The pp conjecture for spaces of orderings of rational conics

Paweł Gładki [a,*], Murray Marshall [b,1]

[a] *Department of Mathematics and Statistics, University of Saskatchewan, 106 Wiggins Road, Saskatoon, SK, Canada, S7N 5E6*

[b] *Mathematical Sciences Group, Department of Computer Science, University of Saskatchewan, 106 Wiggins Road, Saskatoon, SK, Canada, S7N 5E6*

Abstract

First counterexamples are given to a basic question raised in: M. Marshall, *Open questions in the theory of spaces of orderings*, J. Symbolic Logic 67 (2002), 341-352. The paper considers the space of orderings (X, G) of the function field of a real irreducible conic $\mathcal{C}$ over the field $\mathbb{Q}$ of rational numbers. It is shown that the pp conjecture fails to hold for such a space of orderings when $\mathcal{C}$ has no rational points. In this case, it is shown that the pp conjecture 'almost holds' in the sense that, if a pp formula holds on each finite subspace of (X, G), then it holds on each proper subspace of (X, G). For pp formulas which are product-free and 1-related, the pp conjecture is known to be true, at least if the stability index is finite (M. Marshall, *Local-global properties of positive primitive formulas in the theory of spaces of orderings*, to appear). The counterexamples constructed here are the simplest sort of pp formulae which are not product-free and 1-related.

Key words: Quadratic forms, spaces of orderings, local-global principles, pp formulae

1991 MSC: 11E81, 11E25, 06F25, 12J15, 12D15

1 Introduction

The notion of spaces of orderings was introduced by the second author in the 1970's and provides an abstract framework for studying orderings on fields and the reduced theory of quadratic forms over fields. There are several monographs dealing with the subject, [1] and [9] being ones that are frequently referred to. The structure of a space of orderings (X, G) is completely determined by the group structure of G and the ternary relation $a \in D(b, c)$ on G; the groups with additional structure arising in this way are called reduced special groups [6]. We are interested in the elementary language of special groups L_{SG} with $\cong$ as a relational symbol, $\cdot$ as a functional symbol, two constants 1 and -1, and usual logical symbols. Atomic formulae are of the form either $t_1 = t_2$ for terms t_1, t_2 or $(t_1, t_2) \cong (t_3, t_4)$ for terms $t_1, \ldots, t_4$. Using this language one can develop the theory of special groups; see [6, Definition 1.2] for detailed axiomatization. Traditionally we will exchange the quaternary relation $\cong$ with the ternary one $a \in D(b, c)$, according to the following rule:

$$a \in D(b, c) \text{ iff } (b, c) \cong (a, abc).$$

* Corresponding author; phone: +1-306-966-6090, fax: +1-306-966-6086
Email addresses: `gladki@math.usask.ca` (Paweł Gładki),
`marshall@math.usask.ca` (Murray Marshall).

[1] This research was supported in part by NSERC of Canada, and by the University of Paris in cooperation with the European Research and Training Network Real Algebraic and Analytic Geometry

Hence the atomic formulae can be (modulo some of the axioms) exchanged with the ones of the form $1 \in D(a, b)$.

Our main interest is in positive-primitive (pp for short) formulae

$$\exists v_1, \ldots, v_n \psi(v_1, \ldots, v_n, w_1, \ldots, w_k),$$

where $\psi(v_1, \ldots, v_n, w_1, \ldots, w_k)$ is a finite conjunction of atoms of the form

$$1 \in D(a \prod_{i=1}^{n} v_i^{\epsilon_i}, b \prod_{i=1}^{n} v_i^{\delta_i}),$$

for $\epsilon_i, \delta_i \in \{0, 1\}$, $v_i^0 = 1$, $v_i^1 = v_i$ and a, b being products of ± 1 and a finite number of w_j's. Examples of such formulae are"two forms are isometric", "an element is represented by a form", "a form is isotropic". The following problem, known as the pp conjecture, is stated in [10]:

Open Problem: Is it true that every pp formula which holds on every finite subspace of a space of orderings holds on the whole space?

In other words, the problem poses the question of the validity of a very general and highly abstract "local-global principle". The answer to the Open Problem is affirmative for all the examples of pp formulae mentioned above. Another related result is the Extended Isotropy Theorem; see [9]. In [11] a still larger class of pp formulae called product-free and 1-related is introduced and it is proved that, for such formulae and for any space having finite stability index, the answer to the Open Problem is "yes". It has also been shown, that the class of spaces of orderings for which the conjecture is true contains spaces of orderings of finite chain length, spaces of stability index 1 (which includes spaces of orderings of curves over real closed fields) and is closed under direct sum and group extension (see [10]). It has always seemed unlikely that the conjecture has a positive solution in general - but no counterexamples were known.

Both the space of orderings of a rational function field in two variables over a real closed field and the space of orderings of the field $\mathbb{Q}(x)$ are of stability index 2. The former has rather complicated real valuations and in this case the question remains open, while the latter has well-understood real valuations, and it has been shown in [5], that the answer to the Open Problem is affirmative in this case. This suggests looking at finite extensions of $\mathbb{Q}(x)$.

In this paper we investigate the space of orderings of the function field of a real irreducible conic over the field $\mathbb{Q}$. We consider all possible cases and construct counterexamples showing that the pp conjecture fails for the space of orderings of the function field of an ellipse (or hyperbola) without rational points and also in the case of two parallel lines. In [11] the simplest sort of pp formula which is not product-free and 1-related is also considered. The counterexamples we construct are of this type. At the same time, we show that the pp conjecture is 'almost true' for these spaces of orderings in the sense that any pp formula which holds on every finite subspace also holds on every proper subspace. In all the remaining cases, the function field of the conic is purely transcendental over $\mathbb{Q}$ so, by the result for $\mathbb{Q}(x)$ in [5], the pp conjecture is valid in these remaining cases.

* * *

Throughout this paper we shall use the standard notation for the fields and rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$ etc. For any subset S of a field F, we denote the set $S \setminus \{0\}$ by S^*.

For a (formally) real field F and a subset $S \subseteq F$ denote by $\Sigma F^2[S]$ the preordering generated by S. $\Sigma F^2[S]$ consists of all finite sums of terms of the form $f^2 g_1 \dots g_s$, $f \in F$, $g_1, \dots, g_s \in S$. The space of orderings associated to S is (X_S, G_S), where X_S denotes the set of all orderings of F lying over S (or, equivalently, over $\Sigma F^2[S]$), and $G_S := F^*/(\Sigma F^2[S])^*$. Elements of the group G_S are naturally viewed as functions from X_S to $\{-1, 1\}$.

If $S = \emptyset$, then $\Sigma F^2[S]$ is just the set ΣF^2 of sums of squares and the corresponding space of orderings (called the space of orderings of F) will be denoted simply by (X, G), i.e., $(X, G) := (X_\emptyset, G_\emptyset)$. Every subspace of (X, G) is of the form (X_S, G_S) for some subset S of F [9, Theorem 2.4.1].

Writing $\underline{f} \in G_S$ to denote the image of f in F^*, we define the value set:

$$\begin{aligned} &D_S(\underline{g}, \underline{h}) = \{\underline{f} \in G_S : f = sg + th, s, t \in \Sigma F^2[S]\} \\ &= \{\underline{f} \in G_S : \forall Q \in X_S, \underline{f}(Q)\underline{g}(Q) > 0 \text{ or } \underline{f}(Q)\underline{h}(Q) > 0\} \end{aligned}$$

[9, Lemma 2.1.2]. In the case $S = \emptyset$ we shall write $D(\underline{g}, \underline{h})$ instead of $D_S(\underline{g}, \underline{h})$. We denote by $\tau_S : G \to G_S$ the canonical group homomorphism. The map τ_S is a morphism in the category of special groups.

If v is a real valuation on F, the set of orderings compatible with v, denoted X_v, is a subspace of X (equal to X_S where S is the set of elements of F of the form $1 + t$, $v(t) > 0$). The group G_S in this case will be denoted by G_v, value set $D_S(\underline{g}, \underline{h})$ will denoted by $D_v(\underline{g}, \underline{h})$ and the morphism $\tau_S : G \to G_v$ will be denoted by τ_v.

A pp-formula ϕ with parameters $\underline{f_1}, \dots, \underline{f_k}$ in G has the form

$$\phi = \exists t_1 \dots \exists t_n \psi(t_1, \dots, t_n, \underline{f_1}, \dots, \underline{f_k})$$

where $\psi(t_1, \dots, t_n, \underline{f_1}, \dots, \underline{f_k})$ is a finite conjunction of atoms

$$1 \in D(\underline{g} \prod_{i=1}^{n} t_i^{\epsilon_i}, \underline{h} \prod_{i=1}^{n} t_i^{\delta_i}), \tag{1}$$

for $\epsilon_i, \delta_i \in \{0, 1\}$, $i \in \{1, \dots, n\}$, and $\underline{g}$, $\underline{h}$ being products of ± 1 and a finite number of the $\underline{f_j}$. The associated pp formula ϕ_S with parameters in the quotient G_S is obtained by replacing each atom (1) of ϕ with

$$1 \in D_S(\tau_S(\underline{g}) \prod_{i=1}^{n} t_i^{\epsilon_i}, \tau_S(\underline{h}) \prod_{i=1}^{n} t_i^{\delta_i}).$$

For a real valuation v of F, the associated pp-formula ϕ_v with parameters in G_v is obtained by replacing each atom (1) of ϕ with

$$1 \in D_v(\tau_v(\underline{g}) \prod_{i=1}^{n} t_i^{\epsilon_i}, \tau_v(\underline{h}) \prod_{i=1}^{n} t_i^{\delta_i}).$$

2 Coordinate rings and function fields of conics

We want to investigate the space of orderings of the function field $F = \mathbb{Q}(\mathcal{C})$ where $\mathcal{C}$ is a real irreducible conic defined over $\mathbb{Q}$. By definition, F is the field of fractions of $A = \mathbb{Q}[\mathcal{C}]$, the coordinate ring of $\mathcal{C}$. If F is purely transcendental over $\mathbb{Q}$ then the result for $\mathbb{Q}(x)$ in [5] shows that the pp conjecture holds, so we concentrate our attention here on the remaining cases.

Everything we do to begin with works equally well with $\mathbb{Q}$ replaced by any field k of characteristic $\neq 2$, so we begin in this more general setting. After making a linear change in variables we can assume $\mathcal{C}$ is one of the following types:

$$ax^2 + by^2 = c, \quad a, b, c \in k,\ a, b \neq 0,\ \text{(Elliptic/Hyperbolic Type)}, \tag{2}$$

$$x^2 = d, \quad d \in k, \qquad \text{(Parallel Type)}, \tag{3}$$

$$y = x^2, \qquad \text{(Parabolic Type)}. \tag{4}$$

In fact this is true for any conic $\mathcal{C}$ defined over k, irreducible or not; see [3, §151]. Since $ax^2 + by^2 = 0$ is equivalent to $a(\frac{x}{y})^2 + b = 0$ and $k(x, y) = k(\frac{x}{y}, y)$, any irreducible curve of type (2) with $c = 0$ is birationally equivalent to an irreducible curve of type (3) with $d = -\frac{b}{a}$. If $\mathcal{C}$ is of type (4), then $k(\mathcal{C}) = k(x, y) = k(x, x^2) = k(x)$, so $k(\mathcal{C})$ is purely transcendental over k in this case. $k(\mathcal{C})$ is also purely transcendental over k in case $\mathcal{C}$ is of type (2) with $c \neq 0$, and $\mathcal{C}$ has a k-rational point. This is well-known: If (x_0, y_0) is a k-rational point of $\mathcal{C}$, then $k(\mathcal{C}) = k(z)$ where $z := \frac{y-y_0}{x-x_0}$ [14, page 6]. This leaves us with type (2) curves (with $c \neq 0$) without k-rational points and type (3) curves (also without k-rational points, because we assume the curves we are dealing with are irreducible, so $\sqrt{d} \notin k$).

In what we are doing here, we will only be interested in real curves defined over $k = \mathbb{Q}$. Since $ax^2 + by^2 = c$ is equivalent to $a + b(\frac{y}{x})^2 = c(\frac{1}{x})^2$ and $\mathbb{Q}(x, y) = \mathbb{Q}(\frac{1}{x}, \frac{y}{x})$, we see that the type (2) curves that we need to deal with can be assumed to be of elliptic type, i.e., $ax^2 + by^2 = c$, where $a, b, c \in \mathbb{Q}$ are all positive. We need the following:

Lemma 1 *The coordinate ring of an irreducible curve of type (2) over any field k, $char(k) \neq 2$, without k-rational points is a PID.*

See [13] for a proof and for other results of this sort. For completeness, and because we need many of the ideas later, we give the proof. Note that the same result also holds for any irreducible curve of type (3), but the proof is trivial in this case, since the coordinate ring is isomorphic to $k(\sqrt{d})[y]$, the polynomial ring in one variable y over the field $k(\sqrt{d})$.

PROOF. Let $A = k[\mathcal{C}]$, $F = k(\mathcal{C})$. Since $\mathcal{C}$ is defined by $ax^2 + by^2 = c$, $a, b, c \neq 0$, $A = k[x][\sqrt{\Delta}]$, where $\Delta := \frac{1}{b}(c - ax^2)$. On checks that A is the integral closure of $k[x]$ in F, so A is a Dedekind domain; see [16, Theorem V.19]. It suffices to show that each non-zero prime ideal in A is principal. The relationship between non-zero prime ideals $\mathfrak{p}$ in A and irreducible polynomials f in $k[x]$ is well-known. Let $\mathfrak{p}$ be a non-zero prime ideal in A and let (f) denote the intersection of $\mathfrak{p}$ with $k[x]$. There are three cases to consider [16, Theorems V.13 and V.22]:

1. $f = \Delta$. Then $(f)_A$, the extension of (f) to A, is equal to $\mathfrak{p}^2$. In this case, $\mathfrak{p}$ is the principal ideal generated by $y = \sqrt{\Delta}$.

2. Δ is not a square in $\frac{k[x]}{(f)}$. In this case, $(f)_A = \mathfrak{p}$, i.e., $\mathfrak{p}$ is the principal ideal generated by f.

3. Δ is a (non-zero) square in $\frac{k[x]}{(f)}$. In this case $(f)_A = \mathfrak{p}\overline{\mathfrak{p}}$, where $\overline{\mathfrak{p}}$ denotes the conjugate of $\mathfrak{p}$, i.e., the image of $\mathfrak{p}$ under the conjugation map $g + h\sqrt{\Delta} \mapsto g - h\sqrt{\Delta}$, $g, h \in k[x]$. In this case we claim that $rf = \gamma\overline{\gamma}$ for some $\gamma \in A$ and some $r \in k^*$. This will imply that $\mathfrak{p}$ is principal (generated either by γ or $\overline{\gamma}$) and will complete the proof. By assumption, $\Delta = s^2 - rf$, i.e., $rf = s^2 - \Delta = \gamma_0\overline{\gamma_0}$ where $\gamma_0 = s + \Delta$, for some $r, s \in k[x]$. Replacing s by the remainder obtained by dividing s by f, we are reduced to the case where $\deg(s) < \deg(f)$. The proof is by induction on $\deg(f)$. Observe that f is not linear. (If f is linear then f has a root $p \in k$. Then $s(p)^2 - \Delta(p) = 0$, i.e., $ap^2 + bs(p)^2 = c$, contradicting the assumption that $\mathcal{C}$ has no k-rational points.) If $\deg(f) = 2$ then, comparing degrees, we see that $r \in k^*$ and we are done. Suppose $\deg(f) > 2$. Since

$\deg(rf) = \deg(s^2 - \Delta) \leq \max\{\deg(s^2), \deg(\Delta)\}$, we see that $\deg(r) < \deg(f)$. We may assume $\deg(r) > 0$. Consider the (not necessarily distinct) irreducible factors $f_1, \ldots, f_t$ of r. By induction on the degree, $r_i f_i = \gamma_i \overline{\gamma_i}$ for some $\gamma_i \in A$, $r_i \in k^*$, so

$$qf \prod_{i=1}^{t} \gamma_i \overline{\gamma_i} = \gamma_0 \overline{\gamma_0} \tag{5}$$

for some $q \in k^*$. We know that (γ_i) and $(\overline{\gamma_i})$ are prime ideals in A and $(f_i)_A = (\gamma_i)(\overline{\gamma_i})$. Since A is a Dedekind domain, (5) implies that, for each i, (γ_i) or $(\overline{\gamma_i})$ appears in the factorization of (γ_0) into prime ideals. Interchanging γ_i and $\overline{\gamma_i}$ if necessary, we can assume the former is always the case. Then the ideal $(\gamma_1 \ldots \gamma_k)$ is a factor of the ideal (γ_0). This implies that $\gamma_0 = \gamma_1 \ldots \gamma_k \delta$ for some $\delta \in A$. Then $qf = \delta\overline{\delta}$ and the proof is complete. □

We also record the following result which we need later. The hypothesis and notation are the same as in Lemma 1.

Lemma 2 *(1) The units of A are precisely the elements of k^*.*

(2) For any $r, s, t \in k$, $s \neq 0$, $\pi = rx + sy + t$ is irreducible in A.

PROOF. (1) If $\gamma = f - g\sqrt{\Delta}$ is a unit of A, then $\gamma\overline{\gamma} = g^2 - h^2\Delta$ is a unit of $k[x]$, i.e., $g^2 - h^2\Delta = g^2 + \frac{a}{b}h^2x^2 - \frac{c}{b}h^2$ has degree zero. If $h \neq 0$, then, comparing leading coefficients, we see that $-\frac{a}{b}$ is a square in k. Since $(\frac{a+c}{2a}, \frac{a-c}{2a}\sqrt{-\frac{a}{b}})$ is a point on $\mathcal{C}$, this contradicts our assumption that $\mathcal{C}$ has no k-rational points. It follows that $h = 0$ and $\deg(g) = 0$.

(2) $\pi\overline{\pi} = (rx + t)^2 - s^2\Delta = \frac{s^2}{b}(ax^2 + b(\frac{rx+t}{s})^2 - c)$. If this is reducible in $k[x]$, then it has a root in k, contradicting the assumption that $\mathcal{C}$ has no k-rational

points. Thus $\pi\overline{\pi}$ is irreducible in $k[x]$ and, consequently, π is irreducible in A. $\square$

3 The case of an ellipse

In this section we use the notation established above, but now we work exclusively over the base field $k = \mathbb{Q}$. We assume always that $\mathcal{C}$ is the ellipse defined by $ax^2 + by^2 = c$, where a, b, c are positive rationals and that $\mathcal{C}$ has no rational points.

We consider first the relationship between the real points on $\mathcal{C}$ and orderings on F. Suppose $p = (p_1, p_2)$ is a real point on $ax^2 + by^2 = c$. The kernel of the evaluation map $x \mapsto p_1$, $y \mapsto p_2$ from A to $\mathbb{R}$ is either the zero ideal or some maximal ideal (π), where $\pi \in A$ is irreducible and real. In the former case p corresponds to a real embedding of F into $\mathbb{R}$, i.e., to an archimedean ordering on F. In the latter case, since the residue field $\frac{A}{(\pi)}$ is a finite extension of $\mathbb{Q}$ (see [4, Corollary to Theorem I.6.2], [15, Corollary I.1.15]), there are only finitely many real points p on $\mathcal{C}$ satisfying $\pi(p) = 0$. These points correspond to the finitely many embeddings of $\frac{A}{(\pi)}$ into $\mathbb{R}$. Each of these points corresponds to an archimedean ordering on $\frac{A}{(\pi)}$ [12, Corollary 1.3.19] and to a pair of non-archimedean orderings on F compatible with the discrete valuation v_π, one making π positive, and one making π negative [2] [8] [12].

All orderings on F arise in this way: Let P be an ordering of F, let $B \subseteq F$ denote the valuation ring of F consisting of elements which are bounded with respect to P, and let v be the valuation on F corresponding to B. Since $ax^2+by^2 = c$ in F and $a, b, c > 0$, $v(ax^2+by^2) = \min\{v(x^2), v(y^2)\} = v(c) = 0$, so $v(x), v(y) \geq 0$. This implies $x, y \in B$, so $A \subseteq B$. The intersection of the maximal ideal of B with A is some prime ideal of A. If this prime ideal is non-zero then it is the principal ideal generated by some irreducible π. In this case $v = v_\pi$ and P is one of the finitely many orderings on F compatible with v_π. If this prime ideal is the zero ideal, then $B = F$ and P is an archimedean ordering of F.

We make use of the following two results:

Lemma 3 *For any irreducible π of A, π changes sign on $\mathcal{C}$ at each real root p of π on $\mathcal{C}$.*

PROOF. There are two orderings on F compatible with the valuation v_π and pulling back the ordering on $\frac{A}{(\pi)}$ determined by p. One of these orderings makes π positive, and the other makes π negative. By the Transfer Principle, there are real algebraic points on $\mathcal{C}$ arbitrarily close to p where π is positive, and there are real algebraic points on $\mathcal{C}$ arbitrarily close to p where π is negative. Since π has only finitely many real roots on the ellipse $\mathcal{C}$, this forces π to be positive on one side of p and negative on the other side of p. $\square$

¿From Lemma 3 it follows, in particular, that π has an even number of real roots on $\mathcal{C}$.

We use the following 'geometric description' of value sets. See section 1 for the definition of value sets.

Lemma 4 *(1) Suppose S is a finite subset of A with $0 \notin S$, f, g, h are non-zero elements of A and $\overline{f}, \overline{g}, \overline{h}$ denote the associated elements of G_S. Then*

$\overline{f} \in D_S(\overline{g}, \overline{h})$ holds iff $fg \geq 0$ at p or $fh \geq 0$ at p holds for all points p of $\mathcal{C}$ satisfying $s > 0$ at p $\forall$ $s \in S$.

(2) *Suppose $\pi \in A$ is a real irreducible, f, g, h are non-zero elements of A and $\overline{f}, \overline{g}, \overline{h}$ denote the associated elements of G_{v_π}. Then $\overline{f} \in D_{v_\pi}(\overline{g}, \overline{h})$ holds iff $fg \geq 0$ at p or $fh \geq 0$ at p holds for all real points p of $\mathcal{C}$ sufficiently close to the real roots of π.*

PROOF. (1) is a special case of [5, Corollary 3.2]. It can also be seen directly, using the relationship between points and orderings described above. (2) is immediate from the definition of $D_{v_\pi}(\overline{g}, \overline{h})$ given in the introduction, using the correspondence between orderings of X_{v_π} and roots of π. $\square$

Note: For $f, g \in A$ with $f, g \neq 0$, $\frac{f}{g} = (\frac{1}{g})^2(fg)$. It follows that every element of G_S is represented by a non-zero element of A.

We begin by proving a general theorem concerning pp formulae. The proof is a modification of the proof of [5, Theorem 4.1].

Theorem 5 *Let F be the function field of a rational conic $ax^2 + by^2 = c$, where a, b, c are positive, which has no rational points. For a given pp-formula*

$$\phi = \exists t_1 \ldots \exists t_n \psi(t_1, \ldots, t_n, \underline{f_1}, \ldots, \underline{f_k}),$$

$\underline{f_i}$ denoting the image of $f_i \in \mathbb{Q}[\mathcal{C}]^*$ under the homomorphism $f \mapsto \underline{f}$ from F^* to G, let Σ denote the set of all irreducible factors of the f_i, $i \in \{1, \ldots, k\}$, and assume $\Sigma \neq \emptyset$. The following conditions are equivalent:

(1) *$G_{v_\pi} \models \phi_{v_\pi}$, for each $\pi \in \Sigma$.*

(2) *$G_S \models \phi_S$, for each proper subspace (X_S, G_S) of (X, G).*

(3) $G_S \models \phi_S$*, for each finite subspace* (X_S, G_S) *of* (X, G)*.*

We remark that the case $\Sigma = \emptyset$ is not interesting. The units of A are non-zero rationals (by Lemma 2 (1)) so, if $\Sigma = \emptyset$, then the validity of ϕ is equivalent to the validity of ϕ_P at a single $P \in X$.

PROOF. The implications (2) $\Rightarrow$ (3) and (3) $\Rightarrow$ (1) are clear, so it remains to show (1) $\Rightarrow$ (2). If X_S is a proper subspace of X then there exists some non-zero $e \in A$ such that $\underline{e}$ is positive at all orderings in X_S and $\underline{e}$ is negative at some $P \in X$. Then $X_S \subseteq X_{\{e\}}$, so we are reduced to the case $S = \{e\}$ (so, in particular, we can assume S is finite). By the Transfer Principle, the set of points p on the ellipse $\mathcal{C}$ satisfying $e(p) < 0$ is not empty. Since this set is open (by the continuity of e), there exists an open arc J on $\mathcal{C}$ such that $J \neq \emptyset$ and $e(p) < 0$ for all $p \in J$. Replacing J by a possibly smaller arc, we can assume J does not contain any of the (finitely many) real roots of the irreducibles $\pi \in \Sigma$.

Using this, along with Lemma 4 (1), we see that it suffices to show that, for any non-empty open arc J on $\mathcal{C}$ disjoint from the real roots of the $\pi \in \Sigma$, there exist non-zero $t'_1, \ldots, t'_n \in A$ such that, for each atom $1 \in D(\underline{g}t^\alpha, \underline{h}t^\beta)$ (with $g, h \in A$ each being products of ± 1 and a finite number of f_i) appearing in the formula ϕ, and each real point p on $\mathcal{C}$ but not on J, at least one of gt'^α, ht'^β is ≥ 0 at p.

Proceed as follows: The real roots of the various π in Σ divide the ellipse $\mathcal{C}$ in into (finitely many) disjoint open arcs. The arc J lies in exactly one of these arcs. Denote by T the set consisting of all of these open arcs except for the one containing J. For each arc $I \in T$, fix an irreducible π_I in A of the form

$rx + sy + t$, $r, s, t \in \mathbb{Q}$, $s \neq 0$, cutting the ellipse $\mathcal{C}$ at two points p_{1I}, p_{2I} with $p_{1I} \in I$, $p_{2I} \in J$.

By the Chinese Remainder Theorem (or the approximation theorem for independent valuations [12, Theorem A.5.12]) and our assumption (1), we have non-zero $t_1, \ldots, t_n \in A$ such that, for each of the atoms $1 \in D(\underline{g}t^\alpha, \underline{h}t^\beta)$ appearing in the formula ϕ, $1 \in D_{v_\pi}(\tau_{v_\pi}(\underline{g}\,\underline{t}^\alpha), \tau_{v_\pi}(\underline{h}\,\underline{t}^\beta))$ holds in G_{v_π}, for each $\pi \in \Sigma$. We may assume each t_i has the form ± 1 times a product of real irreducibles with no repeated factors. Factor t_i as $t_i' \overline{t_i}$ where t_i' is the product of those $\pi \in \Sigma$ which appear in t_i. Then replace t_i by $u_i = t_i' \tilde{t_i}$ where $\tilde{t_i} = \pm \prod_{I \in T} \pi_I{}^{s_{iI}}$, where $s_{iI} = 0$ or 1 depending on whether $\overline{t_i}$ has the same sign or opposite sign at the opposite ends of the open arc I, and where the sign $\pm$ is chosen so that $\tilde{t_i}$ has the same sign as $\overline{t_i}$ at the ends of each of the arcs $I \in T$.

Consider a typical atom $1 \in D(\underline{g}t^\alpha, \underline{h}t^\beta)$ appearing in the formula ϕ. By Lemma 4 (2), one of gu^α, hu^β is non-negative at p for each real point p on $\mathcal{C}$ sufficiently close to the roots of the $\pi \in \Sigma$. Since the sign of gu^α and hu^β can change on $\mathcal{C} \backslash J$ only at the roots of the $\pi \in \Sigma$ and at the points p_{1I} defined above, it follows that one of gu^α, hu^β is non-negative at p for each $p \in \mathcal{C} \backslash J$. By Lemma 4 (1), this implies that $\psi_S(\tau_S(\underline{u_1}), \ldots, \tau_S(\underline{u_n}), \tau_S(\underline{f_1}), \ldots, \tau_S(\underline{f_k}))$ holds in G_S, i.e., that the formula ϕ_S holds in $G_{F,S}$. $\square$

We come now to the main theorem:

Theorem 6 *Let F be the function field of a rational conic $ax^2 + by^2 = c$, where a, b, c are positive, which has no rational points. Then there exists a pp-formula ϕ with parameters in G such that $G \models \neg\phi$, but $G_S \models \phi_S$ for each* *proper subspace* (X_S, G_S) *of* (X, G).

PROOF. Let $\pi_1, \dots, \pi_6 \in \mathbb{Q}[\mathcal{C}]$ be linear irreducibles having zeros p_{1i}, p_{2i} on the ellipse $\mathcal{C}$, $i \in \{1, \dots, 6\}$, arranged in the following clockwise cyclic order:

$$p_{11}, p_{22}, p_{13}, p_{21}, p_{14}, p_{23}, p_{15}, p_{24}, p_{16}, p_{25}, p_{12}, p_{26}$$

Replacing π_i by $-\pi_i$ if necessary, we can assume $\pi < 0$ on the arc $\overline{\overline{(p_{1i}; p_{2i})}}$. Let $f_1 = \pi_1\pi_6$, $f_2 = \pi_1\pi_4$, $f_3 = -\pi_1\pi_2\pi_3\pi_5$. Consider the pp-formula

$$\phi = \exists t_1 \exists t_2 \left(t_1 \in D(1, \underline{f_1}) \wedge t_2 \in D(1, \underline{f_2}) \wedge \underline{f_3} t_1 t_2 \in D(1, \underline{f_1}\, \underline{f_2}) \right)$$

(see [11] for a general discussion of pp-formulas of this sort).

Suppose that $G \models \phi$. Fix $\underline{t_1}$, $\underline{t_2} \in G$ verifying ϕ. We may assume that $\underline{t_1}$, $\underline{t_2}$ are represented by $t_1, t_2 \in \mathbb{Q}[\mathcal{C}]$ and that t_1, t_2 are square free. The signs of f_1, f_2 and f_3 on the arcs between the successive points p_{ki}, $k \in \{1, 2\}$, $i \in \{1, \dots, 6\}$, are as follows:

	$\overline{\overline{(p_{11};p_{22})}}$	$\overline{\overline{(p_{22};p_{13})}}$	$\overline{\overline{(p_{13};p_{21})}}$	$\overline{\overline{(p_{21};p_{14})}}$	$\overline{\overline{(p_{14};p_{23})}}$	$\overline{\overline{(p_{23};p_{15})}}$	$\overline{\overline{(p_{15};p_{24})}}$	$\overline{\overline{(p_{24};p_{16})}}$	$\overline{\overline{(p_{16};p_{25})}}$	$\overline{\overline{(p_{25};p_{12})}}$	$\overline{\overline{(p_{12};p_{26})}}$	$\overline{\overline{(p_{26};p_{11})}}$
f_1	−	−	−	+	+	+	+	+	−	−	−	+
f_2	−	−	−	+	−	−	−	+	+	+	+	+
f_3	−	+	−	+	+	−	+	+	+	−	+	+

On the arcs $\overline{\overline{(p_{21}; p_{14})}}$, $\overline{\overline{(p_{24}; p_{16})}}$ and $\overline{\overline{(p_{26}; p_{11})}}$ f_1 and f_2 are positive, so t_1 and t_2 are nonnegative. Near p_{23}, f_1 is positive, so t_1 is also positive. Since π_3 is the unique irreducible changing sign at p_{23}, this implies $v_{\pi_3}(t_1)$ is even, so t_1 does not change sign at p_{13}. Near p_{13}, $f_1 f_2$ is positive, so $f_3 t_1 t_2$ is positive and

f_3 changes the sign, so t_2 changes sign. That means that $v_{\pi_3}(t_2)$ is odd and hence t_2 changes sign at p_{23}. To sum up: t_2 changes signs at p_{23} and p_{13}, but t_1 does not.

Near p_{12}, f_2 is positive so t_2 is also positive. Thus $v_{\pi_2}(t_2)$ is even and t_2 does not change sign at p_{22}. Near p_{22}, $f_1 f_2$ is positive so $f_3 t_1 t_2$ is positive and f_3 changes sign, so t_1 must change sign. Thus t_1 changes signs at p_{12} and p_{22}, but t_2 does not. Near p_{11}, $f_1 f_2$ is positive so $f_3 t_1 t_2$ is positive, and f_3 changes sign so $t_1 t_2$ also changes sign. Thus one of t_1 and t_2 changes sign, but not both. Thus at p_{11} and p_{21} either t_1 changes sign (at both points) or t_2 changes sign, but not both.

On the arc $\overline{\overline{(p_{11}; p_{22})}}$ $f_1 f_2$ is positive and f_3 is negative, so $t_1 t_2$ is negative or zero. Hence at any point of this arc if t_1 changes sign, then so does t_2 (and vice versa) - say there are m_1 such simultaneous sign changes. Similarly, there are m_3 simultaneous sign changes of t_1 and t_2 on the arc $\overline{\overline{(p_{13}; p_{21})}}$. On $\overline{\overline{(p_{22}; p_{13})}}$ both $f_1 f_2$ and f_3 are positive, so $t_1 t_2$ is positive or zero. Thus if t_1 changes sign, then so does t_2 - say there are m_2 such sign changes.

On $\overline{\overline{(p_{11}; p_{21})}}$ t_1 and t_2 each change sign $m_1 + m_2 + m_3 + 1$ times. The signs of t_1 and t_2 at p_{11} are the same as at p_{21}, so $m_1 + m_2 + m_3$ is odd. On all the other arcs at least one of f_1 and f_2 is positive, so at least one of t_1 and t_2 is nonnegative. Thus the simultaneous sign changes of t_1 and t_2 occur only at the indicated $m_1 + m_2 + m_3$ points.

Now let $t_1 = u_1 q_1 \ldots q_k r_1 \ldots r_l$ and $t_2 = u_2 q_1 \ldots q_k r'_1 \ldots r'_m$ be factorizations of t_1 and t_2 into irreducibles, $u_1, u_2 \in \mathbb{Q}^*$, $\{r_1, \ldots, r_l\} \cap \{r'_1, \ldots, r'_m\} = \emptyset$. The simultaneous sign changes occur at the zeros of q_i on $\mathcal{C}$. But since for each q_i there is an even number of such points (by Lemma 3) and for $i \neq j$ q_i and q_j

have no common zeros on $\mathcal{C}$, $m_1 + m_2 + m_3$ must be even. This contradicts our assumption and proves $G \models \neg\phi$.

Finally, $G_{v_{\pi_i}} \models \phi_{v_{\pi_i}}$ for $i \in \{1, \ldots, 6\}$ by the substitutions

	π_1	π_2	π_3	π_4	π_5	π_6
t_1	1	f_3	1	1	1	1
t_2	f_3	1	f_3	1	1	1

,

so, by Theorem 5, $G_S \models \phi_S$ for every proper quotient G_S of G. $\square$

4 The case of two parallel lines

In this section we complete our analysis by considering the case of a real irreducible conic of type (3), i.e., we assume $\mathcal{C}$ is defined by $x^2 = d$, where $d \in \mathbb{Q}$, $d > 0$ and d is not a square in $\mathbb{Q}$. This case is similar to the elliptic case, and the main arguments and results from the previous section carry over, with a bit of modification here and there.

The coordinate ring $A = \mathbb{Q}[\mathcal{C}]$ can be identified with $\mathbb{Q}(\sqrt{d})[y]$, the polynomial ring in one variable y with coefficients in the field $\mathbb{Q}(\sqrt{d})$. The valuations that are of interest to us are easy to describe; see [7, Corollary 4.4]. Units are identified with non-zero elements of $\mathbb{Q}(\sqrt{d})$. Unlike what happens in the elliptic case, units no longer necessarily have constant sign on $\mathcal{C}$.

We still have the linear irreducibles $\pi = rx + sy + t$, $r, s, t \in \mathbb{Q}$, $s \neq 0$, but these no longer suffice. To copy certain of the constructions used in the proofs of Theorems 5 and 6, we also use the fact that there are enough quadratic irreducibles in A of the form

$$\pi = x \pm (r(y+s)^2 + t),\ \ r,s,t \in \mathbb{Q},\ \ r > 0,\ \ |t| < \sqrt{d}.$$

Lemma 7 *For given real r, s, t satisfying $r > 0$, $|t| < \sqrt{d}$, there exist rationals r', s' and t' arbitrarily close to r, s and t respectively, such that $x + (r'(y+s')^2 + t')$ and $x - (r'(y+s')^2 + t')$ are irreducible in A.*

PROOF. The discriminant of $\sqrt{d} \pm (r'(y+s')^2 + t') \in \mathbb{Q}(\sqrt{d})[y]$ is $-4r'(t' \pm \sqrt{d})$. We want this to be not a square in $\mathbb{Q}(\sqrt{d})$. Proceed as follows: choose r' to be any rational square close to r, choose s' close to s, choose t' close to t and such that ${t'}^2 - d$ is not a rational square (so then $-t' - \sqrt{d}$ and $-t' + \sqrt{d}$ are not squares in $\mathbb{Q}(\sqrt{d})$). We can, for example, choose t' of the form $t' = p^k t_1$ where p is a prime such that the value of d at p is odd, $2k > v_p(d)$ and $v_p(t_1) \geq 0$. Then $v_p({t'}^2 - d) = v_p(d)$ is odd, so ${t'}^2 - d$ is not a square in $\mathbb{Q}$. $\square$

The correspondence between points on $\mathcal{C}$ and orderings on $F = \mathbb{Q}(\mathcal{C})$ is the same as before, but now there are additional orderings corresponding to the four half-branches of $\mathcal{C}$ at ∞. These are precisely the orderings compatible with the real valuation v_∞ on F defined by $v_\infty(f) = -\deg_y(f)$.

Lemma 3 carries over with the same proof. Using this, we see that an irreducible π has an even (resp., odd) number of roots on the line $x = -\sqrt{d}$, and also on the line $x = \sqrt{d}$, if $\deg_y(\pi)$ is even (resp., if $\deg_y(\pi)$ is odd).

Lemma 4 also carries over without change but, regarding part (2) of Lemma 4, there is also a similar result for the point at infinity: Suppose f, g, h are non-zero elements of A and $\overline{f}, \overline{g}, \overline{h}$ denote the associated elements of G_{v_∞}. Then

$\overline{f} \in D_{v_\infty}(\overline{g}, \overline{h})$ holds iff $fg \geq 0$ at p or $fh \geq 0$ at p holds for all real points $p = (\pm\sqrt{d}, p_2)$ of $\mathcal{C}$ with $|p_2|$ sufficiently large.

With these preliminary remarks out of the way, we are now in a position to state the main results of this section:

Theorem 8 *Let F be the function field of a rational conic $x^2 = d$, where d is a positive and not a square. For a given pp-formula*

$$\phi = \exists t_1 \dots \exists t_n \psi(t_1, \dots, t_n, \underline{f_1}, \dots, \underline{f_k}),$$

$\underline{f_i}$ denoting the image of $f_i \in \mathbb{Q}[\mathcal{C}]^*$ under the homomorphism $f \mapsto \underline{f}$ from F^* to G, let Σ denote the set of all irreducible factors of the f_i, $i \in \{1, \dots, k\}$. The following conditions are equivalent:

(1) $G_{v_\pi} \models \phi_{v_\pi}$, for each $\pi \in \Sigma \cup \{\infty\}$.

(2) $G_S \models \phi_S$, for each proper subspace (X_S, G_S) of (X, G).

(3) $G_S \models \phi_S$, for each finite subspace (X_S, G_S) of (X, G).

The proof of Theorem 8 is the same as the proof of Theorem 5, with minor modifications to allow for the fact that we are now dealing with two parallel lines. In defining the π_I we allow not only linear irreducibles, but also quadratics irreducibles as well (to take care of the case where the intervals I and J are both on the same component of $\mathcal{C}$). In the last step, in the definition of the $\tilde{t_i}$, we define $\tilde{t_i} = \mu_i \prod_{I \in T} {\pi_I}^{s_{iI}}$, where $s_{iI} = 0$ or 1 depending on whether $\overline{t_i}$ has the same sign or opposite sign at the opposite ends of the open interval I, and where $\mu_i \in \{1, -1, x, -x\}$ is chosen so that $\tilde{t_i}$ has the same sign as $\overline{t_i}$ at the ends of each of the intervals $I \in T$.

Theorem 9 *Let F be the function field of a rational conic $x^2 = d$, where d is* *a positive and not a square. Then there exists a pp-formula ϕ with parameters in G such that $G \models \neg\phi$, but $G_S \models \phi_S$ for each proper subspace (X_S, G_S) of (X, G).*

Again, the proof of Theorem 9 is analogous to the proof of Theorem 6, but instead of using just linear irreducibles we also allow suitably chosen quadratic irreducibles. We arrange the zeros p_{1i}, p_{2i}, $i = 1, \ldots, 6$ of these six irreducibles (for example), so that the first six points

$$p_{11}, p_{22}, p_{13}, p_{21}, p_{14}, p_{23}$$

are on the line $x = -\sqrt{d}$, in upward order, and the next six points

$$p_{15}, p_{24}, p_{16}, p_{25}, p_{12}, p_{26}$$

are on the line $x = \sqrt{d}$, in the downward order. The reader may check that this particular arrangement uses two linear irreducibles and four quadratic irreducibles (two opening to the left, and two opening to the right).

References

[1] C. Andradas, L. Bröcker, J.-M. Ruiz, *Constructible sets in real geometry*, Springer, New York 1996.

[2] J. Bochnak, M. Coste, M.-F. Roy, *Real algebraic geometry*, Springer, New York 1998.

[3] K. Borsuk, *Multidimensional analytic geometry*, PWN - Polish Scientific Publishers, Warsaw 1969.

[4] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, AMS, New York 1951.

[5] M. Dickmann, M. Marshall, F. Miraglia, *Lattice-ordered reduced special groups*, Ann. of Pure and Appl. Logic 132 (2005), 27-49.

[6] M. Dickmann, F. Miraglia, *Special groups. Boolean-theoretic methods in the theory of quadratic forms*, Memoirs of the AMS 689, AMS, Providence 2000.

[7] O. Endler, *Valuation theory*, Springer, New York 1972.

[8] T. Y. Lam, *Orderings, valuations and quadratic forms*, AMS, Providence 1983.

[9] M. Marshall, *Spaces of orderings and abstract real spectra*, Springer, New York 1996.

[10] M. Marshall, *Open questions in the theory of spaces of orderings*, J. Symbolic Logic 67 (2002), 341-352.

[11] M. Marshall, *Local-global properties of positive primitive formulas in the theory of spaces of orderings*, to appear.

[12] A. Prestel, C. Delzell, *Positive polynomials*, Springer, New York 2001.

[13] P. Samuel, *On unique factorization domains*, Ill. J. Math. 5 (1961), 1-17.

[14] I. R. Shafarevich, *Basic algebraic geometry*, Springer, New York 1974.

[15] H. Stichtenoth, *Algebraic function fields and codes*, Springer, New York 1993.

[16] O. Zariski, P. Samuel, *Commutative algebra*, vol. I, D. van Nostrand Co. Inc., New York 1958.