Nullstellensatz and Positivstellensatz from cut-elimination

Christophe Raffalli

LAMA, UMR 5127

Abstract

We give in this article an effective proof of Hilbert's nullstellensatz and Krivine-Stengle's positivstellensatz using the cut elimination theorem for sequent calculus. The proof is very similar to the current techniques in constructive algebraic geometry by Henri Lombardi, but seems more modular.

In the case of the positivstellensatz, we think we prove a more general result than the original one, thanks to a new notion of justification of positiveness: PBDD (polynomial binary decision digram). It allows both to recover Krivine-Stengle's justification, but also another one which seems to require lower degree.

We apply the same techniques to the nullstellensatz for differentially closed field and show that the proof is almost unchanged.

Remark: here we do not provide bound, but an effective algorithm, implemented in OCaml, to build the wanted algebraic equality. Nevertheless, we discuss how bounds could probably be obtained.

We also do not deal effectively with the axiom of real closure, but we do deal with the axiom of algebraic closure and inverse in the case of the nullstellensatz. However, in both case, those axioms may be eliminated using standard model theory.

1 Introduction

This work was initiated by a presentation in Chambéry by Marie-Françoise Roy of here work with Michel Coste and Henri Lombardi [2, 3, 4]. The paper revisit their notion of *strong evidence* through the cut elimination theorem of sequent calculus. This idea is not new, it was explored by Friedman in an unpublished manuscript and Whiteley in [1]. However, this paper did not deal with the inverse and albebraic/real closure axioms.

We give three effective proofs for Hilbert's nullstenlensatz, Krivine-Stengle's positivstellensatz [6, 7, 8] and the nullstenlensatz for differential fields [5], all proofs following exactly the same schema:

1. The theory of ring at play can be completed (we do not reprove these results).
2. A Π_1 statement of the ring theory true in the complete theory is provable in the original ring theory. Remark: this is always effective, at worst by enumerating all derivations, but in general there exists decision procedure that will give a proof, but not always in the smallest possible ring.

   We are not aware of an effective proof of the above fact, in the case of ordered rings, that gives a derivation in the smallest possible ring i.e. the ring generated by the coefficient appearing in the statement.
3. This proof can be found in a sequent calculus where the relevant notion of ideal or cone is integrated solely in the axiom rule.
4. Hence, the result is a consequence of the Gentzen's cut-elimination theorem for classical sequent calculus [9].

The only part of the proof that needs to be adapted to each case is the third one to show the completeness of the sequent-calculus. This is relatively easy and natural.

For the positivstellensatz, we use a notion of *polynomial binary decision diagram* (PBDD) to delay the construction of polynomial of high degree in the hope that this may lower the final degree in some cases. This is yet to be proved, but we provide evidence that it is likely. A proof would be a challenge because it required lower bound. In fact, we argue that the result with PBDD is stronger than the original positivstellensatz which can be recovered from it (lemma 13), but in the case where we prove the positiveness of only one polynomial, we show another to obtain a rational fraction which produces in general lower degree (lemma 9).

In the case of the nullstellensatz, in section 7, we show how we can deal directly with the axioms of algebraically closed field and eliminate them in a cut-free proof of a Π_1-formula. This means that we provide an effective way to transform a proof of a Π_1-formula in the theory of an algebraically closed field into a nullstellensatz equality using only coefficients in the ring generated by the coefficients of the original polynomial. Unfortunately, we do not know yet how to extend this techniques to the positivstellensatz.

We think that out proofs via the cut-elimination of the sequent calculus could be used to obtain upper bound. Here we are in first order logic and we know that the cut elimination procedure is of elementary complexity and more knowledge of the proof given by a decision procedure could certainly allow to give a more precise bound (in general the height of the exponential tower is linked to the rank of the formulae in the proof) [10, 11]. Yet, these standard results need to be adapted to our modified sequent calculus where we are interested in the degree of the polynomial used in the axiom rule justification and not the size of the normal proof or the complexity of the cut elimination process. We think it is

possible to construct a notion of degree for proofs that only decreases during cut-elimination and would correspond to the real degree for axioms.

We designed a prototype implementation in OCaml of the cut elimination procedure which takes as input a first-order proof in our sequent calculus. This implementation is a functor taking as input a structure describing the axiom rule.

We tried to write the proofs in this paper with enough details for people that know proof theory or algebra but not both.

2 From truth to provability

Definition 1. Let $(\mathbb{A}, +, \times, 0, 1)$ be an integral domain, *the theory of* $\mathbb{A}$, denoted $\mathcal{T}(\mathbb{A})$, is a first order theory whose language contains $=, +, \times$, a constant for each element of $\mathbb{A}$, and as set of axioms, all the usual axioms of integral ring and all closed equalities and inequalities true in $\mathbb{A}$.

We define similarly $\mathcal{T}(\mathbb{A})$ when $(\mathbb{A}, \leqslant, +, \times, 0, 1)$ is an ordered ring.

Here, the important point is that the models of $\mathcal{T}(\mathbb{A})$ are all integral rings containing $\mathbb{A}$. The closed inequalities forbid models that are quotients of $\mathbb{A}$.

Lemma 1. Let $(\mathbb{A}, +, \times, 0, 1)$ be an integral domain and $\mathbb{K}$ its algebraic closure. If F is a Π_1 formula in $(\mathbb{A}, +, \times, 0, 1)$ (i.e. first-order universal quantifications over a quantifier free formulas), and if F is true in $\mathbb{K}$ ($\mathbb{K} \vDash F$) then it is provable in $\mathcal{T}(\mathbb{A})$ ($\mathcal{T}(\mathbb{A}) \vdash F$).

Remark: the algebraic closure of an integral domain is a field because the existence of the inverse is just the existence of a root for a degree one polynomial.

Proof. If F is true in $\mathbb{K}$, then it is true in any algebraic closure of $\mathbb{A}$ (because the algebraically closed field theory of a given characteristic is complete) and therefore in all rings containing $\mathbb{A}$ because it is a Π_1 formula. This means that $\mathcal{M} \vDash F$ for all models of $\mathcal{T}(\mathbb{A})$ hence $\mathcal{T}(\mathbb{A}) \vdash F$ by the completeness theorem. □

Lemma 2. Let $(\mathbb{A}, \leqslant, +, \times, 0, 1)$ be an ordered ring and $\mathbb{K}$ its real closure. If F is a Π_1 formula F in $(\mathbb{A}, \leqslant, +, \times, 0, 1)$ and $\mathbb{K} \vDash F$ then $\mathcal{T}(A) \vdash F$.

Proof. Same proof as the previous lemma because the real closed field theory is also complete. □

3 Cut elimination in polynomial sequent calculus

We use a specific sequent calculus for first-order predicate calculus parametrised by the axiom rules. We denote $\mathbb{A}[\mathcal{V}]$ the multivariate polynomials with coefficients in $\mathbb{A}$ and indeterminate in a countable set $\mathcal{V}$.

For $P, Q \in \mathbb{A}[\mathcal{V}]$ and $X \in \mathcal{V}$, we write $P[X \leftarrow Q]$ for the substitution of the variable X by Q in P. We will use the notation $\vec{P}$ for a sequence of polynomials and $\vec{n}$ for a sequence of natural numbers. For such a sequence we write $\left|\vec{P}\right|$ for its length and P_n for its nth element (if $1 \leqslant n \leqslant \left|\vec{P}\right|$).

When $\vec{P}, \vec{S}$ are two sequences of polynomials and $\vec{e}$ is a sequence of natural numbers with $\left|\vec{P}\right| = \left|\vec{S}\right| = |\vec{e}|$, we use the following notations:

$$\vec{P}\vec{S} \text{ denotes } \Sigma_{i=1}^{n} P_i S_i \text{ and } \vec{P}^{\vec{e}} \text{ means } \Pi_{i=1}^{n} P_i^{e_i}.$$

Definition 2. (subsumption) We say that a finite sequence of polynomials subsume another sequence, denoted $\vec{P} \sqsubset \vec{Q}$ if and only if for all $1 \leqslant i \leqslant \left|\vec{P}\right|$ there exists $1 \leqslant j \leqslant \left|\vec{Q}\right|$ with $P_i = Q_j$.

We use also the notation $\vec{P} \sqsubset \Delta$ when Δ is a set and for all $1 \leqslant i \leqslant \left|\vec{P}\right|$, $P_i \in \Delta$.

Definition 3. A polynomial sequent calculus is given by $(\mathcal{J}, \mathcal{R})$ where $\mathcal{J}$ is a set of *justifications* and $\mathcal{R}$, a set of *axioms*. $\mathcal{J}$ may be any set while an element of $\mathcal{R}$ is a triple $\left(\vec{P}, \vec{Q}, J\right)$ where $\vec{P}$ and $\vec{Q}$ are finite sequences of polynomials and $J \in \mathcal{J}$. The purpose of justifications is to store an explicit reason for an axiom rule to be valid (see below).

We require four properties for $\mathcal{R}$:

1. At least the standard axiom are available: for all $P \in \mathbb{A}[\mathcal{V}]$, there exists $J \in \mathcal{J}$ such that $((P), (P), J) \in \mathcal{R}$.
2. It is compatible with subsumption: if $\left(\vec{P}, \vec{Q}, J\right) \in \mathcal{R}$, if $\vec{P} \sqsubset \vec{P'}$ and $\vec{Q} \sqsubset \vec{Q'}$, then there exists J' such that $\left(\vec{P'}, \vec{Q'}, J'\right) \in \mathcal{R}$.
3. It is compatible with substitution: For all $((P_1, \ldots, P_n), (Q_1, \ldots, Q_m), J) \in \mathcal{R}$, for all $X \in \mathcal{V}$ and $T \in \mathbb{A}[\mathcal{V}]$, there exits $J' \in \mathcal{J}$ such that $((P_1[X \leftarrow T], \ldots, P_n[X \leftarrow T]), (Q_1[X \leftarrow T], \ldots, Q_m[X \leftarrow T]), J') \in \mathcal{R}$. In general, there will be a canonical J' that we will denote $J[X \leftarrow T]$.
4. It *eliminates cut*: for all $((P_1, \ldots, P_n), (Q_1, \ldots, S, \ldots, Q_m), J) \in \mathcal{R}$ and $((P_1, \ldots, S, \ldots, P_n), (Q_1, \ldots, Q_m), J') \in \mathcal{R}$, there exits J'' such that $((P_1, \ldots, P_n), (Q_1, \ldots, Q_m), J'') \in \mathcal{R}$.

Example 1. For the nullstellensatz, a justification will essentially correspond to the radical of an ideal. It will be a pair $\left(\vec{S}, \vec{e}\right)$ where $\vec{S}$ is a finite sequence of polynomials in $\mathbb{A}[\mathcal{V}]$ and $\vec{e}$ is a finite sequence of natural numbers. Then, we take

$$\mathcal{R} = \left\{\left(\vec{P}, \vec{Q}, \left(\vec{S}, \vec{e}\right)\right) \mid \left|\vec{P}\right| = \left|\vec{S}\right|, \left|\vec{Q}\right| = |\vec{e}|, \vec{P}\vec{S} = \vec{Q}^{\vec{e}}\right\}.$$

Definition 4. The set of first order formulae $\mathcal{F}$ is defined inductively by the following grammar:
- $\mathbb{A}[\mathcal{V}] \subset \mathcal{F}$,
- $A \in \mathcal{F}$ implies $\neg A \in \mathcal{F}$,
- $A, B \in \mathcal{F}$ implies $A \vee B \in \mathcal{F}$,
- $X \in \mathcal{V}$, $A \in \mathcal{F}$ implies $\forall X\ A \in \mathcal{F}$.

As usual, we consider that the variable X is bound in $\forall X\ A$ and that the set of formulae is quotiented by α-equivalence (i.e. renaming of bound variables).

Remark: we directly use polynomial as atomic formulas. The truth of a polynomial will be either that $P = 0$ (for the nullstellensatz) or $P \geqslant 0$ for the positivstellensatz.

Definition 5. A *sequent* is an ordered pair of *contexts* i.e. finite sets of formulae. We write $\Gamma \vdash \Delta$ for such a pair. We also omit braces in context and write $A_1, \ldots, A_m \vdash B_1, \ldots, B_n$. We recall that a sequent is true when the conjunction of the left formulae implies the disjunction of the right ones. Hence, commas on the left must be understood as conjunctions and commas on the right as disjunctions.

Definition 6. Substitution is naturally extended to formulae and contexts. As usual we must rename some bound variables to avoid capture: $(\forall X\ (X \wedge Y))[Y \leftarrow X^2] = \forall Z\ (Z \vee X^2)$.

Definition 7. A sequent is said to be provable if it can be obtained using the following deduction rules:

$$\frac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{\Gamma \vdash \Delta}\mathcal{R} \qquad \frac{\Gamma \vdash \Delta, A \qquad A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}\text{Cut}$$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\neg_l \qquad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\neg_r$$

$$\frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\vee_l \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\vee_r$$

$$\frac{\Gamma \vdash A[X \leftarrow P], \forall X\ A, \Delta}{\Gamma, \forall X\ A \vdash \Delta}\forall_l^* \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall X\ A, \Delta}\forall_r$$

Deduction rules mean that if the premises (above the horizontal bar) are provable the so is the conclusion).

In the $\mathcal{R}$-rule, the premise is not a sequent, it is just a mathematical statement that should be true for some $\overrightarrow{P}, \overrightarrow{Q}, J$ for the axiom to be provable. We use $\overrightarrow{P} \sqsubset \Gamma$ to allow weakening on non atomic formulae at the level of axioms without decomposing them. This is important for the admissible weakening to preserve proof size (see lemma below).

(*) In the $\forall_l$ rule, we must have the usual restriction that X is not free in Γ nor Δ (i.e. not free in the rule's conclusion).

We give some common vocabulary in this setting:

- The *principal formula* of a rule is the new formula that is introduced in the conclusion. The cut rule and the $\mathcal{R}$-rule have no principal formula. This formula is not always new because contexts are sets.
- The *cut formula* of a cut rule is the formula that is eliminated from the premises.
- We will call *logical rules* all rules but the cut rule and the $\mathcal{R}$-rule (i.e. all rule that have a principal formula).
- In the $\forall_r$ rule, we must keep the original formula for the calculus to be complete. We define the *multiplicity* of a quantified formula in the hypotheses as the number of $\forall_e$ rule applied to this formula in the proof. This notion of multiplicity is needed as an argument for the termination of cut elimination and is used only for the multiplicity of a cut formula.

Lemma 3. The following rules are *derivable* (i.e. obtained using the given rules) or *admissible* (i.e. if the premise is provable, so is the conclusion). Moreover, the admissible ones (all but the axiom rule) do preserve the size of the original proof.

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} W_l \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta} W_r$$

$$\frac{}{\Gamma, A \vdash A, \Delta} \text{Ax} \qquad \frac{\Gamma \vdash \Delta}{\Gamma[X \leftarrow P] \vdash \Delta[X \leftarrow P]} \text{Subst}$$

Proof. The usual axiom rule is derivable. The derivation is build by induction on the formula A. When it is atomic (base case of the induction), the axiom rule is a particular case of the $\mathcal{R}$-rule by hypothesis.

The three other rules are admissible and the proof is by induction on the original derivation, just copying it (hence not changing the proof size). Again, the constraints on the $\mathcal{R}$-rule allows us to establish the base case. □

Theorem 4. (Cut elimination) If a sequent is provable, it is provable without using the cut rule.

Proof. First, we consider a cut-rule of maximal height (i.e. a cut-rule with no cut-rule above). Then, it is clear that at least one of the proof transformations given below applies and that this transformations either

- remove the cut-rule or introduce cut on a smaller formula (counting only connective, but not the polynomial size), or
- keep the same cut formula but decreases the *multiplicity of a quantified hypothesis*.
- keep the same cut formula and multiplicity but decreases the size of the derivation of the premises of the cut.

Hence, repeating these operations on maximal cuts will remove them all.

First we give some of the commutation rules. They are the transformation that moves the cut upward in the proof when the principal formula of the rule just above the cut is not the cut formula. For each connective, there are exactly four of this rules (depending if we use the left or right rule on the connective and depending upon the premise of the cut rule we consider).

$$\dfrac{\dfrac{\Gamma, B \vdash \Delta, A}{\Gamma \vdash \neg B, \Delta, A}\neg_r \qquad A, \Gamma \vdash \Delta}{\Gamma \vdash \neg B, \Delta}\text{Cut} \implies \dfrac{\Gamma, B \vdash \Delta, A \qquad \dfrac{A, \Gamma \vdash \Delta}{A, \Gamma, B \vdash \Delta}\text{Weak}_l}{\dfrac{\Gamma, B \vdash \Delta}{\Gamma \vdash \neg B, \Delta}\neg_r}\text{Cut}$$

$$\dfrac{\dfrac{\Gamma, B[X \leftarrow P], \forall X\ B \vdash \Delta, A}{\Gamma, \forall X\ B \vdash \Delta, A}\forall_l \qquad A, \Gamma \vdash \Delta}{\Gamma, \forall X\ B \vdash \Delta}\text{Cut} \implies$$

$$\dfrac{\Gamma, B[X \leftarrow P] \qquad \forall X\ B \vdash \Delta, A \qquad \dfrac{A, \Gamma \vdash \Delta}{A, \Gamma, B[X \leftarrow P], \forall X\ B \vdash \Delta}\text{Weak}_l}{\dfrac{\Gamma, B[X \leftarrow P], \forall X\ B \vdash \Delta}{\Gamma, \forall X\ B \vdash \Delta}\forall_l}\text{Cut}$$

$$\dfrac{\dfrac{\Gamma, B \vdash \Delta, A \qquad \Gamma, C \vdash \Delta, A}{\Gamma, B \vee C \vdash \Delta, A}\vee_l \qquad A, \Gamma \vdash \Delta}{\Gamma, B \vee C \vdash \Delta}\text{Cut} \implies$$

$$\dfrac{\dfrac{\Gamma, B \vdash \Delta, A \qquad \dfrac{A, \Gamma \vdash \Delta}{A, \Gamma, B \vdash \Delta}\text{Weak}_l}{\Gamma, B \vdash \Delta}\text{Cut} \qquad \dfrac{\Gamma, C \vdash \Delta, A \qquad \dfrac{A, \Gamma \vdash \Delta}{A, \Gamma, C \vdash \Delta}\text{Weak}_l}{\Gamma, C \vdash \Delta}\text{Cut}}{\Gamma, B \vee C \vdash \Delta}\vee_l$$

It is important to remark that the height of one of the proofs above the cut rule decreases while the other does not change. Hence, moving a cut upward terminates. Then, when a cut can not be moved upward, it means that on both side we find an $\mathcal{R}$-rule or one of the other rules applied to the cut formula.

The first case to deal with is when on at least one side, there is an $\mathcal{R}$-rule not using the cut formula. In this case, the cut disappear, here is the transformation when the $\mathcal{R}$-rule is on the right, the other case being similar:

$$\dfrac{\dfrac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta}\quad \dfrac{\dfrac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{A, \Gamma \vdash \Delta}\mathcal{R}}{}\text{Cut}}{} \Rightarrow \dfrac{\dfrac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset \Delta, \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{\Gamma \vdash \Delta}\mathcal{R}}{}$$

Then, there is the case of two $\mathcal{R}$ rules using the cut-formula which is therefore atomic:

$$\dfrac{\dfrac{\overrightarrow{P} \sqsubset \Gamma, \overrightarrow{Q} \sqsubset (\Delta, A), \left(\overrightarrow{P}, \overrightarrow{Q}, J\right) \in \mathcal{R}}{\Gamma \vdash \Delta, S}\mathcal{R}\quad \dfrac{\overrightarrow{P'} \sqsubset (S, \Gamma), \overrightarrow{Q'} \sqsubset \Delta, \left(\overrightarrow{P'}, \overrightarrow{Q'}, J'\right) \in \mathcal{R}}{S, \Gamma \vdash \Delta}\mathcal{R}}{\Gamma \vdash \Delta}\text{Cut}$$

This case reduces to an axiom because property 2 in definition 2 allows us to take $\overrightarrow{P} = \overrightarrow{P'}$ and $\overrightarrow{Q} = \overrightarrow{Q'}$ and the last property of the same definition allows to replace the two rules using S by one without S.

Finally, here are the standard transformation moving the cut upward for logical rules. In this cases, given below, the size of the proof may increase, but the size of the cut formula decreases.

$$\dfrac{\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta, \neg A}\neg_r\quad \dfrac{\Gamma \vdash A, \Delta}{\neg A, \Gamma \vdash \Delta}\neg_l}{\Gamma \vdash \Delta}\text{Cut} \Rightarrow \dfrac{\Gamma \vdash A, \Delta \quad \Gamma, A \vdash \Delta}{\Gamma \vdash \Delta}\text{Cut}$$

In the following case of disjunction, we remark that the cut is replaced by two cuts one above the other (which means that one of them may duplicate the other later). It is also important to remark that we could permute the two cuts which means that cut elimination is intrinsically non deterministic.

$$\dfrac{\dfrac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \vee B}\vee_r\quad \dfrac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta}\vee_l}{\Gamma \vdash \Delta}\text{Cut} \Rightarrow \dfrac{\dfrac{\Gamma \vdash \Delta, A, B \quad B, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\text{Cut}\qquad A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}\text{Cut}$$

In the last case for the $\forall$ connective, we use the fact that X does not occur free in Γ and Δ to ensure $\Gamma[X \leftarrow P] = \Gamma$ and $\Delta[X \leftarrow P] = \Delta$ otherwise the Subst rule would be incor-

rect. We also remark that we introduce two cuts, one with a smaller cut formula and the other with a lower multiplicity for the same cut formula:

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, \forall X\, A}\forall_r \qquad \dfrac{A[X \leftarrow P], \forall X\, A, \Gamma \vdash \Delta}{\forall X\, A, \Gamma \vdash \Delta}\forall_l}{\Gamma \vdash \Delta}\text{Cut} \qquad \Rightarrow$$

$$\dfrac{\dfrac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A[X \leftarrow P]}\text{Subst} \qquad \dfrac{\dfrac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, \forall X\, A}\forall_r \qquad A[X \leftarrow P], \forall X\, A, \Gamma \vdash \Delta}{A[X \leftarrow P], \Gamma \vdash \Delta}\text{Cut}}{\Gamma \vdash \Delta}\text{Cut}$$

□

4 The nullstellensatz from cut-elimination

Definition 8. A null-justification will be a pair $\left(\vec{S}, \vec{e}\right)$ where $\vec{S}$ is a finite sequence of polynomials in $\mathbb{A}[\mathcal{V}]$ and $\vec{e}$ is a finite sequence of natural numbers. Then, we take

$$\mathcal{R} = \left\{\left(\vec{P}, \vec{Q}, \left(\vec{S}, \vec{e}\right)\right) \mid \left|\vec{P}\right| = \left|\vec{S}\right|, \left|\vec{Q}\right| = \left|\vec{e}\right|, \vec{P}\vec{S} = \vec{Q}^{\vec{e}}\right\}.$$

We recognise in the above definition, the definition of the radical ideal generated by $\vec{P}$ when the length of $\vec{Q}$ is one.

Lemma 5. The above definition satisfies to the condition of definition 2.

Proof. The three first conditions are immediate. We give details for the last one: by hypothesis, we have $\left(\vec{P}, \left(\vec{Q}, A\right), \left(\vec{S}_1, (\vec{e}_1, f)\right)\right) \in \mathcal{R}$ and $\left(\left(\vec{P}, A\right), \vec{Q}, \left(\left(\vec{S}_2, T\right), \vec{e}_2\right)\right) \in \mathcal{R}$. This means that

$$\vec{P}\,\vec{S}_1 = \vec{Q}^{\vec{e}_1} A^f \text{ and } P\vec{S}_2 + TA = \vec{Q}^{\vec{e}_2}$$

Hence, we have

$$\vec{P}\left(T^f\,\vec{S}_1\right) = \vec{Q}^{\vec{e}_1}\left(\vec{Q}^{\vec{e}_2} - P\vec{S}_2\right)^f$$

and developing the right side and moving terms with P_i on the left will give something of the desired shape:

$$\vec{P}\left(T^f\,\vec{S}_1 + \vec{S}_3\right) = \vec{Q}^{\vec{e}_1 + f\,\vec{e}_2}$$

Remark: there are a lot of ways to choose $\vec{S}_3$ when $f \geqslant 2$ and $\left|\vec{S}_2\right| \geqslant 2$. □

Lemma 6. The polynomial sequent calculus obtained from the null-justification, that we will call *null sequent calculus*, is complete for the theory of any integral domain $\mathbb{A}$ when we encode the atomic formula $P = Q$ by $P - Q$.

Proof. The ring equations are supported because polynomial in $\mathbb{A}[\mathcal{V}]$ are equal under these equations.

It remains only to prove the following:

- Equality is reflexive: $\vdash 0$ is immediate by the $\mathcal{R}$-rule (using an empty sum).
- For the integrity axiom, we just need to remark that the $\mathcal{R}$-rule allows us to derive $PQ \vdash P, Q$ which allow to prove $PQ \to (P \vee Q)$.
- Equality is substitutive (which implies all the other equality axioms) and is expressed by the following rule:
$$\frac{\Gamma \vdash P - Q \quad \Gamma \vdash A[X \leftarrow P], \Delta}{\Gamma \vdash A[X \leftarrow Q], \Delta} =_r$$

  First, we derive this rule when $A = SX + R$ while X is not free in S nor R: we can derive, using the $\mathcal{R}$-rule, $P - Q, SP + R \vdash SQ + R$ and the following equality rule $=_r^l$ is obtained using two cut rules:
$$\frac{\Gamma \vdash P - Q \quad \Gamma \vdash SP + R, \Delta}{\Gamma \vdash SQ + R, \Delta} =_r^l$$

  Second, when A is atomic, it can be written as a polynomial in X: $A = S_0 + S_1 X + \ldots + S_n X^n$ and we have:
$$A[X \leftarrow P] = S_0 + X_1(S_1 + X_2(Q_2 + \ldots X_n S_n))[X_1 \leftarrow S]\ldots[X_n \leftarrow S]$$

  Thus, by multiple application of the previous rule, we derive the $=_r^a$ rule for atomic formula:
$$\frac{\Gamma \vdash P - Q \quad \Gamma \vdash T[X \leftarrow P], \Delta}{\Gamma \vdash T[X \leftarrow Q], \Delta} =_r^a$$

  Third, we obtain a left rule for equality on atomic formula, using a cut:
$$\frac{\Gamma \vdash P - Q \quad \Gamma, T[X \leftarrow P] \vdash \Delta}{\Gamma, T[X \leftarrow Q] \vdash \Delta} =_l^a$$

Here is the derivation:

$$\dfrac{\dfrac{\Gamma \vdash P - Q \qquad \dfrac{}{\Gamma, T[X \leftarrow Q] \vdash \Delta, T[X \leftarrow Q]}\text{Ax}}{\Gamma, T[X \leftarrow Q] \vdash \Delta, T[X \leftarrow P]}=_l^a \qquad \dfrac{\Gamma, T[X \leftarrow P] \vdash \Delta}{\Gamma, T[X \leftarrow Q], T[X \leftarrow P] \vdash \Delta}\text{Weak}_l}{\Gamma, T[X \leftarrow Q] \vdash \Delta}\text{Cut}$$

Finally, using the left and right rule for atomic formulae, an induction on the formula A allows us to derive the left and right rule for non atomic formula. □

Theorem 7. Nullstellensatz Let $(\mathbb{A}, +, \times, 0, 1)$ be an integral domain and $\mathbb{K}$ its algebraic closure. Consider a Π_1 statement of the form $\forall X_1, \ldots, X_d(P_1 = 0 \wedge \ldots \wedge P_m = 0 \rightarrow Q_1 = 0 \vee \ldots \vee Q_n = 0)$ true in $\mathbb{K}$, then there exists polynomial $S_1, \ldots, S_m$ in $\mathbb{A}[\mathcal{V}]$ and n natural numbers $e_1, \ldots, e_n$ such that

$$P_1 S_1 + \ldots + P_m S_m = Q_1^{e_1} \ldots Q_n^{e_n}.$$

Proof. By lemma 1, we know that $\mathcal{T}(\mathbb{A}) \vdash \forall X_1, \ldots, X_n(P_1 = 0 \wedge \ldots \wedge P_m = 0 \rightarrow Q_1 = 0 \vee \ldots \vee Q_n = 0)$ where $\mathcal{T}(\mathbb{A})$ is the theory of the integral domain $\mathbb{A}$. By the previous lemma we know that the null sequent calculus is complete hence it can prove $\vdash \forall X_1, \ldots, X_d(\neg P_1 \vee \ldots \vee \neg P_m \vee Q_1 \vee \ldots \vee Q_n)$. From the cut elimination theorem, a cut free proof of such a sequent will necessarily ends by an $\mathcal{R}$-rule proving: $P_1, \ldots, P_m \vdash Q_1, \ldots, Q_n$. This is easily proved by examining the possible rules. In fact, it may keep some non atomic formula if they are not used by the final $\mathcal{R}$-rule. Then, the definition of the $\mathcal{R}$-rule gives immediately the wanted result. □

5 The positivstellensatz from cut-elimination

For the positivstellensatz, an atomic formula P will mean $P \geqslant 0$. Then, we define $(P \leqslant 0) := -P$, $(P < 0) := \neg P$ and $(P > 0) := \neg(-P)$.

Equality may be encoded in two ways by $(P = 0) := \neg(\neg P \vee \neg(-P))$ or $(P = 0) := -P^2$. To simplify proofs, it is better to use the first coding in negative position (at the left of the sequent) and the second one in positive position. The fact that it is not needed to consider atomic equality because all polynomials are the difference of two squares was remarked by at least Krivine in 1964 [6, 8].

Definition 9. Let us fix a ring $\mathbb{A}$ and consider only polynomials in $\mathbb{A}[\mathcal{V}]$. The *cone* $\mathcal{C}(P_1, \ldots, P_m)$ generated by the polynomials $P_1, \ldots, P_m$ is the set of polynomial that can be written as a sums of products of the P_i (each used at most once) multiplied by a sum of squares. $\mathcal{C}(P_1, \ldots, P_m)$ may also be defined as the smallest set containing all squares, $P_1, \ldots, P_m$ and closed by sums and products.

For instance $\mathcal{C}(P_1, P_2) = \{S_1 + S_2P_1 + S_3P_2 + S_4P_1P_2 \mid S_i = \Sigma_j T_{i,j}^2, T_{i,j} \in \mathbb{A}[\mathcal{V}]\}$

Definition 10. The *monoid* $\mathcal{M}(P_1, \ldots, P_m)$ is a subset of $\mathcal{C}(P_1, \ldots, P_m)$ whose elements are product of the P_i (possibly 1, for the empty product).

Definition 11. The set $\mathcal{B}_n(P_1, \ldots, P_m ; S_1, \ldots, S_l)$ of *polynomial binary decision diagram* (PBDD) is the smallest set such that:

- $L(M, k, C) := (0, M, k, C) \in \mathcal{B}_n(P_1, \ldots, P_m ; S_1, \ldots, S_l)$ if $1 \leqslant k \leqslant n$, $M \in \mathcal{M}(S_1, \ldots, S_l)$ and $C \in \mathcal{C}(P_1, \ldots, P_m, S_1, \ldots, S_l)$.
- $If(R, T_1, T_2) := (1, S, T_1, T_2) \in \mathcal{B}_n(P_1, \ldots, P_m ; S_1, \ldots, S_l)$ if $R \in \mathbb{A}[\mathcal{V}]$, $T_1 \in \mathcal{B}_n(P_1, \ldots, P_m, R ; S_1, \ldots, S_l)$ and $T_2 \in \mathcal{B}_n(P_1, \ldots, P_m ; S_1, \ldots, S_l, -R)$. Intuitively, in T_1, we justify the case when $R \geqslant 0$ and in T_2, the case $R < 0$.

Definition 12. A positive-justification will be an element of $\mathcal{B}_n(P_1, \ldots, P_m ;)$ and $\mathcal{R}$ will be the set of triple $\left(\overrightarrow{P}, \overrightarrow{Q}, T\right)$ with $m = \left|\overrightarrow{P}\right|$, $n = \left|\overrightarrow{Q}\right|$ and where $T \in \mathcal{B}_n(P_1, \ldots, P_m ;)$ such that for all leafs $L(M, k, C)$ in the tree T, we have $M\,Q_k = C$.

Example 2. A positive-justification for the sequent $\vdash (X^3 - Y^3)(X - Y)$ may be:

$$\begin{aligned} If(X,\ & If(Y,\ L(1,1,(X-Y)^2(X^2+2XY+Y^2)),\\ & \qquad L(1,1,(X^4+Y^4-X^3Y-XY^3))),\\ & If(Y,\ L(1,1,(X^4+Y^4-X^3Y-XY^3)),\\ & \qquad L(1,1,(X-Y)^2(X^2+2XY+Y^2)))) \end{aligned}$$

Indeed, when X and Y have the same sign, $(X-Y)^2(X^2+2XY+Y^2) \in \mathcal{C}(X, Y)$ (resp. $\mathcal{C}(-X, -Y)$). When they have opposite sign, $X^4+Y^4-X^3Y-XY^3 \in \mathcal{C}(X, -Y)$ (resp. $\mathcal{C}(-X, Y)$). In fact, the polynomial $(X^3-Y^3)(X-Y)$ is a sum of squares and, therefore, has a shorter justification.

Remark: in the above definition, we do not allow the use of the right member of the sequent in the monoid. To do so if suffices to add a node: to justify $P^3 \vdash P$, we can not use $L(P^2, 1, P^3)$ but we can use $If(P, L(1, 1, P), L((-P)^2, 1, P^3))$. We force to test the sign of P in the PBDD and this test will be preserved (unless optimisation erases it) by cut elimination even if P is a cut formula. This is the main reason while PBDD seems to require lower degree that Krivine-Stengle's justification.

Lemma 8. If $\left(\overrightarrow{P}, \overrightarrow{Q}, T\right)$ in $\mathcal{R}$, then the sequent $\overrightarrow{P} \vdash \overrightarrow{Q}$ is true in all extension of $\mathbb{A}$.

Proof. We prove that if $T \in \mathcal{B}_n(P_1, \ldots, P_m ; S_1, \ldots, S_l)$ and if $\overrightarrow{Q}$ is a sequence of polynomials of length n such that for all leafs $L(M, k, C)$ in the tree T, we have $M\,Q_k = C$, then, the sequent $\overrightarrow{P} \vdash \overrightarrow{Q}, -\overrightarrow{S}$ is true in $\mathbb{A}$ and in its extensions. The case $l = 0$ correspond to the lemma and we proceed by induction on T.

For the base case, we have $M\,Q_i = C$ for some i where $M \in \mathcal{M}\left(\overrightarrow{S}\right)$ and $C \in \mathcal{C}\left(\overrightarrow{P}, \overrightarrow{S}\right)$. If some of the S_i are negative or null, then the sequent $\overrightarrow{P} \vdash \overrightarrow{Q}, -\overrightarrow{S}$ is true. Otherwise, they are all positive and M is positive too. Finally, assuming $\overrightarrow{P}$ non negative we also get C non negative, hence Q_i non negative from $M\,Q_i = C$. This proves that $\overrightarrow{P} \vdash \overrightarrow{Q}, -\overrightarrow{S}$ is true.

If T is a node $If(R, T_1, T_2)$, by induction hypothesis, using the definition of $\mathcal{B}_n$, we have $\overrightarrow{P}, R \vdash \overrightarrow{Q}, -\overrightarrow{S}$ true from $T_1 \in \mathcal{B}_n(P_1, \ldots, P_m, R ; S_1, \ldots, S_l)$ and $\overrightarrow{P} \vdash \overrightarrow{Q}, -\overrightarrow{S}, R$ true from $T_2 \in \mathcal{B}_n(P_1, \ldots, P_m ; S_1, \ldots, S_l, -R)$. Using the cut rule, we deduce that $\overrightarrow{P} \vdash \overrightarrow{Q}, -\overrightarrow{S}$ is true too. □

This notion of PBDD is not the usual generalisation of the positivstellensatz to deal with multiple formulae on the right. But it still allows to show that a positive polynomial is a sum of squares of rational fraction:

Lemma 9. If $\left(\overrightarrow{P}, (Q), T\right)$ in $\mathcal{R}$ (i.e. T is PBDD proving that $Q \geqslant 0$), then there exists C, $C' \in \mathcal{C}\left(\overrightarrow{P}\right)$ such that $C\,Q = C'$ and $C \neq 0$.

Proof. The result is immediate when T is a leaf, because in a leaf $L(M, k, C)$, M belongs to a monoid which is a subset of the allowed cone for C and it does not contain 0.

We finish the proof by induction on the height of T. Let $T = If(S, T_1, T_2)$, the induction hypotheses gives $C_1, C_2 \in \mathcal{C}\left(\overrightarrow{P}, S\right)$, $D_1, D_2 \in \mathcal{C}\left(\overrightarrow{P}, -S\right)$ such that $C_1\,Q = C_2$ and $D_1\,Q = D_2$.

We can always write $C_1 = C_1'\,S + C_1''$, $C_2 = C_2'\,S + C_2''$, $D_1 = D_1'(-S) + D_1''$ and $D_2 = D_2'(-S) + D_2''$. This gives $(C_1'\,Q - C_2')\,S = -C_1''\,Q + C_2''$ and $(D_1'\,Q - D_2')\,(-S) = -D_1''\,Q + D_2''$. By a linear combination eliminating S we find:

$$(D_1'\,Q - D_2')\,(-C_1''\,Q + C_2'') + (C_1'\,Q - C_2')\,(-D''1\,Q + D_2'') = 0$$

Which is equivalent to

$$(D_1'\,C_2'' + D_2'\,C_1'' + C_1'\,D_2'' + C_2'\,D_1'')\,Q = D_1'\,C_1''\,Q^2 + C_1'\,D_1''\,Q^2 + D_2'\,C_2'' + C_2'\,D_2''$$

It remains to deal with the case where $E := D_1'\,C_2'' + D_2'\,C_1'' + C_1'\,D_2'' + C_2'\,D_1'' = 0$ or $F := D_1'\,C_1''\,Q^2 + C_1'\,D_1''\,Q^2 + D_2'\,C_2'' + C_2'\,D_2'' = 0$. This is possible (even frequent in practice). When it appends some of the following simplification are possible:

- $C_1'' = C_2'' = 0$, in this case, we have $C_1'\,S\,Q = C_2'\,S$ and we may simplify by S.
- $D_1'' = D_2'' = 0$ to find $D_1'(-S)\,Q = D_2'(-S)$, again simplifying.

- $C_1' = C_2' = 0$, in this case, we have $C_1'' Q = C_2''$.
- $D_1' = D_2' = 0$, in this case, we have $D_1'' Q = D_2''$.
- Finally if none of the above applies, at least two terms in E or F are not zero (recall that $C_1 \neq 0$ and $D_1 \neq 0$ hence we also have that at least $C_1' \neq 0$ or $C_1'' \neq 0$ and at least $D_1' \neq 0$ or $D_1'' \neq 0$). When $C_1'' = C_2' = D_1'' = D_2'' = 0$, all terms in E are null but two terms in F are non zero. There are three similar *worst* cases.

  Assume, without loss of generality, that it is E which has at least to non zero term. The polynomial E being in $\mathcal{C}\left(\overrightarrow{P}\right)$, it uses at least one of the P_i (and $\overrightarrow{P}$ can not be an empty sequence) because a sum of squares can only be zero if all its terms are zero. Consider P_j appearing in e with maximum index (the lowest one above the node in consideration in the PBDD). Hence E can be written $E' P_j + E'' = 0$. Now, we consider the node $If(P_j, T_1', T_2')$ or $If(-P_j, T_1', T_2')$ introducing P_j. Let us consider the case $If(P_j, T_1', T_2')$ where the node $If(S, T_1, T_2)$ occur in T_1'. But we have $E'(-P_j) = E''$, hence we may simplify the PBDD and replace the node $If(P_j, T_1', T_2')$ by the node T_2' multiplied by E' (meaning we multiply by E' all the cone in the leafs, but not the polynomial in the node) and replacing $E'(-P_j)$ by E'' everywhere P_j occurs. This means that we do not have to consider the tree T_1' at all, hence the problematic note $If(S, T_1, T_2)$.

Remark: the last simplification is not correct in general and is just enough for this lemma and PBDD justifying the positiveness of one polynomial, because after the simplification, the leafs $L(C, k, C')$ only verify $C, C' \in \mathcal{C}(P_1, \ldots, P_m, S_1, \ldots, S_l)$, loosing $C \in \mathcal{M}(S_1, \ldots, S_l)$. Hence we can not use this trick to systematically simplify PBDD. □

Example 3. Let us apply the previously given positive-justification for the sequent $\vdash (X^3 - Y^3)(X - Y)$:

$$\begin{aligned} If(X,\ & If(Y,\ L(1,1,(X-Y)^2(X^2+2XY+Y^2)),\\ & \qquad L(1,1,(X^4+Y^4-X^3Y-XY^3))),\\ & If(Y,\ L(1,1,(X^4+Y^4-X^3Y-XY^3)),\\ & \qquad L(1,1,(X-Y)^2(X^2+2XY+Y^2)))) \end{aligned}$$

Let us call $Q = (X^3 - Y^3)(X - Y)$. First, we consider the subtree $If(Y, L(1,1,(X-Y)^2(X^2+XY+Y^2)), L(1,1,(X^4+Y^4-X^3Y-XY^3)))$. We have to combine $Q = (X-Y)^2 XY + (X-Y)^2(X^2+Y^2)$ and $Q = (X^3+XY^2)(-Y) + X^4 + Y^4$. This gives

$$\left((X-Y)^2 X + X^3 + XY^2\right) Q = \left(X^3 + XY^2\right)(X-Y)^2\left(X^2+Y^2\right) + (X-Y)^2 X\left(X^4+Y^4\right)$$

Which simplifies to

$$X\left((X-Y)^2 + X^2 + Y^2\right) Q = X(X-Y)^2\left(\left(X^2+Y^2\right)^2 + X^4 + Y^4\right)$$

For the second subtree, we find the opposite and for the top tree, the simplification by X yield the final result:

$$\left((X-Y)^2+X^2+Y^2\right)Q = (X-Y)^2\left(\left(X^2+Y^2\right)^2+X^4+Y^4\right)$$

Compared to Stengle's justification, we seem to loose the fact that the denominator is zero only when the polynomial is null as well. However, it seems to require smaller degree (see below) and we are not sure to loose this property (in the above example $((X-Y)^2+X^2+Y^2)$ only vanishes when $X = Y = 0$ and this implies $Q = 0$).

Lemma 10. The above definition satisfies to the conditions of definition 2.

Proof. The three first conditions are immediate. Let us consider the fourth one. We assume $\left(\vec{P}, \left(\vec{Q}, S\right), T_1\right) \in \mathcal{R}$ and $\left(\left(\vec{P}, S\right), \vec{Q}, T_2\right) \in \mathcal{R}$ and we want to construct T_3 such that $\left(\vec{P}, \vec{Q}, T_3\right)$ in $\mathcal{R}$. Let us define $m = \left|\vec{P}\right|$ and $n = \left|\vec{Q}\right|$.

First, consider all leafs in T_1 that uses S (other leafs are kept unchanged), i.e. leaf with value like $L(M_1, n+1, C_1)$. For such a leaf, we have $M_1 S = C_1$. We replace such a leaf with a tree T_2' obtained from T_2 as follows: the leaf in T_2 that do not use S are unchanged otherwise we have a leaf in T_2 of the shape $L(M_2, k, C_2)$ with $M_2 Q_k = C_2$. Then, we factorise S and write $C_2 = C_2' S + C_2''$. M_2 is not allowed to use this occurrence of S. There may be other S introduced by a node $If(-S, T_1, T_2)$ above the leaf we consider, but then, we may consider that M_2 does not use the cut formula S either.

Combining the above equality, we find:

$$M_1 M_2 Q_k = M_1(C_2' S + C_2'') = C_1 C_2' + M_1 C_2''$$

Finally, we need to remark that $M_1 M_2$ does belong to the required monoid because it is the product of M_1 and M_2 that are in the required monoid (which depends upon the position of the leafs in the PBDD trees). Similarely, $C_1 C_2' + M_1 C_2''$ is in the required cone and the leaf $L(M_1 M_2, k, C_1 C_2' + M_1 C_2'')$ may replace the leaf $L(M_2, k, C_2)$ in T_2'. □

Remark: PBDD are subject to the usual optimisations for classical BDD: if we choose an order on polynomials, we may combine them in a more economical way by avoiding to introduce twice a node using the same polynomial. We can even do better: a node $If(R, T_1, T_2) \in \mathcal{B}_n(P_1, \ldots, P_m; S_1, \ldots, S_l)$ where R is in the cone $\mathcal{C}(P_1, \ldots, P_m, S_1, \ldots, S_l)$ can be replaced by T_1. Similarely, if $-R$ is in the monoid $\mathcal{M}(S_1, \ldots, S_l)$, it can be replaced by T_2.

Lemma 11. The polynomial sequent calculus obtained from the positive-justification, that we will call *positive sequent calculus* is complete for the theory $\mathcal{T}(\mathbb{A})$ of any ordered ring $\mathbb{A}$ when we encode the atomic formula $P \geqslant Q$ by $P - Q$ and $P = Q$ by $P - Q \wedge Q - P$ or $-$

$(P-Q)^2$ (the former coding of equality yield shorter when used for negative occurrences of equality).

Proof. The equations in the theory are supported because polynomials in $\mathbb{A}[\mathcal{V}]$ are equal under these equations.

It remains only to prove the following:

- Square are positive and addition and multiplication are increasing: The $\mathcal{R}$-rule allows us to derive $\vdash P^2$; $P, Q \vdash P+Q$ and $P, Q \vdash PQ$ using just leafs in the PBDD.
- Reflexivity of the order is simply $\vdash 0$ (because $P \leqslant P$ is encoded as $P-P$).
- Transitivity is immediate from the $\mathcal{R}$-rule: $P-Q, Q-R \vdash P-R$.
- Equivalence of the two coding for equality: clearly $P, -P \vdash -P^2$. For the converse, we proceed in two steps: $-P^2 \vdash P^3$ using $P^3 = \frac{1}{4}(P^2(P+1)^2 - P^2(P-1)^2)$ and $P^3 \vdash P$ using the tree $\mathrm{If}(P, \mathrm{L}(1,1,P), \mathrm{L}((-P)^2, 1, P^3))$ giving $-P^2 \vdash P$ using a cut. Then, replacing P by $-P$ we also get $-P^2 \vdash -P$.
- Anti-symmetry is direct because we encoded $P = Q$ as $(P-Q) \wedge (Q-P)$.
- Total ordering: because we encoded $P < 0$ as $\neg P$, and because the sequent calculus is classical, we immediately have $\vdash P \vee -P$. Still, we have to prove that $P < 0$ and $P > 0$ are incompatible or that $P > 0$ implies $P \geqslant 0$. Through our coding both sequent $P < 0, P > 0 \vdash \bot$ and $P > 0 \vdash P \geqslant 0$ are consequences (through the $\neg_l$ rule) of $\vdash P, -P$ which can be derived from the $\mathcal{R}$-rule using $T = \mathrm{If}(P, \mathrm{L}(1,1,P), \mathrm{L}(1,2,-P))$.
- Equality is reflexive directly from the reflexivity of the order.
- Equality is substitutive: first we remark that the cone $\mathcal{C}(P, -P, \ldots)$ contains the ideal generated by P because $PS = \frac{1}{4}P(S+1)^2 - P(S-1)^2$. This allows to do the same proof as in the case of the nullstellensatz.
- The integrity axiom is a consequence of $-PQ \vdash P, Q$ which is derived by the tree $\mathrm{If}(P, \mathrm{L}(1,1,P), \mathrm{L}(-P, 2, -PQ))$. Similarly we have $-PQ \vdash -P, -Q$, $PQ \vdash -P, Q$ and $PQ \vdash P, -Q$ and this implies $PQ, -PQ \vdash -P^2, -Q^2$ by considering cases introduced be the four sequents. □

Theorem 12. Postivstellensatz Let $(\mathbb{A}, \geqslant, +, \times, 0, 1)$ be an ordered ring and $(\mathbb{K}, \geqslant, +, \times, 0, 1)$ its real closure. Consider a Π_1 statement of the form $\forall X_1, \ldots, X_d (P_1 \geqslant 0 \wedge \ldots \wedge P_m \geqslant 0 \to Q_1 \geqslant 0 \vee \ldots \vee Q_n \geqslant 0)$ true in $\mathbb{K}$, then there exists a PBDD in $\mathcal{B}_n(P_1, \ldots, P_m;)$ such that for all leafs $\mathrm{L}(C, k, C')$ in the tree T, we have $CQ_k = C'$.

Proof. Basically the same proof that for the nullstellensatz using the corresponding lemmas. □

6 Experiments and comparison with Krivine-Stengle justification.

Krivine-Stengle justification for a sequent $P_1, \dots, P_n \vdash Q_1, \dots, Q_m$ is the existence of $M \in \mathcal{M}(-Q_1, \dots, -Q_n)$ and $C \in \mathcal{C}(P_1, \dots, P_n, -Q_1, \dots, -Q_m)$ such that $M + C = 0$. This justification is natural when one remark that the sequent $P_1, \dots, P_n \vdash Q_1, \dots, Q_m$ means $P_1 \geqslant 0, \dots, P_n \geqslant 0 \vdash Q_1 \geqslant 0, \dots, Q_m \geqslant 0$, which is equivalent to $P_1 \geqslant 0, \dots, P_n \geqslant 0, -Q_1 > 0, \dots, -Q_m > 0 \vdash \bot$.

We first can prove an analogous of lemma 9:

Lemma 13. If $\left(\overrightarrow{P}, \overrightarrow{Q}, T\right)$ in $\mathcal{R}$ (i.e. T is PBDD proving that $Q \geqslant 0$), then there exists $M \in \mathcal{M}(-Q_1, \dots, -Q_n)$ and $C \in \mathcal{C}(P_1, \dots, P_n, -Q_1, \dots, -Q_m)$ such that $M + C = 0$.

Proof. We proceed by induction on T. More precisely, we prove that if $T \in \mathcal{B}_n(P_1, \dots, P_m; S_1, \dots, S_l)$ and if $\overrightarrow{Q}$ is a sequence of polynomials of length n such that for all leafs $L(M, k, C)$ in the tree T, we have $M\,Q_k = C$. Then, there exists $M \in \mathcal{M}(-Q_1, \dots, -Q_n, S_1, \dots, S_l)$ and $C \in \mathcal{C}(P_1, \dots, P_n, -Q_1, \dots, -Q_n, S_1, \dots, S_l)$ such that $M + C = 0$.

The case $l = 0$ gives the wanted result and the leaf case is immediate. For the induction case, we have $T = \mathrm{If}(R, T_1, T_2)$ and by induction hypothesis, we find $M_1 \in \mathcal{M}(-Q_1, \dots, -Q_n, S_1, \dots, S_l)$ and $C_1 \in \mathcal{C}(P_1, \dots, P_n, -Q_1, \dots, -Q_n, S_1, \dots, S_l, R)$ such that $M_1 + C_1 = 0$ (i). and $M_2 \in \mathcal{M}(-Q_1, \dots, -Q_n, S_1, \dots, S_l, -R)$ and $C_2 \in \mathcal{C}(P_1, \dots, P_n, -Q_1, \dots, -Q_n, S_1, \dots, S_l, -R)$ such that $M_2 + C_2 = 0$ (ii).

We can write $C_1 = R\,C_1' + C_1''$, $M_2 = (-R)^e M_2'$ and $C_2 = -R\,C_2' + C_2''$. Thus, we have $-R\,C_1' = C_1'' - C_1 = C_1'' + M_1$. Moreover, we may assume that $e > 0$ otherwise we multiply (ii) by $-R$ to find $(-R)^{e+1} M_2' = -R\,C_2'' + R^2\,C_2'$.

Then we can combine (i) and (ii) to find:

$$0 = (C_1'' + M_1)^e M_2' + C_1'(-R\,C_2' + C_2'') = (C_1'' + M_1)^e M_2' + C_1'(C_1'' + M_1)\,C_2' + C_1' C_2''$$

Then, developing the right member gives C_3 such that $M_1^e M_2' + C_3 = 0$ with $M_1^e M_2' \in \mathcal{M}(-Q_1, \dots, -Q_n, S_1, \dots, S_l)$ and $C_3 \in \mathcal{C}(P_1, \dots, P_n, -Q_1, \dots, -Q_n, S_1, \dots, S_l)$. □

Therefore, we may wonder what are the respective interests of lemma 9 and 13:

- The previous lemma applies with an arbitrary sequent while lemma 9 require $l = 1$ (only one conclusion in the sequent).
- Even in the case with one conclusion, Krivine-Stengle justification gives a fraction for a positive polynomial whose denominator only vanishes when $Q = 0$ which lemma 9 does not seem to provide.
- However, the way we combine polynomial in lemma 9 is more efficient. In Krivine-Stengle justification, we raise a polynomial to the power e. If we want a simple bound, we may say that the final polynomial M and C have degree which is less that the product of the degree of polynomials in the leafs of the PBDD. In the case of lemma 9, we only do a linear combination and get a degree which is less that the sum of the degree of polynomials in the leafs of the PBDD.

Remark, we may also directly use Krivine-Stengle justification to define the axiome rule of a polynomial sequent calculus. But here again, cut elimination on axiom will produce polynomials with degree less than the product of the original polynomials while PBDD have degree and size bounded by the sum of the original degrees.

Actually, we have implement cut elimination in both cases (PBDD and Krivine-Stengle justification) and applied it to exactly the same proof that Motzkin's polynomial is positive. More precisely, a proof that

$$Q := \left(T^6 + X^4 Y^2 + X^2 Y^4\right)^3 - \left(3 T^2 X^2 Y^2\right)^3 \geqslant 0$$

It is easy to remove the cube to find Motzkin's polynomial. We found a rather large PBDD of height 4 (each branch had 4 nodes before reaching the leaf), hence it has 16 leafs. All leafs in the tree have the same degree 18.

Then, the lemma 9 gives an equality $CQ = C'$ with C' of degree 48 and therefore C of degree 30. This is rather large, but the proof we started from is a proof by induction that the arithmetic mean is greater than the geometric one (AM-GM inequality) without any optimisation to minimize the degree.

In the case of Krivine-Stengle justification, the cut-elimination did not finish in a reasonable time, probably due to the degree and size of the involved polynomials.

Then, we used the same proof of the AM-GM inequality to obtain a (too complex) proof of the trivial result

$$Q := \left(T^4 + X^2 Y^2\right)^2 - \left(2 X^2\right)^2 \geqslant 0$$

In this case, we get using PBDD and our lemma: $Q = (T^4 - X^4)^2$. While the same proof using Krivine-Stengle justification yield

$$Q^3 + 1/64\left(8 T^{12} - 24 X^4 T^8 + 24 X^8 T^4 - 8 X^{12}\right)^2 = 0\,.$$

7 Dealing with inverse and closure.

The defect of the previous result is that we need to start from a derivation in the theory of the ring of the coefficients of the polynomial, and the proof we gave that such a derivation exists is non constructive (in fact, the underlying theorem of proof theory, like the completeness theorem, can probably be made effective, but the underlying algorithm is not easy to analyse [12]).

However, we can solve this problem. In the case of the nullstellensatz, using these rules:

$$\frac{\Gamma,\, P X - Q \vdash \Delta \qquad \Gamma,\, P \vdash \Delta}{\Gamma \vdash \Delta}\,\mathrm{Inv} \qquad \frac{\Gamma,\, X^n + \Sigma_{i=0}^{n-1} A_i X^i \vdash \Delta}{\Gamma \vdash \Delta}\,\mathrm{AlgClos}$$

In the above rule, there should be no occurrence of X other than the explicit ones (i.e. X must not occur in Γ, Δ, P, Q, A_0, ..., A_{n-1}. Moreover, $n \geqslant 1$ in the second rule.

Lemma 14. The above rule are equivalent to the traditional axioms for the existence of the inverse and existence of the root for any non constant polynomial.

Proof. These are just easy derivations. □

Lemma 15. The above rules preserves the cut-elimination theorem of the null sequent calculus.

Proof. The rules do not introduce a formula in the conclusion sequent, therefore it suffices to remark that any cut below such a rule can be moved (and duplicated) above the rule. □

Lemma 16. A proof of a π_1-formula in the null sequent calculus using the Inv and AlgClos rules can be transformed into a proof not using these rules.

Proof. First, we use the previous lemma to eliminate cuts. Then, we remark that any rule, other than $\forall_l$, cut or axiom, applied to one of the premise of the Inv and AlgClos rules can be moved below the rule.

Because we are proving a Π_1 formula, and because we first eliminated cuts, the proof can not use the $\forall_l$ rule: it introduces a negative $\forall$ quantifier that would still be in the conclusion which is impossible if the proved formula is Π_1.

Then, we only need to show how to eliminate those rules when they follow immediately an axiom. We start with the Inv rule:

$$\dfrac{\dfrac{}{\Gamma, P\,X - Q \vdash \Delta}\text{Ax} \qquad \dfrac{}{\Gamma, P \vdash \Delta}\text{Ax}}{\Gamma \vdash \Delta}\text{Inv}$$

If the formula $P\,X - Q$ or the formula P are not used in one of the axioms, then the rule is replaced by this axiom. Otherwise we have two equalities of the following shape:

$$\vec{\Delta^{e_1}} = T_1(P\,X - Q) + \vec{S_1}\Gamma \qquad\qquad \vec{\Delta^{e_2}} = T_2\,P + \vec{S_2}\Gamma$$

where T_1 and T_2 are non zero. Beware, X does not occur in Γ, Δ, P and Q but may occur in T_1, and $\vec{S_1}$. If X occur in T_2 and $\vec{S_2}$, it can be replaced by 0.

We may replace in the first equality X by $\frac{Q}{P}$ and P itself by $\frac{\vec{\Delta^{e_2}} - \vec{S_2}\Gamma}{T_2}$, which gives the following equality on rational fraction:

$$\vec{\Delta^{e_1}} = \vec{S_1}\left[X \leftarrow \frac{Q\,T_2}{\vec{\Delta^{e_2}} - \vec{S_2}\,\Gamma}\right]\Gamma$$

If $Q = 0$, we can stop here (and the rule was mostly useless). Otherwise, we can eliminate all denominator by multiplying by a large enough power of $\vec{\Delta^{e_2}} - \vec{S_2}\,\Gamma$, which gives an equality of the following shape for some $\vec{S_3}$:

$$\vec{\Delta^{e_1}}\left(\vec{\Delta^{e_2}} - \vec{S_2}\,\Gamma\right)^k = \vec{S_3}\,\Gamma$$

Finally, developing the right-hand side allows us to find $\vec{S_4}$ with:

$$\vec{\Delta^{e_1 + k e_2}} = \vec{S_4}\,\Gamma$$

Which means that the rule can be replaced by an axiom.

It remains the case of the AlgClos rule with an axiom:

$$\dfrac{\dfrac{}{\Gamma,\, X^n + \Sigma_{i=0}^{n-1} A_i X^i \vdash \Delta}\,\text{Ax}}{\Gamma \vdash \Delta}\,\text{AlgClos}$$

Which means we have an equlity of the following shape:

$$\vec{\Delta^{e}} = T\left(X^n + \Sigma_{i=0}^{n-1} A_i X^i\right) + \vec{S}\,\Gamma$$

Let us introduce names $\lambda_1, \ldots, \lambda_n$ for all roots of $X^n + \Sigma_{i=0}^{n-1} A_i X^i$, this means that we have $\vec{\Delta^{e}} = \vec{S}[X \leftarrow \lambda_i]\Gamma$ for all $i \in \{1, \ldots, n\}$ which is true in a large enough field. Then, using Newtons's theorem expressing symmetric polynomial in the root as a polynomial in the coefficient, we find that $R[A_1, \ldots, A_n] = \Pi_{i=0}^{n} \vec{S}[X \leftarrow \lambda_i]$ leading to:

$$\vec{\Delta^{n e}} = R[A_1, \ldots, A_n]\,\Gamma^n$$

This justifies again that the rule may be replaced by an axiom (because $n \geqslant 1$).

Remark: if we have an inverse for each integer in our ring, we may use that arithmetic mean instead of the product to lower the degree of polynomials, but this is not always possible. □

In the case of the positivstellensatz, we can also give the following axioms to extend the positive sequent calculus into a complete calculus for real closed field while preserving cuts:

$$\frac{\Gamma, P\,X - Q\,, Q - P\,X \vdash \Delta \qquad \Gamma, P, -P \vdash \Delta}{\Gamma \vdash \Delta}\,\text{Inv}'$$

$$\frac{\Gamma, P(X)\,, -P(X) \vdash \Delta \qquad \Gamma, P(U)P(V)\,, -P(U)P(V) \vdash \Delta}{\Gamma \vdash \Delta}\,\text{RealClos}$$

Lemma 17. The above rules preserves the cut-elimination theorem of the positive sequent calculus.

Proof. Identical to the proof of lemma 15. □

Lemma 18. A proof of a π_1-formula in the positive sequent calculus using the Inv' and RealClos rules can be transformed into a proof not using these rules.

Proof. Similar to the proof of lemma 16. All needed compitation can in fact be found in page 277-280. Beware, that the computation has to be done for some leafs of the PBDD (those using the new formulas in the sequent), as in the proof of lemma 10. □

8 Nullstellensatz for differential ring.

This theory of differential ring is obtained from the theory of ring by adding one or more function symbols ∂_x satisfying the following axioms:

- $\partial_x \partial_y P = \partial_y \partial_x P$
- $\partial_x (P + Q) = \partial_x P + \partial_x Q$
- $\partial_x (P\,Q) = P\,\partial_x Q + Q\,\partial_x P$
- $\partial_x 0 = 0$ and $\partial_x 1 = 0$ which are consequences of the above axioms.

We will denote $\mathbb{A}^{\partial}[\mathcal{V}]$ the set of differential polynomials with coefficient in $\mathbb{A}$ and indeterminates in $\mathcal{V}$.

The theory of differential ring can be completed into the theory of differentially closed field hence supporting the first part of our proof schema. For the rest of the proof, the above equality are automatically managed if we use differential polynomial in place of polynomials.

There is only one change to do because we have to support the equality axiom on the new function symbols hence our $\mathcal{R}$-rule should prove the sequent $P \vdash \partial_x P$ whose meaning is $P = 0$ implies $\partial_x P = 0$. Doing this is immediate by changing the definition of null-justification to correspond to the radicals of differential ideals:

Definition 13. A differential-null-justification will be a quadruple $\left(\vec{S}, \vec{d}, \vec{f}, \vec{e}\right)$ where $\vec{S}$ is a finite sequence of polynomials in $\mathbb{A}^{\partial}[\mathcal{V}]$ (sequence of differential polynomial), $\vec{d}$ is a finite

sequence of derivation operator (composition of ∂_x, ∂_y, ...) and $\vec{f}$, $\vec{e}$ are finite sequences of natural numbers. Then, we take

$$\mathcal{R} = \left\{ \left(\vec{P}, \vec{Q}, \left(\vec{S}, \vec{d}, \vec{f}, \vec{e} \right) \right) \mid \left| \vec{f} \right| = \left| \vec{S} \right| = \left| \vec{d} \right| = n, \left| \vec{Q} \right| = \left| \vec{e} \right|, \sum_{1 \leqslant i \leqslant n} \left(d_i P_{f_i} \right) S_i = \vec{Q}^{\vec{e}} \right\}.$$

Using the same proof schema, we get the following usual differential nullstellensatz:

Theorem 19. Differential nullstellensatz Let $(\mathbb{A}, +, \times, 0, 1, \partial_x, ...)$ be a differential ring and $\mathbb{K}$ its differential closure. Consider a Π_1 statement of the form $\forall X_1, ..., X_d (P_1 = 0 \wedge ... \wedge P_m = 0 \rightarrow Q_1 = 0 \vee ... \vee Q_n = 0)$ true in $\mathbb{K}$, then there exists differential polynomials $S_1, ..., S_N$ in $\mathbb{A}^{\partial}[\mathcal{V}]$, $d_1, ..., d_N$ a finite sequence of composition of derivation symbols, $f_1, ..., f_N$ and $e_1, ..., e_n$ some natural numbers such that:

$$\left(d_1 P_{f_1} \right) S_1 + ... + \left(d_N P_{f_N} \right) S_N = Q_1^{e_1} ... Q_n^{e_n}.$$

This proof is not fully effective and it remains to write a rule allowing cut elimination for the axiom expressing that a differential field is closed and to prove that this axiom may be eliminated. We hope that this is possible.

9 Bibliography

[1] W. Whiteley, Invariant computations for analytic projective geometry, in: J. of symbolic computation, volume 11 (1989), 549--578

[2] Henri Lombardi, Effective real Nullstellensatz and variants, in: Effective Methods in Algebraic Geometry, volume 94 (1991), Birkhäuser Boston, 263-288, M. Teo, T. Carlo (eds.)

[3] Michel Coste, Henri Lombardi, Marie-Françoise Roy, Dynamical method in algebra: effective Nullstellensätze, in: Annals of Pure and Applied Logic, volume 111 (2001), 203 - 256

[4] Henri Lombardi, Relecture constructive de la théorie d'Artin-Schreier, in: Annals of Pure and Applied Logic, volume 91 (1998), 59 - 92

[5] David Marker, Model theory of differentiable fields, in: Lecture Notes in Logic 5, 1996, Springer

[6] Jean-Louis Krivine, Anneaux pr'eordonn'es, in: Journal d'Analyse Math'ematique, volume 12 (1964), p. 307-326

[7] Gilbert Stengle, A Nullstellensatz and a Positivestellensatz in semialgebraic geometry, in: Annals of Math, volume 207 (1974), 87--97

[8] Jean-Louis Krivine, Anneaux préordonnés, in: Journal d'Analyse Mathématique, volume 12 (1964), p. 307-326

[9] G. Gentzen, New version of the consistency proof for elementary number theory, in: In: Collected Papers of Gerhard Gentzen, M. E. Szabo, ed, 1938, 252--286

[10] Jean-Yves Girard, Proof theory and logical complexity Vol.I, 1987, Bibliopolis
[11] R.O. Gandy, Proofs of strong normalization, 1980, Academic Press, London, 457-477, J.R. Hindley, J.P. Seidin (eds.)
[12] Jean-Louis Krivine, Une preuve formelle et intuitionistique du Théorème de Complétude de la Logique Classique, in: Bull. Symbolic Logic, volume 2 (1996), 405 - 421