}^2) = \min_{i,j}\{v(a_{ij}\sigma_{ij}^2)\}$. Multiplying the equation above by $c_k^{-1} b_{kl}^2 \sigma_{kl}^{-2}$ one has

$$0 = \sum_{i,j \quad i \neq k} a_{kl} c_k^{-1} b_{kl}^2 (a_{kl}^{-1} \sigma_{kl}^{-2} a_{ij} \sigma_{ij}^2) + \sum_j a_{kj} c_k^{-1} b_{kj}^2 \alpha_j^2 \quad ,$$

where $\alpha_j = b_{kj}^{-1}\sigma_{kj}b_{kl}\sigma_{kl}^{-1} \in \mathcal{O}_v$. Note that for $i \neq k$, by the definition of the a_{ij}, the value of $a_{ij}\sigma_{ij}^2$ has to be strictly greater than the value of $a_{kl}\sigma_{kl}^2$. Thus, passing to the residue field K_v, one obtains that the residue form $\overline{\rho_{(k)}}$ is isotropic.
($\Leftarrow$) Suppose that the residue form $\overline{\rho_{(k)}}$ is isotropic over the field K_v. Thus,

$$\sum_j \overline{a_{kj}c_{kj}^{-1}b_{kj}^2}.\overline{\sigma_{kj}}^2 = 0,$$

for some $\sigma_{kj} \in \mathcal{O}$ and, say $\sigma_{k1} \notin \mathfrak{m}$. So, the polynomial $p := a_{k1}c_{k1}^{-1}X^2 + \sum\limits_{j>1} a_{kj}c_{kj}^{-1}b_{kj}^2\sigma_{kj}^2$ has a simple non-zero root in K_v. By Hensel's Lemma, there exists an $\alpha_{k1} \in K^\times$ such that $p(\alpha_{k1}) = 0$. So, the form ρ is isotropic over K.

The statement about weakly isotropic is proved similarly.

□

Now the Characterization Theorem of Jacobi-Prestel can be stated and proved. The symbol $\Re_\infty(\mathfrak{p})$ below denotes the set of all residually real valuations v of $F_\mathfrak{p}$ with $v(\bar{X}_i) < 0$ for some $i \in \{1, \ldots, n\}$.

Theorem 2.12 (Characterization Theorem of Jacobi-Prestel). *Let $h_1, \ldots, h_m \in A$ such that $W(h)$ is compact and $M(h)$ is a quadratic module, then $M(h)$ is Archimedean if, and only if, for every real prime ideal $\mathfrak{p}$ of A and for every valuation $v \in \Re_\infty(\mathfrak{p})$ the regular quadratic form $\langle 1, \bar{h}_1, \ldots, \bar{h}_s\rangle^*$ is weakly isotropic over the Henselization $H(F_\mathfrak{p}, v)$ of $F_\mathfrak{p}$ with respect to the valuation v.*

Proof: ($\Rightarrow$) If $M(h)$ is Archimedean, then from Theorem 2.8 it follows that for all real prime ideals $\mathfrak{p}$ of A the regular quadratic form

$$\tau := \langle 1, -\bar{f}, \bar{h}_1, \ldots, \bar{h}_s\rangle^*$$

, where $f := N - \sum X_i^2$, is weakly isotropic over the field $F_\mathfrak{p}$ and, *a fortiori*, over the henselization $H(F_\mathfrak{p}, v)$ of $F_\mathfrak{p}$ with respect to every valuation v. Let $v \in \Re_\infty(\mathfrak{p})$. Without loss of generality $v(\bar{X}_1) < 0$. As $v(N) \geq 0$, it follows that

$$v(\frac{N}{\bar{X}_1^2}) > 0.$$

Therefore, the polynomial $T^2 - (1 - \frac{N}{\bar{X}_1^2})$ has a simple zero in $\mathcal{O}/\mathfrak{m}$ and, by Hensel's lemma, there exists an $x \in H(F_\mathfrak{p}, v)$ such that $x^2 = 1 - \frac{N}{\bar{X}_1^2}$. So, one has

$$-\bar{f} = x^2\bar{X}_1^2 + \sum_{i>1} \bar{X}_i^2.$$

Hence, $-\bar{f} \in \sum H(F_\mathfrak{p}, v)^2$, and consequently the weak isotropy of τ over $H(F_\mathfrak{p}, v)$ implies that $\rho := \langle 1, \bar{h}_1, \ldots, \bar{h}_s\rangle^*$ is also weakly isotropic over $H(F_\mathfrak{p}, v)$.

($\Leftarrow$) From $W(h)$ being compact, it follows that there is an $N \in \mathbb{N}$ such that $f := N - \sum X_i^2$ is strictly positive on the semialgebraic set $W(h)$. It will be proved by induction on the Krull-dimension d of the ring $A/\mathfrak{p}$, that the form $\tau := \left\langle 1, -\bar{f}, \bar{h}_1, \dots, \bar{h}_s \right\rangle^*$ is weakly isotropic over the field $F_\mathfrak{p}$. Then Theorem 2.8 yields that $M(h)$ is Archimedean.

For $d = 0$: In this case one has $F_\mathfrak{p} = \mathbb{R}$. Thus $a := (\bar{X}_1, \dots, \bar{X}_n) \in \mathbb{R}^n$. If $a \in W(h)$, then $f(a) > 0$ and therefore $-\bar{f} < 0$. So the form $\tau := \left\langle 1, -\bar{f}, \bar{h}_1, \dots, \bar{h}_s \right\rangle^*$ is indefinite over $F_\mathfrak{p} = \mathbb{R}$ and therefore (weakly) isotropic. Similarly, if $a \notin W(h)$, then there is an $i \in \{1, \dots, s\}$ for which $h_i(a) < 0$. Hence the form τ is isotropic over $F_\mathfrak{p} = \mathbb{R}$.

For $d > 0$: In this case the field $F_\mathfrak{p}$ has no Archimedean orderings. Therefore, the first condition on the Local-Global Principle is automaticly satisfied. So it remains to check the second one, i. e., that the form τ is weakly isotropic over all henselizations $H(F_\mathfrak{p}, v)$ with respect all non-trivial residually real valuations v of $F_\mathfrak{p}$. If $v \in \Re_\infty(\mathfrak{p})$ this follows from the hypothesis. So let v satisfy $v(\bar{X}_i) \geq 0$ for each $i = 1, \dots, s$, i.e., with $\bar{A} \subset \mathcal{O}_v$. Let $\mathfrak{p}' := \mathfrak{m}_v \cap \bar{A}$. Thus $\mathfrak{p}'$ is a real prime ideal of the ring $\bar{A}$ and $d' := dim(\bar{A}/\mathfrak{p}') < d$. By the induction hypotheses, the form $\left\langle 1, -\bar{f} + \mathfrak{p}', \bar{h}_1 + \mathfrak{p}', \dots, \bar{h}_s + \mathfrak{p}' \right\rangle^*$ is weakly isotropic over $F' := Quot(\bar{A}/\mathfrak{p}')$. Since this form is a subform of the first residue form of τ and F' is a subfield of the residue field of v , it follows from proposition 2.11 that τ is weakly isotropic over $H(F_\mathfrak{p}, v)$.

$\square$

As an application of Theorem 2.12 we will come back to Example 2.7. Consider the ideal $\mathfrak{p} = (0)$. Thus, $F_\mathfrak{p} \cong \mathbb{R}(X_1, \dots, X_n)$. Let $v : F_\mathfrak{p}^\times \longrightarrow \Gamma$, with the value group $\Gamma := \mathbb{Z} \times \cdots \times \mathbb{Z}$ ordered lexicographically, defined by $v(X_i) = (0, \dots, -1, \dots, 0)$, where -1 is in the i-th coordinate. So, the elements of the form $\rho = \langle 1, h_1, \dots, h_{n+1} \rangle$ have pairwise different value modulo 2Γ. Thus, all the residue forms are equal to $\langle 1 \rangle$, and therefore ρ is not weakly isotropic over $H(\mathbb{R}(X), v)$.

Next we state a generalization of Witt's famous Local-Global Principle for isotropy, which will be useful in the next chapter. The proof we will omit. For a proof and more comments see, e.g., [PD] Theorem 3.4.11.

Theorem 2.13. *Let R be a real closed field, and F/R a real, finitely generated field extension of transcendence degree* 1*. Then every regular quadratic form ρ over F of dimension > 2 that is totally indefinite*[1] *over F is isotropic over F.*

[1]that is, indefinite with respect to all orderings.

Chapter 3

Crucial Results

In this chapter we would like to present crucial results, whose proof will be essential to the description of the algorithm in the next chapter. First we will proceed in order to state a version of the Jacobi-Prestel Criterion in dimension two.

From now on $h_1, \ldots, h_m$ will always denote polynomials in $A := \mathbb{R}[X, Y]$ such that the semialgebraic set $W(h)$ is compact. So, there is an $N \in \mathbb{N}$ for which $W(h)$ is contained in the open ball $B(0, N^{1/2}) \subset \mathbb{R} \times \mathbb{R}$ with center in the origin and radius $N^{1/2}$. Define $f := N - X^2 - Y^2$. Note that f is strictly positive on $W(h)$.

For a prime ideal $\mathfrak{p}$ of A we remember that

$$^{-}: A \twoheadrightarrow A/\mathfrak{p}$$

denotes the canonical residue homomorphism and $F_{\mathfrak{p}}$ the quotient field $Quot(A/\mathfrak{p})$. The set of valuations v on $F_{\mathfrak{p}}$ with real residue field and $v(\overline{X}) < 0$ or $v(\overline{Y}) < 0$ will be denoted by $\mathfrak{R}_{\infty}(\mathfrak{p})$.

Remark 3.1. The valuations $v \in \mathfrak{R}_{\infty}(\mathfrak{p})$ are trivial on $\mathbb{R}$. In fact, as $(F_{\mathfrak{p}}, \mathcal{O}_v)$ has real residue field, the restriction $\mathcal{O}_v \cap \mathbb{R}$ is a valuation ring of $\mathbb{R}$ with real residue field. Thus, $\mathcal{O}_v \cap \mathbb{R}$ must be convex[1] with respect to the only ordering of $\mathbb{R}$ (see,e.g., [PD] exercise 1.4.10 (b)). Since $\mathbb{R}$ is Archimedean, for all $a \in \mathbb{R}_+$ there is a $b \in \mathbb{N}$ with $a < b$. By the convexity of $\mathcal{O}_v$ we obtain $a \in \mathcal{O}_v$. Thus, $\mathbb{R} \subset \mathcal{O}_v$.

The Jacobi-Prestel Criterion (see Theorem 2.12) says that the quadratic module $M(h)$ is Archimedean iff the following condition is satisfied:

For each real prime ideal $\mathfrak{p}$ *of* A *and for each valuation* $v \in \mathfrak{R}_{\infty}(\mathfrak{p})$ *the regular quadratic form* $\rho := \langle 1, \bar{h}_1, \ldots, \bar{h}_m \rangle^*$ *is weakly isotropic over the Henselization* $H(F_{\mathfrak{p}}, v)$.

[1] It means, for all a, b: $0 < a < b \in \mathcal{O}_v \Rightarrow a \in \mathcal{O}_v$.

Let $d \in \mathbb{N}$ be the *Krull-dimension* of the ring $A/\mathfrak{p}$. Since $A = \mathbb{R}[X, Y]$ we have $d \leq 2$ (see, for example, [AM]).

For the prime ideals $\mathfrak{p}$ with $d = 0$ or $d = 1$ the condition above is always satisfied (independent on the number of variables). This fact is a corollary of the following theorem (see also [PD], Theorem 6.2.2 (1)), whose proof use Tarski's Transfer Principle. About Tarski's Principle see, e.g., [BCR].

Theorem 3.2. *For every real prime ideal* $\mathfrak{p}$ *of* A *and all* $v \in \Re_\infty(\mathfrak{p})$ *the regular quadratic form* $\rho = \langle 1, \bar{h}_1, \ldots, \bar{h}_m \rangle^*$ *is indefinite with respect to all orderings of the Henselization* $H(F_\mathfrak{p}, v)$.

Proof: First we will prove that the form $\tau := \langle 1, -\bar{f}, \bar{h}_1, \ldots, \bar{h}_m \rangle^*$ is indefinite with respect to all orderings of $F_\mathfrak{p}$. With this purpose we define the following formula in the formal language of the ordered fields:

$$\varphi := \quad \forall x, y : (f(x, y) > 0) \vee (\vee_{i=1}^m h_i(x, y) < 0).$$

The formula φ holds in $\mathbb{R}$, by the definition of f. Let $\leq$ be an arbitrary ordering of $F_\mathfrak{p}$. Consider the corresponding real closure $(\tilde{F}_\mathfrak{p}, \tilde{\leq})$. By Tarski's Transfer Principle, the formula φ also holds in $(\tilde{F}_\mathfrak{p}, \tilde{\leq})$. Thus, for $x = \overline{X}$ and $y = \overline{Y}$ we get $f(\overline{X}, \overline{Y}) > 0$ or $h_i(\overline{X}, \overline{Y}) < 0$ for some i, since $\tilde{\leq}$ equals $\leq$ in $F_\mathfrak{p}$. Hence, τ is indefinite with respect to all orderings of $F_\mathfrak{p}$.

Let $v \in \Re_\infty(\mathfrak{p})$. To see that ρ is indefinite with respect to all orderings of $H(F_\mathfrak{p}, v)$ we will prove that $-\overline{f}$ is a sum of squares of $H(F_\mathfrak{p}, v)$. In fact, without loss of generality $v(\overline{X}) < 0$, and therefore $v(N/\overline{X}^2) > 0$, since $v(N) \geq 0$. Thus, the polynomial $T^2 - (1 - N/\overline{X}^2)$ has a simple zero in $\mathcal{O}/\mathfrak{m}$. Then, by Hensel's lemma there exists an $\alpha \in H(F_\mathfrak{p}, v)$ with $1 - N/\overline{X}^2 = \alpha^2$. Therefore $-\overline{f} = \overline{X}^2\alpha^2 + \overline{Y}^2$. □

Corollary 3.3. *For every real prime ideal* $\mathfrak{p}$ *of* A *with Krull-dimension* $d < 2$ *and all* $v \in \Re_\infty(\mathfrak{p})$ *the regular quadratic form* $\rho = \langle 1, \bar{h}_1, \ldots, \bar{h}_m \rangle^*$ *is weakly isotropic over the Henselization* $H(F_\mathfrak{p}, v)$.

Proof:
<u>Case $d = 0$:</u> In this case we have $F_\mathfrak{p} = \mathbb{R}$ and therefore $\Re_\infty(\mathfrak{p}) = \emptyset$, since the valuations in $\Re_\infty(\mathfrak{p})$ must be trivial on $\mathbb{R}$ (see Remark 3.1).

<u>Case $d = 1$:</u> In this case $F_\mathfrak{p}$ is a function field in one variable over $\mathbb{R}$. By the proof of Theorem 3.2 the form τ (whose dimension is clearly greater than 2) is totally indefinite over $F_\mathfrak{p}$. Thus, by Witt's famous Local-Global Principle for isotropy (see [PD], Theorem 3.4.11) it must be isotropic over $F_\mathfrak{p}$. Since $-\overline{f}$ is a sum of squares of $H(F_\mathfrak{p}, v)$ (see proof of Theorem 3.2), ρ is weakly isotropic over the Henselization $H(F_\mathfrak{p}, v)$. □

Notation From now on K will denote the field $\mathbb{R}(X,Y)$ and $H(K,v)$ the Henselization of K with respect to the valuation v. The residue field will be denoted by K_v and we will refer to the residue forms with respect to v as the v-residue forms.

By Corollary 3.3 and the Jacobi-Prestel Criterion, we have the following :

Theorem 3.4. (Jacobi-Prestel Criterion for $n = 2$) *For polynomials $h_1, \dots, h_m \in \mathbb{R}[X,Y]$ such that the semialgebraic set $W(h)$ is compact are equivalent:*

(a) The module $M(h)$ is Archimedean ;

(b) For all valuations v on K with real residue field and $v(X) < 0$ or $v(Y) < 0$ the regular quadratic form $\rho := \langle 1, h_1, \dots, h_m\rangle^*$ is weakly isotropic over $H(K,v)$.

We would like to present an algorithm to check the condition (b) of Theorem 3.4. For this purpose we will use the fact that a quadratic form over a Henselian field with real residue field is (weakly) isotropic iff at least one of its residue forms is (weakly) isotropic over the residue field (see Proposition 2.11). In our case, i.e. $K = \mathbb{R}(X,Y)$, this fact will be specially useful, since K_v (which is also the residue field of the Henselization $H(K,v)$) is either $\mathbb{R}$ or a function field in one variable over $\mathbb{R}$ (see the proof of the lemma below). Thus, we have to check if at least one v-residue form is totally indefinite over K_v. We state this in the following lemma.

Lemma 3.5. *For all $v \in \Re_\infty(K)$ the form ρ is weakly isotropic over $H(K,v)$ if and only if at least one v-residue form of ρ is totally indefinite over K_v.*

Proof: First we will prove that K_v is $\mathbb{R}$ or a function field in one variable over $\mathbb{R}$. Let $\Gamma := v(K^\times)$. As $(\mathbb{R}, \mathcal{O}_v \cap \mathbb{R}) \subset (K, \mathcal{O}_v)$ and $\mathcal{O}_v \cap \mathbb{R} = \mathbb{R}$, we have [2]

$$trdeg(K_v/\mathbb{R}) + rr(\Gamma) \leq trdeg(K/\mathbb{R}) = 2, \tag{3.1}$$

where $rr(\Gamma)$ is the rational rank of Γ [3]. Since $rr(\Gamma) \geq 1$, it follows that $trdeg(K_v/\mathbb{R}) \leq 1$. If $trdeg(K_v/\mathbb{R}) = 1$, we have $rr(\Gamma) = 1$ and equality in (3.1). By equality we have that $K/\mathbb{R}$ being finitely generated implies that $K_v/\mathbb{R}$ is also finitely generated (See [B], Chapter VI, §10.3 Corollary 1). Thus, K_v is a function field in one variable over $\mathbb{R}$. If $trdeg(K_v/\mathbb{R}) = 0$, we get $K_v = \mathbb{R}$. Otherwise, K_v would be a proper real algebraic extension of $\mathbb{R}$.

In $\mathbb{R}$ it is clear that the concepts of weak isotropy, isotropy and indefiniteness coincide.

If K_v is a function field in one variable over $\mathbb{R}$, by Theorem 2.13, each regular quadratic form over K_v with dimension greater than 2 that is totally indefinite

[2] See, e.g., Theorem A.6.6 in [PD].

[3] $rr(\Gamma) :=$ sup $\{n \in \mathbb{N} | \exists \alpha_1, \dots \alpha_n \in \Gamma$ linearly independent over $\mathbb{Z}\}$.

over K_v is isotropic over K_v. For forms with dimension 2, taking a multiple of them and using Theorem 2.13 we get weak isotropy instead of isotropy. Conversely, a weakly isotropic regular quadratic form over any field F is indefinite with respect to all semiorderings of F, and therefore totally indefinite over F. □

For some valuations v in $\Re_\infty(K)$ we can already conclude that the form ρ is weakly isotropic over $H(K, v)$, if we know *a priori* something about the v-residue forms. This will be clear with the following lemma. We would like to emphasize that it is a consequence of the compactness of the semialgebraic set $W(h)$. For the definition of the residue forms see Definition 2.10.

Lemma 3.6. *Let v be a valuation in $\Re_\infty(K)$ with value group Γ. The following facts then hold:*

(i) If the form $\rho = \langle 1, h_1, \ldots, h_m\rangle$ has exactly one v-residue form, then ρ is weakly isotropic over $H(K, v)$.

(ii) If the form ρ has exactly two v-residue forms with entries in $\mathbb{R}$, then ρ is weakly isotropic over $H(K, v)$.

Proof: (i) By assumption we must have $v(h_i) \equiv v(1) \bmod 2\Gamma$ for each i. Thus, there exists $b_i \in K^\times$ with $h_i b_i^{-2} \in \mathcal{O}_v^\times$. By Definition 2.10, the first (and only) v-residue form can be chosen as

$$\overline{\rho_0} = \left\langle 1, \overline{h_1 b_1^{-2}}, \ldots, \overline{h_m b_m^{-2}} \right\rangle .$$

Suppose that ρ is not weakly isotropic over $H(K, v)$. By Lemma 3.5, $\overline{\rho_0}$ is not totally indefinite over K_v. Let $P \subset K_v$ be a positive cone with $\overline{h_i b_i^{-2}} \in P$ for all i. Define

$$Q := \{ \quad \sum_{i=1}^{n} p_i a_i^2 \quad | \quad n \in \mathbb{N} \quad , \quad \overline{p_i} \in P \backslash \{0\} \quad , \quad \alpha_i \in H(K, v)\}.$$

Clearly Q is closed under addition and multiplication, and contains all squares from K. Suppose $-1 \in Q$. Thus, $-1 = \sum_{i=1}^n p_i a_i^2$ and

$$\overline{-1/a_k}^2 = \overline{p_k} + \sum_{i \neq k} \overline{p_i} \overline{(a_i/a_k)}^2,$$

where a_k has minimal value among the a_i's. Therefore $\overline{p_k} \in P \cap -P = \{0\}$, a contradiction. Thus, Q is a prepositive cone of $H(K, v)$ and can be extended to a positive cone , which contains all the h_i's (as $\overline{h_i b_i^{-2}} \in P$ for each i). Hence, ρ is positive definite with respect to the corresponding ordering, contradicting Theorem 3.2.

(ii) The v-residue forms can be chosen as $\overline{\rho_0} := \left\langle 1, \dots, \overline{h_i b_i^2}, \dots \right\rangle$ and $\overline{\rho_1} := \left\langle \dots, \overline{\pi^{-1} h_j b_j^2}, \dots \right\rangle$ with $v(\pi) \notin 2\Gamma$. As above, ρ being not weakly isotropic over $H(K,v)$ implies that $\overline{\rho_0}$ and $\overline{\rho_1}$ are not totally indefinite over K_v. So, there are positive cones P and P' of K_v (not necessarily the same) such that all entries of $\overline{\rho_0}$ are in P and all entries of $\overline{\rho_1}$ are, say, in P'. Define Q as in (i) and $Q' := Q + \pi Q$. (In case that the entries of $\overline{\rho_1}$ are in $-P'$ we replace π by $-\pi$). Then Q' is closed under addition and multiplication, and contains all squares from K. Moreover, $-1 \notin Q'$. Otherwise,

$$-1 = \sum_i p_i a_i^2 + \pi \sum_i q_i c_i^2.$$

If $a_i^2, c_i^2 \in \mathcal{O}$ for all i, passing to the residue field we get $-1 \in P$, absurd. Thus, if $v(a_k^2) = \min_i\{v(a_i^2), v(\pi c_i^2)\}$ we necessarily have $v(a_k^2) < 0$ and $v(a_k^2) < v(\pi c_i^2)$, as $v(\pi) \notin 2\Gamma$. Multiplying with $1/a_k^2$ and going to the residue field we get

$$\overline{0} = \overline{-(1/a_k)}^2 = \overline{p_k} + \sum_{i \neq k} \overline{p_i} \overline{(a_i/a_k)}^2,$$

a contradiction. Similarly, if $v(\pi c_k^2) = \min_i\{v(a_i^2), v(\pi c_i^2)\}$, then $v(\pi c_k^2) < v(a_i^2)$ and $v(\pi c_k^2) < 0$. Multiplying with $1/\pi c_k^2$ and going to the residue field we obtain

$$\overline{0} = \overline{q_k} + \sum_{i \neq k} \overline{q_i} \overline{(c_i/c_k)}^2,$$

a contradiction. Then, Q' can be extended to a positive cone of $H(K,v)$. By the definition of Q we have $h_i = b_i^{-2}(h_i b_i^2) \in Q \subset Q'$, since $\overline{h_i b_i^2} \in P - \{0\}$ for all entries of $\overline{\rho_0}$. We have also $\overline{\pi^{-1} h_j b_j^2} \in P - \{0\}$ for all entries of $\overline{\rho_1}$, since they are in $\mathbb{R}^\times \cap P'$. Hence, $h_j = \pi b_j^{-2}(\pi^{-1} h_j b_j^2) \in \pi Q \subset Q'$. Thus, ρ is positive definite with respect to the ordering defined by the positive cone containing Q', contradicting Theorem 3.2. $\square$

Lemma 3.6 above will help us to obtain a finite subset $\{w_1, \dots, w_n\} \subset \Re_\infty(K)$ such that ρ is weakly isotropic over $H(K,v)$ for all $v \in \Re_\infty(K)$ if and only if ρ is weakly isotropic over $H(K,w_i)$ for each $1 \leq i \leq n$.

To describe the idea we need some definitions that will be given below. Most of them can be found in many introductory books about Algebraic Curves. We cite for example [Ki].

Let $F(x,y)$ be a polynomial in two variables over $\mathbb{R}$. The set of real solutions of the equation $F(x,y) = 0$ defines an algebraic curve in $\mathbb{R} \times \mathbb{R}$, which we will denote by $C(F)$.

Note that since $F(x,y)$ is a polynomial it has a finite Taylor expansion

$$F(x,y) = \sum_{i,j \geq 0} \frac{\partial^{i+j} F}{\partial x^i \partial y^j}(a,b) \frac{(x-a)^i (y-b)^j}{i!j!}$$

about any point (a, b). The *multiplicity* of the curve $C(F)$ at the point (a, b) is the smallest positive integer m such that

$$\frac{\partial^{i+j} F}{\partial x^i \partial y^j}(a, b) \neq 0$$

for some $i \geq 0$,$j \geq 0$ with $i + j = m$. Sometimes we will refer to this multiplicity as the multiplicity of the polynomial F at the point (a, b) which will be denoted by $m_{(a,b)}(F)$. For $(a, b) = (0, 0)$ we will write $m(F)$ instead of $m_{(0,0)}(F)$.

It is clear that the point (a, b) lies on the curve $C(F)$ iff $m_{(a,b)}(F) \geq 1$. If $m_{(a,b)}(F) = 1$ we say that (a, b) is a *regular* point of $C(F)$. Otherwise, it is called *singular*.

As the polynomial

$$\sum_{i+j=m} \frac{\partial^{i+j} F}{\partial x^i \partial y^j}(a, b) \frac{(x - a)^i (y - b)^j}{i!j!}$$

in the variables $x - a$ and $y - b$ is homogeneous of degree m, it has a factorization in m linear factors over $\mathbb{C}$ as follows

$$\prod_{j=1}^{r} [\alpha_j(x - a) + \beta_j(y - b)]^{\epsilon_j},$$

where $m = \sum\limits_{j=1}^{r} \epsilon_j$ and the r lines

$$\alpha_j(x - a) + \beta_j(y - b) = 0$$

are distinct. They are called the *tangent lines to* $C(F)$ *at* (a, b). The positive integers ϵ_j are the multiplicity of the corresponding tangent line at the point (a, b).

Definition 3.7. We say that the curves $C(F)$ and $C(G)$ have *normal crossing* at the point (a, b) iff (a, b) is a regular point of both curves and their tangent lines at (a, b) are different.

We call a polynomial without repeated irreducible factors a *reduced polynomial*. For each polynomial p the *reduction of* p, denoted by $\sqrt{p}$, is the reduced polynomial obtained from p by discarding all repeated irreducible factors.

We would like to obtain a finite subset $\{w_1, \ldots, w_n\} \subset \Re_\infty(K)$ such that: ρ is weakly isotropic over $H(K, v)$ for all $v \in \Re_\infty(K)$ if, and only if, ρ is weakly isotropic over $H(K, w_i)$ for each $1 \leq i \leq n$. Moreover, for the valuations w_i we should be able to test the weak isotropy of ρ over the Henselization. So, we must know the w_i-residue forms of ρ.

In general, for an arbitrary $v \in \mathfrak{R}_\infty(K)$ we know almost nothing about the v-residue forms of ρ. Nevertheless, if we make a suitable change of variables, in some cases we can immediately find them.

With this purpose in mind we will consider separately the following two subsets of $\mathfrak{R}_\infty(K)$:

$$\mathfrak{R}_\infty(K)_X := \{ \quad v \in \mathfrak{R}_\infty(K) \quad | \quad v(X^{-1}Y) \geq 0\} \tag{3.2}$$

and

$$\mathfrak{R}_\infty(K)_Y := \{ \quad v \in \mathfrak{R}_\infty(K) \quad | \quad v(Y^{-1}X) \geq 0\}. \tag{3.3}$$

Clearly,

$$\mathfrak{R}_\infty(K) = \mathfrak{R}_\infty(K)_X \cup \mathfrak{R}_\infty(K)_Y. \tag{3.4}$$

Consider for instance the subset $\mathfrak{R}_\infty(K)_X$. We will make the change

$$(x, y) := (X^{-1}, X^{-1}Y) \tag{3.5}$$

in order to obtain $\mathbb{R}[x, y] \subset \mathcal{O}_v$ for all valuations v in $\mathfrak{R}_\infty(K)_X$. Note that $\mathbb{R}(X, Y) = \mathbb{R}(x, y)$.

The idea is to collect all valuations $v \in \mathfrak{R}_\infty(K)_X$ with the same center $\mathfrak{p}$ in the ring $\mathbb{R}[x, y]$ [4] and, among those, find a *"distinguished"* valuation w. Here *"distinguished"* for $\mathfrak{p}$ means: the following conditions are satisfied:

(1) w has center $\mathfrak{p}$ in $\mathbb{R}[x, y]$, and if ρ is weakly isotropic in $H(K, w)$ then ρ is weakly isotropic in $H(K, v)$ for every $v \in \mathfrak{R}_\infty(K)_X$ with center $\mathfrak{p}$ in $\mathbb{R}[x, y]$;

(2) We can effectively construct the w-residue forms of ρ, in particular we can explicitly describe the value group and the residue field of w.

By the definition of $\mathfrak{R}_\infty(K)$ and $\mathfrak{R}_\infty(K)_X$, we see easily that $v(x) > 0$ for all $v \in \mathfrak{R}_\infty(K)$. Thus, the center $\mathfrak{p}_v := \mathfrak{m}_v \cap \mathbb{R}[x, y]$ must necessarily contain the ideal (x). Hence, if $\mathfrak{p}_v$ is not maximal, we have $\mathfrak{p}_v = (x)$ (the Krull-dimension of $\mathbb{R}[x, y]$ is two, since $\mathbb{R}(X, Y) = \mathbb{R}(x, y)$). If $\mathfrak{p}_v$ is maximal, we have $\mathfrak{p} = (x, y - \alpha)$, for some $\alpha \in \mathbb{R}$.

Remark 3.8. Defining $(x, y) := (Y^{-1}, Y^{-1}X)$, we get the same results for the valuations in $\mathfrak{R}_\infty(K)_Y$.

In what follows the definitions below will be useful:

Definition 3.9. For $x, y \in K = \mathbb{R}(X, Y)$ such that $\mathbb{R}(X, Y) = \mathbb{R}(x, y)$ we define

$$\mathcal{T}_{(x,y)} := \{v \in \mathfrak{R}_\infty(K) | \text{ the center of } v \text{ in } \mathbb{R}[x, y] \text{ is } (x)\} \tag{3.6}$$

[4] For a valuation v on a field F and a subring $B \subset F$ the *center of v in* B is the ideal $\mathfrak{p} := \mathfrak{m}_v \cap B$, which is a prime ideal of B.

and, for each $\alpha \in \mathbb{R}$:

$$\mathcal{R}_{(x,y-\alpha)} := \{v \in \Re_\infty(K) | \text{ the center of } v \text{ in } \mathbb{R}[x,y] \text{ is } (x, y-\alpha)\}. \tag{3.7}$$

In particular, we must have $\mathbb{R}[x,y] \subset \mathcal{O}_v$ for all v in $\mathcal{T}_{(x,y)}$, resp. in $\mathcal{R}_{(x,y-\alpha)}$ (since the notion of the center of v in the ring B presupposes $B \subset \mathcal{O}_v$).

Remark 3.10. As usual, the symbol $\cong$ between quadratic forms over K will denote that they are isometric over K. For $x, y \in K$ such that $K = \mathbb{R}(x,y)$ and polynomials $f, g \in \mathbb{R}[x,y]$ we will write $f \cong g$ to denote that they are equal up to square factors of $K^\times$, that is, $\langle f \rangle \cong \langle g \rangle$. As we are interested on weak isotropy it will be also useful to consider the polynomial obtained from f by discarding all its square factors, which will be denoted by f_*. In particular, $f_* \cong f$.

Proposition 3.11. *Let $x, y \in K$ be such that $\mathbb{R}(X,Y) = \mathbb{R}(x,y)$. Suppose that*

$$\rho \cong \langle 1, \ldots, x^{\mu_i} a_i'(x,y), \ldots \rangle \,,$$

with reduced polynomials $x^{\mu_i} a_i' \in \mathbb{R}[x,y]$ and a_i' not divisible by x. Then, for all valuations $v \in \mathcal{T}_{(x,y)}$ we have:

(i) If $v(x) = 0 \bmod 2\Gamma_v$, the form ρ is weakly isotropic over $H(K,v)$;

(ii) If $v(x) \neq 0 \bmod 2\Gamma_v$, the v-residue forms of ρ can be chosen as

$$\overline{\rho_o} := \langle 1, \ldots, a_i'(0, \overline{y}), \ldots \rangle_{i \text{ with } \mu_i = 0}$$

and

$$\overline{\rho_1} := \langle \ldots, a_i'(0, \overline{y}), \ldots \rangle_{i \text{ with } \mu_i = 1} \,.$$

Proof: Let $v \in \mathcal{T}_{(x,y)}$. We must have $\overline{y} \notin \mathbb{R}$. Otherwise, $\overline{y - \alpha} = 0$ for some $\alpha \in \mathbb{R}$ and therefore $y - \alpha \in \mathfrak{m}_v \cap \mathbb{R}[x,y] = (x)$, absurd. Then, $\overline{y} \notin \mathbb{R}$, and consequently $\overline{y}$ must be transcendental over $\mathbb{R}$. Since x does not divide a_i' in $\mathbb{R}[x,y]$, we have $a_i'(0,y) \neq 0$. Hence, $0 \neq a_i'(0,\overline{y}) = a_i'(\overline{x},\overline{y}) = \overline{a_i'}$. Thus, $v(x^{\mu_i} a_i') = \mu_i v(x)$.
(*i*) If $v(x) = 0 \bmod 2\Gamma_v$, we have $v(x^{\mu_i} a_i') = \mu_i v(x) = 0 \bmod 2\Gamma_v$ for each i. Hence, ρ has only one v-residue form (see Definition 2.10). By Lemma 3.6 (i), ρ is weakly isotropic over $H(K,v)$.
(*ii*) If $v(x) \neq 0 \bmod 2\Gamma_v$, we take $c_2 = x$ (see Definition 2.10). Thus, the v-residue forms of ρ can be chosen as $\overline{\rho_0}$ and $\overline{\rho_1}$. □

Lemma 3.12. *Let $x, y \in K$ be with $\mathbb{R}(X,Y) = \mathbb{R}(x,y)$. There exists a valuation w on K with center (x) in $\mathbb{R}[x,y]$ such that : if $w \in \Re_\infty(K)$, the following facts are equivalent:*

(i) ρ is weakly isotropic over $H(K,v)$ for all $v \in \mathcal{T}_{(x,y)}$;

(ii) ρ *is weakly isotropic over* $H(K,w)$.

Moreover, one can effectively test the condition (ii).

Proof: Let w be the x-adic valuation on $\mathbb{R}(y)(x) = K$, that is, if $z = x^n f/g$ for $f, g \in \mathbb{R}[x,y]$ not divisible by x and n a integer, we have $w(z) := n$. So, it is clear that $\mathfrak{m}_v \cap \mathbb{R}[x,y] = (x)$. Moreover, $\Gamma_w := w(K^\times) = \mathbb{Z}$ and the residue field K_w is isomorphic to $\mathbb{R}(y)[x]/(x) \cong \mathbb{R}(y)$.

If $w \in \Re_\infty(K)$, we have $w \in \mathcal{T}_{(x,y)}$ and $(i) \Rightarrow (ii)$ is trivial.
$(ii) \Rightarrow (i)$: As $\mathbb{R}(X,Y) = \mathbb{R}(x,y)$, each $h_i(X,Y) = c_i/d_i$ for some polynomials $c_i, d_i \in \mathbb{R}[x,y]$. So, $h_i \cong (c_i d_i)_*$. Writing $(c_i d_i)_* = x^{\mu_i} a_i'$ with a_i' not divisible by x we have

$$\rho \cong \langle 1, \ldots, x^{\mu_i} a_i'(x,y), \ldots \rangle .$$

Since $w(x) = 1 \neq 0 \bmod 2\mathbb{Z}$, the w-residue forms of ρ are those defined in Proposition 3.11 *(ii)*.

If ρ is weakly isotropic over $H(K,w)$, by Lemma 3.5 at least one w-residue form of ρ must be totally indefinite over $K_w \cong \mathbb{R}(y)$. Suppose that this is the case for $\overline{\rho_0}$. Then, the following formula in the formal language of ordered fields

$$\varphi_0 := \forall t : \bigwedge\nolimits_{i \text{ s.t. } \mu_i = 0} a_i'(0,t) \neq 0 \rightarrow \bigvee\nolimits_{i \text{ s.t. } \mu_i = 0} a_i'(0,t) < 0$$

holds in $\mathbb{R}$. Otherwise, there would be an $\gamma \in \mathbb{R}$ such that $a_i'(0,\gamma) > 0$ for all i with $\mu_i = 0$. Then, there is an open interval $(\alpha, \beta) \subset \mathbb{R}$ containing γ and such that for all $t \in (\alpha,\beta)$, and for all i with $\mu_i = 0$ we have $a_i'(0,t) > 0$. Hence, the formula

$$\varphi' := \forall t : \alpha < t \wedge t < \beta \rightarrow \bigwedge\nolimits_{i \text{ with } \mu_i = 0} a_i'(0,t) > 0$$

holds in $\mathbb{R}$. Take in $\mathbb{R}(\overline{y}) \cong K_w$ an ordering $<_\gamma$ such that $\alpha < \overline{y} < \beta$. By Tarski's Transfer Principle, φ' holds in the real closure $(\widetilde{\mathbb{R}(\overline{y})}, \tilde{<}_\gamma)$. In particular, $a_i'(0,\overline{y}) >_\gamma 0$ for all i with $\mu_i = 0$ and $\overline{\rho_0}$ is positive definite with respect to $<_\gamma$, a contradiction.

Similarly, if $\overline{\rho_1}$ is totally indefinite over K_w we prove that, for a fixed k with $\mu_k = 1$,

$$\varphi_1 := \forall t : \bigwedge\nolimits_{i \text{ s.t. } \mu_i = 1} a_i'(0,t) \neq 0 \rightarrow \bigvee\nolimits_{i \text{ s.t. } \mu_i = 1} a_i'(0,t) a_k'(0,t) < 0$$

holds in $\mathbb{R}$.

Thus,

$$\rho \text{ is weakly isotropic over } H(K,w) \Rightarrow \varphi_0 \text{ or } \varphi_1 \text{ holds in } \mathbb{R}.$$

Take an arbitrary $v \in \mathcal{T}_{(x,y)}$. We want to prove that ρ is weakly isotropic over $H(K,v)$. By Proposition 3.11(i), we can assume that $v(x) \neq 0 \bmod 2\Gamma_v$. Thus, the v-residue forms are those defined in Proposition 3.11(ii). Since, say φ_0, holds in $\mathbb{R}$, taking an arbitrary ordering $<$ of K_v, by Tarski's Transfer Principle, φ_0 holds also in the real closure $(\tilde{K_v}, \tilde{<})$. As $\overline{y} \notin \mathbb{R}$, we have $\overline{y}$ transcendental over $\mathbb{R}$. Thus, $\prod_{i \text{ s.t. } \mu_i=0} a_i'(0, \overline{y}) \neq 0$ and therefore $a_i'(0, \overline{y}) \tilde{<} 0$ for some i with $\mu_i = 0$. So, $\overline{\rho_0}$ is totally indefinite over K_v and therefore we have the result. $\square$

Remark 3.13. One can easily check that for $(x, y) := (X^{-1}, X^{-1}Y)$ we have

$$\Re_\infty(K)_X = \mathcal{T}_{(x,y)} \dot{\cup} (\dot{\bigcup_{\alpha \in \mathbb{R}}} \mathcal{R}_{(x,y-\alpha)}).$$

Analogously, if $(x, y) := (Y^{-1}, Y^{-1}X)$ we get

$$\Re_\infty(K)_Y = \mathcal{T}_{(x,y)} \dot{\cup} (\dot{\bigcup_{\alpha \in \mathbb{R}}} \mathcal{R}_{(x,y-\alpha)}).$$

Moreover, for these choices of (x, y), we get that the valuation w defined in the proof of Lemma 3.12 is in $\Re_\infty(K)$. Therefore, in these cases we found immediately a *"distinguished"* valuation for $\mathcal{T}_{(x,y)}$ that we are looking for. It remains to consider the sets $\mathcal{R}_{(x,y-\alpha)}$.

For the valuations in $\mathcal{R}_{(x,y-\alpha)}$, in general is not so easy to find a "distinguished" valuation. Writing the form ρ in these new variables, that is,

$$\rho \cong \langle 1, \dots, a_i(x, y), \dots \rangle,$$

with reduced polynomials $a_i \in \mathbb{R}[x, y]$, it will then depend on certain geometric conditions of the curve

$$C(\sqrt{\prod_i a_i})$$

at the point $(0, \alpha)$.

This motivates the following definitions:

Definition 3.14. Let $x, y \in K$ be such that $\mathbb{R}(X, Y) = \mathbb{R}(x, y)$. For polynomials $f, p \in \mathbb{R}[x, y]$, with p irreducible, we define $f \backslash p$ to be the polynomial in $\mathbb{R}[x, y]$ obtained from f by discarding all factors p of the factorization of f.

Definition 3.15. Let $x, y \in K$ be such that $\mathbb{R}(X, Y) = \mathbb{R}(x, y)$. If

$$\rho \cong \langle 1, \dots, a_i(x, y), \dots \rangle,$$

with $a_i \in \mathbb{R}[x, y]$ *reduced in* $\mathbb{R}[x, y]$, define the polynomials $f_{(x,y)}$ and $G_{(x,y)}$ in $\mathbb{R}[x, y]$ by

$$f_{(x,y)}(x, y) := \sqrt{\prod_{i=1}^{m} a_i(x, y)} \quad \text{and} \quad G_{(x,y)}(x, y) := f_{(x,y)} \backslash x.$$

Define $\mathcal{Z}_{(x,y)} := C(x) \cap C(G_{(x,y)}) \subset \mathbb{R} \times \mathbb{R}$. For each $(0, \alpha) \in \mathcal{Z}_{(x,y)}$ define

$$F_{\alpha(x,y)} := f_{(x,y)} \backslash (y - \alpha). \tag{3.8}$$

For $\alpha = 0$ we will write $F_{(x,y)}$ instead of $F_{0(x,y)}$.

The next proposition says that we do not need to test the valuations centered in a point $(0, \alpha)$ that is not in the intersection $C(x) \cap C(G_{(x,y)})$.

Proposition 3.16. *Let $x, y \in K$ be with $\mathbb{R}(X, Y) = \mathbb{R}(x, y)$ and suppose that*

$$\rho \cong \langle 1, \ldots, a_i(x, y), \ldots \rangle ,$$

for reduced polynomials $a_i \in \mathbb{R}[x, y]$. If $(0, \alpha) \notin \mathcal{Z}_{(x,y)}$, the form ρ is weakly isotropic over $H(K, v)$ for all $v \in \mathcal{R}_{(x,y-\alpha)}$.

Proof: For each i write $a_i = x^{\mu_i} a'_i(x, y)$, with $a'_i \in \mathbb{R}[x, y]$ not divisible by x. Thus,

$$\rho \cong \langle 1, \ldots, x^{\mu_i} a'_i(x, y), \ldots \rangle .$$

By the definition of $G_{(x,y)}$, we get

$$G_{(x,y)} = \sqrt{\prod_i a'_i}.$$

Thus, since $(0, \alpha) \notin \mathcal{Z}_{(x,y)}$, for each i we have $a'_i(0, \alpha) \neq 0$. Let $v \in \mathcal{R}_{(x,y-\alpha)}$. As $\mathfrak{m}_v \cap \mathbb{R}[x, y] = (x, y - \alpha)$, we have $(\overline{x}, \overline{y}) = (0, \alpha)$, and therefore $\overline{a'_i} = a'_i(\overline{x}, \overline{y}) \neq 0$. Thus, $v(a_i) = \mu_i v(x)$ for each i. Hence, ρ will have at most two v-residue forms with entries in $\mathbb{R}$. By Lemma 3.6, we get the result. □

We collect in the set $\tilde{\mathcal{R}}_{(x,y)}$ all valuations that satisfy the assumptions of Proposition 3.16.

For $(x, y) := (X^{-1}, X^{-1}Y)$, by Remark 3.13, we have

$$\Re_\infty(K)_X = \mathcal{T}_{(x,y)} \dot{\cup} \tilde{\mathcal{R}}_{(x,y)} (\dot{\bigcup_{(0,\alpha) \in \mathcal{Z}_{(x,y)}}} \mathcal{R}_{(x,y-\alpha)}). \tag{3.9}$$

In $\mathcal{T}_{(x,y)}$ we can find a "distinguished" valuation and test, by Lemma 3.12. It follows from Proposition 3.16 that we do not need to test the valuations in $\tilde{\mathcal{R}}_{(x,y)}$. It remains to consider the subsets of the finite disjoint union

$$\dot{\bigcup_{(0,\alpha) \in \mathcal{Z}_{(x,y)}}} \mathcal{R}_{(x,y-\alpha)}.$$

The following lemma states in which situations we can immediately find a *"distinguished"* valuation w in $\mathcal{R}_{(x,y-\alpha)}$ with $(0, \alpha) \in \mathcal{Z}_{(x,y)}$.

Lemma 3.17. *Let $x, y \in K$ be with $\mathbb{R}(X,Y) = \mathbb{R}(x,y)$. Suppose that*

$$\rho \cong \langle 1, \dots, a_i(x,y), \dots \rangle ,$$

with reduced polynomials $a_i(x,y) \in \mathbb{R}[x,y]$. Let $(0,\alpha) \in \mathcal{Z}_{(x,y)}$. If $C(x)$ and $C(G_{(x,y)})$ have normal crossing at $(0,\alpha)$, or $C(y-\alpha)$ and $C(F_{\alpha(x,y)})$ have normal crossing at $(0,\alpha)$, one can construct a valuation w on K with center $(x, y-\alpha)$ in $\mathbb{R}[x,y]$ such that: if $w \in \Re_\infty(K)$, the following facts are equivalent:

(i) ρ is weakly isotropic over $H(K,v)$ for all $v \in \mathcal{R}_{(x,y-\alpha)}$;

(ii) ρ is weakly isotropic over $H(K,w)$.

Moreover, one can effectively test the condition (ii).

Proof: Suppose that $C(x)$ and $C(G_{(x,y)})$ have normal crossing at $(0,\alpha)$. In particular, $(0,\alpha)$ is a regular point of $C(G_{(x,y)})$. Thus, there is only one irreducible factor q of $G_{(x,y)}$ that vanishes at $(0,\alpha)$. So, writing

$$a_i(x,y) = x^{\mu_i} q^{\nu_i} b_i, \tag{3.10}$$

with $b_i \in \mathbb{R}[x,y]$ divisible neither by x nor by q, we get

$$\begin{aligned}\rho \cong \langle 1, \dots, b_i, \dots \rangle_{(\mu_i,\nu_i)=(0,0)} &\perp x \langle \dots, b_i, \dots \rangle_{(\mu_i,\nu_i)=(1,0)} \\ \perp q \langle \dots, b_i, \dots \rangle_{(\mu_i,\nu_i)=(0,1)} &\perp xq \langle \dots, b_i, \dots \rangle_{(\mu_i,\nu_i)=(1,1)}\end{aligned}$$

with $b_i(0,\alpha) \neq 0$ for each i. Hence, for all valuations v on K with center $(x, y-\alpha)$ in $\mathbb{R}[x,y]$, the b_i's are units in $\mathcal{O}_v$.

If $v(1), v(x), v(q)$ and $v(xq)$ are pairwise distinct modulo $2\Gamma_v$, taking the representatives $c_2 = x$, $c_3 = q$ and $c_4 = xq$ in the definition of the residue forms (see Definition 2.10), they can be chosen as

$$\overline{\rho}_{(0,0)} := \langle 1, \dots, b_i(0,\alpha), \dots \rangle_{i \text{ with } (\mu_i,\nu_i)=(0,0)} ,$$

$$\overline{\rho}_{(1,0)} := \langle \dots, b_i(0,\alpha), \dots \rangle_{i \text{ with } (\mu_i,\nu_i)=(1,0)} ,$$

$$\overline{\rho}_{(0,1)} := \langle \dots, b_i(0,\alpha), \dots \rangle_{i \text{ with } (\mu_i,\nu_i)=(0,1)}$$

and

$$\overline{\rho}_{(1,1)} := \langle \dots, b_i(0,\alpha), \dots \rangle_{i \text{ with } (\mu_i,\nu_i)=(1,1)} .$$

Suppose that $v(1), v(x), v(q)$ and $v(xq)$ are not pairwise distinct modulo $2\Gamma_v$. Without loss of generality, assume that $v(1) = v(x) \bmod 2\Gamma_v$. Hence, $v(q) = v(xq) \bmod 2\Gamma_v$. So, if $v(1) = v(q) \bmod 2\Gamma_v$, the form ρ has only one v-residue form and therefore must be weakly isotropic over $H(K,v)$, by Lemma 3.6. If $v(1) \neq v(q) \bmod 2\Gamma_v$, the v-residue forms of ρ can be chosen as

$$\overline{\rho}_0 := \overline{\rho}_{(0,0)} \perp \overline{xd^{-2}}\overline{\rho}_{(1,0)} \quad \text{and} \quad \overline{\rho}_1 := \overline{\rho}_{(0,1)} \perp \overline{xd^{-2}}\overline{\rho}_{(1,1)}, \tag{3.11}$$

where $d \in K^\times$ is such that $v(x) = 2v(d)$.

Let $w : \mathbb{R}(y)^\times \twoheadrightarrow \mathbb{Z}$ be given by $w(y-\alpha) := 1$ and being trivial on $\mathbb{R}$ (that is, the p-adic valuation on $\mathbb{R}(y)$ for the prime $p = y - \alpha$). As $\mathbb{Z} \cong_{ord} \{0\} \times \mathbb{Z}$ is an ordered subgroup of $(\mathbb{Z}\times\mathbb{Z}, lex)$, there is a unique extension of w to the field $K = \mathbb{R}(y)(x)$ (also denoted by w) with $w(x) = (1,0)$. (see [PD] Corollary A.6.2). Thus, $\overline{x} = 0$ and $\overline{y} = \alpha$ and the center of w in $\mathbb{R}[x,y]$ is $(x, y-\alpha)$. Moreover, since $C(x)$ and $C(q)$ have normal crossing at $(0,\alpha)$, we have

$$q(x,y) = ax + b(y-\alpha) + \text{ “Terms of higher degree “},$$

with $b \in \mathbb{R}\backslash\{0\}$ and therefore $w(q) = (0,1)$. It follows that the w-residue forms of ρ can be chosen as $\overline{\rho}_{(0,0)}$, $\overline{\rho}_{(1,0)}$, $\overline{\rho}_{(0,1)}$ and $\overline{\rho}_{(1,1)}$ defined above. By Lemma 3.5, ρ is weakly isotropic over $H(K,w)$ iff at least one of these forms is indefinite. In this case, it follows from (3.11), that $\overline{\rho}_0$ or $\overline{\rho}_1$ must be also indefinite. So, if $w \in \Re_\infty(K)$, we get the result.

The proof in the case that $C(y-\alpha)$ and $C(F_{\alpha(x,y)})$ have normal crossing at $(0,\alpha)$ is similar. □

In the finite set $\mathcal{Z}_{(x,y)} = C(x) \cap C(G_{(x,y)})$ we will distinguish two disjoint subsets: that of *"good"* points and that of *"bad"* points. Under *"good"* points we mean the points that satisfies the assumptions of Lemma 3.17.

Definition 3.18. Let $\mathcal{G}_{(x,y)} \subset \mathcal{Z}_{(x,y)}$ be the set of points $(0,\alpha) \in \mathcal{Z}_{(x,y)}$ such that at least one of the following conditions is satisfied:

(a) $C(x)$ and $C(G_{(x,y)})$ have normal crossing at $(0,\alpha)$;

(b) $C(y-\alpha)$ and $C(F_{\alpha(x,y)})$ have normal crossing at $(0,\alpha)$.

Define $\mathcal{B}_{(x,y)}$ to be the complement of $\mathcal{G}_{(x,y)}$ in $\mathcal{Z}_{(x,y)}$.

Using the notation of Definition 3.18, if $(x,y) := (X^{-1}, X^{-1}Y)$, we have that

$$\Re_\infty(K)_X = \mathcal{T}_{(x,y)} \dot\cup \tilde{\mathcal{R}}_{(x,y)} \dot\cup \mathcal{R}_{\mathcal{G}_{(x,y)}} \dot\cup \mathcal{R}_{\mathcal{B}_{(x,y)}} \tag{3.12}$$

with

$$\mathcal{R}_{\mathcal{G}_{(x,y)}} := \dot{\bigcup_{(0,\alpha)\in\mathcal{G}_{(x,y)}}} \mathcal{R}_{(x,y-\alpha)} \tag{3.13}$$

and

$$\mathcal{R}_{\mathcal{B}_{(x,y)}} := \dot{\bigcup_{(0,\beta)\in\mathcal{B}_{(x,y)}}} \mathcal{R}_{(x,y-\beta)}. \tag{3.14}$$

Moreover, we can find a “distinguished” $w_0 \in \mathcal{T}_{(x,y)}$ (by Lemma 3.12); the valuations in $\tilde{\mathcal{R}}_{(x,y)}$ do not need to be tested (by Proposition 3.16); and for each $(0,\alpha) \in \mathcal{G}_{(x,y)}$ we can also find a "distinguished" valuation in $\mathcal{R}_{(x,y-\alpha)}$ (by Lemma 3.17). For $r := \#\mathcal{G}_{(x,y)}$ let $w_1, \ldots, w_r \in \mathcal{R}_{\mathcal{G}_{(x,y)}}$ be these "distinguished" valuations. Thus, if $\mathcal{B}_{(x,y)} = \emptyset$, we obtain that ρ is weakly isotropic over $H(K,v)$ for every $v \in \Re_\infty(K)_X$ if, and only if, ρ is weakly isotropic over $H(K,w_j)$ for each $0 \leq j \leq r$.

If we would have also this *"ideal situation"* (see Figure 3.1) for the set $\Re_\infty(K)_Y$ (that is, after the change $(x,y) := (Y^{-1}, Y^{-1}X))$, we would not have anything else to do. We could immediately test if $M(h)$ is Archimedean or not.

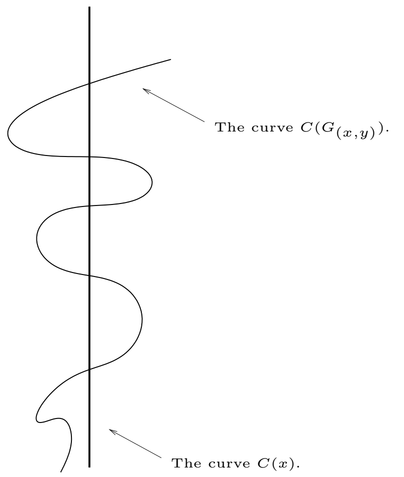

Figure 3.1: The ideal situation .

But in general $\mathcal{B}_{(x,y)} \neq \emptyset$. In this case we shall consider separately each point $(0,\beta) \in \mathcal{B}_{(x,y)}$ and make a suitable change of variables in order to obtain a better geometric situation. This is explained below:

<u>*Bad case :*</u> Valuations v with $(\overline{x}, \overline{y}) = (0,\beta) \in \mathcal{B}_{(x,y)}$.

Since $(0,\beta) \in \mathcal{B}_{(x,y)}$, the curves $C(x)$ and $C(G_{(x,y)})$ intersect at $(0,\beta)$ without normal crossing, as well as $C(y-\beta)$ and $C(F_{\beta(x,y)})$ do. After a translation (if necessary) we can assume that $(\overline{x}, \overline{y}) = (0,0)$ and (abusing the notation) the curves $C(x)$ and $C(G_{(x,y)})$ intersect at $(0,0)$ without normal crossing, as well as $C(y)$ and $C(F_{(x,y)})$ do.

We will consider separately the following cases:

$$(1) \quad y/x \notin \mathcal{O}_v$$
$$(2) \quad y/x \in \mathcal{O}_v.$$

<u>Case (1):</u>

Necessarily $x_1 := x/y \in \mathfrak{m}_v$ and we have $(\overline{x_1}, \overline{y}) = (0,0)$ for all valuations in this case. We then write the form ρ in terms of x_1 and y. If $(\overline{x_1}, \overline{y}) = (0,0) \notin$

$\mathcal{B}_{(x_1,y)}$, there is nothing else to do, except to consider the case (2). Otherwise, we are in the bad case again and repeat the procedure.
Case (2):

Define $y_1 := y/x$. There are two possibilities: $\overline{y_1} \notin \mathbb{R}$ or $\overline{y_1} \in \mathbb{R}$, that is, $v \in \mathcal{T}_{(x,y_1)}$ or $v \notin \mathcal{T}_{(x,y_1)}$. We then write the form ρ in terms of x and y_1 and obtain the set of "good" points $\mathcal{G}_{(x,y_1)}$ and the set $\mathcal{B}_{(x,y_1)}$ of "bad" points defined in Definition 3.18. If $v \in \mathcal{T}_{(x,y_1)}$, by Lemma 3.12 we can test if ρ is weakly isotropic over $H(K,v)$. If $v \in \mathcal{R}_{\mathcal{G}_{(x,y_1)}}$, we can also test using Lemma 3.17. So, if $\mathcal{B}_{(x,y_1)} = \emptyset$, we have nothing else to do. Otherwise, we are in the bad case again and repeat the procedure (for the finitely many points in $\mathcal{B}_{(x,y_1)}$).

We will need Lemmas 3.19 and 3.21 to prove that the procedure above will terminate, that is, we can not be always in the bad case.

Lemma 3.19. *Let $F \in \mathbb{R}[x,y]$ be a reduced polynomial such that the curve $C(F)$ has more than one possibly complex tangents at the point $(0,0)$. Then:*

(i) After the transformation $x = x_1 y$ one gets $\mathbb{R}[x,y] \subset \mathbb{R}[x_1,y]$ and

$$F = y^{m(F)} F_{(1)}(x_1, y)$$

with $F_{(1)}(x_1,y)$ reduced in $\mathbb{R}[x_1,y]$ and $m_{(a,b)}(F_{(1)}) < m(F)$ for the finitely many points $(a,b) \in C(F_{(1)}) \cap C(y)$.

(ii) After the transformation $y = y_1 x$ one gets $\mathbb{R}[x,y] \subset \mathbb{R}[x,y_1]$ and

$$F = x^{m(F)} F_{(2)}(x, y_1)$$

with $F_{(2)}(x,y_1)$ reduced in $\mathbb{R}[x,y_1]$ and $m_{(a,b)}(F_{(2)}) < m(F)$ for the finitely many points $(a,b) \in C(F_{(2)}) \cap C(x)$.

Proof: It follows from the assumption that for suitable $(\alpha_i, \beta_i) \in \mathbb{C} \times \mathbb{C} \backslash \{(0,0)\}$,

$$F(x,y) = \prod_{j=1}^{r} (\alpha_j x - \beta_j y)^{\epsilon_j} + \text{“Terms of higher degree”},$$

with $m(F) = \sum_{j=1}^{r} \epsilon_j$ and each $\epsilon_j < m(F)$. After the change $x = x_1 y$, each form of degree $i \geq m(F)$ that appears in F will be divisible by $y^{m(F)}$. Thus,

$$F = y^{m(F)} F_{(1)} = y^{m(F)} \{ \quad \prod_{j=1}^{r} (\alpha_j x_1 - \beta_j)^{\epsilon_j} + y F'(x_1, y) \quad \}.$$

Let $J := \{ \quad 1 \leq j \leq r \quad | \quad \alpha_j \neq 0 \}$. We see easily that $(a,0) \in C(F_{(1)})$ iff $a = \beta_j / \alpha_j \in \mathbb{R}$ for some $j \in J$. Suppose, without loss of generality, that

$a = \beta_1/\alpha_1$. Since $(\alpha_j, \beta_j) \neq (0,0)$, we have $c := \prod_{j \notin J} \beta_j^{\epsilon_j} \prod_{j \in J} \alpha_j^{\epsilon_j} \neq 0$. As the r tangent lines are distinct, for each $1 \neq j \in J$ we get $a - \beta_j \alpha_j^{-1} \neq 0$. Thus,

$$F_{(1)}(x_1, y) = c(x_1 - a)^{\epsilon_1} \prod_{1 \neq j \in J} [(x_1 - a) + (a - \beta_j \alpha_j^{-1})]^{\epsilon_j} + yF'(x_1, y)$$

and therefore

$$F_{(1)}(x_1, y) = d(x_1 - a)^{\epsilon_1} + \sum_{i > \epsilon_1} c_i (x_1 - a)^i + yF'(x_1, y)$$

for some $d \in \mathbb{R}\backslash\{0\}$ and $c_i \in \mathbb{R}$. Hence, one obtains $m_{(a,0)}(F_{(1)}) \leq \epsilon_1 < m(F)$.

The proof of (ii) is analogous. □

Definition 3.20. For any reduced polynomial $p \in \mathbb{R}[x, y]$ we define $p_{(1)}$, resp. $p_{(2)}$, to be the reduced polynomial obtained after the change $x = x_1 y$, resp. $y = y_1 x$. More precisely, by Lemma 3.19,

$$p_{(1)}(x_1, y) := y^{-m(p)} p(x_1 y, y) \quad \text{and} \quad p_{(2)}(x, y_1) := x^{-m(p)} p(x, y_1 x)$$

For iterated changes of this type we will use the following convention: Instead of $p_{(1)(1)}$, resp. $p_{(1)(2)}$, we will write $p_{(1.1)}$, resp. $p_{(1.2)}$. Analogously for $p_{(2)(1)}$, resp. $p_{(2)(2)}$. By induction, for each positive integer $n \geq 2$ we define $p_{(1^n)} := p_{(1^{n-1})(1)}$, where $p_{(1^1)} := p_{(1)}$. Analogously we define $p_{(2^n)}$.

Lemma 3.21. *Let $F \in \mathbb{R}[x, y]$ be a reduced polynomial such that the curve $C(F)$ has only one (real) tangent at the point $(0,0)$ with multiplicity $m(F) > 1$. Then*

(i) If $C(x)$ is the tangent of $C(F)$ at $(0,0)$, there exists a positive integer q such that the reduced curve $C(F_{(1^q)})$ has multiplicity strictly less than $m(F)$ at the point $(0,0)$. Moreover, $C(x) \cap C(F_{(2)}) = \emptyset$.

(ii) Analogously, if $C(y)$ is the tangent of $C(F)$ at $(0,0)$, there exists a positive integer l such that the reduced curve $C(F_{(2^l)})$ has multiplicity strictly less than $m(F)$ at the point $(0,0)$. Moreover, $C(y) \cap C(F_{(1)}) = \emptyset$.

Proof: (i) Set $m := m(F)$. Let $\gamma x^\eta y^\zeta$ be a monomial of F with minimal exponent η of x. Since F is reduced and $m > 1$, we must have $\eta \leq 1 < m$, and therefore $m - \eta > 0$. Moreover, $\zeta + \eta > m$. Let q and r natural numbers, resp. the quotient and the rest of the Euclidean division of $\zeta + \eta$ by $m - \eta$, that is, $\zeta + \eta = q(m - \eta) + r$ with $r < (m - \eta) \leq m$. By assumption we have

$$F = cx^m + \gamma x^\eta y^\zeta + \text{ “other terms” },$$

with constants $c, \gamma \in \mathbb{R}\backslash\{0\}$. Thus, after the change $x = x_1 y$ we get

$$F = y^m F_{(1)} = y^m[cx_1^m + \gamma x_1^\eta y^{\zeta-(m-\eta)} + \text{ ``other terms''}].$$

If $F_{(1)}$ has a monomial with degree strictly less than m, then we are done. Else, we make the change $x_1 = x_2 y$ and obtain

$$F = y^{2m} F_{(1.1)} = y^{2m}[cx_2^m + \gamma x_2^\eta y^{\zeta-2(m-\eta)} + \quad ''other \quad terms''].$$

If $F_{(1.1)}$ does not have a monomial with degree strictly less than m we make one more change. By iteration we will get in the q-th transformation

$$F = y^{qm} F_{(1^q)} = y^{qm}[cx_q^m + \gamma x_q^\eta y^{\zeta-q(m-\eta)} + \quad ''other \quad terms''].$$

Therefore the polynomial $F_{(1^q)}$ has a monomial with degree $\zeta + \eta - q(m - \eta) = r < m$ as desired.

By the change $y = y_1 x$ on F we get

$$F = x^m F_{(2)} = x^m[c + xF''(x, y_1)].$$

Hence $F_{(2)}(0, y_1) = c \neq 0$ and therefore $C(x) \cap C(F_{(2)}) = \emptyset$.

The proof of (ii) is analogous. □

Now we can prove the main result of this chapter:

Theorem 3.22. *Let $\rho := \langle 1, h_1, \ldots, h_m\rangle$ be a quadratic form with entries in $\mathbb{R}[X, Y]$. If the semialgebraic set $W(h)$ is compact, one can construct finitely many valuations $w_1, \ldots, w_n \in \Re_\infty(K)$ for which the following conditions are equivalent:*

(i) For all $v \in \Re_\infty(K)$: ρ is weakly isotropic over $H(K, v)$;

(ii) For each $1 \leq i \leq n$: ρ is weakly isotropic over $H(K, w_i)$.

Moreover, one can effectively test the condition (ii).

Proof: Let v be an arbitrary valuation in $\Re_\infty(K)$. Suppose that $v \in \Re_\infty(K)_X$ (if $v \in \Re_\infty(K)_Y$ we proceed analogously). Write the form ρ in the variables $(x, y) := (X^{-1}, X^{-1}Y)$ and obtain the set $\mathcal{Z}_{(x,y)} = C(x) \cap C(G_{(x,y)})$, where the polynomial $G_{(x,y)}$ is the reduction of the product of the entries of ρ without the factor x (see Definition 3.15). Write $\mathcal{Z}_{(x,y)} = \mathcal{G}_{(x,y)} \dot\cup \mathcal{B}_{(x,y)}$ with the sets $\mathcal{G}_{(x,y)}$ and $\mathcal{B}_{(x,y)}$ like in Definition 3.18 ("good" points and "bad" points, resp.).

We have that

$$\Re_\infty(K)_X = \mathcal{T}_{(x,y)} \dot\cup \tilde{\mathcal{R}}_{(x,y)} \dot\cup \mathcal{R}_{\mathcal{G}_{(x,y)}} \dot\cup \mathcal{R}_{\mathcal{B}_{(x,y)}}.$$

If $v \in \mathcal{T}_{(x,y)}$, by Lemma 3.12, we can construct a $w \in \mathcal{T}_{(x,y)}$ such that: ρ being weakly isotropic over $H(K,w)$ implies that ρ is weakly isotropic over $H(K,v)$.

If $v \in \mathcal{R}_{\mathcal{G}_{(x,y)}}$ using Lemma 3.17, we can also find a valuation $w \in \mathcal{R}_{\mathcal{G}_{(x,y)}}$ with this property.

If $v \in \tilde{\mathcal{R}}_{(x,y)}$ the form ρ is weakly isotropic over $H(K,v)$, by Proposition 3.16.

Thus, it remains to consider the case $v \in \mathcal{R}_{\mathcal{B}_{(x,y)}}$, that is, v is centered in a "bad" point $(0,\beta) \in \mathcal{B}_{(x,y)}$. After the translation $(x, y-\beta) \mapsto (x,y)$ (if necessary), we can assume that $(\overline{x}, \overline{y}) = (0,0)$ and (abusing the notation) we have the following:

Bad case : The curves $C(x)$ and $C(G_{(x,y)})$ intersect at $(\overline{x}, \overline{y}) = (0,0)$ without normal crossing, as well as $C(y)$ and $C(F_{(x,y)})$ do.

We will make the following:

Procedure :

Case (1): $y/x \notin \mathcal{O}_v$.

Define $x_1 := x/y$. Write the form ρ in terms of x_1 and y and obtain the set $\mathcal{Z}_{(x_1,y)} = \mathcal{G}_{(x_1,y)} \dot{\cup} \mathcal{B}_{(x_1,y)}$.

Case (2): $y/x \in \mathcal{O}_v$.

Define $y_1 := y/x$. Write the form ρ in terms of x and y_1 and obtain the set $\mathcal{Z}_{(x,y_1)} = \mathcal{G}_{(x,y_1)} \dot{\cup} \mathcal{B}_{(x,y_1)}$.

Suppose that v is in the case (1). In particular, $(\overline{x_1}, \overline{y}) = (0,0)$. If $(0,0) \notin \mathcal{Z}_{(x_1,y)}$, by Proposition 3.16 there is nothing to do. Let $(0,0) \in \mathcal{Z}_{(x_1,y)}$. If $(0,0) \in \mathcal{G}_{(x_1,y)}$, we apply Lemma 3.17. Else, we are in the bad case again. However, since $F_{(x_1,y)} = F_{(x,y)(1)}$, by Lemmas 3.19 and 3.21 we obtain:

$$0 \leq m(F_{(x_1,y)}) \leq m(F_{(x,y)}). \tag{3.15}$$

In the worst case we have $m(F_{(x_1,y)}) = m(F_{(x,y)})$. It means that the curve $C(F_{(x,y)})$ has only one (real) tangent at the origin, which must be $C(x)$. In fact, if

$$F_{(x,y)} = (ax+by)^{m(F_{(x,y)})} + \text{“Terms of higher degree”},$$

for some $b \in \mathbb{R}$ not zero, then $F_{(x_1,y)} = F_{(x,y)(1)} = ax_1 + b + yF'(x_1,y)$, and therefore $F_{(x_1,y)}(0,0) \neq 0$, which contradicts $m(F_{(x_1,y)}) = m(F_{(x,y)}) \geq 1$. Set $x_0 := x$ and define, by induction, $x_{n+1} := x_n/y$ for each $n \in \mathbb{N}$. If $m(F_{(x,y)}) > 1$, we can use Lemma 3.21(i) to ensure that applying the procedure $n = q-1$ times we will get

$$m(F_{(x_q,y)}) < m(F_{(x,y)}). \tag{3.16}$$

Suppose that v is in the case (2). If $\overline{y_1} \notin \mathbb{R}$, we have $v \in \mathcal{T}_{(x,y_1)}$ and can apply Lemma 3.12. Let $\overline{y_1} \in \mathbb{R}$. If $(0, \overline{y_1}) \notin \mathcal{Z}_{(x,y_1)}$, by Proposition 3.16 there is nothing to do. Assume that $(0, \overline{y_1}) \in \mathcal{Z}_{(x,y_1)}$. If $(0, \overline{y_1}) \in \mathcal{G}_{(x,y_1)}$, we can apply Lemma 3.17. Else, $(0, \overline{y_1}) = (0, \gamma) \in \mathcal{B}_{(x,y_1)}$. Since $G_{(x,y_1)} = G_{(x,y)(2)}$, Lemmas 3.19 and 3.21 ensure that

$$0 < m_{(0,\gamma)}(G_{(x,y_1)}) \leq m(G_{(x,y)}). \tag{3.17}$$

If we have $m_{(0,\gamma)}(G_{(x,y_1)}) < m(G_{(x,y)})$, after the translation $(x, y_1 - \gamma) \mapsto (x, y_1)$ (if necessary) and (abusing the notation) we are in the assumptions of the "bad"case again, this time with

$$m(G_{(x,y_1)}) < m(G_{(x,y)}). \tag{3.18}$$

In case that $m_{(0,\gamma)}(G_{(x,y_1)}) = m(G_{(x,y)})$, the curve $C(G_{(x,y)})$ has only one (real) tangent at $(0,0)$, namely $C(y - \gamma x)$. Consider the homomorphism

$$\sigma : \mathbb{R}[x, y] = \mathbb{R}[x, y - \gamma x] \longrightarrow \mathbb{R}[x, y]$$

given by $(x, y - \gamma x) \mapsto (x, y)$. If we write (abusing the notation) $G_{(x,y)}(x, y)$ for its image under σ, we are in the assumptions of Lemma 3.21(ii). Hence, there is a positive integer l for which

$$m(G_{(x,y_l)}) < m(G_{(x,y)}) \tag{3.19}$$

and therefore $m_{(0,\gamma')}(G_{(x,y_l)}) < m(G_{(x,y)})$ for each $(0, \gamma') \in \mathcal{Z}_{(x,y_l)}$. So, if $(0, \overline{y_l}) = (0, \gamma') \in \mathcal{B}_{(x,y_l)}$, after the translation $(x, y_l - \gamma') \mapsto (x, y_l)$ (if necessary) we have the assumptions of the "bad" case again, however with $G_{(x,y_l)}$(actually its image under the transaltion) satisfying (3.19).

Thus, it follows from (3.16) and (3.19) that, by induction, we will obtain $u, z \in \mathbb{R}(x, y) = K$ with $m(F_{(u,z)}) \leq 1$ or $m(G_{(u,z)}) \leq 1$.

Suppose, without loss of generality, that $m(F_{(u,z)}) \leq 1$. If $m(F_{(u,z)}) = 0$, by the definition of $F_{(u,z)}$ (see Definiton 3.15), we can write

$$\rho \cong \rho' \perp z^\mu \rho'', \tag{3.20}$$

with $\mu \in \{0, 1\}$ and the entries of ρ' and ρ'' in $\mathcal{O}_v^\times$. So, (as in the proof of Proposition 3.16) ρ have at most two v-residue forms with entries in $\mathbb{R}$ and, by Lemma 3.6, must be weakly isotropic over $H(K, v)$.

Let $m(F_{(u,z)}) = 1$ and suppose that we still are in the bad case. Writing $f_{(u,z)} = u^\mu z^\nu g(u, z)$ with g divisible neither by u nor by z, by Definition 3.15 we get $F_{(u,z)} = u^\mu g(u, z)$. Since $m(F_{(u,z)}) = 1$, either $\mu = 0$ and $m(g) = 1$ or $\mu = 1$ and $m(g) = 0$. The last can not occur, otherwise the curves $C(z)$ and $C(F_{(u,z)})$ would have normal crossing at $(0,0)$. Hence,

$$f_{(u,z)} = G_{(u,z)} = z^\nu g(u, z) = z^\nu (du + cz + \text{ “Terms of higher degree” }),$$

for $c, d \in \mathbb{R}$ not simultaneously zero. Since we are in the bad case, we must necessarily have $\nu = 1$ and $d = 0$. So, applying the procedure again, after the change in case (1) we obtain $F_{(u_1,z)} = g_{(1)}(u_1, z) = c + zF''(u_1, z)$. Hence, $m(F_{(u_1,z)}) = 0$. Like above, we can write ρ as in (3.20) and are done. Consider the case (2). Among the monomials of $g(u, z)$ not divisible by z, let du^ζ be those of less degree. So,

$$G_{(u,z_1)}(u, z_1) = z_1[cz_1 + du^{\zeta-1} + uG'(u, z_1)]$$

and we see easily that for $l = \zeta$, we will obtain

$$G_{(u,z_l)}(u, z_l) = dz_l + cz_l^2 + uz_lG''(u, z_1).$$

Hence, the curves $C(u)$ and $C(G_{(u,z_l)})$ intersect at $(0, 0)$ with normal crossing and we can apply Lemma 3.17. □

Remark 3.23. If the curve $C(F_{(x,y)})$ has only complex tangents at $(0, 0)$, after the change $x = x_1y$ we will get $F_{(x,y)(1)}(a, 0) \neq 0$ for all $a \in \mathbb{R}$, and therefore $(0, 0) \notin \mathcal{B}_{(x_1,y)}$. Analogously, if $C(G_{(x,y)})$ has only complex tangents at $(0, 0)$, after the change $y = y_1x$ we will obtain $G_{(x,y)(2)}(0, a) \neq 0$ for all $a \in \mathbb{R}$. So, $\mathcal{Z}_{(x,y_1)} = \emptyset$.

Chapter 4

The Algorithm and Examples

Let $h_1, \ldots, h_m$ be polynomials in *two* variables over $\mathbb{R}$ that define the semialgebraic compact set $W(h)$ in the plane $\mathbb{R} \times \mathbb{R}$. In this chapter we will describe an algorithmic procedure to check whenever the quadratic module $M(h_1, \ldots, h_m)$ is Archimedean or not.

The results of the previous chapter will be essential to guarantee that the procedure will terminate. Although we used valuations to describe the idea behind the algorithm in the previous chapter, we do not need to mention any valuation to describe it.

We will use the notation of the previous chapter. The sets $\mathcal{G}_{(x,y)}$ and $\mathcal{B}_{(x,y)}$ are those defined in Definition 3.18.

Theorem 4.1. *Let $h_1, \ldots, h_m \in \mathbb{R}[X, Y]$ such that the semialgebraic set $W(h)$ is compact. Then there exists an algorithm to decide whether the quadratic module $M(h_1, \ldots, h_m)$ is Archimedean or not.*

Proof: We will describe the procedure:

1. Define $(x, y) := (X^{-1}, X^{-1}Y)$.

2. Write the form ρ in the following way:

$$\rho \cong \langle 1, \ldots, x^{\mu_i} a'_i(x, y), \ldots \rangle ,$$

with the polynomials $x^{\mu_i} a'_i(x, y)$ being reduced in $\mathbb{R}[x, y]$ and each $a'_i(x, y)$ not divisible by x.

3. Test if at least one of the following conditions is satisfied:

   I. For all $t \in \mathbb{R}$: if $\prod_{i \text{ with } \mu_i = 0} a'_i(0, t) \neq 0$, then $a'_i(0, t) < 0$ for some i with $\mu_i = 0$;

   II. For all $t \in \mathbb{R}$: if $\prod_{i \text{ with } \mu_i = 1} a'_i(0, t) \neq 0$, then $a'_i(0, t) a'_j(0, t) < 0$ for some i, j with $\mu_i = \mu_j$.

If the test is negative, stop the procedure. The module $M(h)$ is not Archimedean.

If the test is positive, make the following:

4. For each $(0, \alpha) \in \mathcal{G}_{(x,y)}$:

   If $(0, \alpha)$ satisfies the condition (a) of Definition 3.18, write

   $$\rho \cong \langle 1, \dots, x^{\mu_i} q^{\nu_i} b_i(x, y), \dots \rangle ,$$

   with q being the only irreducible factor of $G_{(x,y)}$ that vanishes at $(0, \alpha)$, the polynomials $x^{\mu_i} q^{\nu_i} b_i(x, y)$ being reduced in $\mathbb{R}[x, y]$ and each $b_i(x, y)$ divisible neither by x nor by q.

   If $(0, \alpha)$ satisfies the condition (b) of Definition 3.18, write

   $$\rho \cong \langle 1, \dots, (y - \alpha)^{\mu_i} q^{\nu_i} b_i(x, y), \dots \rangle ,$$

   with q being the only irreducible factor of $F_{\alpha(x,y)}$ that vanishes at $(0, \alpha)$, the polynomials $(y - \alpha)^{\mu_i} q^{\nu_i} b_i(x, y)$ being reduced in $\mathbb{R}[x, y]$ and each $b_i(x, y)$ divisible neither by $y - \alpha$ nor by q.

5. Test if for each $(0, \alpha) \in \mathcal{G}_{(x,y)}$: $b_i(0, \alpha) < 0$ for some i with $(\mu_i, \nu_i) = (0, 0)$; or $b_i(0, \alpha) b_j(0, \alpha) < 0$ for some i, j with $(\mu_i, \nu_i) = (\mu_j, \nu_j)$.

   If the test is negative, stop the procedure. The module $M(h)$ is not Archimedean.

   If the test is positive, make the following:

6. If $(x, y) = (X^{-1}, X^{-1}Y)$ and $\mathcal{B}_{(x,y)} = \emptyset$, define $(x, y) := (Y^{-1}, Y^{-1}X)$ and proceed from item 2 on.

   If $(x, y) = (Y^{-1}, Y^{-1}X)$ and $\mathcal{B}_{(x,y)} = \emptyset$, stop the procedure. The module $M(h)$ is Archimedean.

7. If $\mathcal{B}_{(x,y)} \neq \emptyset$, for each $(0, \beta) \in \mathcal{B}_{(x,y)}$ proceed as follows:

   (i) Make the translation $(x, y - \beta) \mapsto (x, y)$. Denote by $a_i(x, y)$ the entries of ρ after the translation and consider the reduced polynomials $f_{(x,y)}$, $G_{(x,y)}$ and $F_{(x,y)}$ defined in Definition 3.15.

   (ii) If $C(y - \gamma x)$ is the only tangent of the curve $C(G_{(x,y)})$ at $(0, 0)$, for some $\gamma \in \mathbb{R}$, abuse the notation writing $f_{(x,y)}$, $G_{(x,y)}$ and $F_{(x,y)}$ respectively for its image under the homomorphism $\sigma : \mathbb{R}[x, y] \longrightarrow \mathbb{R}[x, y]$ given by $(x, y - \gamma x) \mapsto (x, y)$.

   (iii) Let $n = 0$ and $x_0 := x$.
   If $(0, 0) \in \mathcal{B}_{(x_n,y)}$ make the change $x_n = x_{n+1} y$ in the entries of ρ and consider the next n.

   (iv) Define k to be the smallest positive integer such that $(0, 0) \notin \mathcal{B}_{(x_n,y)}$.

(v) In case that $(0,0) \in \mathcal{G}_{(x_k,y)}$:

If $(0,0)$ satisfies the condition (a) of Definition 3.18, write

$$\rho \cong \left\langle 1, \dots, x_k^{\mu_i} q^{\theta_i} c_i(x_k, y), \dots \right\rangle,$$

with q being the only irreducible factor of $G_{(x_k,y)}$ that vanishes at $(0,0)$, the polynomials $x_k^{\mu_i} q^{\theta_i} c_i(x_k, y)$ being reduced in $\mathbb{R}[x_k, y]$ and each $c_i(x_k, y)$ divisible neither by x_k nor by q.

If $(0,0)$ satisfies the condition (b) of Definition 3.18, write

$$\rho \cong \left\langle 1, \dots, y^{\mu_i} q^{\theta_i} c_i(x_k, y), \dots \right\rangle,$$

with q being the only irreducible factor of $F_{(x_k,y)}$ that vanishes at $(0,0)$, the polynomials $y^{\mu_i} q^{\theta_i} c_i(x_k, y)$ being reduced in $\mathbb{R}[x_k, y]$ and each $c_i(x_k, y)$ divisible neither by y nor by q.

Test if $c_i(0,0) < 0$ for some i with $(\mu_i, \theta_i) = (0,0)$; or $c_i(0,0)c_j(0,0) < 0$ for some i, j with $(\mu_i, \theta_i) = (\mu_j, \theta_j)$.

If the test is negative, stop the procedure. The module $M(h)$ is not Archimedean.

If the test is positive, make the following:

(vi) For each $j \in \{0, \dots, k\}$:

Let $y_{j+1} := y/x_j$. Define $(x, y) := (x_j, y_{j+1})$ and proceed from item 2 on.

□

Example 4.2. Let $h_1 = X$, $h_2 = Y$ and $h_3 = 1 - X^2 - X^3Y - Y^6$. Writing the form ρ in the variables $(x, y) := (X^{-1}, X^{-1}Y)$, we obtain

$$\rho \cong \left\langle 1, x, xy, -x^2y - x^4 + x^6 - y^6 \right\rangle \tag{4.1}$$

The only i for which $\mu_i = 0$ is $i = 3$. Since $a_3'(0,t) = -t^6$, the condition I is satisfied and the test in the item 3 is positive.

The set $\mathcal{G}_{(x,y)}$ is empty and $\mathcal{B}_{(x,y)} = \{(0,0)\}$. Thus, there is nothing to do in the items 4,5 and 6.

Changing $x = x_1 y$ in (4.1), we get

$$\rho \cong \left\langle 1, x_1 y, x_1, -x_1^2 - x_1^4 y + x_1^6 y^3 - y^3 \right\rangle.$$

Since $(0,0) \in \mathcal{B}_{(x_1,y)}$, we make the change $x_1 = x_2 y$ and get

$$\rho \cong \left\langle 1, x_2, x_2 y, -x_2^2 - x_2^4 y^3 + x_2^6 y^7 - y \right\rangle.$$

Since $(0,0) \in \mathcal{B}_{(x_2,y)}$, we make the change $x_2 = x_3 y$ and get

$$\rho \cong \left\langle 1, x_3 y, x_3, -x_3^2 y - x_3^4 y^6 + x_3^6 y^{12} - 1 \right\rangle .$$

Thus, $(0,0) \in \mathcal{G}_{(x_3,y)}$. Since $c_3(0,0) = -1$, the test in the item (v) is positive and we shall make the item (vi).

For $j = 0$ we have $(x,y) := (x, y_1)$ with $y = y_1 x$. Writing the form ρ in this new variables, we get

$$\rho \cong \left\langle 1, x, y_1, x(-y_1 - x + x^3 - y_1^6 x^3) \right\rangle .$$

Now the only $\mu_i = 0$ is μ_2. Since, $a_2'(x, y_1) = y_1$, the condition I does not hold. Since $a_1'(0,t) = 1$ and $a_3'(0,t) = -t$, the condition II does not hold too.

Thus, the module $M(h)$ is not Archimedean.

Remark 4.3. If we consider $(x,y) = (Y^{-1}, Y^{-1}X)$, the set $\mathcal{B}_{(x,y)}$ is empty and $\mathcal{G}_{(x,y)} = \{(0,0)\}$. Moreover, we can easily see that the tests in the item 3 and 5 are positive. Thus, Example 4.2 shows that we really need to make the iteration procedure described in item 7 of the algorithm for the "bad" point $(0,0) \in \mathcal{B}_{(X^{-1}, X^{-1}Y)}$.

In order to consider the next example, we need the following definition.

Definition 4.4. For $p \in \mathbb{R}[X,Y] \backslash \{0\}$, let $\tilde{p} \in \mathbb{R}[X,Y] \backslash \{0\}$ be the homogeneous component of p of highest (total) degree.

Remark 4.5. The compactness of the set $W(h)$ implies that for all $(a,b) \in \mathbb{R} \times \mathbb{R} \backslash \{(0,0)\}$ and $s > 0$ large enough, there is an i with $h_i(sa, sb) < 0$. It follows that for all $(a,b) \in \mathbb{R} \times \mathbb{R} \backslash \{(0,0)\}$, there is an i with $\tilde{h}_i(a,b) \leq 0$.

Example 4.6. For each $i = 1, \ldots, m$ let h_i be given by

$$h_i(X,Y) = A_i X + B_i Y + C_i,$$

with $C_i \geq 0$, $(A_i, B_i) \neq (0,0)$ and $W(h)$ compact. Suppose that there are no parallel lines among the lines defined by these polynomials. (After a suitable linear transformation (if necessary), we can obtain this situation).

For $(x,y) := (X^{-1}, X^{-1}Y)$ we obtain $h_i \cong x(A_i + B_i y + C_i x)$. Thus, $\mu_i = 1$ and $a_i'(x,y) = A_i + B_i y + C_i x$, for all i.

Take an arbitrary $t \in \mathbb{R}$ with $a_i'(0,t) \neq 0$ for all i. Since $a_i'(0,t) = A_i + B_i t = \tilde{h}_i(1,t)$, by Remark 4.5, we get that $a_k'(0,t) < 0$ for some k. On the other hand, considering the point $(-1,-t)$ we must have $\tilde{h}_j(-1,-t) \leq 0$ for some j. Thus, $a_j'(0,t) = \tilde{h}_j(1,t) = -\tilde{h}_j(-1,-t) \geq 0$. As $a_j'(0,t) \neq 0$ we get $a_j'(0,t) > 0$. Thus, the test in the item 3 is positive.

Since we do not have parallel lines

$$G_{(x,y)} = \prod_i (A_i + B_i y + C_i x).$$

Thus,

$$\mathcal{Z}_{(x,y)} = \mathcal{G}_{(x,y)} = \{(0, -A_i/B_i) | i \text{ with } B_i \neq 0\}.$$

This set is not empty(by the compactness we must have $B_i < 0$ for at least one i).

For each $(0, \alpha) \in \mathcal{G}_{(x,y)}$, if $(0, \alpha) = (0, -A_k/B_k)$, then $q = A_k + B_k y + C_k x$ and therefore $(\mu_i, \nu_i) = (1, 0)$ and $a'_i(x, y) = A_i + B_i y + C_i x$ for each $i \neq k$, while $(\mu_k, \nu_k) = (1, 1)$ and $a'_k(x, y) = 1$.

Take an arbitrary $(0, \alpha) = (0, -A_k/B_k) \in \mathcal{G}_{(x,y)}$. For each $i \neq k$ we have $a'_i(0, \alpha) = A_i + B_i \alpha \neq 0$. Hence, $a'_i(0, \alpha) = \tilde{h}_i(1, \alpha) \neq 0$. If we have $a'_i(0, \alpha) > 0$ for all $i \neq k$, we would have $h_i(s(1, \alpha)) = s\tilde{h}_i(1, \alpha) + C_i > 0$ for s large enough, contradicting Remark 4.5. So, $a'_i(0, \alpha) < 0$ for some $i \neq k$. Similarly, if $a'_i(0, \alpha) < 0$ for all $i \neq k$, then $\tilde{h}_i(-1, -\alpha) > 0$ for all $i \neq k$ and $h_i(s(-1, -\alpha)) = s\tilde{h}_i(-1, -\alpha) + C_i > 0$ contradicting Remark 4.5. Thus, the test in the item 5 is positive.

Since $\mathcal{B}_{(x,y)} = \emptyset$, by the item 6 we shall define $(x, y) = (Y^{-1}, Y^{-1}X)$ and repeat from item 2 on. For this new variables we have $h_i \cong x(A_i y + B_i + C_i)$. Thus, it is easy to see that by the same arguments as above, we will get that the test in item 3, as well as that in item 5 are positive.

Thus, $M(h)$ is Archimedean.

Example 4.7. Let $h_1 = X$, $h_2 = Y$ and $h_3 = -B(X^2+Y^2) - CXY - A(X+Y) + 1$, with $A, B, C \in \mathbb{R}$, $B \neq 0$ or $C \neq 0$ and $W(h)$ compact.

Writing ρ in terms of $(x, y) := (X^{-1}, X^{-1}Y)$ we get

$$\rho \cong \left\langle 1, x, xy, -B - Cy - By^2 + x(-A - Ay + x) \right\rangle.$$

Thus, the condition II of the test in 3 is not satisfied. Since

$$a'_3(0, t) = -B - Ct - Bt^2,$$

the condition I is satisfied if, and only if, $C^2 - 4B^2 \leq 0$.

Suppose that $C^2 - 4B^2 < 0$. Then, $\mathcal{Z}_{(x,y)} = \mathcal{G}_{(x,y)} = \{(0, 0)\}$. Since $W(h)$ is compact, $B > 0$. Therefore, the test in 5 is positive.

Now suppose that $C^2 - 4B^2 = 0$. So, either $C = -2B$ or $C = 2B$. In the first case, the compactness of $W(h)$ implies that $A > 0$. In this case, $\mathcal{B}_{(x,y)} = \{(0, -C/2B)\}$. Defining $u := y + C/2B$, we have

$$\rho \cong \left\langle 1, x, x(u - C/2B), -Bu^2 + x^2 - A(u - C/2B)x - Ax \right\rangle.$$

Thus, for $x = x_1 u$ we get

$$\rho \cong \left\langle 1, x_1 u, x_1 u(u - C/2B), u[-Bu - Ax_1 + x_1^2 u - A(u - C/2B)x_1] \right\rangle,$$

and therefore $(0, 0) \in \mathcal{B}_{(x_1, u)}$. So, we make the change $x_1 = x_2 u$. After that we get

$$\rho \cong \left\langle 1, x_2, x_2(u - C/2B), [-B - Ax_2 + x_2^2 u^2 - A(u - C/2B)x_2] \right\rangle.$$

Thus, $(0,0) \in \mathcal{G}_{(x_1,u)}$. Since $B > 0$, the test in 5 is positive.

Note that if we have $C^2 - 4B^2 = 0$, either $C = -2B$ or $C = 2B$. In the first case, the compactness of $W(h)$ implies that $A > 0$.

Thus,

$$\begin{aligned} M(h) \text{ Archimedean and } W(h) \text{ compact } \Leftrightarrow & (B > 0, 4B^2 > C^2) \text{ or} \\ & (B, A > 0, C = -2B) \text{ or} \\ & (B > 0, C = 2B). \end{aligned}$$

Bibliography

[AM] Atiyah, M.; Macdonald, I.G. *Introduction to Commutative Algebra.* Addison-Wesley series in Mathematics(1969).

[BCR] Bochnak, J.; Coste, M.; Roy, M.-F. *Real algebraic geometry.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, Bd. 12, Berlin: Springer-Verlag (1987).

[B] Bourbaki, Nicolas. *Elements of mathematics.* Commutative algebra. Chapters 1–7. 1989.

[Ha] Hartshorne, Robin. *Algebraic Geometry.* Graduate Texts in Mathematics, 52. New York-Heidelberg-Berlin: Springer- Verlag. (1983).

[Ja] Jacobi, T. *A representation theorem for certain partially ordered commutative rings.* Math. Z. 237, No.2, 259-273 (2001).

[JP] Jacobi, T.; Prestel, A. *Distinguished representations of strictly positive polynomials.* J. Reine Angew. Math. 532, 223-235 (2001).

[Ki] Kirwan, F. *Complex algebraic curves.* London Mathematical Society Student Texts. 23. Cambridge etc.: Cambridge University Press (1992).

[Ma] Marshall, M. *Positive Polynomials and Sums of Squares.* Univ. Pisa. Dipart. Mat., Instituti Editoriali e Poligrafici Internazionali. 2000.

[PD] Prestel, A.; Delzell, C. *Positive polynomials. From Hilbert's 17th problem to Real Algebra.* Springer Monographs in Mathematics (2001).

[Pr1] Prestel, A. *Lectures on formally real fields.* Lecture Notes in Mathematics. 1093. Springer-Verlag (1984).

[Pr2] Prestel, A. *Einführung in die mathematische Logik und Modelltheorie.* Vieweg Studium, 60. Aufbaukurs Mathematik. (1986).

[SaZ] Samuel, Pierre; Zariski, Oscar; *Commutative Algebra.* Vol. II. Reprint of the 1958-1960 Van Nostrand edition. Graduate Texts in Mathematics. 29. New York - Heidelberg -Berlin: Springer-Verlag. (1976).

[Sch] Schülting, H.W. *Prime divisors on real varieties and valuation theory.* J. Algebra 98, 499-514 (1986).

[Wa] Walker, R.J. *Algebraic Curves.* New York - Heidelberg -Berlin: Springer-Verlag.1978.