Dynamical method in algebra: Effective Nullstellensätze

Michel Coste, Henri Lombardi, Marie-Françoise Roy

Dynamical method in algebra: Effective Nullstellensätze

Michel Coste [*],
Henri Lombardi [†],
Marie-Françoise Roy[‡]

revised, October 2000

Abstract

We give a general method for producing various effective Null and Positivstellensätze, and getting new Positivstellensätze in algebraically closed valued fields and ordered groups. These various effective Nullstellensätze produce algebraic identities certifying that some geometric conditions cannot be simultaneously satisfied. We produce also constructive versions of abstract classical results of algebra based on Zorn's lemma in several cases where such constructive version did not exist. For example, the fact that a real field can be totally ordered, or the fact that a field can be embedded in an algebraically closed field. Our results are based on the concepts we develop of dynamical proofs and simultaneous collapse.

MSC: 03F65, 06F15, 12J10, 12J15, 18B25

Keywords: Dyamical proof, Constructive algebra, Positivstellensatz

[*]IRMAR (UMR CNRS 6625), Université de Rennes 1, Campus de Beaulieu 35042 Rennes cedex FRANCE, coste@maths.univ-rennes1.fr, supported in part by European Community contract CHRX-CT94-0506

[†]Laboratoire de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25 030 BESANCON cedex, FRANCE, henri.lombardi@univ-fcomte.fr, supported in part by the project ESPRIT-BRA 6846POSSO

[‡]IRMAR (UMR CNRS 6625), Université de Rennes 1, Campus de Beaulieu 35042 Rennes cedex FRANCE, mfroy@maths.univ-rennes1.fr supported in part by the project ESPRIT-BRA 6846POSSO and by European Community contract CHRX-CT94-0506

Contents

Introduction **3**

1 Dynamical proofs **4**
1.1 Dynamical theories and dynamical proofs 4
1.2 Collapse 10
1.3 Dynamical theories and coherent toposes 10

2 Hilbert's Nullstellensatz **13**
2.1 Direct theories 13
2.2 Some simultaneous collapses 14
2.3 Decision algorithm and constructive Nullstellensatz 17
2.4 Provable facts and algebraic theory of quasi-domains 20

3 Stengle's Positivstellensatz **21**
3.1 Some simultaneous collapses 21
3.2 Decision algorithm and constructive Positivstellensatz 26
3.3 Provable facts and generalized Positivstellensätze 28

4 A Positivstellensatz for valued fields **29**
4.1 Some simultaneous collapses 29
4.2 Decision algorithm and constructive Positivstellensatz 33
4.3 Provable facts and generalized Positivstellensätze 34
4.4 Related results of Prestel-Ripoli 37

5 A Positivstellensatz for ordered groups **38**

Introduction

Our aim is to interpret constructively non-constructive classical algebraic proofs. The idea is that there is a constructive content hidden in the proof of theorems like "a ring with a non-trivial ideal has a prime ideal", "a field can be embedded in an algebraically closed fields" even if their proof is based on Zorn's lemma. The constructive content is the following "rings with non-trivial ideal and fields collapse simultaneously", "fields and algebraically closed fields collapse simultaneously" : if facts can be shown to be contradictory inside the theory of algebraically closed fields, using dynamical proofs, they are contradictory as well inside the theory of non-trivial rings, and the second contradiction can be explicitly constructed from the first one. Dynamical proofs are particularly simple: you want to prove a fact in a field and you do not know whether a given element is null or invertible. You just open branches corresponding to the two possible cases and prove this fact in all subcases. It turns out that many classical algebraic proofs have this very simple structure.

A similar example is the following "a real field can be embedded in an ordered field", to be replaced by "real fields and ordered fields collapse simultaneously". Constructively, we are not able to say that there exists a model of the stronger theory extending a model of the weaker one, but only that working with the stronger theory does not create more contradiction than working with the weaker one.

In the particular cases that we consider here, simultaneous collapse takes very explicit forms, and produces algebraic certificates, which are precisely algebraic identities given by various effective Nullstellensätze and Positivstellensätze. We consider Hilbert's Nullstellensatz, and Stengle's Positivstellensatz, as well as new Positivstellensätze for algebraically closed valued fields and ordered groups, with the same method. Here is the statement for valued fields:

Theorem (Positivstellensatz for algebraically closed valued fields) *Let (K, A) be a valued field and let U_A the invertible elements of A, I_A the maximal ideal of A. Suppose that (K', A') is an algebraically closed valued field extension of K (so that $A = A' \cap K$). Denote by $U_{A'}$ the invertible elements of A', $I_{A'}$ the maximal ideal of A'.*
Consider five finite families $(R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$ of elements of the polynomial ring $K[x_1, x_2, \ldots, x_m] = K[x]$. Let $\mathcal{I}_{=0}$ be the ideal of $K[x]$ generated by $R_{=0}$, $\mathcal{M}_{\neq 0}$ the monoid of $K[x]$ generated by $R_{\neq 0}$, $\mathcal{V}_{\mathrm{Vr}}$ the subring of $K[x]$ generated by $R_{\mathrm{Vr}} \cup R_{\mathrm{Rn}} \cup R_{\mathrm{U}} \cup A$, $\mathcal{I}_{\mathrm{Rn}}$ the ideal of $\mathcal{V}_{\mathrm{Vr}}$ generated by $R_{\mathrm{Rn}} \cup I_A$, $\mathcal{M}_{\mathrm{U}}$ the monoid generated by $R_{\mathrm{U}} \cup U_A$.
Define $\mathcal{S} \subset K'^m$ as the set of points satisfying the following conditions: $n(x) = 0$ for $n \in R_{=0}$, $t(x) \neq 0$ for $t \in R_{\neq 0}$, $c(x) \in A'$ for $c \in R_{\mathrm{Vr}}$, $v(x) \in U_{A'}$ for $v \in R_{\mathrm{U}}$, $k(x) \in I_{A'}$ for $k \in R_{\mathrm{Rn}}$.

The set $\mathcal{S}$ is empty if and only if there is an equality

$$m(u + j) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$.

The statement has a trivial part: if there is an equality

$$m(u + j) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$ it is clear that $\mathcal{S}$ is empty. The converse implication, from the geometric fact "$\mathcal{S}$ is empty" to the existence of an algebraic identity

$$m(u + j) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$, is far from trivial. The fact that moreover this algebraic identity can be explicitly constructed from a proof that $\mathcal{S}$ is empty is the main point in the present paper.

The previous theorem is closely related to results of Prestel and Ripoli [30]. We discuss this point in section 4.4.

This paper is a first step in a general program of constructivization of classical abstract algebra using dynamical methods (see also [20, 21, 22, 23, 24, 25, 26]).

Our theory has many connections with the following papers ([6, 7, 8, 9, 10, 11, 12, 13, 15]), based on ([1, 3, 4, 14]), and with the theory of coherent toposes as well.

We thank the referee for valuable remarks and bibliographical references.

1 Dynamical proofs

Consider the following proof of $x^3 - y^3 = 0 \vdash x - y = 0$ in the theory of ordered fields.

Suppose that $x^3 - y^3 = 0$. There are two cases to consider

- $x = 0$, then $y^3 = 0$, and it follows $y = 0$, hence $x - y = 0$,
- $x^2 > 0$ then $x^3 - y^3 = (x - y)(x^2 + xy + y^2) = (x - y)(3x^2/4 + (y + x/2)^2)$ and since $x^2 > 0$, $(3x^2/4 + (y + x/2)^2) > 0$. Introducing the inverse z of $(3x^2/4 + (y + x/2)^2)$ and multiplying $x^3 - y^3$ by z we see that $x - y = 0$.

This proof is the prototype of a dynamical proof as we shall see soon.

1.1 Dynamical theories and dynamical proofs

We start from a language $\mathcal{L}$ with variables, constants, symbols of functions and symbols of relations, including at least the equality. All the theories we shall consider will allow the substitution of equal terms. A *presentation* in the language $\mathcal{L}$ is a couple $(G; R)$ where R is a set of atomic formulas and G is a set of variables containing the variables appearing in R. The variables in G are called the *generators* and the atomic formulas in R are called the *relations* of the presentation. The sets G and R are allowed to be infinite, but only a finite part of them is used in proofs.

A *fact* in a presentation $(G; R)$ is any atomic formula of $\mathcal{L}$ involving only variables in G.

A *model* of a presentation $(G; R)$ is a set-theoretic interpretation A of the language $\mathcal{L}$ and a mapping f from G to A such that the relations of R are valid inside A after substituting variables x in G by $f(x)$.

We say that *the presentation* (G, R) *contains the presentation* (G', R') when $G' \subset G$ and $R' \subset R$. The *union of two presentations* $(G; R)$ and $(G'; R')$ is the presentation $(G \cup G'; R \cup R')$ and will be also denoted by $(G; R) \cup (G'; R')$. More generally we use the notation $(G; R) \cup (G'; R')$ in case that $(G; R)$ is a presentation and relations in R' are relations about terms constructed on $G \cup G'$.

To a set-theoretic interpretation A of the language $\mathcal{L}$ one associates the *diagram* of A, $\mathcal{DG}(A)$ which is the presentation where every element a of A is represented by a variable X_a and the relations are all atomic formulas true inside A. Remark that $\mathcal{DG}(A)$ does not contain negations of atomic formulas (it is often called the positive diagram of A). So e.g. in the theory of rings, the fact that two elements a and b of a ring A are distinct does not appear in the diagram of A.

A *dynamical theory* $\mathcal{D}$ has *dynamical axioms* i.e. axioms of the form

$$H(\mathbf{x}) \vdash \exists \mathbf{y}_1 \ A_1(\mathbf{x}, \mathbf{y}_1) \ \vee \ \cdots \ \vee \ \exists \mathbf{y}_k \ A_k(\mathbf{x}, \mathbf{y}_k)$$

where $H(\mathbf{x})$ and $A_i(\mathbf{x}, \mathbf{y}_i)$ are conjunctions of atomic formulas of $\mathcal{L}$, $\mathbf{x}$ and $\mathbf{y}_i$ are lists of variables. These theories are also known in categorical logic under the name of *coherent theories*, because of their connection with coherent toposes (see section 1.3).

A special kind of dynamical axiom is an axiom with empty disjunction, denoted $\bot$, on the right-hand side. An axiom with $\bot$ in the right-hand side and a conjunction of variable-free atomic formulas on the left- hand side is called a *collapse axiom*.

An *algebraic theory* $\mathcal{T}$ has only *algebraic axioms* i.e. axioms of the form

$$H(\mathbf{x}) \vdash K(\mathbf{x})$$

where $H(\mathbf{x})$ is a conjunction of atomic formulas and $K(\mathbf{x})$ is an atomic formula of $\mathcal{L}$.

A *purely equational theory* is an algebraic theory with only *purely equational axioms* i.e. axioms of the form

$$\vdash t = t'$$

where t and t' are terms of the language.

For example the theory of commutative rings is a purely equational theory, the theories of fields, of algebraically closed fields, of ordered fields, or real closed fields are dynamical theories.

A *covering of the presentation* $(G; R)$ in the dynamical theory $\mathcal{D}$ is a tree constructed in the following way:

- at each node n of the tree, there is a *presentation* $(G_n; R_n)$, where G_n is the disjoint union of G and a finite set of new generators, and R_n is the union of R and a finite set of new relations,
- at the root $[0]$ of the tree, the presentation is $(G; R_0)$, where the new relations are consequences of R under algebraic axioms of $\mathcal{D}$,
- new nodes are created only in the following way: if $\mathbf{t}$ is a list of terms in the variables of G_n, $H(\mathbf{t})$ is a conjunction of relations in R_n and

  $$H(\mathbf{x}) \vdash \exists \mathbf{y}_1 A_1(\mathbf{x}, \mathbf{y}_1) \ \vee \ \cdots \ \vee \ \exists \mathbf{y}_k \ A_k(\mathbf{x}, \mathbf{y}_k)$$

  is an axiom of $\mathcal{D}$, then one can create k new nodes $[n, 1], \ldots, [n, k]$ (note that k may be $0, 1$ or > 1) taking $G_{n,i} = G_n \cup \{\mathbf{z}_i\}$ (where variables $\mathbf{z}_i$ are new in the branch), and $R_{n,i}$ contains $R'_{n,i} = R_n \cup \{A_i(\mathbf{t}, \mathbf{z}_i)\}$ and some consequences of $R'_{n,i}$ under the algebraic axioms of $\mathcal{D}$.

A *dead branch* of the tree is one ended by an empty disjunction $\bot$. A *leaf* of the tree is a terminal node of a non-dead branch.

Definition 1 *A* dynamical proof *in $\mathcal{D}$ of a fact $B(\mathbf{t})$ in a presentation $(G; R)$ is a covering of $(G; R)$ for the theory $\mathcal{D}$ where $B(\mathbf{t})$ is a valid fact at every leaf of the tree, i.e., $B(\mathbf{t})$ is one of the relations in the presentation at this leaf. We say that this is a dynamical proof in the theory $\mathcal{D}$ of $R \vdash B(\mathbf{t})$.*

Note that a dynamical proof can be represented by a finite object: it is sufficient to keep in $(G; R)$ only the generators and relations that are used in the proof. Remark also that dynamical proofs involve only atomic relations of the language. Moreover, the "logical part" of a dynamical proof is nothing but direct applications of the dynamical axioms (where variables are replaced by terms). So there are some drastic restrictions on dynamical proofs when compared to usual proofs. This is the reason why some algebraic consequences are more easily deduced from dynamical proofs than from usual ones.

In dynamical proofs, we can use some *valid dynamical rules*, i.e., deduction rules used in the same way as dynamical axioms, and provable from the axioms of the dynamical theory. A valid dynamical rule is of the type

$$H(\mathbf{x}) \vdash \exists \mathbf{y}_1 A_1(\mathbf{x}, \mathbf{y}_1) \ \vee \ \cdots \ \vee \ \exists \mathbf{y}_k \ A_k(\mathbf{x}, \mathbf{y}_k) \ .$$

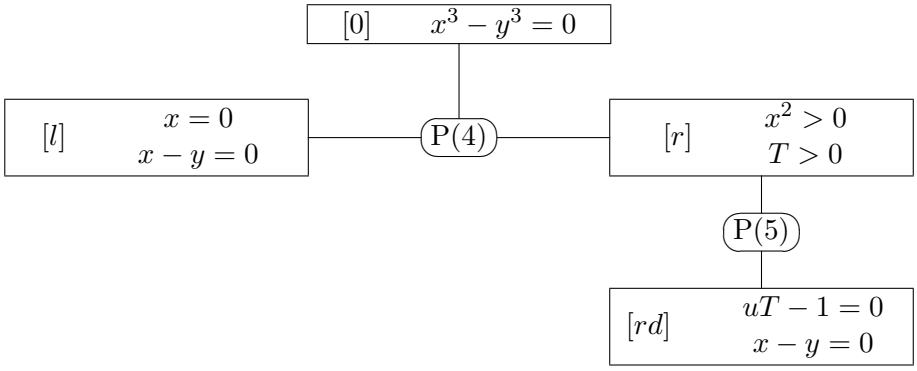
It is provable in $\mathcal{D}$ if there is a covering of the presentation $(\mathbf{x}; H)$ in $\mathcal{D}$ such that every leaf of this covering contains a valid fact $A_i(\mathbf{x}, \mathbf{t}_i)$, for some i and some list of terms $\mathbf{t}_i$.

Let us construct the tree of our prototype dynamical proof of $x^3 - y^3 = 0 \vdash x - y = 0$ in ordered fields. We use in particular the following properties of ordered fields:

$$\begin{array}{rcll} & \vdash & x^2 \geq 0 & P(1) \\ x > 0, \ y \geq 0 & \vdash & x + y > 0 & P(2) \\ x^2 = 0 & \vdash & x = 0 & P(3) \\ & \vdash & x = 0 \ \vee \ x^2 > 0 & P(4) \\ x > 0 & \vdash & \exists z \ zx - 1 = 0 & P(5) \end{array}$$

The tree consists of four nodes:

- The root of the tree: [0] where the generators are (x, y) and the relations are $(x^3 - y^3 = 0)$. Under the root, there are two nodes $[l]$ and $[r]$, using $P(4)$ ($x = 0$ or $x^2 > 0$).
  - $[l]$ where the generators are (x, y) and the relations are $(x^3 - y^3 = 0,\ x = 0,\ -y^3 = 0,\ y^4 = 0,\ y^2 = 0,\ y = 0,\ x - y = 0)$, (the last relations are a consequence of the first two, using $P(1), P(2), P(3)$ and computations in rings).
  - $[r]$ with presentation $((x, y); (x^3 - y^3 = 0, x^2 > 0, T > 0))$ where $T = 3x^2/4 + (y + x/2)^2 = x^2 + xy + y^2$. The fact $T > 0$ follows from $P(1)$ and $P(2)$. Under this node there is another node $[rd]$, where the inverse of T has been added according to $P(5)$.
    - $[rd]$ with presentation $((x, y, u); (x^3 - y^3 = 0, x^2 > 0, T > 0, uT = 1, x - y = 0))$, since $(x - y) = uT(x - y) = u(x^3 - y^3) = 0$.



Dynamical proofs prove facts and dynamical rules which are obviously valid in the first order theory $\mathcal{D}$. Actually they have the same strength as usual first order logic, for what may be expressed in this fragment.

Theorem 1.1 *Let $\mathcal{D}$ be a dynamical theory in the language $\mathcal{L}$, $(G; R)$ a presentation and $B(\mathbf{t})$ a fact of (G, R). There is a construction associating to every proof of $R \vdash B(\mathbf{t})$ in the classical first order theory $\mathcal{D}$ a dynamical proof of $B(\mathbf{t})$.*

Proof (sketch): In a dynamical theory, some elementary predicates are given in the language, but it is not possible to construct predicates using all logical connectives and quantifiers of first order logic. In order to get the full strength of usual first order theories, it is necessary to allow these constructions of predicates and their use with correct logical rules.

In this sketch of proof, we describe the introduction of new predicates corresponding to disjunction, existential quantifier and classical negation (with the law of the excluded middle). In each case, we prove that the correct use of a new predicate does not change provable facts. In classical logic (with the law of the excluded middle), all the predicates can be introduced with only these three constructions. So, if we have a classical proof of a fact, we shall consider two distinct dynamical theories, the first one is the given dynamical theory, the second one is a dynamical theory where all predicates used in the classical proof have a name as individual predicates. The classical proof is a dynamical proof in the second theory (with convenient axioms). Then deleting the new predicates one after the other, beginning by the more intricate ones, we see that when dealing with facts of the first dynamical theory, the two dynamical theories prove the same facts.

The first two lemmas about disjunction and existential quantification are very easy.

Lemma 1.2 *Assume that we have a dynamical theory $\mathcal{D}$ with some predicates $Q_1, \ldots, Q_k$. Consider a new dynamical theory $\mathcal{D}'$, with one more predicate Q, expressing the disjunction of $Q_1, \ldots, Q_k$ and the following axioms:*

$$\begin{array}{ll} Q_1 \vdash Q & Disj_{In,1}(Q_1, \ldots, Q_k, Q) \\ \ldots \vdash \ldots & \ldots \\ Q_k \vdash Q & Disj_{In,k}(Q_1, \ldots, Q_k, Q) \\ Q \vdash Q_1 \vee \ldots \vee Q_k & Disj_{El}(Q_1, \ldots, Q_k, Q) \end{array}$$

The dynamical theories $\mathcal{D}$ and $\mathcal{D}'$ prove the same facts that do not involve the predicate Q.

Proof: We remark that a fact $Q(\mathbf{t})$ in a dynamical proof inside $\mathcal{D}'$ can appear only after an application of an axiom $Disj_{In,j}(Q_1, \ldots, Q_k, Q)$ for some j $(1 \leq j \leq k)$. Consider the first use of the axiom $Disj_{El}(Q_1, \ldots, Q_k, Q)$ in the considered proof tree. It is clear that, if the predicate Q had not been introduced, we could get a simpler proof with only the branch corresponding to Q_j (replacing the k branches appearing after the use of $Disj_{El}(Q_1, \ldots, Q_k, Q)$). □

Lemma 1.3 *Assume that we have a dynamical theory $\mathcal{D}$ with some predicate $R(\mathbf{x}, y)$. Consider a new dynamical theory $\mathcal{D}'$, with one more predicate $S(\mathbf{x})$, expressing $\exists y\, R(\mathbf{x}, y)$, and the following axioms, where t is an arbitrary term:*

$$\begin{array}{rll} R(\mathbf{x}, t) & \vdash S(\mathbf{x}) & Exis_{In}(R, y, S, t) \\ S(\mathbf{x}) & \vdash \exists y\, R(\mathbf{x}, y) & Exis_{El}(R, y, S) \end{array}$$

The dynamical theories $\mathcal{D}$ and $\mathcal{D}'$ prove the same facts that do not involve the predicate S.

Proof: We remark that a fact $S(\mathbf{u})$ in a dynamical proof inside $\mathcal{D}'$ can appear only after an application of an axiom $Exis_{In}(R, y, S, t)$. Consider the first use of the axiom $Exis_{El}(R, y, S)$ in the considered proof tree. It is clear that, if the predicate S had not been introduced, we could get another proof by replacing y by the term t that allowed its introduction. □

The most difficult part of the proof is the following lemma about negation.

Lemma 1.4 *Assume that we have a dynamical theory $\mathcal{D}$ with some predicate $T(\mathbf{x})$. Consider a new dynamical theory $\mathcal{D}'$, with one more predicate $F(\mathbf{x})$, expressing the negation of $T(\mathbf{x})$ and the following axioms:*

$$\begin{array}{rll} & \vdash T(\mathbf{x}) \ \vee \ F(\mathbf{x}) & Neg_{In}(T, F) \\ T(\mathbf{x}),\ F(\mathbf{x}) & \vdash \bot & Neg_{El}(T, F) \end{array}$$

The dynamical theories $\mathcal{D}$ and $\mathcal{D}'$ prove the same facts that do not involve the predicate F.

Proof: Let us consider a fact $\vdash A(\mathbf{u})$ (where $\mathbf{u}$ is a list of terms) involving a predicate A distinct from F. Let us assume it is proved in the dynamical theory $\mathcal{D}'$. We have to transform this dynamical proof of $\vdash A(\mathbf{u})$ in another one, with no use of the predicate F. The proof tree of $\vdash A(\mathbf{u})$ has dead branches and branches ending with the fact $A(\mathbf{u})$. The predicate F is used in the proof by creating dead nodes, using the axiom $Neg_{El}(T, F)$. Consider one such dead node, and assume w.l.o.g. that the use of this axiom is the leftmost one in the proof-tree. (Here we assume that the tree is organized in such a manner that at each use of the axiom $Neg_{In}(T, F)$ the branch with T is the left- branch and the branch with F is the right-branch.) We call n the dead node, i.e., the node to which $Neg_{El}(T, F)$ is applied.

It suffices to prove that we can transform the proof tree and suppress this use of $Neg_{El}(T, F)$. Remark first that, if F is present in the tree at the left of n, it is useless in this part of the tree and it can be suppressed (i.e., the occurrences of $Neg_{In}(T, F)$ at the left of n can be suppressed, keeping only the right branch).

Since $F(\mathbf{t})$ (where $\mathbf{t}$ is a list of terms) is valid at the node n, it has necessarily been introduced by the use of axiom $Neg_{In}(T, F)$ at some node m above n. Two branches have thus been opened at the node m : the left one with $T(\mathbf{t})$, the right one with $F(\mathbf{t})$. The subtree $\mathcal{A}$ under $T(\mathbf{t})$ contains no use of $Neg_{El}(T, F)$ and proves $A(\mathbf{u})$ from $T(\mathbf{t})$ inside $\mathcal{D}$. On the other hand, $T(\mathbf{t})$ is a valid fact at the node n. So we proceed as follows:

- Suppress the use of $Neg_{In}(T, F)$ at the node m and keep only the right branch, suppressing $F(t)$ on the path between m an n and at the left of this path.
- Introduce the use of $Neg_{In}(T, F)$ at the beginning of each branch opened at the right of the path between m an n, gluing the subtree $\mathcal{A}$ as the left branch after this use of $Neg_{In}(T, F)$.

- Suppress the use of $Neg_{El}(T, F)$ at the node n, and glue the subtree $\mathcal{A}$ under this node.

□

These three lemmas complete the sketch of the proof of the theorem. □

We give now an example of elimination of negation. We consider the theory of ordered domains expressed with the only unary predicates $x = 0$ and $x \geq 0$.

The axioms we use are:

$$\begin{array}{rcll}
x = 0 & \vdash & xy = 0 & Alg(1, x, y) \\
x = 0 & \vdash & x \geq 0 & Alg(2, x) \\
x \geq 0,\ -x \geq 0 & \vdash & x = 0 & Alg(3, x) \\
x \geq 0,\ y \geq 0 & \vdash & x + y \geq 0 & Alg(4, x, y) \\
x \geq 0,\ y \geq 0 & \vdash & xy \geq 0 & Alg(5, x, y) \\
 & \vdash & x \geq 0 \vee -x \geq 0 & Dyn(1, x) \\
xy = 0 & \vdash & x = 0 \vee y = 0 & Dyn(2, x, y)
\end{array}$$

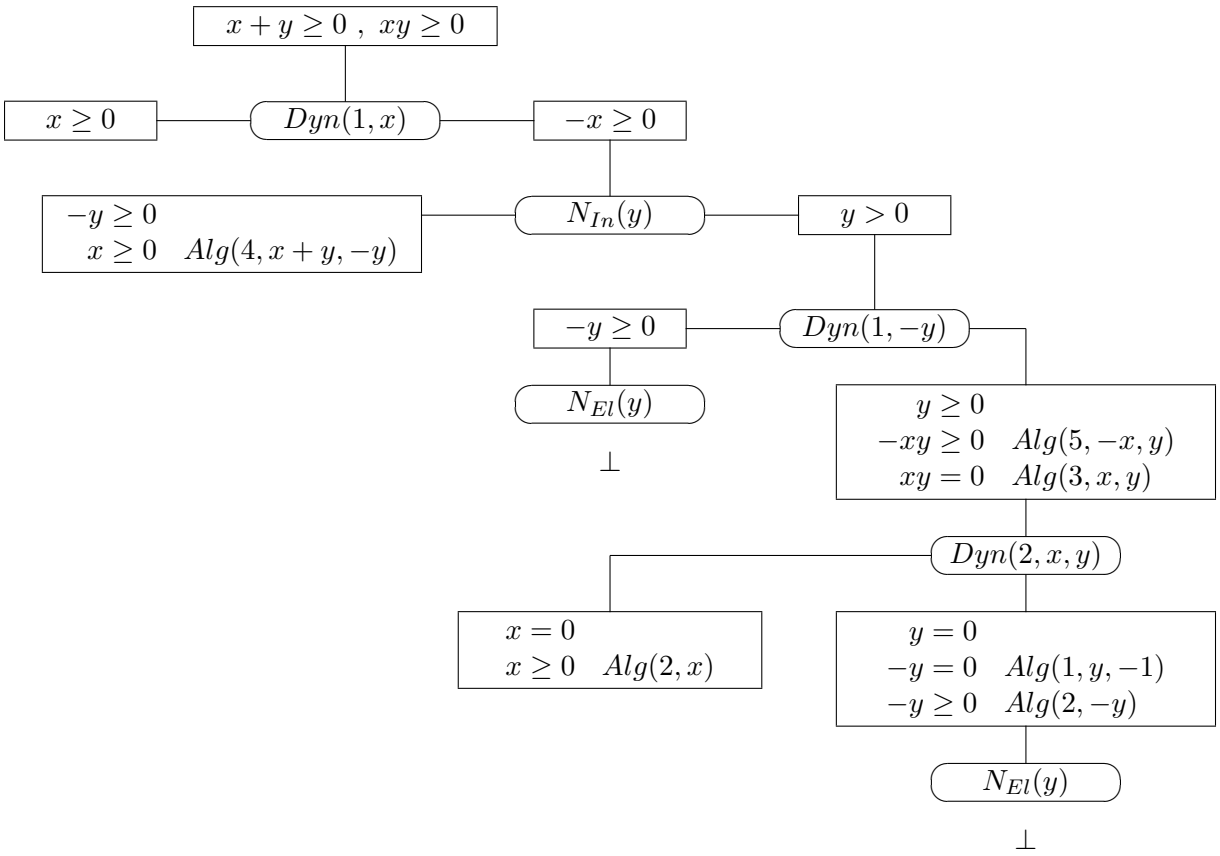
The predicate $x > 0$ is introduced as the predicate opposed to $-x \geq 0$ by the two defining axioms

$$\begin{array}{rcll}
 & \vdash & -x \geq 0 \vee x > 0 & N_{In}(x) \\
-x \geq 0,\ x > 0 & \vdash & \bot & N_{El}(x)
\end{array}$$

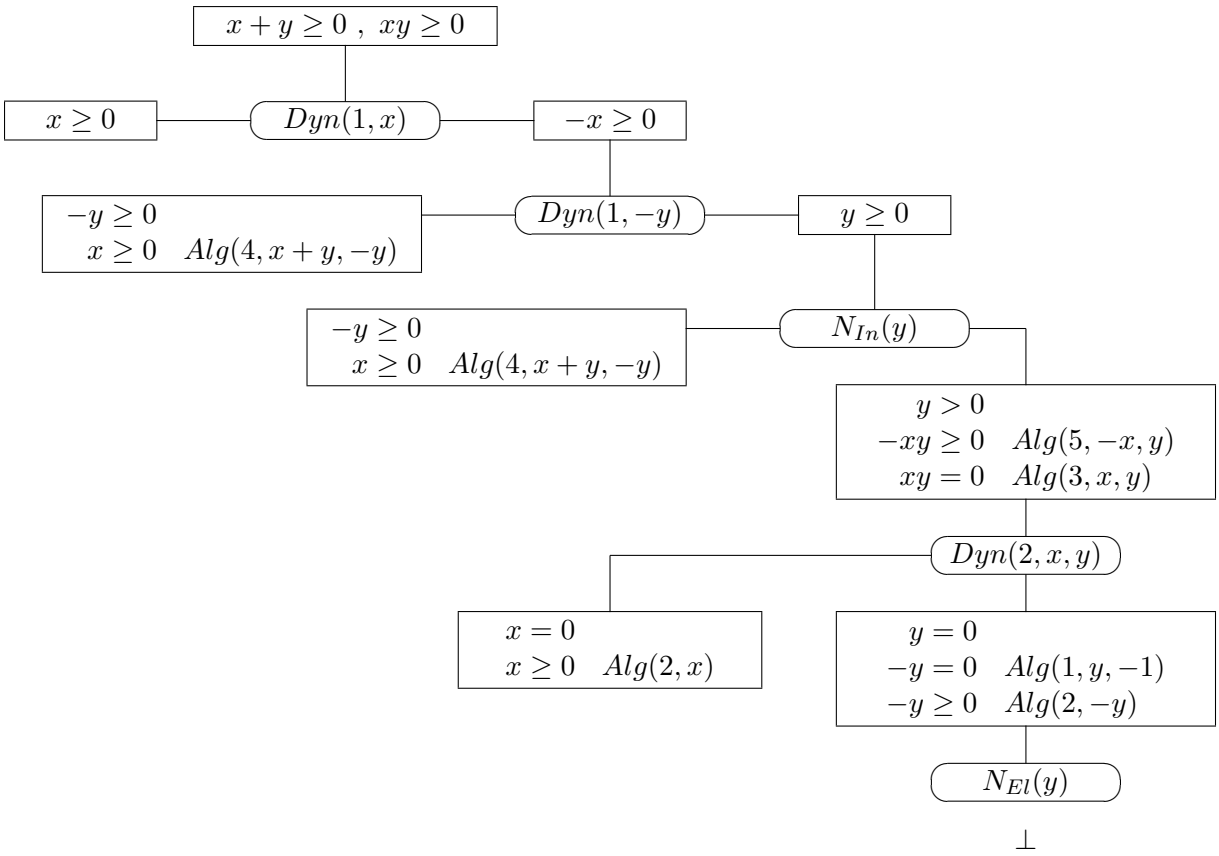
and it will be used to prove

$$x + y \geq 0,\ xy \geq 0 \quad \vdash \quad x \geq 0$$

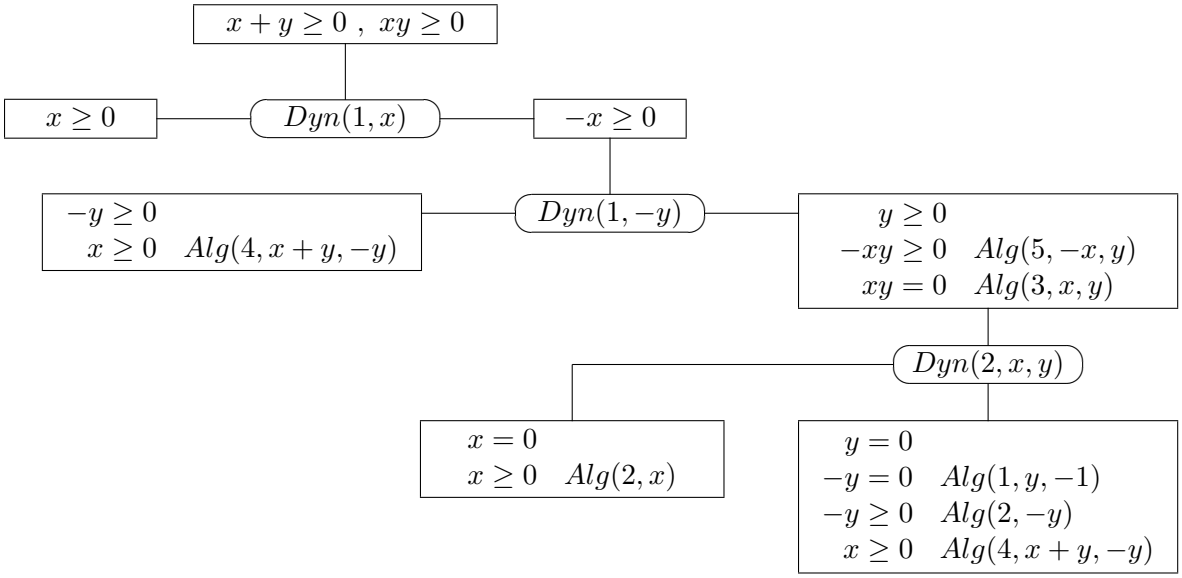
We want to transform the following proof (this is surely not a clever one):



We proceed in two steps. First we suppress the leftmost occurrence of $N_{El}(y)$.



It is now possible to suppress the last occurrence of $N_{El}(y)$ and not to use $N_{In}(y)$ anymore.



The theorem 1.1 can be seen as a "cut elimination theorem", with a constructive sense: there is a procedure to transform any proof of a fact in a deduction system for first order logic, into a dynamical proof. This seems very closely related to a lemma of Troelstra-Schwichtenberg (cf. proposition p. 84 in [33]) concerning intuitionnistic proof systems. A non-constructive proof via topos theory will be outlined in subsection 1.3.

1.2 Collapse

We consider now dynamical theories with one or several collapse axioms. Collapse axioms express that a particular fact (or conjunction of facts) involving only constants cannot be true in a model of $\mathcal{D}$. For example in an ordered field the collapse axiom is

$$0 > 0 \vdash \bot .$$

Definition 2 *A presentation* $(G; R)$ collapses *in the theory* $\mathcal{D}$ *when one has constructed a covering of* $(G; R)$ *in* $\mathcal{D}$ *where all branches finish with a dead node. Such a covering is a dynamical proof of* $R \vdash \bot$ *in* $\mathcal{D}$*, and will be called a* collapse of (G, R).

Remark that a collapse of a presentation $(G; R)$ gives a dynamical proof of any fact $B(t)$ in the presentation.

For example the presentation $((x, y), (x^3 - y^3 = 0, (x - y)^2 > 0))$ collapses in the theory of ordered fields: take the following dynamical proof

- [0] where the generators are (x, y) and the relations are $(x^3 - y^3 = 0, (x - y)^2 > 0)$,
  - $[l]$ where the generators are (x, y) and the relations are $(x^3 - y^3 = 0, (x - y)^2 > 0, x = 0, x - y = 0, 0 > 0)$, so that it is a dead node,
  - $[r]$ where the generators are (x, y) and the relations are $(x^3 - y^3 = 0, (x - y)^2 > 0, x^2 > 0, (3x^2/4 + (y + x/2)^2) > 0)$,
    - $[rd]$ where the generators are (x, y, z) and the relations are $(x^3 - y^3 = 0, (x - y)^2 > 0, x^2 > 0, (3x^2/4 + (y + x/2)^2) > 0, z(3x^2/4 + (y + x/2)^2) - 1 = 0, x - y = 0, 0 > 0)$, so that it is a dead node too.

Definition 3 *Let* $\mathcal{D}$ *and* $\mathcal{D}'$ *be two dynamical theories with the same language. We say that* $\mathcal{D}$ *and* $\mathcal{D}'$ collapse simultaneously *if for any presentation* $(G; R)$ *it is possible to construct a collapse of* (G, R) *in* $\mathcal{D}$ *from any collapse of* (G, R) *in* $\mathcal{D}'$*, and vice versa.*

Some dynamical theories that are very different may nevertheless collapse simultaneously. For example, we are going to prove that the theory of commutative rings with a proper monoid (see below section 2.2) and the theory of algebraically closed fields collapse simultaneously.

A stronger connection between dynamical theories is the following:

Definition 4 *Let* $\mathcal{D}$ *and* $\mathcal{D}'$ *be two theories with the same language. The theories* $\mathcal{D}$ *and* $\mathcal{D}'$ prove the same facts *if for any presentation* $(G; R)$ *and any fact* $B(t)$ *in this presentation, it is possible to construct a dynamical proof of* $R \vdash B(t)$ *in* $\mathcal{D}$ *from any dynamical proof of* $R \vdash B(t)$ *in* $\mathcal{D}'$*, and vice versa.*

For example, we are going to prove that the dynamical theories of ordered fields and of real closed fields prove the same facts, when written in the language of rings with three unary relations $x = 0$, $x > 0$ and $x \geq 0$.

1.3 Dynamical theories and coherent toposes

The concept of a dynamical theory has also been known in categorical logic under the name of *coherent theory*, and it is related to *coherent toposes*. This subsection is an extended remark to make this connection clear. Some familiarity with Grothendieck topologies and toposes is useful to read this subsection.

See for instance [28] for the relations between toposes and coherent theories.

Let us consider a dynamical theory $\mathcal{D}$ in a language $\mathcal{L}$, and let $\mathcal{D}_0$ be an algebraic subtheory of $\mathcal{D}$. We will associate to these data a site consisting of a category with finite projective limits, equipped

with a Grothendieck topology generated by finite coverings. The category $\mathbf{C}(\mathcal{D}_0)$ depends only on the algebraic subtheory $\mathcal{D}_0$, while the topology $\mathbf{T}(\mathcal{D})$ is associated to the extra dynamical axioms of $\mathcal{D}$.

The objects of $\mathbf{C}(\mathcal{D}_0)$ are finite presentations $(G;R)$ in the language $\mathcal{L}$. A morphism from $(G;R)$ to $(F;Q)$ will be a mapping φ from F to the set of terms of $\mathcal{L}$ built on G, such that for any relation $A(x_1,\dots,x_n)$ in Q (the x_i's are in F), the fact $A(\varphi(x_1),\dots,\varphi(x_n))$ is a consequence of the relations R in the theory $\mathcal{D}_0$. This syntactic description of $\mathbf{C}(\mathcal{D}_0)$ has obviously a semantic counterpart: $\mathbf{C}(\mathcal{D}_0)$ is (equivalent to) the dual of the category of finitely presented models of $\mathcal{D}_0$. This shows by the way that $\mathbf{C}(\mathcal{D}_0)$ has all finite projective limits.

It is easy to see that for any morphism $\varphi : (G,R) \to (F,Q)$, there is an isomorphism $(F \cup F', Q \cup Q') \to (G,R)$ such that the composition of φ with this isomorphism is the canonical morphism $(F \cup F', Q \cup Q') \to (F,Q)$.

Consider now an extra dynamical axiom of $\mathcal{D}$:

$$H(\mathbf{x}) \vdash \exists \mathbf{y}_1\, A_1(\mathbf{x},\mathbf{y}_1) \vee \dots \vee \exists \mathbf{y}_k\, A_k(\mathbf{x},\mathbf{y}_k)\ .$$

To this axiom we associate the finite family of the k obvious arrows in $\mathbf{C}(\mathcal{D}_0)$ with common target $(\mathbf{x};H)$ and sources $(\mathbf{x}\cup\mathbf{y}_i; H\cup A_i)$ for $i=1,\dots,k$. These finite families associated to axioms generate the coverings of a topology $\mathbf{T}(\mathcal{D})$ on $\mathbf{C}(\mathcal{D}_0)$, according to the following rules:

1. The identity $f : M \to M$ is a covering of M.
2. Let $(g_j : N_j \to N)_{j=1,\dots,k}$ be a covering of N. Let $\varphi : M \to N$ be any morphism, and let

$$\begin{array}{ccc} M_j & \xrightarrow{f_j} & M \\ \downarrow & & \downarrow\varphi \\ N_j & \xrightarrow{g_j} & N \end{array}$$

   be cartesian squares for $j=1,\dots,k$. Then the family $(f_j : M_j \to M)_{j=1,\dots,k}$ is a covering of M
3. Let $(f_i : M_i \to M)_{i\in I}$ be a covering of M, and for each i let $(g_{i,j} : N_{i,j} \to M_i)_{j=1,\dots,k_i}$ be a covering of M_i. Then the family $(f_i \circ g_{i,j} : N_{i,j} \to M)_{i,j}$ is a covering of M.
4. Let $(f_i : M_i \to M)_{i\in I}$ be a covering of M. If $(g_j : N_j \to M)_{j\in J}$ is another family such that there is an application $\mu : I \to J$, and for each i a morphism $\rho_i : M_i \to N_{\mu(i)}$ satisfying $g_{\mu(i)} \circ \rho_i = f_i$, then $(g_j)_{j\in J}$ is also a covering of M.

It is easy to see that, in the generation of coverings for the topology, this fourth rule can always be used in the last place.

Of course, these rules (at least the first three) parallel the rules of construction of coverings of a presentation (G,R) in $\mathcal{D}$. This implies that the family

$$\Big((G\cup F_j; R\cup Q_j) \longrightarrow (G;R)\Big)_{j=1,\dots,k}$$

is a covering for the topology if and only if there is a covering of the presentation $(G;R)$ such that every leaf contains one of the presentations $(G\cup F_j; R\cup Q_j)$, for $j=1,\dots,k$. Stated in another way, the "sequent"

$$H(\mathbf{x}) \vdash \exists \mathbf{y}_1\, A_1(\mathbf{x},\mathbf{y}_1) \vee \dots \vee \exists \mathbf{y}_k\, A_k(\mathbf{x},\mathbf{y}_k)$$

is a valid dynamical rule in $\mathcal{D}$ if and only if the family

$$((\mathbf{x}\cup\mathbf{y}_i; H\cup A_i) \longrightarrow (\mathbf{x},H))_{i=1,\dots,k}$$

is a covering for the topology $\mathbf{T}(\mathcal{D})$.

Once we have the category $\mathbf{C}(\mathcal{D}_0)$ and its topology $\mathbf{T}(\mathcal{D})$, we can define the sheaves on it. The category of these sheaves is a Grothendieck topos $\mathbf{E}(\mathcal{D})$, which is known in categorical logic as *the*

classifying topos of the theory $\mathcal{D}$. It is a coherent topos since the topology $\mathbf{T}(\mathcal{D})$ is generated by finite coverings. There is a canonical functor $\epsilon : \mathbf{C}(\mathcal{D}_0) \to \mathbf{E}(\mathcal{D})$ which sends the object M of $\mathbf{C}(\mathcal{D}_0)$ to the sheaf associated to the presheaf $\hom_{\mathbf{C}(\mathcal{D}_0)}(-, M)$. A family $(f_i : M_i \to M)_{i\in I}$ is carried by ϵ to a surjective family if and only if it is a covering for the Grothendieck topology $\mathbf{T}(\mathcal{D})$.

It is possible to define what is a model of a coherent (or dynamic) theory $\mathcal{D}$ in a topos, and inverse images of geometric morphisms of toposes carry models of $\mathcal{D}$ to models of $\mathcal{D}$. The classifying topos $\mathbf{E}(\mathcal{D})$ comes equipped with a model $\mathbf{M}(\mathcal{D})$ of the theory $\mathcal{D}$, which is *generic* in the following sense: for any model $\mathcal{M}$ of $\mathcal{D}$ in any topos $\mathcal{E}$, there is a geometric morphism of toposes $f : \mathcal{E} \to \mathbf{E}(\mathcal{D})$ such that $\mathcal{M}$ is isomorphic to $f^*(\mathbf{M}(\mathcal{D}))$. It is easy to describe what is the generic model of $\mathcal{D}$ in the presentation of the classifying topos we gave. The assignment, to any presentation $(G; R)$, of the model of $\mathcal{D}_0$ with this presentation defines a presheaf of models of $\mathcal{D}_0$ on $\mathbf{C}(\mathcal{D}_0)$. The sheaf associated to this presheaf for the topology $\mathbf{T}(\mathcal{D})$ is the generic model of $\mathcal{D}$. In other words, the generic model is the image by ϵ of the presentation $(z; \emptyset)$ (where z is one variable).

It follows from the interpretation of the language in the generic model of $\mathcal{D}$ that a "sequent"

$$H(\mathbf{x}) \vdash \exists \mathbf{y}_1\, A_1(\mathbf{x}, \mathbf{y}_1) \vee \cdots \vee \exists \mathbf{y}_k\, A_k(\mathbf{x}, \mathbf{y}_k)$$

is valid in the generic model if and only if the family of morphisms

$$((\mathbf{x} \cup \mathbf{y}_i; H \cup A_i) \longrightarrow (\mathbf{x}, H))_{i=1,\ldots,k}$$

in $\mathbf{C}(\mathcal{D}_0)$ is sent by ϵ to a surjective family, i.e., if and only if it is a covering for the topology $\mathbf{T}(\mathcal{D})$. By what was said before, this is equivalent to the fact that the sequent is a valid dynamical rule in $\mathcal{D}$. We can then get a non-constructive version of theorem 1.1 from a theorem of Deligne asserting that "a coherent topos has enough points". A point of the topos $\mathbf{E}(\mathcal{D})$ is a geometric morphism from the topos of sets to $\mathbf{E}(\mathcal{D})$, so it corresponds to a set-theoretic model of $\mathcal{D}$. Deligne's theorem says that the "sequent"

$$H(\mathbf{x}) \vdash \exists \mathbf{y}_1\, A_1(\mathbf{x}, \mathbf{y}_1) \vee \cdots \vee \exists \mathbf{y}_k\, A_k(\mathbf{x}, \mathbf{y}_k)$$

is valid in the generic model of $\mathcal{D}$ if and only if it is valid in any set- theoretic model of $\mathcal{D}$. In conclusion, the sequents valid in every (set- theoretic) model of $\mathcal{D}$ are exactly the valid dynamical rules.

A collapse axiom in a dynamical theory $\mathcal{D}$ gives, by the construction of the topology $\mathbf{T}(\mathcal{D})$, an empty covering of a subobject U of the terminal object $(\emptyset; \emptyset)$ in $\mathbf{C}(\mathcal{D}_0)$. If $\mathcal{D}$ consists of $\mathcal{D}_0$ plus a collapse axiom, then the classifying topos for $\mathcal{D}$ is a closed subtopos of the topos of presheaves $\mathbf{C}(\mathcal{D}_0)\hat{}$, complement to $\epsilon(U)$.

In the presentation of dynamical proofs and collapses, we have considered possibly infinite presentations $(G; R)$ to start with. To deal with this situation, one may add to the language the generators in G as new constants and the relations in R as new axioms to $\mathcal{D}$ (or $\mathcal{D}_0$). We denote by $(G; R)/\mathcal{D}$ the dynamical theory thus obtained (whose models are those of $\mathcal{D}$ "under" $(G; R)$). We can then construct a site as above, and a classifying topos $\mathbf{E}((G; R)/\mathcal{D})$.

Now we can take into account, in this topos- theoretic setting, the non-constructive aspects of the collapse of a presentation $(G; R)$ in the theory $\mathcal{D}$: it collapses if and only if the classifying topos $\mathbf{E}((G; R)/\mathcal{D})$ is the trivial topos, where the initial object is also terminal. In case that the presentation $(G; R)$ is finite, it means also that the object $(G; R)$ has an empty covering in the topology $\mathbf{T}(\mathcal{D})$, or equivalently that its image in the classifying topos of $\mathcal{D}$ is the initial object 0.

It is also possible to describe the simultaneous collapsing along the same lines. For simplicity we shall consider two dynamical theories $\mathcal{D}$ and $\mathcal{D}'$ in the same language, with $\mathcal{D}$ a subtheory of $\mathcal{D}'$. This gives a geometric morphism $f : \mathbf{E}(\mathcal{D}') \to \mathbf{E}(\mathcal{D})$ ($\mathbf{T}(\mathcal{D}')$ is finer than $\mathbf{T}(\mathcal{D})$). Forgetting the constructive aspects, we get:

Proposition 1.5 *The theories $\mathcal{D}$ and $\mathcal{D}'$ collapse simultaneously if and only if, for every object X of $\mathbf{E}(\mathcal{D})$, $f^*(X) = 0$ implies $X = 0$ (i.e., f^* reflects the initial object).*

So the simultaneous collapsing is in some sense independent of the syntax, since it can be formulated only in terms of the classifying toposes. In the topos- theoretic framework, the "syntax" means the

choice of the site $\mathbf{C}(\mathcal{D}_0)$ defining the topos $\mathbf{E}(\mathcal{D})$ (or more precisely its image in $\mathbf{E}(\mathcal{D})$ by the functor ε). In this sense, the stronger relation of "proving the same facts" depends on the syntax. Let us take an ad- hoc example. Consider the theories of commutative rings with a proper multiplicative monoid whose elements are not zero divisors (resp. are invertible). If these two theories are formulated in the language with one unary relation symbol for the monoid, they prove the same facts: indeed, the morphism from a ring A to its ring of fractions $M^{-1}A$ is injective if the monoid M contains no zero divisor. On the other hand, if one adds another unary relation symbol interpreted as "being invertible", the two theories no longer prove the same facts.

Two theories $\mathcal{D}$ and $\mathcal{D}'$ as in the proposition prove the same facts if and only if every monomorphism in $\mathbf{C}(\mathcal{D}_0)$ which becomes an isomorphism in $\mathbf{E}(\mathcal{D}')$ already becomes an isomorphism in $\mathbf{E}(\mathcal{D})$. If every monomorphism of $\mathbf{C}(\mathcal{D}_0)$ becomes complemented in $\mathbf{E}(\mathcal{D})$, then simultaneous collapsing implies proving the same facts.

2 Hilbert's Nullstellensatz

2.1 Direct theories

We begin this section by a discussion about the theory of rings.

The *unary language of rings* $\mathcal{L}_r$ has constants 0, 1, -1 and binary functions $+$ and $\times$ and only one unary relational symbol $= 0$. As usual, $x \times y$ will often be denoted by xy, $-t$ will stand for $(-1) \times t$ and $s - t$ for $s + (-t)$.

The *theory of rings* i.e., the purely equational theory of commutative rings, expressed in this language will be denoted $\mathcal{R}_r$.

In this setting, a presentation in the language is nothing but a set of variables G and a set of polynomials $R_{=0} \subset \mathbf{Z}[G]$, with relations $p(G) = 0$ for $p(G) \in R_{=0}$. We denote it by $(G; R_{=0})$.

We see immediately that terms provably $= 0$ in $\mathcal{R}_r$ (for the presentation we consider) are just the polynomials belonging to the ideal of $\mathbf{Z}[G]$ generated by $R_{=0}$.

In other words:

- we manipulate polynomials in $\mathbf{Z}[G]$ rather than terms of the language $\mathcal{L}_r$,
- addition and multiplication are directly defined as operations on polynomials (this hides logical axioms of rings behind algebraic computations in $\mathbf{Z}[G]$),
- the only relation is the unary relation $x = 0$,
- we do not have the binary equality relation, $x = y$ is only an abbreviation for $x - y = 0$,
- the only axioms are three very simple algebraic axioms:

$$\begin{array}{rll} & \vdash 0 = 0 & D(1)_r \\ x = 0,\ y = 0 & \vdash x + y = 0 & D(2)_r \\ x = 0 & \vdash xy = 0 & D(3)_r \end{array}$$

This reformulation of the theory of rings is exactly what we need for Nullstellensätze as we shall see soon.

This leads us to the notion of *direct theory.*

A *direct algebraic axiom* is an axiom of the form

$$A_1(x_1), \cdots, A_k(x_k) \vdash A(t(x_1, \ldots, x_k))$$

where the A_i and A are unary relation symbols, the x_i are distinct variables and $t(x_1, \ldots, x_k)$ is a term of the language.

For example the axioms

$$x > 0,\ y > 0 \vdash x + y > 0 \qquad \text{and} \qquad \vdash x^2 \geq 0$$

are direct algebraic axioms, while

$$x \geq 0,\ x \neq 0 \vdash x > 0 \qquad \text{and} \qquad x^2 > 0 \vdash x \neq 0$$

are not direct algebraic axioms: the first one because x appears twice on the left, the second because x^2 is not a variable.

Now we say that a purely equational theory *is put in unary form* when we have replaced syntactical terms by objects of free algebraic structures (free w. r. t. equational axioms), binary equality relation by a unary one (the old binary equality with a fixed constant in right-hand side), and equational axioms by two ingredients: computations in the free algebraic structure on the one hand and some direct algebraic axioms on the other hand (as we did for theory of rings). A *simple collapse axiom* is a collapse axiom of the form

$$A(c) \vdash \bot$$

where A is a unary relation symbol and c is a constant

A *direct theory* is a dynamical theory based on a purely equational theory put in unary form, allowing as other axioms only direct algebraic axioms and exactly one simple collapse axiom.

We now write down the axioms of non-trivial rings.

A *non-trivial ring* is a ring where $1 = 0$ is impossible. The corresponding theory, expressed in the language $\mathcal{L}_r$, is the direct theory extending $\mathcal{R}_r$ by adding only a simple collapse axiom:

$$1 = 0 \quad \vdash \bot \qquad\qquad C_r$$

Proposition 2.1 *Let $(G; R_{=0})$ be a presentation in the language of rings. A collapse of the presentation $(G; R_{=0})$ in the theory of non-trivial rings produces an equality $1 = a_1 i_1 + \cdots + a_k i_k$ in $\mathbf{Z}[G]$ with i_j in $R_{=0}$. Reciprocally, such an equality produces a collapse of $(G; R_{=0})$.*

Proof: In a direct theory, such as the theory of non-trivial rings, the only dynamical axiom is the axiom of collapse. So proofs have a very simple structure "without branches". The elements of $\mathbf{Z}[G]$ which are provable $= 0$ without using the collapse axiom (in the presentation $(G; R_{=0})$) are exactly elements of the form $a_1 i_1 + \cdots + a_k i_k$ with i_j in $R_{=0}$. This is clear by induction on the number of times the direct algebraic axioms are used in the proof. We can apply the collapse axiom only after such a proof of $1 = 0$. So the presentation collapses in the theory of non-trivial rings if and only if there exists an algebraic identity $1 - (a_1 i_1 + \cdots + a_k i_k) = 0$ in $\mathbf{Z}[G]$ with i_j in $R_{=0}$. □

2.2 Some simultaneous collapses

We consider the *unary language of fields* $\mathcal{L}_f$, which is the unary language of rings with a new unary relation $\neq 0$. A presentation in the language $\mathcal{L}_f$ consists of two sets $(R_{=0}, R_{\neq 0})$ of polynomials in $\mathbf{Z}[G]$ with relations $p(G) = 0$ for $p(G) \in R_{=0}$ and $p(G) \neq 0$ for $p(G) \in R_{\neq 0}$. We denote it by $(G; R_{=0}, R_{\neq 0})$.

A *ring with a proper monoid* is a ring with a multiplicative monoid not containing 0. It is the same as a realization of the language $\mathcal{L}_f$ satisfying the axioms of rings and the following axioms

$$\begin{array}{rll} x = 0,\ y \neq 0 & \vdash x + y \neq 0 & D(1)_f \\ x \neq 0,\ y \neq 0 & \vdash xy \neq 0 & D(2)_f \\ & \vdash\ 1 \neq 0 & D(3)_f \\ 0 \neq 0 & \vdash \bot & C_f \end{array}$$

where the proper monoid is the realization of the unary relation $\neq 0$. Note that a non-trivial ring is a ring with a proper monoid, the proper monoid being $\{1\}$.

Direct algebraic axioms are denoted by D and collapse axioms by C. Remark that axiom $D(1)_f$ is a disguised axiom of stability of the relation $\neq 0$ for equality, written using only unary predicates.

Considering axiom $D(3)_f$ we see that the collapse axiom of non-trivial rings is a valid dynamical rule in rings with proper monoid.

Adding three extra axioms we get the axioms of the theory of *fields*:

$$\begin{array}{rll} xy-1=0 & \vdash\ x\neq 0 & S(1)_f \\ x\neq 0 & \vdash\ \exists y\ xy-1=0 & Dy(1)_f \\ & \vdash\ x=0\ \vee\ x\neq 0 & Dy(2)_f \end{array}$$

The first axiom is a *simplification axiom*: an algebraic axiom but not a direct algebraic one. The two last ones are dynamical axioms.

The theory of *algebraically closed fields* is obtained by adding a scheme of axioms. For every degree n we have the axiom:

$$\vdash\ \exists y\ y^n + x_{n-1}y^{n-1} + \cdots + x_1 y + x_0 = 0 \quad Dy_n(3)_f$$

The theory of rings with proper monoid has been chosen because as we shall see later it is a direct theory which collapses simultaneously with the theory of algebraically closed fields.

The collapse in the theory of rings with proper monoid has a very simple form:

Proposition 2.2 *Let $\mathcal{K} = (G; R_{=0}, R_{\neq 0})$ be a presentation in the language $\mathcal{L}_f$. A collapse of the presentation $\mathcal{K}$ in the theory of rings with proper monoid produces an equality in $\mathbf{Z}[G]$:*

$$m_1 \cdots m_\ell + a_1 i_1 + \cdots + a_k i_k = 0$$

with m_j in $R_{\neq 0}$ and i_j in $R_{=0}$. Reciprocally, such an equality produces a collapse of $\mathcal{K}$.

Proof: First consider dynamical proofs of facts using *only direct algebraic axioms*. These are algebraic proofs without branching. The elements of $\mathbf{Z}[G]$ which are provable $= 0$ in the presentation $(G; R_{=0}))$ are exactly elements of the form $a_1 i_1 + \cdots + a_k i_k$ with i_j in $R_{=0}$. This is clear by induction on the number of times the direct algebraic axioms are used in the proof. Then provably $\neq 0$ elements are exactly elements of the form $m_1 \cdots m_\ell + a_1 i_1 + \cdots + a_k i_k$ with $m_j \in R_{\neq 0}$ and $i_j \in R_{=0}$ (same inductive proof).

Now a proof of collapse is given by a proof of $0 \neq 0$ using only direct algebraic axioms. It produces an equality $m_1 \cdots m_\ell + a_1 i_1 + \cdots + a_k i_k = 0$ in $\mathbf{Z}[G]$ with m_j in $R_{\neq 0}$ and i_j in $R_{=0}$. □

The content of the preceding proposition is that the collapse of a presentation in the direct theory we consider may be certified by an algebraic identity of some type. We will try in the following remark to analyze the ingredients we used to establish this property, and we will check in the other sections that these ingredients are again at work.

Remark 2.3 There is an ordering on the predicates, which appears in the proof of Proposition 2.2. First comes $= 0$, then $\neq 0$. This appears also in the syntactic description of the theory of rings with proper monoid. We can see the axioms $D(i)_r$ as *construction axioms* for $= 0$, and the axioms $D(i)_f$ as construction axioms for $\neq 0$. The rule is that, in a construction axiom for a predicate Q (with Q appearing at the right side of $\vdash$), another predicate P may appear at the left of $\vdash$ only if P precedes Q. The collapse of the direct theory involves the last predicate. It appears that, when this scheme is present, a collapse of a presentation in the direct theory produces an algebraic identity of a certain type, certifying the collapse.

So we have algebraic identities certifying collapses in a direct theory. We are not interested in this theory, but in some of its extensions. It remains to obtain a result of simultaneous collapsing.

Theorem 2.4 *The theory of rings with a proper monoid, the theory of fields and the theory of algebraically closed fields collapse simultaneously.*

Proof: The proof is by induction on the number of times the axioms of algebraically closed fields $S(1)_f$, $Dy(1)_f$, $Dy(2)_f$ and $Dy_n(3)_f$ are used in the proof. We have to see that if after one use of such an axiom we get a collapse of the new presentations in the theory of rings with a proper monoid then we can also get the collapse of the preceding presentation in the same theory.

Thus the theorem is an immediate consequence of the following lemma. □

Before stating and proving the lemma, we introduce some conventional abuse of notations to be used when the context is clear.

Notation 2.5 Assume we have a presentation $\mathcal{K} = (G; R_{=0}, R_{\neq 0})$, z is a new variable, p, q are in $\mathbf{Z}[G]$, $r(z)$ and $s(z)$ are in $\mathbf{Z}[G][z]$, then the presentation $(G \cup \{z\}; R_{=0} \cup \{p, r(z)\}, R_{\neq 0} \cup \{q, s(z)\})$ will be denoted by $\mathcal{K} \cup (p = 0, r(z) = 0, q \neq 0, s(z) \neq 0)$

Lemma 2.6 *Let $\mathcal{K} = (G; R_{=0}, R_{\neq 0})$ be a presentation in the language $\mathcal{L}_f$. Let $p, r \in \mathbf{Z}[G]$. Let z be a new variable and $q(z)$ a monic non-constant polynomial in $\mathbf{Z}[G][z]$.*

a) If the presentation $\mathcal{K} \cup (p \neq 0)$ collapses in the theory of rings with proper monoid, so does the presentation $\mathcal{K} \cup (pr - 1 = 0)$

b) If the presentation $\mathcal{K} \cup (pz - 1 = 0)$ collapses in the theory of rings with proper monoid, so does the presentation $\mathcal{K} \cup (p \neq 0)$

c) If the presentations $\mathcal{K} \cup (p = 0)$ and $\mathcal{K} \cup (p \neq 0)$ collapse in the theory of rings with proper monoid, so does the presentation $\mathcal{K}$.

d) If the presentation $\mathcal{K} \cup (q(z) = 0)$ collapses in the theory of rings with proper monoid, so does the presentation $\mathcal{K}$.

Proof: Denote by $\mathcal{I}_{=0}$ the ideal of $\mathbf{Z}[G]$ generated by $R_{=0}$ and by $\mathcal{M}_{\neq 0}$ the monoid generated by $R_{\neq 0}$.

a) We have an identity $p^n m = i$ with m is in $\mathcal{M}_{\neq 0}$ and $i \in \mathcal{I}_{=0}$. We can multiply it by r^n. We can write $1 - (pr)^n = (pr - 1)s$ so that $m = (1 - (pr)^n)m + ir^n = (pr - 1)sm + ir^n$, which produces a collapse of $\mathcal{K} \cup (pr - 1 = 0)$

b) This is Rabinovitch's trick. Suppose we have a collapse of the presentation $\mathcal{K} \cup (pz - 1 = 0)$. This is written in the form $m = j(z) + (pz - 1)s(z)$, where m is in $\mathcal{M}_{\neq 0}$, j is a polynomial with coefficients in $\mathcal{I}_{=0}$ and s is a polynomial with coefficients in $\mathbf{Z}[G]$. If n is the z-degree of j, multiply both sides by p^n and replace in $p^n j(z)$ all the $p^k z^k$ by 1 modulo $(pz - 1)$. After this transformation, we obtain an equality $p^n m = i + (pz - 1)s_1(z)$ in $\mathbf{Z}[G, z]$, where $i \in \mathcal{I}_{=0}$. We can assume that p is not $0 \in \mathbf{Z}[G]$, otherwise $\mathcal{K} \cup (p \neq 0)$ collapses trivially. It follows that $p^n m = i$, which is the collapse we are looking for.

c) Since the presentation $\mathcal{K} \cup (p \neq 0)$ collapses, we have an equality $mp^n = i$ in $\mathbf{Z}[G]$ with $m \in \mathcal{M}_{\neq 0}$ and $i \in \mathcal{I}_{=0}$. Similarly we have an equality $v = i' + pa$ in $\mathbf{Z}[G]$ with $v \in \mathcal{M}_{\neq 0}$ and $i' \in \mathcal{I}_{=0}$. So we get equalities in $\mathbf{Z}[G]$

$$ia^n = mp^n a^n = m(v - i')^n = mv^n + i_2$$

with $i_2 \in \mathcal{I}_{=0}$, which gives $mv^n + i_3 = 0$ with $mv^n \in \mathcal{M}_{\neq 0}$ and $i_3 = i_2 - ia^n \in \mathcal{I}_{=0}$.

d) We suppose that there is an equality in $\mathbf{Z}[G, z]$ of the form

$$m + \sum_i r_i a_i(z) + q(z)a(z) = 0 \tag{1}$$

where the r_i belong to $R_{=0}$ and m belongs to $\mathcal{M}_{\neq 0}$, the monoid generated by $R_{\neq 0}$. Dividing the a_i by the monic polynomial q, we get an algebraic identity

$$m + \sum_i r_i b_i(z) + q(z)b(z) = 0 \tag{2}$$

where the b_i are of degree smaller that $\deg(q)$ in z. So $b(z) = 0$ and

$$m + \sum_i r_i b_i(0) = 0 \tag{3}$$

which is the collapse we are looking for. □

Remark 2.7 This kind of result is particularly easy because we have stated an algebraic form of collapse (in proposition 2.2). The algebraic computation constructing a collapse from several other ones is in fact present (and often hidden) in classical proofs of "embedding theorems" as "every proper ideal is contained in a prime ideal" or "every field is embeddable in an algebraically closed field".

The proofs of simultaneous collapsing that we will encounter in this paper will always use this technique of lifting algebraic identities certifying the collapses along the extra dynamical axioms.

All examples we give in this paper present simultaneous collapsing between a dynamical theory and some direct subtheory. It would be interesting to have general criteria for such a simultaneous collapsing.

As an immediate consequence of theorem 2.4 we get:

Corollary 2.8 *(constructive versions of non-constructive embedding theorems) Let A be a ring. If the diagram of A collapses in the theory of algebraically closed fields, then A is trivial. In particular we get:*

a) Let A be a non-trivial ring. The diagram of A does not collapse in the theory of fields.

b) Let K be a field. The diagram of K does not collapse in the theory of algebraically closed fields.

In this proposition, the claim a) is a constructive version of the following result: "if a ring is non-trivial, it has a prime ideal".

In the same way, the claim b) is a constructive version of the fact that "every field can be embedded in an algebraically closed field".

Constructive versions of embedding results similar to the ones stated above are announced in a note by Joyal [16]. They rely on a lattice-theoretic description of the spectrum of a ring.

Theorem 2.4 can also be settled in the following form.

Proposition 2.9 *Let $\mathcal{K} = (G; R_{=0}, R_{\neq 0})$ be a presentation in the language $\mathcal{L}_f$. A collapse of the presentation $\mathcal{K}$ in the theory of algebraically closed fields produces an equality $m_1 \cdots m_\ell + a_1 i_1 + \cdots + a_k i_k = 0$ with m_j in $R_{\neq 0}$ and i_j in $R_{=0}$.*

We can deduce from this last result a non-constructive formal version of Hilbert Nullstellensatz.

Proposition 2.10 *Let A be a ring, and $R_{=0}$ and $R_{\neq 0}$ families of elements of A. Denote by $\mathcal{I}_{=0}$ the ideal generated by $R_{=0}$ and by $\mathcal{M}_{\neq 0}$ the monoid generated by $R_{\neq 0}$. The following properties are equivalent:*

i) There exist $i \in \mathcal{I}_{=0}$ and $m \in \mathcal{M}_{\neq 0}$ with $i + m = 0$

ii) There exists no homomorphism $\phi : A \to L$ with L an algebraically closed field, $\phi(i) = 0$ for $i \in R_{=0}$ and $\phi(m) \neq 0$ for $m \in R_{\neq 0}$.

iii) There exists no prime ideal I containing $\mathcal{I}_{=0}$ and not intersecting $\mathcal{M}_{\neq 0}$.

Proof: Use the preceding result taking as presentation $\mathcal{DG}(A) \cup (\emptyset; R_{=0}, R_{\neq 0})$, and apply the non-constructive completeness theorem of model theory. □

2.3 Decision algorithm and constructive Nullstellensatz

Since the theory of algebraically closed fields has a decision algorithm for determining emptiness of sets defined by equations and negations of equations which is particularly simple, we are able to prove the following:

Proposition 2.11 *Let K be a field and $R_{=0}$, $R_{\neq 0}$ two finite families of polynomials of $K[x_1, \ldots, x_n]$. There is a decision algorithm answering yes or no to the question "does the presentation $\mathcal{DG}(K) \cup (\{x_1, \ldots, x_n\}; R_{=0}, R_{\neq 0})$ implies $\perp$ in the theory of algebraically closed fields ?" If the answer is yes, the algorithm produces a collapse of the presentation in the theory of fields.*

Proof: We assume that, from a constructive point of view, all our fields are discrete. This means that we have a way of deciding exactly if an element is zero or not. Precisely, G_1 being the finite set of coefficients of polynomials belonging to $R_{=0} \cup R_{\neq 0}$, we can decide for any $\mathbf{Z}$-polynomial whether it vanishes or not when evaluated on G_1 in K.

We give a sketch of an elementary decision algorithm, very near to dynamical evaluation in the dynamical constructible closure of a field (see [15]).

We deal first with only one variable x, and we show that any finite set of constraints $(p_i(x) = 0)_{1 \leq i \leq h}$, $(q_j(x) \neq 0)_{1 \leq j \leq k}$ (h and k are natural integers) is equivalent to only one constraint. Moreover the equivalence is provable by a dynamical proof within the theory of fields.

If $h > 0$, the constraints $(p_i(x) = 0)_{1 \leq i \leq h}$ are equivalent to a single one $p(x) = 0$ where p is some gcd of p_i's. We remark that the computation of p by Euclid's algorithm is a computation in the fraction field of the ring $\mathbf{Z}[G_1] \subset K$. Using pseudo-remainders instead of remainders we have a computation within $\mathbf{Z}[G_1]$. We get a Bezout relation $\gamma p = a_1 p_1 + \ldots a_h p_h$, and divisibility relations $\alpha_i p_i = b_i p$ (greek letters mean non-zero elements of K). So dynamical proofs of

$$\mathcal{DG}(K),\ p = 0 \vdash\ (p_1 = 0, \ldots,\ p_h = 0) \qquad \text{and}$$

$$\mathcal{DG}(K),\ p_1 = 0, \ldots,\ p_h = 0 \vdash\ p = 0$$

are very easy.

If $k > 0$, the constraints $(q_j(x) \neq 0)_{1 \leq j \leq k}$ are equivalent to a single one, $q \neq 0$ where $q = q_1 \ldots q_k$. A dynamical proof for this equivalence is also very easy.

Finally, we have to see the case of a system of two constraints $(p = 0,\ q \neq 0)$. If $q = 0$ or $p = 0$ in $K[x]$, the system is equivalent to $q \neq 0$. Else, we can compute within the subring $\mathbf{Z}[G_1]$ the part of p prime to q. More precisely we get some equalities involving polynomials in $\mathbf{Z}[G_1]$: $\beta p = p_1 p_2,\ p_1 u + q v = \alpha,\ p_2 q_2 = \gamma q^k$. From these equalities we get dynamical proofs of

$$\mathcal{DG}(K),\ p = 0,\ q \neq 0 \vdash\ p_1 = 0 \qquad \text{and} \qquad \mathcal{DG}(K),\ p_1 = 0 \vdash\ (p = 0,\ q \neq 0)\ .$$

So we can always reduce the problem to only one constraint. After this reduction, we get a collapse if we obtain as constraint $t = 0$ with a non-zero constant t of K, or a constraint $q \neq 0$ with $q = 0$ in the case that $h = 0$ (this means that one q_j is actually 0).

We have to see that in the other cases the collapse is impossible.

In the case of only one constraint $t(x) = 0$ with $deg(t) > 0$, we may assume that $t(x)$ is monic. Now Lemma 2.6 d) implies that if $(\mathcal{DG}(K),\ t(x) = 0)$ collapses, then $\mathcal{DG}(K)$ collapses also, which is impossible.

In the case of only one constraint $q(x) \neq 0$, the constraint is true in the field $K(x)$ of rational fractions.

This ends the proof of the one variable case. For the general case we need the following lemma.

Lemma 2.12 *Let $\mathcal{K} = (G; R_{=0}, R_{\neq 0})$ be a presentation in the language $\mathcal{L}_f$. Let z a new variable and $q(z)$ a monic non-constant polynomial in $\mathbf{Z}[G][z]$. Let $q_1(z)$ be a polynomial $\mathbf{Z}[G][z]$ with leading coefficient p.*

i) If the presentation $\mathcal{K} \cup (q(z) \neq 0)$ collapses in the theory of rings with proper monoid, so does the presentation $\mathcal{K}$.

ii) If the presentation $\mathcal{K} \cup (q_1(z) = 0, p \neq 0)$ collapses in the theory of rings with proper monoid, so does the presentation $\mathcal{K} \cup (p \neq 0)$.

iii) If the presentation $\mathcal{K} \cup (q_1(z) \neq 0, p \neq 0)$ collapses in the theory of rings with proper monoid, so does the presentation $\mathcal{K} \cup (p \neq 0)$.

Proof: i) We suppose that there is an equality in $\mathbf{Z}[G,z]$ of the form

$$mq(z)^n + \sum_i r_i a_i(z) = 0$$

where the r_i belong to $R_{=0}$ and m belongs to $\mathcal{M}_{\neq 0}$, the monoid generated by $R_{\neq 0}$. Let n' be the z-degree of q. This equality in $\mathbf{Z}[G,z] = \mathbf{Z}[G][z]$ gives for the coefficient of $z^{nn'}$ in $\mathbf{Z}[G]$ exactly an equality in the form of the collapse we are looking for.

ii) We get the result by combination of items a), b) and d) of Lemma 2.6.

iii) We get the result by combination of i) and of items a), b) in Lemma 2.6. □

We now turn to the multivariate case. Let us call S our system of polynomial constraints. We consider the variables $x_1,\ldots,x_{n-1}$ as parameters and the variable x_n as our true variable. We try to make the same computations as in the one variable case. Computations are essentially pseudo-remainder computations. With coefficients depending on parameters, such a computation splits in many cases, depending on the degrees of the polynomials, i.e., depending on the nullity or nonnullity of polynomials in the parameters. This gives a (very big) finite tree, which is precisely a covering of the presentation $\mathcal{DG}(K) \cup (\{x_1,\ldots,x_n\}; R_{=0}, R_{\neq 0})$ in the theory of fields. At each leaf L of this tree, we have a presentation with a system S_L of polynomial constraints on $x_1,\ldots,x_{n-1}$ and only one constraint s_L on x_n which is either $p_L = 0$ or $p_L \neq 0$, where p_L is an x_n-polynomial with coefficients in $K[x_1,\ldots,x_{n-1}]$.

If p_L is not a "constant" (i.e., an element of $K[x_1,\ldots,x_{n-1}]$), the fact that the leading x_n-coefficient of p_L is $\neq 0$ is given by a polynomial constraint in S_L. Moreover, in each case we have dynamical proofs for $S_L, s_L \vdash S$ and $S_L, S \vdash s_L$.

If p_L is a "constant" the system $S'_L = (S_L, s_L)$ does not involve x_n and the presentation $((x_1,\ldots,x_n),(S_L,S))$ collapses if and only if the presentation $((x_1,\ldots,x_{n-1}),S'_L)$ collapses.

If p_L is not a "constant", by Lemma 2.12 ii) and iii), the presentation $((x_1,\ldots,x_n),(S_L,s_L))$ collapses if and only if the presentation $((x_1,\ldots,x_{n-1}),S_L)$ collapses. So, the presentation $((x_1,\ldots,x_n),(S_L,S))$ collapses if and only if the presentation $((x_1,\ldots,x_{n-1}),S_L)$ collapses.

Finally, S collapses iff all the presentations $((x_1,\ldots,x_n),(S_L,S))$ at the leaves of the big tree collapse. So we can finish the proof arguing by induction.

□

Theorem 2.13 *(constructive version of Hilbert's Nullstellensatz) Let K be a field and $R_{=0}$, $R_{\neq 0}$ two finite families of polynomials of $K[x_1,\ldots,x_n]$. There is an algorithm deciding if the presentation $\mathcal{DG}(K) \cup (\{x_1,\ldots,x_n\}; R_{=0}, R_{\neq 0})$ collapses in the theory of algebraically closed fields. In case of positive answer one can produce an equality $m = a_1p_1 + \cdots + a_kp_k$ with p_j in $R_{=0}$ and m in the monoid $\mathcal{M}_{\neq 0}$ generated by $R_{\neq 0}$.*

Proof: We use proposition 2.11, theorem 2.4 saying that the theory of fields collapses simultaneously with the theory of rings with proper monoids, and finally proposition 2.2 describing collapse in rings with proper monoids. □

In general, the algebraic closure of a field cannot be constructed. But in several important particular cases, for example if the field K is discrete and enumerable, or discrete and ordered, the algebraic closure can be constructed (see [29] and [27].). The effective Hilbert's Nullstellensatz has a nicer formulation then.

Theorem 2.14 *Let K be a field contained in an algebraically closed field L. Let $R_{=0}$ be a finite family of polynomials of $K[x_1,\ldots,x_n]$. One can decide whether a polynomial $q \in K[x_1,\ldots,x_n]$ is 0 on the common zeroes of polynomials $p_j \in R_{=0}$ in L^n. In case of positive answer one can produce an equality $q^n = a_1p_1 + \cdots + a_kp_k$, with p_j in $R_{=0}$. In case of negative answer, one can produce a point in L^n which is a zero of all p_j in $R_{=0}$ and not of q.*

Proof: Consider the algorithm in the proof of proposition 2.11 with $R_{\neq 0} = \{q\}$. If we are in the situation where the decision algorithm answers "yes", we conclude by the preceding theorem. In the other case, we consider a leaf of the covering built by induction on the number of variables in the proof of Proposition 2.11, such that the "triangular system" at this leaf does not collapse: this system contains only one constraint $r_i(x_1, \ldots, x_i) = 0$ or $\neq 0$ for each i, where $\deg_{x_i}(r_i) > 0$ in the case $= 0$ and the constraints involving $x_1, \ldots, x_{i-1}$ imply that the leading coefficient of r_i with respect to x_i is $\neq 0$. So the construction of a point satisfying this triangular system is easy. □

So the constructive character of Hilbert Nullstellensatz comes in our approach from two different ingredients:

- the fact that, when the decision algorithm produces a proof of $\bot$ in the theory of algebraically closed fields, the presentation collapses in the theory of fields,
- the fact that a collapse in the theory of fields gives rise to a construction of an algebraic identity certifying this collapse.

2.4 Provable facts and algebraic theory of quasi-domains

We give now the axioms of the theory of *quasi-domains*: the axioms of rings with a proper monoid and the following *simplification axioms*.

$$\begin{array}{rll} x^2 = 0 & \vdash\ x = 0 & S(2)_f \\ xy = 0,\ x \neq 0 & \vdash\ y = 0 & S(3)_f \\ xy \neq 0 & \vdash\ x \neq 0 & S(4)_f \end{array}$$

Remark that the simplification axiom $S(1)_f$ is a valid dynamical rule in the theory of quasi-domains.

Note also that a field is a quasi-domain. More precisely, axioms of quasi-domains are axioms of fields or valid dynamical rules in the theory of fields. So quasi-domains are between rings with proper monoid and fields, and we get the following lemma.

Lemma 2.15 *The theories of rings with proper monoid, quasi-domains, fields and algebraically closed fields collapse simultaneously.*

Proposition 2.16 *The theories of quasi-domains, fields and algebraically closed fields prove the same facts.*

Proof: It is easy to see that in the theory of fields a fact is provable (from a presentation) if and only if the "opposite" fact (obtained by replacing $= 0$ with $\neq 0$ and vice-versa) produces a collapse (when added to the presentation). This is because we have the axiom $\vdash x = 0 \ \vee\ x \neq 0$ and the valid dynamical rule $x = 0,\ x \neq 0 \vdash \bot$. A fortiori the same result is true for the theory of algebraically closed fields.

For quasi-domains, the simplification axioms imply the same result.

Let us prove first that $p = 0$ has a dynamical proof from $\mathcal{K} = (G; R_{=0}, R_{\neq 0})$ in the theory of quasi-domains if and only if $\mathcal{K} \cup (p \neq 0)$ collapses. The "only if" part follows from the valid dynamical rule $(x = 0,\ x \neq 0) \vdash \bot$. Suppose now that we have $mp^n + i = 0$ with $m \in \mathcal{M}_{\neq 0}$ and $i \in \mathcal{I}_{=0}$ where $\mathcal{M}_{\neq 0}$ is the monoid generated by $R_{\neq 0}$ and $\mathcal{I}_{=0}$ is the ideal generated by $R_{=0}$. The presentation $\mathcal{K}$ proves $-i = 0$ since $-i \in \mathcal{I}_{=0}$, so it proves $mp^n = 0$ since $mp^n = (mp^n + i) + (-i)$. Then we deduce $p^n = 0$ using axiom $S(3)_f$ hence $p = 0$ using several times axiom $S(2)_f$.

Finally let us prove that $p \neq 0$ has a dynamical proof from $\mathcal{K}$ in the theory of quasi-domains if and only if $\mathcal{K} \cup (p = 0)$ collapses in the theory of rings with proper monoid. Suppose that we have $m + i + pa = 0$ with $m \in \mathcal{M}$ and $i \in \mathcal{I}_{=0}$ We deduce $pa \neq 0$ and then $p \neq 0$ using $S(4)_f$.

So the theories of quasi-domains, fields and algebraically closed fields prove the same facts since they collapse simultaneously. □

Remark 2.17 If we take the theory of rings with proper monoid and add the axiom

$$\vdash\ x=0\ \vee\ x\neq 0$$

we get the theory of *domains*. It is easy to see that axioms of quasi-domains are valid dynamical rules for domains. Moreover it is interesting to remark that the algorithm in proposition 2.11 gives a collapse in the theory of domains. The theories of quasi-domains, domains, fields and algebraically closed fields prove the same facts. Moreover they collapse simultaneously with the theory of rings with proper monoid.

This has interesting consequences for Heyting fields (see [29]). Heyting fields are a weak notion of field: the equality relation $x=0$ is equivalent to $\neg(x\neq 0)$ (where we interpret $x\neq 0$ as meaning the invertibility of x), but the law of the excluded middle $x=0\vee x\neq 0$ is not assumed, Heyting fields satisfy axioms of quasi-domains and axioms of local rings

$$x\neq 0\vdash\exists y\ yx-1=0\qquad\text{and}\qquad\vdash\ x\neq 0\ \vee\ 1+x\neq 0$$

but it seems that there is no purely dynamical description of an axiomatic for Heyting fields. This is because there are no dynamical axioms for saying that $\neg P$ means $P\vdash\bot$.

A consequence of the Nullstellensatz is that any fact within a Heyting field which can be proved in the theory of algebraically closed fields can also be proved in the theory of Heyting fields. So, when dealing with facts in a Heyting field, we can use freely all the axioms of algebraically closed fields. In particular the axiom $Dy(2)_f$ meaning the decidability of equality to 0 causes no trouble with facts.

3 Stengle's Positivstellensatz

We give in this paragraph a new constructive proof of Stengle's Positivstellensatz [32]. This new proof is close to [18].

3.1 Some simultaneous collapses

The central theory we consider is the theory of ordered fields. The *unary language of ordered fields* $\mathcal{L}_{of}$ is the unary language of rings $\mathcal{L}_r$ with two more unary predicates ≥ 0 and >0.

Axioms of *proto-ordered ring* are axioms of rings and the following axioms.

$$\begin{array}{rll}
 & \vdash\ x^2\geq 0 & D(1)_{of}\\
x=0,\ y\geq 0 & \vdash\ x+y\geq 0 & D(2)_{of}\\
x\geq 0,\ y\geq 0 & \vdash\ x+y\geq 0 & D(3)_{of}\\
x\geq 0,\ y\geq 0 & \vdash\ xy\geq 0 & D(4)_{of}\\
 & \vdash\ 1>0 & D(5)_{of}\\
x=0,\ y>0 & \vdash\ x+y>0 & D(6)_{of}\\
x>0,\ y\geq 0 & \vdash\ x+y>0 & D(7)_{of}\\
x>0,\ y>0 & \vdash\ xy>0 & D(8)_{of}\\
x>0 & \vdash\ x\geq 0 & D(9)_{of}\\
0>0 & \vdash\ \bot & C_{of}
\end{array}$$

Axioms of *ordered fields* are axioms of proto-ordered rings and the following axioms.

$$\begin{array}{rll}
x\geq 0,\ -x\geq 0 & \vdash\ x=0 & S(1)_{of}\\
xy-1=0 & \vdash\ x^2>0 & S(2)_{of}\\
x^2>0 & \vdash\ \exists y\ xy-1=0 & Dy(1)_{of}\\
 & \vdash\ x\geq 0\ \vee\ -x\geq 0 & Dy(2)_{of}\\
 & \vdash\ x=0\ \vee\ x^2>0 & Dy(3)_{of}
\end{array}$$

Remark that if we introduce $x\neq 0$ as an abbreviation for $x^2>0$ then the axioms of rings with proper monoid are valid dynamical rules in the theory of proto-ordered rings.

The set of elements x of a proto-ordered ring satisfying $x \geq 0$ is a *proper cone*. Recall that a subset C of a ring A is called a *cone* if the squares of A are in C, $C + C \subset C$ and $C\,C \subset C$. A cone C is said to be *proper* if $-1 \notin C$.

We write $t \geq t'$ as an abbreviation for $t - t' \geq 0$, $t \geq t' \geq t$" as an abbreviation for $t \geq t',\ t' \geq t$" and $t' \leq t$ as another way of writing $t \geq t'$.

A *real closed field* is an ordered field with the extra axioms:

$$-p(a)p(b) \geq 0 \vdash \exists y \;\; p(y) = 0 \qquad Dy_n(4)_{of}$$

($a,\ b,\ y$ and coefficients of the monic degree n polynomial p are distinct variables, and there is an axiom for each degree). Of course,

$$-p(a)p(b) \geq 0,\ b - a \geq 0 \vdash \exists y\ (p(y) = 0,\ b - y \geq 0,\ y - a \geq 0)$$

is a valid dynamical rule in the theory of real closed fields.

Notice that there are again direct algebraic axioms, collapse axioms, simplification axioms and dynamical axioms.

A presentation in the language $\mathcal{L}_{of}$ is a set of variables G and three subsets $R_{=0}, R_{\geq 0}, R_{>0}$ contained in $\mathbf{Z}[G]$. It is denoted by $(G; R_{=0}, R_{\geq 0}, R_{>0})$.

The theory of proto-ordered rings has been chosen because the collapse takes a very simple form and is very easy to prove as we shall see immediately (this is due to the fact that it is a direct theory), and because it collapses simultaneously with the theory of real closed fields as we shall see next.

Proposition 3.1 *Let $\mathcal{K} = (G; R_{=0}, R_{\geq 0}, R_{>0})$ be a presentation in the language $\mathcal{L}_{of}$. Let $\mathcal{I}_{=0}$ be the ideal of $\mathbf{Z}[G]$ generated by $R_{=0}$, $\mathcal{M}_{>0}$ the monoid generated by $R_{>0}$ ($\mathcal{M}_{>0}$ contains at least the element 1), $\mathcal{C}_{\geq 0}$ the cone generated by $R_{\geq 0} \cup R_{>0}$. A collapse of the presentation $\mathcal{K}$ in the theory of proto-ordered rings produces an equality in $\mathbf{Z}[G]$:*

$$m + q + i = 0$$

with $m \in \mathcal{M}_{>0}$, $q \in \mathcal{C}_{\geq 0}$ and $i \in \mathcal{I}_{=0}$. Reciprocally, such an equality produces a collapse of $\mathcal{K}$.

Proof: First consider dynamical proofs of facts using *only direct algebraic axioms*. These are algebraic proofs without branching.

Arguing inductively on the number of times the direct algebraic axioms are used in the proof we see successively that:

- provably $= 0$ elements, are exactly elements of $\mathcal{I}_{=0}$,
- provably ≥ 0 elements, are exactly elements of the form $q + i$ with $q \in \mathcal{C}_{\geq 0}$ and $i \in \mathcal{I}_{=0}$,
- provably > 0 elements, are exactly elements of the form $m + q + i$

with $m \in \mathcal{M}_{>0}$, $q \in \mathcal{C}_{\geq 0}$ and $i \in \mathcal{I}_{=0}$.

Now a proof of collapse is given by a proof of $0 > 0$ using only direct algebraic axioms. Necessarily it produces an equality $m + q + i = 0$ in $\mathbf{Z}[G]$. □

Remark 3.2 In the line of Remark 2.3, we can see in the preceding proof an order between the unary predicates we have in the language: first comes $= 0$, then ≥ 0, and last > 0, and the collapse is concerned with this last predicate > 0. The axioms $D(1)_{of}$ to $D(4)_{of}$ are construction axioms for ≥ 0, and the axioms $D(5)_{of}$ to $D(8)_{of}$ are construction axioms for > 0. Actually, the situation here is a little more complex, since the remaining direct algebraic axiom $D(9)_{of}$ contains > 0 at the left and ≥ 0 at the right, which violates the order of construction. This axiom plays a special role: it expresses the inclusion of > 0 in ≥ 0. One can realize that any proof in the theory of proto-ordered rings can be transformed into a proof where the axiom $D(9)_{of}$ is only used at the beginning, i.e., before the application of any other axiom. Indeed, any axiom $D(i+4)_{of}$ of construction for > 0 is doubled by an axiom $D(i)_{of}$, and it is easy to check that an application of $D(9)_{of}$ following an application of $D(i)_{of}$ can be transformed to an application of $D(9)_{of}$ preceding an application of $D(i+4)_{of}$. To make things

clearer, let us take an example. If $s = 0$ and $t > 0$, then $s + t > 0$ by $D(6)_{of}$ and $s + t \geq 0$ by $D(9)_{of}$; but one could also use first $D(9)_{of}$ to have $t \geq 0$, then $D(2)_{of}$ to have $s + t \geq 0$.

Another way of formulating this remark is to say that the axiom $D(9)_{of}$ may be replaced by the stipulation that any presentation must satisfy $R_{>0} \subset R_{\geq 0}$. This reflects the fact that the construction of the cone $\mathcal{C}_{\geq 0}$ starts with $R_{\geq 0} \cup R_{>0}$. So we have to distinguish between the direct algebraic axioms expressing construction of predicates, and those expressing an inclusion of predicates (here $D(9)_{of}$). The axioms of inclusion violate the order of construction, but they can be lifted at the beginning of proofs. This preserves the possibility of constructing the predicates one after the other.

The proposition 3.1 means that a collapse of a presentation in the theory of proto-ordered rings can always be certified by an algebraic identity of a very precise type.

Let us return to the example of the presentation $(x^3 - y^3 = 0,\ (x-y)^2 > 0,\ x = 0)$ which collapses in the theory of proto-ordered rings. This is certified by the equality

$$(x-y)^4 + y(x^3 - y^3) - (x^3 - 3x^2y + 6xy^2 - 4y^3)x = 0 \qquad (Ex_1)$$

since $(x-y)^4$ belongs to the monoid generated by $(x-y)^2$ and $y(x^3-y^3) - (x^3 - 3x^2y + 6xy^2 - 4y^3)x$ belongs to the ideal generated by $x^3 - y^3$ and x.

Similarly, the presentation $(x^3 - y^3 = 0,\ (x-y)^2 > 0,\ x^2 > 0)$ collapses in the theory of proto-ordered rings and this is certified by the equality

$$(x-y)^2x^2 + 2(x-y)^2x^2 + (x-y)^2(2y+x)^2 - 4(x-y)(x^3-y^3) = 0 \qquad (Ex_2)$$

since

- $(x-y)^2x^2$ belongs to the monoid generated by $(x-y)^2$ and x^2,
- $2(x-y)^2x^2 + (x-y)^2(2y+x)^2$ belongs to the cone generated by $(x-y)^2$,
- $4(x-y)(x^3-y^3)$ belongs to the ideal generated by (x^3-y^3).

Theorem 3.3 *The theory of ordered fields and the theory of proto-ordered rings collapse simultaneously.*

Proof: We are going to prove the following lemma, with abuses of notations similar to Notation 2.5.

Lemma 3.4 *Let $\mathcal{K} = (G; R_{=0}, R_{\geq 0}, R_{>0})$ be a presentation in the language $\mathcal{L}_{of}$, $p, r \in \mathbf{Z}[G]$ and z a new variable.*

a) If the presentation $\mathcal{K} \cup (p = 0)$ collapses in the theory of proto-ordered rings, then so does the presentation $\mathcal{K} \cup (p \geq 0,\ -p \geq 0)$.

b) If the presentation $\mathcal{K} \cup (p^2 > 0)$ collapses in the theory of proto-ordered rings, then so does the presentation $\mathcal{K} \cup (pr - 1 = 0)$

c) If the presentation $\mathcal{K} \cup (pz - 1 = 0)$ collapses in the theory of proto-ordered rings, then so does the presentation $\mathcal{K} \cup (p^2 > 0)$.

d) If the presentations $\mathcal{K} \cup (p \geq 0)$ and $\mathcal{K} \cup (-p \geq 0)$ collapse in the theory of rings with proper cone, then so does the presentation $\mathcal{K}$.

e) If the presentations $\mathcal{K} \cup (p = 0)$ and $\mathcal{K} \cup (p^2 > 0)$ collapse in the theory of proto-ordered rings, then so does the presentation $\mathcal{K}$.

The lemma 3.4 proves that the five additional axioms of ordered fields do not change the collapse, which proves the theorem.

Let us prove now the lemma.

Let $\mathcal{M}_{>0}$ be the monoid generated by $R_{>0}$ in $\mathbf{Z}[G]$, $\mathcal{C}_{\geq 0}$ the cone generated by $R_{>0} \cup R_{\geq 0}$ and $\mathcal{I}_{=0}$ the ideal generated by $R_{=0}$.

a) We start with one identity $m+q+i=pb$ in $\mathbf{Z}[G]$ with $m \in \mathcal{M}_{>0}$, $q \in \mathcal{C}_{\geq 0}$, $i \in \mathcal{I}_{=0}$ and $b \in \mathbf{Z}[G]$. Squaring, we get an identity $m_1 + q_1 + i_1 = p^2b^2$ and we rewrite it as $m_1 + q_1 + (p)(-p)b^2 + i_1 = 0$ which gives the collapse we are looking for.

b) Left to the reader (see the analogous computation in lemma 2.6 a))

c) This is again Rabinovitch's trick. We can assume that p is not $0 \in \mathbf{Z}[G]$. There is an equality in $\mathbf{Z}[G, z]$:

$$m + \sum_j q_j b_j(z)^2 + i(z) + (pz-1)b(z) = 0$$

with m in $\mathcal{M}_{>0}$, $q_j \in \mathcal{C}_{\geq 0}$, b_j and b in $\mathbf{Z}[G, z]$, and $i(z)$ is a polynomial with coefficients in $\mathcal{I}_{=0}$.

Multiply by p^{2n} where $2n$ is bigger than the z degree of the polynomials $i(z)$ and $b_j(z)^2$. Replace in $(p^n b_j(z))^2$ and in $p^{2n}i(z)$ all $p^k z^k$ by 1 modulo $(pz-1)$. The new polynomial $b(z)$ is necessarily 0 and since there is no more z in what remains, we get an equality which gives the collapse we are looking for.

d) We start with two identities in $\mathbf{Z}[G]$

$$m_1 + q_1 + q_1'p + i_1 = 0 \ (1) \qquad \text{and} \qquad m_2 + q_2 - q_2'p + i_2 = 0 \ (2)$$

with m_1 and $m_2 \in \mathcal{M}_{>0}$, q_1, q_1' and $q_2, q_2' \in \mathcal{C}_{\geq 0}$ and i_1 and i_2 in $\mathcal{I}_{=0}$. From (1) we deduce $-q_1'p = m_1 + q_1 + i_1$ and from (2) $q_2'p = m_2 + q_2 + i_2$. Multiplying these two equalities we get $-q_1'q_2'p^2 = (m_1 + q_1 + i_1)(m_2 + q_2 + i_2)$ and since $q_1'q_2'p^2$ is in $\mathcal{C}_{\geq 0}$, this can be rewritten $m + q + i = 0$ in $\mathbf{Z}[G]$ with $m \in \mathcal{M}_{>0}$, $q \in \mathcal{C}_{\geq 0}$, $i \in \mathcal{I}_{=0}$.

e) We start with two identities in $\mathbf{Z}[G]$

$$p^{2n}m_1 + q_1 + i_1 = 0 \ (1) \qquad \text{and} \qquad m_2 + q_2 + ap + i_2 = 0 \ (2)$$

with m_1 and $m_2 \in \mathcal{M}_{>0}$, q_1 and q_2 in $\mathcal{C}_{\geq 0}$ and i_1 and i_2 in $\mathcal{I}_{=0}$. Using (2), we get $a^{2n}p^{2n} = (m_2 + q_2 + i_2)^{2n} = m_3 + q_3 + i_3$ (3) with m_3 in $\mathcal{M}_{>0}$, $q_3 \in \mathcal{C}_{\geq 0}$ and $i_3 \in \mathcal{I}_{=0}$. Multiplying now (1) by a^{2n} and substituting $p^{2n}a^{2n}$ by $m_3 + q_3 + i_3$ using (3), we obtain an equality $m_4 + q_4 + i_4 = 0$ in $\mathbf{Z}[G]$. This gives the collapse we are looking for. □

The proof of the lemma gives very explicit methods for constructing identities certifying collapses. For instance, in our example, from the algebraic identities (Ex_1) and (Ex_2) certifying that the presentations $(x^3 - y^3 = 0, (x-y)^2 > 0, x = 0)$ and $(x^3 - y^3 = 0, (x-y)^2 > 0, x^2 > 0)$ collapse in the theory of proto-ordered rings, we can deduce an algebraic identity certifying that the presentation $(x^3 - y^3 = 0, (x-y)^2 > 0)$ collapses in the theory of proto-ordered rings as in the preceding lemma e): since $(x^3-3x^2y+6xy^2-4y^3)x = (x-y)^4+y(x^3-y^3)$, $(x^3-3x^2y+6xy^2-4y^3)^2x^2 = ((x-y)^4+y(x^3-y^3))^2$ and using (Ex_2) multiplied by $(x^3 - (x^2y + 6xy^2 - 4y^3)^2$ and replacing $(x^3 - 3x^2y + 6xy^2 - 4y^3)^2x^2$ by $((x-y)^4 + y(x^3 - y^3))^2$ we get an expression $(x-y)^6 +$ a sum of squares $+ (x^3 - y^3)A(x, y) = 0$ which is the algebraic identity we are looking for.

Corollary 3.5 *Let K be a real field (i.e., -1 is not a sum of squares in K). The diagram of K in the language $\mathcal{L}_{of}$ does not collapse in the theory of ordered fields*

Proof: Apply theorem 3.3 with the presentation $\mathcal{DG}(K) \cup (\emptyset; \emptyset, C, \emptyset)$, where C is the subset of sums of squares. □

This corollary is a constructive version of the non-constructive theorem according to which "every real field can be totally ordered". Next theorem gives a constructive version of the fact that "every ordered field can be embedded in a real closed field".

Theorem 3.6 *The theory of real closed fields and the theory of ordered fields collapse simultaneously.*

Proof: We prove that the use of the extra axiom of real closed fields

$$-p(a)\,p(b) \geq 0 \vdash \exists z\ p(z) = 0$$

does not modify the collapse. This is the content of the following lemma. Due to the induction procedure, we have to consider polynomials $p(z)$ which may be non-monic. □

Lemma 3.7 *Let $\mathcal{K} = (G; R_{=0}, R_{\geq 0}, R_{>0})$ be a presentation in the language $\mathcal{L}_{of}$, a and b elements of $\mathbf{Z}[G]$, z a new variable and $p(z) \in \mathbf{Z}[G][z]$ (not necessarily monic). If the presentation $\mathcal{K} \cup (p(z) = 0)$ collapses in the theory of ordered fields, then so does the presentation $\mathcal{K} \cup (-p(a)p(b) \geq 0)$*

Proof Let $\mathcal{M}_{>0}$ be the monoid generated by $R_{>0}$, $\mathcal{C}_{\geq 0}$ the cone generated by $R_{\geq 0} \cup R_{>0}$ and $\mathcal{I}_{=0}$ the ideal generated by $R_{=0}$.

The proof is by induction on the formal degree of p in z (we say "formal" because $p(z)$ is not necessarily monic). For degree 0 and 1 it is easy. Suppose now that $\deg(p) \geq 2$.

Consider first the case when p is monic. From the collapse of $\mathcal{K} \cup (p(z) = 0)$, we obtain an equality of polynomials in the variable z :

$$m + \sum_i p_i s_i^2(z) + \sum_j n_j t_j(z) + p(z)t(z) = 0 \tag{1}$$

with $m \in \mathcal{M}_{>0}$, the p_i in $\mathcal{C}_{\geq 0}$ and the n_j in $\mathcal{I}_{=0}$. This is an algebraic identity in $\mathbf{Z}[G, z]$. We divide s_i and t_j by p and obtain an equality:

$$m + \sum_i p_i r_i^2(z) + \sum_j n_j q_j(z) - p(z)q(z) = 0 \tag{2}$$

with $m \in \mathcal{M}_{>0}$, the p_i in $\mathcal{C}_{\geq 0}$, the n_j in $\mathcal{I}_{=0}$ and $\deg(q(z)) \leq p - 2$.

This equality provides a collapse of the presentation $\mathcal{K} \cup (q(z) = 0)$ in the theory of ordered fields. By induction hypothesis, we have thus a collapse of the presentation $\mathcal{K} \cup (-q(a)q(b) \geq 0)$

On the other hand, substituting a (resp. b) to z in equality (2), we obtain:

$$m + \sum_i p_i r_i^2(a) + \sum_j n_j q_j(a) = p(a)q(a) \tag{3}$$

$$m + \sum_i p_i r_i^2(b) + \sum_j n_j q_j(b) = p(b)q(b) \tag{4}$$

Equalities (3) and (4) show that in the presentation $\mathcal{K}$ the atomic formulas $p(a)q(a) > 0$ and $p(b)q(b) > 0$ are provable, hence also $p(a)p(b)q(a)q(b)) > 0$.
Thus the presentation $\mathcal{K} \cup (-p(a)p(b) \geq 0)$ proves that $-q(a)q(b) \geq 0$ (it is easy to see that the dynamical rule $(xy > 0,\ x \geq 0) \vdash y \geq 0$ is valid in the theory or ordered fields) and collapses.

In the case that p is not monic, it is possible to open two branches. In the first one, the leading coefficient of p is zero, and the induction hypothesis can be used. In the second branch, the leading coefficient of p is invertible and we are reduced to the monic case using the axiom $Dy(1)_{of}$ of ordered fields. □

Theorem 3.8 *The theory of real closed fields and the theory of proto-ordered rings collapse simultaneously.*

Corollary 3.9 *Let $\mathcal{K} = (G; R_{=0}, R_{\geq 0}, R_{>0})$ be a presentation in the language $\mathcal{L}_{of}$. Let $\mathcal{I}_{=0}$ be the ideal of $\mathbf{Z}[G]$ generated by $R_{=0}$, $\mathcal{M}_{>0}$ the monoid generated by $R_{>0}$, $\mathcal{C}_{\geq 0}$ the cone generated by $R_{\geq 0} \cup R_{>0}$. A collapse of the presentation $\mathcal{K}$ in the theory of real closed fields produces an equality in $\mathbf{Z}[G]$:*

$$m + q + i = 0$$

with $m \in \mathcal{M}_{>0}$, $q \in \mathcal{C}_{\geq 0}$ and $i \in \mathcal{I}_{=0}$.

Proposition 3.10 (non-constructive formal version of Stengle's Positivstellensatz) *Let A be a ring, $(R_{=0}, R_{\geq 0}, R_{>0})$ three families of elements. Denote by $\mathcal{M}_{>0}$ the monoid generated by $R_{>0}$, $\mathcal{C}_{\geq 0}$ the cone generated by $R_{\geq 0} \cup R_{>0}$, $\mathcal{I}_{=0}$ the ideal generated by $R_{=0}$. The following properties are equivalent*

i) There exists $i \in \mathcal{I}_{=0}$, $p \in \mathcal{C}_{\geq 0}$ and $m \in \mathcal{M}_{>0}$ with $m + p + i = 0$ in A

ii) There exists no homomorphism $\phi : A \to L$ with L real closed, $\phi(a) = 0$ for $a \in R_{=0}$, $\phi(p) \geq 0$ for $p \in R_{\geq 0}$ and $\phi(m) > 0$ for $m \in R_{>0}$.

Proof: Apply the preceding corollary to the presentation

$$\mathcal{DG}(A) \cup (\emptyset; R_{=0}, R_{\geq 0}, R_{>0}) \ ,$$

and use the non-constructive completeness theorem of model theory. □

3.2 Decision algorithm and constructive Positivstellensatz

In the next theorem, we mention the real closure of an ordered field. A constructive proof of the existence and uniqueness (up to unique isomorphism) of this real closure is for example given in [27]. So the situation is easier to describe than for algebraically closed fields and we can use more directly semantics.

Since the theory of real closed fields has a decision algorithm for testing emptiness with a very simple structure, we are able to prove the following:

Theorem 3.11 *Let K be an ordered field, R its real closure, and $R_{=0}$, $R_{\geq 0}$, $R_{>0}$ three finite families of $K[x_1, x_2, \cdots, x_n] = K[x]$. The system of sign conditions $[u(x) > 0, q(x) \geq 0, j(x) = 0]$ for $u \in R_{>0}$, $q \in R_{\geq 0}$, $j \in R_{=0}$ is impossible in R^n if and only if the presentation*

$$\mathcal{DG}(K) \ \cup (\{x_1, x_2, \cdots, x_n\}; R_{=0}, R_{\geq 0}, R_{>0})$$

collapses in the theory of real closed fields.

Proof: We assume that from a constructive point of view, all our ordered fields are discrete, this means that we have a way of deciding exactly if an element is zero or not. Precisely, G_1 being the finite set of coefficients of polynomials belonging to $R_{=0}$, $R_{\geq 0}$, and $R_{>0}$, we can decide for any $\mathbf{Z}$-polynomial whether, when it is evaluated on G_1 in K, we get 0, > 0 or < 0.

We first deal with only one variable x. Recall Cohen-Hörmander algorithm. We call Hörmander tableau of a finite list of polynomials with coefficients in the ordered field K the tableau

- whose columns correspond to roots of the polynomials in the real closure of K and to open intervals cut out by these roots, listed in the canonical order,
- and which has a line for each polynomial, whose entries are the sign (> 0, $= 0$ or < 0) which the polynomial has at each of the roots or on each of the intervals.

Lemma 3.12 *Let K be an ordered field, subfield of a real closed field R. Let $L = [P_1, P_2, \ldots, P_k]$ be a list of polynomials of $K[x]$. Let $\mathcal{P}$ be the family of polynomials generated by the elements of L and by the operations $P \mapsto P'$, and $(P, Q) \mapsto \mathrm{Rem}(P, Q)$. Then:*

1) *$\mathcal{P}$ is finite.*

2) *One can set up the Hörmander tableau for $\mathcal{P}$ using only the following information:*

- *the degree of each polynomial in the family;*
- *the diagrams of the operations $P \mapsto P'$, and $(P, Q) \mapsto \mathrm{Rem}(P, Q)$ (where $\deg(P) \geq deg(Q)$) in $\mathcal{P}$; and*
- *the signs of the constants of $\mathcal{P}$.*

Proof: 1) is easy.

2) We number the polynomials in $\mathcal{P}$ so that the degree is nondecreasing. Let $\mathcal{P}_m$ be the subfamily of $\mathcal{P}$ made of polynomials numbered 1 to m. Let us denote by $\mathcal{T}_m$ the Hörmander tableau corresponding to the family $\mathcal{P}_m$: i.e., the tableau where all the real roots of the polynomials of $\mathcal{P}_m$ are listed in increasing order, and where all the signs of the polynomials of $\mathcal{P}_m$ are indicated, at each root, and on each interval between two consecutive roots (or between $-\infty$ and the first root, or between the last root and $+\infty$). Then by induction on m it is easy to prove that one can construct the tableau $\mathcal{T}_m$ from the allowed information. □

When one inspects the details of the preceding construction, one sees that it means an elementary proof of a big disjunction (all the systems of sign conditions for the list L that appear when x is in R). This elementary proof leads directly to a covering of the presentation $\mathcal{DG}(K) \cup (\{x\}; \emptyset, \emptyset, \emptyset)$ in the theory of real closed fields.

Now, if $R_{=0}$, $R_{\geq 0}$, $R_{>0}$ are three finite sets whose union is L, and if the corresponding sign conditions do not appear in the Hörmander tableau, we see that, considering the preceding covering as a covering of $\mathcal{DG}(K) \cup (\{x\}; R_{=0}, R_{\geq 0}, R_{>0})$ we are able to "kill" each leaf of the tree by a collapse, since we get at each leaf a pair of contradictory sign conditions on at least one of the P_i's.

Let us see now the multivariate case. We consider the variables $x_1, \ldots, x_{n-1}$ as parameters and the variable x_n as our true variable. We try to make the same computations as in the one variable case. Computations for setting the family $\mathcal{P}$ are essentially derivations and pseudo-remainder computations. With coefficients depending on parameters, such a computation splits in many cases, depending on the degrees of the polynomials (i.e., depending on the nullity or nonnullity of polynomials in the parameters). Finally, the construction of the Hörmander tableau depends also on the signs of the "constants" (i.e., some polynomials in the parameters) of the family $\mathcal{P}$. So, computing all possible signs conditions for a finite family of polynomials of $K[x_1, \ldots, x_n]$ depends on computing all possible signs conditions for another (much bigger) finite family of polynomials of $K[x_1, \ldots, x_{n-1}]$.

By induction we get a covering of the presentation

$$\mathcal{DG}(K) \cup (\{x_1, x_2, \cdots, x_n\}; \emptyset, \emptyset, \emptyset)$$

in the theory of real closed fields. At the leaves of our tree, we get all possible signs conditions (when evaluated in R^n) for polynomials in $R_{=0} \cup R_{\geq 0} \cup R_{>0}$. So if the system is impossible, the corresponding sign conditions give a collapse at each leaf of our tree when we consider this covering as a covering of the presentation $\mathcal{DG}(K) \cup (\{x_1, x_2, \cdots, x_n\}; R_{=0}, R_{\geq 0}, R_{>0})$

Remark finally that a contrario, if one leaf of the tree has good sign conditions, then we are able to explicit a point in R^n satisfying the sign conditions, and the presentation cannot collapse in the theory of real closed fields. □

Remark 3.13 When we say that the correctness of the Hörmander tableau has a very elementary proof, we mean that the proof is only made of direct application of our real closed fields axioms. The detailed inspection shows that only one argument is "indirect": the fact that a polynomial whose derivative is positive on an interval must be increasing on the interval. This fact has a very simple proof based on algebraic identities (see e.g. in [27] the "algebraic mean value theorem"). In the context of Hörmander tableaux, these identities lead to "generalized Taylor formulas" (see [19]). Using these formulas, one gets a direct way of constructing the covering from the Hörmander tableau. We can summarize this remark as "Hörmander tableaux and generalized Taylor formulas produce dynamical proofs of collapses".

Theorem 3.14 (Positivstellensatz) *Let K be an ordered field, R its real closure, and $R_{=0}, R_{\geq 0}, R_{>0}$ three finite families of $K[x] = K[x_1, x_2, \cdots, x_n]$.*

Define $\mathcal{M}_{>0}$ as the monoid generated by $R_{>0}$, $\mathcal{C}_{\geq 0}$ as the cone of $K[x]$ generated by $R_{>0} \cup R_{\geq 0} \cup K^{>0}$ and $\mathcal{I}_{=0}$ as the ideal of $K[x]$ generated by $R_{=0}$.

If the system of sign conditions $[u(x) > 0,\ q(x) \geq 0,\ j(x) = 0]$ *for* $u \in R_{>0}$, $q \in R_{\geq 0}$, $j \in R_{=0}$ *is impossible in* R^n *then one can construct an algebraic identity*

$$m + p + i = 0$$

where $m \in \mathcal{M}_{>0}$, $p \in \mathcal{C}_{\geq 0}$ *and* $i \in \mathcal{I}_{=0}$

Proof: Apply the preceding theorem and corollary 3.9. □

So the constructive character of Stengle's Positivstellensatz comes in our approach from two different ingredients:

- the fact that the decision algorithm for testing emptiness produces, when the set realizing the presentation is empty in the real closure, a collapse of the presentation,
- the fact that a collapse in the theory of real closed fields gives rise to a construction of algebraic identities certifying this collapse.

3.3 Provable facts and generalized Positivstellensätze

We give in the next theorem some classical variants of Stengle's theorem. It is an immediate consequence of theorem 3.14.

Corollary 3.15 *Let* K *be an ordered field,* R *its real closure,* $R_{=0}$, $R_{\geq 0}$, $R_{>0}$ *three finite families of* $K[x] = K[x_1, x_2, \cdots, x_n]$ *and* p *another polynomial.*

Define $\mathcal{M}_{>0}$ *as the monoid generated by* $R_{>0}$, $\mathcal{C}_{\geq 0}$ *as the cone of* $K[x]$ *generated by* $R_{>0} \cup R_{\geq 0} \cup K^{>0}$, *and* $\mathcal{I}_{=0}$ *as the ideal of* $K[x]$ *generated by* $R_{=0}$.

Let $\mathcal{S}$ *the semialgebraic set of* $x \in R^n$ *such that* $u(x) > 0$ *for* $u \in R_{>0}$, $v(x) \geq 0$ *for* $v \in R_{\geq 0}$, $j(x) = 0$ *for* $j \in R_{=0}$

a) The polynomial p *is nonzero on* $\mathcal{S}$ *if and only if one can construct an algebraic identity* $pb = m + q + i$ *with* $m \in \mathcal{M}_{>0}$, $i \in \mathcal{I}_{=0}$, $q \in \mathcal{C}_{\geq 0}$ *and* $b \in K[X]$.

b) The polynomial p *is positive on* $\mathcal{S}$ *if and only if one can construct an algebraic identity* $pq' = m + q + i$ *with* $m \in \mathcal{M}_{>0}$, $i \in \mathcal{I}_{=0}$ *and* $q, q' \in \mathcal{C}_{\geq 0}$.

c) The polynomial p *is zero on* $\mathcal{S}$ *if and only if one can construct an algebraic identity* $p^{2n}m + q + i = 0$ *with* $m \in \mathcal{M}_{>0}$, $i \in \mathcal{I}_{=0}$ *and* $q \in \mathcal{C}_{\geq 0}$.

d) The polynomial p *is nonnegative on* $\mathcal{S}$ *if and only if one can construct an algebraic identity* $pq = p^{2n}m + q' + i$ *with* $m \in \mathcal{M}_{>0}$, $i \in \mathcal{I}_{=0}$ *and* $q, q' \in \mathcal{C}_{\geq 0}$.

Proof: It is easy to see that in the theory of ordered fields a fact is provable (from a presentation) if and only if the "opposite" fact produces a collapse (when added to the presentation). This is because we have the valid dynamical rules $\vdash x = 0 \ \vee \ x^2 > 0$, $\vdash x > 0 \ \vee \ -x \geq 0$, $(x = 0,\ x^2 > 0) \vdash \bot$ and $(x > 0,\ -x \geq 0) \vdash \bot$. So the corollary is an easy consequence of theorem 3.14 □

We give now the axioms of *quasi-ordered rings*: it is the theory of proto-ordered rings together with the following simplification axioms:

$$\begin{array}{rcll} x^2 \leq 0 & \vdash & x = 0 & S(3)_{of} \\ x > 0,\ xy \geq 0 & \vdash & y \geq 0 & S(4)_{of} \\ x \geq 0,\ xy > 0 & \vdash & y > 0 & S(5)_{of} \\ c \geq 0,\ x(x^2 + c) \ \geq 0) & \vdash & x \geq 0 & S(6)_{of} \end{array}$$

Remark that simplification axioms $S(1)_{of}$ and $S(2)_{of}$ (given for ordered fields) are valid dynamical rules in the theory of quasi-ordered rings. Note also that the theory of quasi-ordered rings has only algebraic axioms and one collapse axiom.

An ordered field is a quasi-ordered ring. More precisely, axioms of quasi-ordered rings are axioms of ordered fields or valid dynamical rules in the theory of ordered fields. So quasi-ordered rings are between proto-ordered rings and ordered fields, and we get the following lemma.

Lemma 3.16 *The theories of proto-ordered rings, quasi-ordered rings, ordered fields and real closed fields collapse simultaneously.*

Proposition 3.17 *The theories of quasi-ordered rings, ordered fields and real closed fields prove the same facts.*

Proof: We have already said that, in the theory of ordered fields, a fact is provable (from a presentation) if and only if the opposite fact produces a collapse (when added to the presentation). A fortiori the same result is true for the theory of real closed fields.

For quasi-ordered rings, the simplification axioms give the same result (note that the two collapse axioms are easy).

We give the more tricky case and leave the other ones to the reader.

Assume that the presentation $(G; R_{=0}, R_{\geq 0}, R_{>0} \cup \{-p\})$ collapses in the theory of proto-ordered rings. So we get an equality $(-p)^\ell m + q + i = pq'$ in $\mathbf{Z}[G]$ with m in the monoid $\mathcal{M}_{>0}$ generated by $R_{>0}$, i in the ideal $\mathcal{I}_{=0}$ generated by $R_{=0}$, and q and q' in the cone $\mathcal{C}_{\geq 0}$ generated by $R_{>0} \cup R_{\geq 0}$. We may assume that $\ell = 2n$ is even (if not, we multiply by $-p$ and rewrite the equality). So we have $(p^n)^2 m + q = pq' - i$. We may assume that n is odd (if not multiply by p^2). Multiplying by p^n, we get an equality $p^n((p^n)^2 m + q) = q_1 + i_1$. Hence, $p^n((p^n)^2 m + q) \geq 0$. Applying $S(6)_{of}$ we get $p^n \geq 0$ with n odd. A consequence of $S(6)_{of}$ is the simplification rule $x^3 \geq 0 \vdash x \geq 0$, which allows to deduce here $p \geq 0$ (multiply p^n by an even power of p in order to get $p^{3^k} \geq 0$).

So the theories of quasi-ordered rings, ordered fields and real closed fields prove the same facts since they collapse simultaneously. □

4 A Positivstellensatz for valued fields

We give in this section a new "Positivstellensatz" for valued fields. As we obtained in the last paragraph a constructive analog of the classical theorem "every real field can be totally ordered" we shall obtain here as a consequence a constructive version of the following theorem "the intersection of valuation rings of a field K containing a subring A is the integral closure of A" (Corollary 4.16).

4.1 Some simultaneous collapses

We need to consider a subring A of a field K. The language $\mathcal{L}_v$ will include the language $\mathcal{L}_1$ with its two unary predicates $= 0$ and $\neq 0$, and three more unary predicates $\mathrm{Vr}(x)$, $\mathrm{Rn}(x)$ and $\mathrm{U}(x)$ corresponding respectively to the elements of the valuation ring, the elements becoming zero in the residue field and the elements becoming invertible in the residue field.

A presentation in the language $\mathcal{L}_v$ is a set of variables G and five subsets $R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}}$ of $\mathbf{Z}[G]$. It is denoted by $(G; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$.

The most basic notion is the notion of valued field. The structure of proto-valued rings will be the simplest direct theory that we shall consider. We introduce this theory because it is a direct theory which collapses simultaneously with the theory of valued fields.

The axioms for *proto-valued rings* are axioms of rings and the following axioms.

$$\begin{array}{rll}
 & \vdash \mathrm{Vr}(-1) & D(1)_v \\
x=0,\ \mathrm{Vr}(y) & \vdash \mathrm{Vr}(x+y) & D(2)_v \\
\mathrm{Vr}(x),\ \mathrm{Vr}(y) & \vdash \mathrm{Vr}(xy) & D(3)_v \\
\mathrm{Vr}(x),\ \mathrm{Vr}(y) & \vdash \mathrm{Vr}(x+y) & D(4)_v \\
 & \vdash \mathrm{Rn}(0) & D(5)_v \\
x=0,\ \mathrm{Rn}(y) & \vdash \mathrm{Rn}(x+y) & D(6)_v \\
\mathrm{Rn}(x),\ \mathrm{Vr}(y) & \vdash \mathrm{Rn}(xy) & D(7)_v \\
\mathrm{Rn}(x),\ \mathrm{Rn}(y) & \vdash \mathrm{Rn}(x+y) & D(8)_v \\
 & \vdash \mathrm{U}(1) & D(9)_v \\
x=0,\ \mathrm{U}(y) & \vdash \mathrm{U}(x+y) & D(10)_v \\
\mathrm{U}(x),\ \mathrm{U}(y) & \vdash \mathrm{U}(xy) & D(11)_v \\
\mathrm{Rn}(x),\ \mathrm{U}(y) & \vdash \mathrm{U}(x+y) & D(12)_v \\
\mathrm{U}(x) & \vdash x\neq 0 & D(13)_v \\
x=0,\ y\neq 0 & \vdash x+y\neq 0 & D(14)_v \\
x\neq 0,\ y\neq 0 & \vdash xy\neq 0 & D(15)_v \\
\mathrm{U}(x) & \vdash \mathrm{Vr}(x) & D(16)_v \\
\mathrm{Rn}(x) & \vdash \mathrm{Vr}(x) & D(17)_v \\
(0\neq 0) & \vdash \bot & C_v
\end{array}$$

We add now the following axioms for *valued fields*

$$\begin{array}{rll}
xu-1=0 & \vdash x\neq 0 & S(1)_v \\
\mathrm{Vr}(xy),\ \mathrm{U}(x) & \vdash \mathrm{Vr}(y) & S(2)_v \\
x\neq 0 & \vdash \exists u\ xu-1=0 & Dy(1)_v \\
 & \vdash x=0\ \vee\ x\neq 0 & Dy(2)_v \\
xy=1 & \vdash \mathrm{Vr}(x)\ \vee\ \mathrm{Vr}(y) & Dy(3)_v \\
\mathrm{Vr}(x) & \vdash \mathrm{U}(x)\ \vee\ \mathrm{Rn}(x) & Dy(4)_v
\end{array}$$

Finally, the theory of *algebraically closed valued field* is obtained when adding the axioms of algebraic closure

$$\vdash \exists y\ y^n+x_{n-1}y^{n-1}+\cdots+x_1y+x_0=0 \qquad\qquad Dy_n(5)_v$$

Remark 4.1 We can extend the remarks 2.3 and 3.2 to this new theory. Here the order of the predicates is $=0$, Vr, Rn, U, $\neq 0$, and the collapse concerns this last predicate. The inclusion axioms are $D(16)_v$ and $D(17)_v$. Any proof using direct algebraic axioms may be transformed to a proof where the inclusion axioms are used only at the beginning. The facts $\vdash \mathrm{Vr}(1)$ and $\vdash \mathrm{Vr}(0)$ can be proved from the construction axioms for Vr. The construction axioms for Rn and U are doubled by construction axioms for Vr which allow to lift the inclusions at the beginning.

The order on the predicates and the inclusion axioms that we have distinguished agree with the characterization of the collapse of a presentation in the theory of proto-valued rings, and its proof. This collapse is particularly simple.

Proposition 4.2 *Let $\mathcal{K}=(G;R_{=0},R_{\neq 0},R_{\mathrm{Vr}},R_{\mathrm{Rn}},R_{\mathrm{U}})$ be a presentation in the language $\mathcal{L}_v$. Let $\mathcal{I}_{=0}$ be the ideal of $\mathbf{Z}[G]$ generated by $R_{=0}$, $\mathcal{M}_{\neq 0}$ the monoid generated by $R_{\neq 0}$, $\mathcal{V}_{\mathrm{Vr}}$ the subring generated by $R_{\mathrm{Vr}}\cup R_{\mathrm{Rn}}\cup R_{\mathrm{U}}$, $\mathcal{I}_{\mathrm{Rn}}$ the ideal of $\mathcal{V}_{\mathrm{Vr}}$ generated by R_{Rn} and $\mathcal{M}_{\mathrm{U}}$ the monoid generated by R_{U}.*

The presentation $\mathcal{K}$ collapses in the theory of proto-valued rings if and only if there is an equality in $\mathbf{Z}[G]$

$$m(u+j)+i=0$$

with $m\in\mathcal{M}_{\neq 0}$, $u\in\mathcal{M}_{\mathrm{U}}$, $j\in\mathcal{I}_{\mathrm{Rn}}$ and $i\in\mathcal{I}_{=0}$.

Proof: First consider dynamical proofs of facts using *only direct algebraic axioms*. These are algebraic proofs without branching.

Arguing inductively on the number of times the direct algebraic axioms are used in the proof we see successively that:

- provably $= 0$ elements, are exactly elements of $\mathcal{I}_{=0}$,
- provably Vr-elements, are exactly elements of the form $b + i$ with $b \in \mathcal{V}_{\mathrm{Vr}}$ and $i \in \mathcal{I}_{=0}$.
- provably Rn-elements, are exactly elements of of the form $j + i$ with $j \in \mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$.
- provably U-elements, are exactly elements of the form $u + j + i$ with $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$,
- provably $\neq 0$-elements, are exactly elements of the form $m(u + j) + i$ with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$.

Now a proof of collapse is given by a proof of $0 \neq 0$ using only direct algebraic axioms. Necessarily it produces an equality $m(u + j) + i = 0$ in $\mathbf{Z}[G]$. □

Theorem 4.3 *The theories of proto-valued rings, valued fields and algebraically closed valued field collapse simultaneously.*

Proof: The theorem is proved by induction on the number of times that the extra axioms for algebraically closed valued fields are used. So it is enough to prove the following lemma.

Lemma 4.4 *Let $\mathcal{K} = (G; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$ be a presentation in the language $\mathcal{L}_v$, $p, q \in \mathbf{Z}[G]$, z a new variable and $r(z)$ a z-monic polynomial in $\mathbf{Z}[G][z]$.*

a) If the presentation $\mathcal{K} \cup (p \neq 0)$ collapses in the theory of proto-valued rings, then so does the presentation $\mathcal{K} \cup (pq - 1 = 0)$.

b) If the presentation $\mathcal{K} \cup (\mathrm{Vr}(q))$ collapses in the theory of proto-valued rings, then so does the presentation $\mathcal{K} \cup (\mathrm{Vr}(pq), \mathrm{U}(p))$.

c) If the presentation $\mathcal{K} \cup (zp - 1 = 0)$ collapses in the theory of proto-valued rings, then so does the presentation $\mathcal{K} \cup (p \neq 0)$.

d) If the presentations $\mathcal{K} \cup (p \neq 0)$ and $\mathcal{K} \cup (p = 0)$ collapse in the theory of proto-valued rings, then so does the presentation $\mathcal{K}$.

e) If the presentations $\mathcal{K} \cup (\mathrm{Vr}(p))$ and $\mathcal{K} \cup (\mathrm{Vr}(q))$ collapse in the theory of proto-valued rings, then so does the presentation $\mathcal{K} \cup (qp - 1 = 0)$

f) If the presentations $\mathcal{K} \cup (\mathrm{U}(p))$ and $\mathcal{K} \cup (\mathrm{Rn}(p))$ collapse in the theory of proto-valued rings, then so does the presentation $\mathcal{K} \cup (\mathrm{Vr}(p))$.

g) If the presentation $\mathcal{K} \cup (r(z) = 0)$ collapse in the theory of proto-valued rings, then so does the presentation $\mathcal{K}$.

Proof: We take the following notations. Letters m, u, j, i, a, b (possibly with indices) represent always respectively elements of $\mathcal{M}_{\neq 0}, \mathcal{M}_{\mathrm{U}}, \mathcal{I}_{\mathrm{Rn}}, \mathcal{I}_{=0}, \mathcal{V}_{\mathrm{Vr}}, \mathbf{Z}[G]$ (defined as in proposition 4.2). The symbol $b(z)$ stands for a polynomial with coefficients in $\mathbf{Z}[G]$ and so on.

a) Left to the reader (see the analogous computation in lemma 2.6 a))

b) There is an equality $m(u + j(q)) + i = 0$. If the polynomial j is of degree n, multiplying the equality by p^n gives $m(p^n u + j_1(p, pq)) + i_1 = 0$ which is the collapse we want.

c) This is Rabinovitch's trick. There is an equality

$$m(u + j(z)) + i(z) + (zp - 1)b(z) = 0 \,.$$

Multiply by p^n where n is the maximum z-degree of the polynomials $i(z)$ and $j(z)$. Replace in $p^n i(z)$ and in $p^n j(z)$ all the $p^k z^k$ by 1 modulo $(zp - 1)$. We can assume that p is not $0 \in \mathbf{Z}[G]$. The new polynomial $b(z)$ is necessarily 0 and this gives the equality $p^n m(u + j_1) + i_1 = 0$ which is the collapse we want.

d) There are two equalities in $\mathbf{Z}[G]$:

$$p^n m_1(u_1 + j_1) + i_1 = 0 \qquad \text{and} \qquad m_2(u_2 + j_2) + i_2 = pb_2.$$

Raise the second one to the power n, multiply the result by $m_1(u_1 + j_1)$, multiply the first one by b_2^n and combine the two equalities so obtained in order to get the collapse we want.

e) There are two equalities in $\mathbf{Z}[G]$:

$$m_1(u_1 + j_1(p)) + i_1 = 0 \qquad \text{and} \qquad m_2(u_2 + j_2(q)) + i_2 = 0 \ .$$

Without loss of generality we can suppose that $m_1 = m_2 = m$. If n is the degree in p of j_1 one multiplies the first equality by q^n. Modulo $(pq - 1)$ the polynomial $q^n(u_1 + j_1(p))$ can be rewritten as a *nice* polynomial in q, $n_1(q)$, i. e. its leading coefficient is $u_1 + j_{1,0}$ (in $\mathcal{M}_{\mathrm{U}} + \mathcal{I}_{\mathrm{Rn}}$) and the other coefficients are in $\mathcal{I}_{\mathrm{Rn}}$. This gives an equality:

$$mn_1(q) + i_3 + (pq - 1)b_1 = 0 \qquad (1)$$

Doing the same manipulation with the second equality gives

$$mn_2(p) + i_4 + (pq - 1)b_2 = 0 \qquad (2)$$

One can then compute two polynomials $r_1(p, q)$ and $r_2(p, q)$ with coefficients in $\mathcal{V}_{\mathrm{Vr}}$ such that there is an equality $n_1(q)r_1(p, q) + n_2(p)r_2(p, q) = n_3(pq)$ where n_3 is nice too: take as n_3 the general polynomial whose roots are the products of a root of n_1 and a root of n_2.

Multiplying (1) by $r_1(p, q)$ and (2) by $r_2(p, q)$ and adding, we obtain:

$$mn_3(pq) + i_5 + (pq - 1)b_5 = 0 \ .$$

It remains to replace the pq in n_3 by 1 modulo $(pq - 1)$ to find the wanted collapse: $m(u_6 + j_6) + i_5 + (pq - 1)b_6 = 0$.

f) There are two equalities

$$m_1(p^n u_1 + j_1(p)) + i_1 = 0 \qquad \text{and} \qquad m_2(u_2 + j_2 + pa_2(p)) + i_2 = 0 \ .$$

Rewrite the second equality in the form $m_2(u_2 + j_2) = -(m_2 p a_2(p) + i_2)$. Raise it to the power n and multiply by $m_1 u_1$, so that the right-hand side becomes $(-1)^n m_1 m_2^n p^n u_1 a_2^p(n) + i_3$, and so on in order to get the collapse we want (last details to the reader).

g) We have an equality $m(u + j(z)) + i(z) = r(z)b(z)$. Reduce i and j modulo r, the right-hand side becomes identically zero and this gives an equality which is a collapse of $\mathcal{K}$. □

□

Corollary 4.5 *Let (K, A) be a valued field and L a field extension of K. Then the presentation obtained from diagrams of (K, A) and L does not collapse in the theory of valued fields.*

Proof: A collapse would give an equality $m(u + j) = 0$ in L, with u invertible in A, j in the maximal ideal of A and m nonzero in L. But this implies $u + j = 0$ in L, hence in K and this is impossible. □

Remark 4.6 The preceding corollary is a constructive version of the non-constructive theorem saying that a valuation of a field K can always be extended to any field extension L of K. This non-constructive theorem is a direct consequence of the corollary, obtained using completeness theorem of model theory.

In the same way we get a constructive version of the classical theorem saying that a local subring of a field K is always dominated by a valuation ring of K.

Corollary 4.7 *Let K be a valued field and $A \subset K$ a local ring. Then the presentation obtained from the diagram of (K, A) by adding* $\mathrm{Rn}(a)$ *when a is in the maximal ideal of A does not collapse in the theory of valued fields.*

In the same way we get a "formal Positivstellensatz for valued fields".

Proposition 4.8 (formal non-constructive version of Positivstellensatz for valued fields) *Let B be a ring and $(R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$ subsets of B. Let $\mathcal{I}_{=0}$ be the ideal of B generated by $R_{=0}$, $\mathcal{M}_{\neq 0}$ the monoid of B generated by $R_{\neq 0}$, $\mathcal{V}_{\mathrm{Vr}}$ the subring of B generated by $R_{\mathrm{Vr}} \cup R_{\mathrm{Rn}} \cup R_{\mathrm{U}}$, $\mathcal{I}_{\mathrm{Rn}}$ the ideal of $\mathcal{V}_{\mathrm{Vr}}$ generated by R_{Rn}, $\mathcal{M}_{\mathrm{U}}$ the monoid generated by R_{U}.*

The following properties are equivalent:

i) There exists $i \in \mathcal{I}_{=0}$, $s \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$ and $j \in \mathcal{I}_{\mathrm{Rn}}$ with $m(u+j)+i=0$

ii) There exists no homomorphism $\phi : B \to L$ with (L, A, I, U) an algebraically closed valued field, $\phi(n)=0$ for $n \in R_{=0}$, $\phi(t) \neq 0$ for $t \in R_{\neq 0}$, $\phi(c) \in A$ for $c \in R_{\mathrm{Vr}}$, $\phi(k) \in I$ for $k \in R_{\mathrm{Rn}}$ and $\phi(v) \in U$ for $v \in R_{\mathrm{U}}$.

Proof: Use the preceding results taking as presentation

$$\mathcal{DG}(B) \cup (\emptyset; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}}) \ ,$$

and apply the non-constructive completeness theorem of model theory. □

4.2 Decision algorithm and constructive Positivstellensatz

Theorem 4.9 (Positivstellensatz for algebraically closed valued fields) *Let (K, A) be a valued field and U_A the invertible elements of A, I_A the maximal ideal of A. Suppose that (K', A') is an algebraically closed valued field extension of K (so that $A = A' \cap K$). Denote by $U_{A'}$ the invertible elements of A', $I_{A'}$ the maximal ideal of A'.*

Consider five finite families $(R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$ in the polynomial ring $K[x_1, x_2, \cdots, x_m] = K[x]$.

Let $\mathcal{I}_{=0}$ be the ideal of $K[x]$ generated by $R_{=0}$, $\mathcal{M}_{\neq 0}$ the monoid of $K[x]$ generated by $R_{\neq 0}$, $\mathcal{V}_{\mathrm{Vr}}$ the subring of $K[x]$ generated by $R_{\mathrm{Vr}} \cup R_{\mathrm{Rn}} \cup R_{\mathrm{U}} \cup A$, $\mathcal{I}_{\mathrm{Rn}}$ the ideal of $\mathcal{V}_{\mathrm{Vr}}$ generated by $R_{\mathrm{Rn}} \cup I_A$, $\mathcal{M}_{\mathrm{U}}$ the monoid generated by $R_{\mathrm{U}} \cup U_A$.

Let $\mathcal{S} \subset K'^m$ be the set of points x satisfying the conditions: $n(x)=0$ for $n \in R_{=0}$, $t(x) \neq 0$ for $t \in R_{\neq 0}$, $c(x) \in A'$ for $c \in R_{\mathrm{Vr}}$, $v(x) \in U_{A'}$ for $v \in R_{\mathrm{U}}$, $k(x) \in I_{A'}$ for $k \in R_{\mathrm{Rn}}$.

The set $\mathcal{S}$ is empty if and only if there is an algebraic identity

$$m(u+j)+i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$.

Proof: We have the following result (see e.g. [34] section 3 or [17] section 3). The formal theory $\mathcal{V}(K, A)$ of algebraically closed valued fields extensions of a valued field (K, A) is complete and has a decision algorithm using only computations inside (K, A).

Consider now the presentation

$$\mathcal{P} = \mathcal{DG}(K, A) \cup (\{x_1, \ldots, x_m\}; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$$

in the language $\mathcal{L}_v$. Since the system of sign conditions we consider is impossible in (K', A'), it is thus proved impossible in $\mathcal{V}(K, A)$. According to theorem 1.1, the presentation $\mathcal{P}$ collapses in the theory of algebraically closed valued fields. We conclude by theorem 4.3 and proposition 4.2. □

Note that the same proof could have been used in the cases of algebraically closed fields and real closed fields, but there we were able to prove directly the existence of dynamical proofs because of particular features of the decisions algorithms for testing emptiness we used in these two cases. In fact, the proof in [17] can be transformed as well into an algorithm producing a dynamical proof in a more direct way.

4.3 Provable facts and generalized Positivstellensätze

We now discuss provability of facts in the theory of valued fields.

We define a *quasi-valued ring* as a proto-valued ring satisfying the following simplification axioms (the first one is an axiom of valued fields).

$$\begin{array}{rll} \mathrm{Vr}(xy),\ \mathrm{U}(x) & \vdash\ \mathrm{Vr}(y) & S(2)_v \\ \mathrm{U}(xy), \mathrm{Vr}(x), \mathrm{Vr}(y) & \vdash\ \mathrm{U}(y) & S(3)_v \\ \mathrm{Rn}(xy),\ \mathrm{U}(x) & \vdash\ \mathrm{Rn}(y) & S(4)_v \\ \mathrm{Rn}(x^2) & \vdash\ \mathrm{Rn}(x) & S(5)_v \\ xy \neq 0 & \vdash\ x \neq 0 & S(6)_v \\ xy = 0,\ x \neq 0 & \vdash\ y = 0 & S(7)_v \\ x^2 = 0 & \vdash\ x = 0 & S(8)_v \\ x^{n+1} - \sum_{k=0}^n a_k x^k = 0, \mathrm{Vr}(a_n), \cdots, \mathrm{Vr}(a_0) & \vdash\ \mathrm{Vr}(x) & S(9)_v \end{array}$$

The theory of quasi-valued rings is an algebraic theory and we shall see soon that it proves the same facts as the theory of algebraically closed valued fields.

It is easy to check the following lemmas.

Lemma 4.10 *Axioms of quasi-valued rings are valid dynamical rules in the theory of valued fields.*

Proof: Let us prove for example that $S(9)_v$ is a valid dynamical rule. Assume

$$x^{n+1} - \sum_{k=0}^{n} a_k x^k = 0,\ \mathrm{Vr}(a_n), \cdots,\ \mathrm{Vr}(a_0)\ . \tag{1}$$

Open two branches using axiom $Dy(2)_v$, the first one with $x = 0$ (so $\mathrm{Vr}(x)$) and the second one with $x \neq 0$. Here use axiom $Dy(1)_v$ and introduce the inverse y of x (so $xy = 1$). Then use axiom $Dy(3)_v$ and open two branches, the first one with $\mathrm{Vr}(x)$ (we are done) and the second one with $\mathrm{Vr}(y)$. Multiply the equality in (1) by y^n. Since $xy = 1$, we get $x = \sum_{k=0}^n a_k y^{n-k}$ and we deduce easily $\mathrm{Vr}(x)$. □

Lemma 4.11 *We have the following valid dynamical rules in the theory of quasi-valued rings.*

$$\begin{array}{rll} \mathrm{U}(xy),\ \mathrm{U}(x) & \vdash\ \mathrm{U}(y) & S(10)_v \\ x^{n+1} - \sum_{k=0}^n a_k x^k = 0, \mathrm{Vr}(a_n), \cdots, \mathrm{Vr}(a_1),\ \mathrm{U}(a_0) & \vdash\ \mathrm{U}(x) & S(11)_v \end{array}$$

Lemma 4.12 *The theories of proto-valued rings, quasi-valued rings, valued fields and algebraically closed valued fields collapse simultaneously.*

Lemma 4.13 *Let $\mathcal{K} = (G; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$ be a presentation in the language $\mathcal{L}_v$. Let p be an element of $\mathbf{Z}[G]$ and z a new variable.*

a) In the theory of valued fields, the fact $p = 0$ is provable from the presentation $\mathcal{K}$ if and only if the presentation $\mathcal{K} \cup (p \neq 0)$ collapses.

b) In the theory of valued fields, the fact $p \neq 0$ is provable from the presentation $\mathcal{K}$ if and only if the presentation $\mathcal{K} \cup (p = 0)$ collapses.

c) In the theory of valued fields, the fact $\mathrm{Vr}(p)$ is provable from the presentation $\mathcal{K}$ if and only if the presentation $\mathcal{K} \cup (zp - 1 = 0, \mathrm{Rn}(z))$ collapses.

d) In the theory of valued fields, the fact $\mathrm{Rn}(p)$ is provable from the presentation $\mathcal{K}$ if and only if the presentation $\mathcal{K} \cup (zp - 1 = 0, \mathrm{Vr}(z))$ collapses.

e) In the theory of valued fields, the fact $\mathrm{U}(p)$ is provable from the presentation $\mathcal{K}$ if and only if the presentations $\mathcal{K} \cup (zp - 1 = 0, \mathrm{Rn}(z))$ and $\mathcal{K} \cup (\mathrm{Rn}(p))$ collapse.

Remark that the last lemma is a fortiori true for algebraically closed valued fields. So theories of valued fields and algebraically closed valued fields prove the same facts since they collapse simultaneously.

From the last lemma and the algebraic characterization of collapses of presentations in the theory of valued fields, one can prove the following proposition.

Proposition 4.14 *Let $\mathcal{K} = (G; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$ be a presentation in the language $\mathcal{L}_v$. Let p be an element of $\mathbf{Z}[G]$. Define $\mathcal{I}_{=0}$, $\mathcal{M}_{\neq 0}$, $\mathcal{V}_{\mathrm{Vr}}$, $\mathcal{I}_{\mathrm{Rn}}$ and $\mathcal{M}_{\mathrm{U}}$ as in proposition 4.2.*

a) In the theory of valued fields, a dynamical proof of the fact $p = 0$ from the presentation $\mathcal{K}$ produces an equality in $\mathbf{Z}[G]$ of the following type

$$p^n m(u + j) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$.

b) In the theory of valued fields, a dynamical proof of the fact $p \neq 0$ from the presentation $\mathcal{K}$ produces an equality in $\mathbf{Z}[G]$ of the following type

$$m(u + j) + i + bp = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$, $i \in \mathcal{I}_{=0}$ and $b \in \mathbf{Z}[G]$.

c) In the theory of valued fields, a dynamical proof of the fact $\mathrm{Vr}(p)$ from the presentation $\mathcal{K}$ produces an equality in $\mathbf{Z}[G]$ of the following type

$$m((u + j)p^{n+1} + a_n p^n + \ldots + a_1 p + a_0) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$, the $a_k \in \mathcal{V}_{\mathrm{Vr}}$ and $i \in \mathcal{I}_{=0}$.

d) In the theory of valued fields, a dynamical proof of the fact $\mathrm{Rn}(p)$ from the presentation $\mathcal{K}$ produces an equality in $\mathbf{Z}[G]$ of the following type

$$m((u + j)p^{n+1} + j_n p^n + \ldots + j_1 p + j_0) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, j and the j_k in $\mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$.

e) In the theory of valued fields, a dynamical proof of the fact $\mathrm{U}(p)$ from the presentation $\mathcal{K}$ produces an equality in $\mathbf{Z}[G]$ of the following type

$$m((u + j)p^{n+1} + a_n p^n + \ldots + a_1 p + (u' + j')) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u, u' \in \mathcal{M}_{\mathrm{U}}$, $j, j' \in \mathcal{I}_{\mathrm{Rn}}$, the a_k in $\mathcal{V}_{\mathrm{Vr}}$ and $i \in \mathcal{I}_{=0}$.

Proof: We use the same letter notations as in lemma 4.4.

We get a) and b) as immediate consequences of lemma 4.13 a) and b).

In c), d) and e) the stated conditions are sufficient because valued fields have good simplification axioms (cf. lemmas 4.10 and 4.11). Let us see that they are necessary conditions.

For c), use lemma 4.13 c) and write the collapse of the presentation $\mathcal{K} \cup (zp - 1 = 0, \mathrm{Rn}(z))$. We get an equality $(u_1 + j_1 + za_1(z)) + i_1(z) = (pz - 1)b_1(z)$. Let n be the maximum of the z-degrees of $za_1(z)$ and $i_1(z)$. Multiply the equality by p^n and replace in the left-hand side each $p^k z^k$ by 1 modulo $(zp - 1)$. After this transformation the right-hand side becomes 0 and we get an equality $m_1((u_1 + j_1)p^n + a_2(p)) + i_2 = 0$ where the p-degree of a_2 is $\leq n$. So we are done.

Same proof for d).

For e) we have two equalities from collapses: $m_1((u_1+j_1)p^{n+1}+a_{1,n}p^n+\cdots+a_{1,1}p+a_{1,0})+i_1 = 0$ and $m_2(a_{2,m}p^m + \cdots + a_{2,1}p + (u_2 + j_2)) + i_2 = 0$. We assume w.l.o.g. that $m_1 = m_2 = m$, Multiply the first equality by a convenient power of p (e.g. p^{n+1}) and add the two equalities. □

Remark 4.15 From c) we get as corollary a constructive version of the classical theorem saying that the intersection of valuation rings containing the subring A of a field K is the integral closure of A in K.

Corollary 4.16 *Let A be subring of a field K. Consider the presentation $\mathcal{K}$ obtained from the diagram of K adding $\mathrm{Vr}(a)$ for each $a \in A$. Let $u \in K$. Then the fact $\mathrm{Vr}(u)$ is provable from $\mathcal{K}$ in the theory of valued fields if and only if u is in the integral closure of A in K.*

Theorem 4.17 *The theories of quasi-valued rings, valued fields and algebraically closed valued fields prove the same facts.*

Proof: The proposition 4.14 gives necessary and sufficient conditions for provable facts in the theory of valued fields. It is thus sufficient to see that the necessary conditions are also sufficient in the theory of quasi-valued rings.

The case $p = 0$ is taken care of by the axioms

$$\begin{aligned} x \neq 0, xy = 0 &\vdash y = 0 \\ x^2 = 0 &\vdash x = 0 \end{aligned}$$

The case $p \neq 0$ is taken care of by $xy \neq 0 \vdash x \neq 0$

The case $\mathrm{Vr}(p)$ is taken care of by

$$\begin{aligned} x \neq 0, xy = 0 &\vdash y = 0 \\ x^{n+1} - \sum_{k=0}^{n} a_k x^k = 0, \mathrm{Vr}(a_n), \cdots, \mathrm{Vr}(a_0) &\vdash \mathrm{Vr}(x) \\ \mathrm{Vr}(xy), \mathrm{U}(x) &\vdash \mathrm{Vr}(y) \end{aligned}$$

The case $\mathrm{Rn}(p)$ is taken care of by

$$\begin{aligned} x \neq 0, xy = 0 &\vdash y = 0 \\ x^{n+1} - \sum_{k=0}^{n} a_k x^k = 0, \mathrm{Vr}(a_n), \cdots, \mathrm{Vr}(a_0) &\vdash \mathrm{Vr}(x) \\ \mathrm{Rn}(xy), \mathrm{U}(x) &\vdash \mathrm{Rn}(y) \\ \mathrm{Rn}(x^2) &\vdash \mathrm{Rn}(x) \end{aligned}$$

The case $\mathrm{U}(p)$ is taken care of by

$$\begin{aligned} x \neq 0, xy = 0 &\vdash y = 0 \\ x^{n+1} - \sum_{k=0}^{n} a_k x^k = 0, \mathrm{Vr}(a_n), \cdots, \mathrm{Vr}(a_1), \mathrm{U}(a_0) &\vdash \mathrm{U}(x) \\ \mathrm{U}(xy), \mathrm{U}(x) &\vdash \mathrm{U}(y) \end{aligned}$$

□

Finally, we get from theorem 4.9 (with the same proof as in proposition 4.14) the following generalized Positivstellensatz.

Theorem 4.18 (generalized Positivstellensatz for algebraically closed valued fields) *Let (K, A) be a valued field and let U_A be the invertible elements of A, I_A the maximal ideal of A. Suppose that (K', A') is an algebraically closed valued field extension of K (so that $A = A' \cap K$). Denote by $U_{A'}$ the invertible elements of A', $I_{A'}$ the maximal ideal of A'.*

Consider five finite families $(R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$ in the polynomial ring $K[x_1, x_2, \cdots, x_m] = K[x]$.

Let $\mathcal{I}_{=0}$ be the ideal of $K[x]$ generated by $R_{=0}$, $\mathcal{M}_{\neq 0}$ the monoid of $K[x]$ generated by $R_{\neq 0}$, $\mathcal{V}_{\mathrm{Vr}}$ the subring of $K[x]$ generated by $R_{\mathrm{Vr}} \cup R_{\mathrm{Rn}} \cup R_{\mathrm{U}} \cup A$, $\mathcal{I}_{\mathrm{Rn}}$ the ideal of $\mathcal{V}_{\mathrm{Vr}}$ generated by $R_{\mathrm{Rn}} \cup I_A$, $\mathcal{M}_{\mathrm{U}}$ the monoid generated by $R_{\mathrm{U}} \cup U_A$.

Let $\mathcal{S}$ be the set of $x \in K'^m$ such that $n(x) = 0$ for $n \in R_{=0}$, $t(x) \neq 0$ for $t \in R_{\neq 0}$, $c(x) \in A'$ for $c \in R_{\mathrm{Vr}}$, $v(x) \in U_{A'}$ for $v \in R_{\mathrm{U}}$ and $k(x) \in I_{A'}$ for $k \in R_{\mathrm{Rn}}$.

a) The polynomial p is everywhere zero on $\mathcal{S}$ if and only if there is an equality

$$p^n m(u + j) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$ and $i \in \mathcal{I}_{=0}$.

b) The polynomial p is everywhere nonzero on $\mathcal{S}$ if and only if there is an equality:

$$m(u + j) + i + bp = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$, $i \in \mathcal{I}_{=0}$ *and* $b \in K[x]$.

c) $p(\mathcal{S}) \subset A'$ *if and only if there is an equality*

$$m((u+j)p^{n+1} + a_n p^n + \cdots + a_1 p + a) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j \in \mathcal{I}_{\mathrm{Rn}}$, *the* $a_k \in \mathcal{V}_{\mathrm{Vr}}$ *and* $i \in \mathcal{I}_{=0}$.

d) $p(\mathcal{S}) \subset I_{A'}$ *if and only if there is an equality*

$$m((u+j)p^{n+1} + j_n p^n + \cdots + j_1 p + j) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, j *and the* j_k *in* $\mathcal{I}_{\mathrm{Rn}}$ *and* $i \in \mathcal{I}_{=0}$.

e) $p(\mathcal{S}) \subset U_{A'}$ *if and only if there is an equality:*

$$m((u+j)p^{n+1} + a_n p^n + \cdots + a_1 p + (u'+j')) + i = 0$$

with $m \in \mathcal{M}_{\neq 0}$, $u, u' \in \mathcal{M}_{\mathrm{U}}$, $j, j' \in \mathcal{I}_{\mathrm{Rn}}$, *the* a_k *in* $\mathcal{V}_{\mathrm{Vr}}$ *and* $i \in \mathcal{I}_{=0}$.

4.4 Related results of Prestel-Ripoli

Our Positivstellensatz for valued fields is closely related to some results of Prestel and Ripoli (cf. [30]). The paper [5] of Coquand and Persson also contains another kind of formal "IntegralvalueStellensatz".

The direct part of Theorem 3.1 in [30] has the following consequence.

Theorem 4.19 (integral-valued rational functions on algebraically closed valued fields) *Let* (K, A) *be a valued field,* U_A *the group of invertible elements of* A *and* I_A *the maximal ideal of* A. *Let* (K', A') *be an algebraic closure of* (K, A) *as valued field (so that* $A = A' \cap K$*). Let us denote* $A[x_1, x_2, \ldots, x_m] = A[x]$, $K(x_1, x_2, \ldots, x_m) = K(x)$ *and* $\mathcal{I}_{\mathrm{Rn}} = I_A[x]$ *the ideal of* $A[x]$ *generated by* I_A.
Assume that K *is dense in* K', *i.e., the residue field is algebraically closed and the value group is divisible. Consider a rational function* $f = f_1/f_2 \in K(x)$ *with* f_1 *and* f_2 *in* $A[x]$ $(f_2 \neq 0)$.
Then the following two assertions are equivalent:

a) Whenever $\xi \in A^m$ *and* $f_2(\xi) \neq 0$ *then* $f(\xi) \in A$ *(in this case we write* $f(A) \subset A$*).*

b) There exists an algebraic identity in $A[x]$*:*

$$(1+j)f_1 = af_2$$

with $j \in I_A[x]$ *and* $a \in A[x]$ *(in this case* $f(x) = a(x)/(1+j(x))$ *and we write* $f \in A[x]/(1+I_A[x])$*)*

A. Prestel also told us that he had obtained a Nullstellensatz (characterizing polynomials g s.t. $g(\xi) = 0$ whenever $\xi \in A^m$ and $h_1(\xi) = \cdots = h_m(\xi) = 0$) when K is algebraically closed, by using the same techniques as in [30].

We remark that in [30] the result is an abstract one, with no constructive proof. Let us deduce this result (as an algorithmic one) from our Positivstellensatz.

First remark that it suffices to consider the case that K is algebraically closed.

In a more general case, with K not necessarily dense in K' we get the slightly more general following result, which is a "rational version" of theorem 4.19.

Theorem 4.20 (integral-valued rational functions on valued fields) *Let* (K, A) *be a valued field,* U_A *the group of invertible elements of* A *and* I_A *the maximal ideal of* A. *Let* (K', A') *be an algebraic closed valued field extension of* (K, A) *(so that* $A = A' \cap K$*). Let us denote* $A[x_1, x_2, \ldots, x_m] = A[x]$, $K(x_1, x_2, \ldots, x_m) = K(x)$ *and* $\mathcal{I}_{\mathrm{Rn}} = I_A[x]$ *the ideal of* $A[x]$ *generated by* I_A.
Consider a rational function $f = f_1/f_2 \in K(x)$ *with* f_1 *and* f_2 *in* $A[x]$ $(f_2 \neq 0)$.
Then the two following assertions are equivalent:

a) Whenever $\xi \in A'^m$ *and* $f_2(\xi) \neq 0$ *then* $f(\xi) \in A'$ *(i.e.,* $f(A') \subset A'$*).*

b) There exists an algebraic identity in $A[x]$:

$$(1+j)f_1 = af_2$$

with $j \in I_A[x]$ and $a \in A[x]$ (i.e., $f \in A[x]/(1+I_A[x])$)

Proof: Clearly b) implies a). Assume now a). The fact that $f(A') \subset A'$ means the same thing as the incompatibility of the following system of "sign conditions":

$$\mathrm{Vr}(\xi_1),\ \ldots,\ \mathrm{Vr}(\xi_m),\ f_2(\xi) \neq 0,\ \mathrm{Rn}(\zeta),\ f_2(\xi) = \zeta f_1(\xi)$$

From theorem 4.9 this implies an equality in $K[x,z]$

$$sf_2^k(x)(u + j(x) + za(x,z)) = (f_2(x) - zf_1(x))\, b(x,z)$$

with $s \neq 0$ in K, $u \in U_A$, $j \in I_A[x]$, $a(x,z) \in A[x,z]$ and $b \in K[x,z]$. Multiplying by $(su)^{-1}$ we get an algebraic identity:

$$f_2^k(x)[1 + j_1(x) + za_1(x,z)] = (f_2(x) - zf_1(x))\, b_1(x,z)$$

Let $a_1(x,z) = a_{1,0} + a_{1,1}z + \cdots + a_{1,p-1}z^{p-1}$. Applying the Rabinowitch's trick, we multiply by f_1^p, replace in the left-hand side $z^h f_1^h$ by f_2^h modulo $(f_2(x) - zf_1(x))$, and we get an algebraic identity:

$$f_2^k(x)[(1 + j_1(x))f_1^p + a_{1,0}(x)f_1^{p-1}f_2 + a_{1,2}(x)f_1^{p-2}f_2^2 + \cdots + a_{1,p-1}(x)f_2^p] \ = 0$$

We deduce:

$$(1 + j_1(x))f_1^p + a_{1,0}(x)f_1^{p-1}f_2 + a_{1,2}(x)f_1^{p-2}f_2^2 + \cdots + a_{1,p-1}(x)f_2^p = 0$$

i.e., $f = f_1/f_2$ is in the integral closure of $A[x]_S$ where S is the monoid $1 + I_A[x]$. It is well known that $A[x]$ is integrally closed. So $A[x]_S$ is also integrally closed. And we get what we want. □

5 A Positivstellensatz for ordered groups

Our theory is based on the purely equational theory of abelian groups. The group law is denoted additively. We have 0 as only constant. The purely equational theory of abelian groups can be put in unary form. The free abelian group generated by a set of generators G will be denoted by $\mathrm{Ab}(G)$. The unary predicate is $x = 0$. Terms are replaced by elements of $\mathrm{Ab}(G)$. We call $\mathcal{L}_g$ the unary language of abelian groups. There are three direct algebraic axioms:

$$\begin{array}{rll} & \vdash\ 0 = 0 & D(1)_g \\ x = 0, y = 0 & \vdash\ x + y = 0 & D(2)_g \\ x = 0 & \vdash\ -x = 0 & D(3)_g \end{array}$$

If H is an abelian group and $x_1, \ldots, x_n$ are variables, the abelian group generated by H and $x_1, \ldots, x_n$ (i.e., the group of affine forms with variables $x_1, \ldots, x_n$, constant part in H and coefficients in $\mathbf{Z}$) will be denoted by $H\{x_1, \ldots, x_n\}$.

In the sequel we say group instead of abelian group.

The central theory we consider is the theory of *(abelian) ordered groups.*

The language $\mathcal{L}_{og}$ of ordered groups is the unary language of abelian groups $\mathcal{L}_g$ with two more unary predicates $x \geq 0$ and $x > 0$.

Axioms of *proto-ordered groups* are the following.

$$\begin{array}{rll} x = 0,\ y \geq 0 & \vdash\ x + y \geq 0 & D(1)_{og} \\ x \geq 0,\ y \geq 0 & \vdash\ x + y \geq 0 & D(2)_{og} \\ & \vdash\ 0 \geq 0 & D(3)_{og} \\ x = 0,\ y > 0 & \vdash\ x + y > 0 & D(4)_{og} \\ x > 0,\ y \geq 0 & \vdash\ x + y > 0 & D(5)_{og} \\ x > 0 & \vdash\ x \geq 0 & D(6)_{og} \\ 0 > 0 & \vdash\ \bot & C_{og} \end{array}$$

Axioms of *ordered groups* are axioms of proto-ordered groups and the three axioms

$$\begin{array}{rll} x \geq 0,\ -x \geq 0 & \vdash\ x = 0 & S(1)_{og} \\ & \vdash\ x \geq 0\ \vee\ -x \geq 0 & Dy(1)_{og} \\ x \geq 0 & \vdash\ x = 0\ \vee\ x > 0 & Dy(2)_{og} \end{array}$$

Remark 5.1 Here also we can see a structure similar to that outlined in Remark 2.3. The order on the predicates is $= 0, \geq 0, > 0$. The axiom $D(6)_{og}$ is an inclusion axiom, and the other direct algebraic axioms are construction axioms.

A *divisible ordered group* is an ordered group satisfying the following dynamical axioms (one for each integer $n > 1$):

$$\vdash\ \exists y\ ny = x \qquad Dy_n(3)_{og}$$

We have easily the following results.

Proposition 5.2 *Let $\mathcal{H} = (G; R_{=0}, R_{\geq 0}, R_{>0})$ be a presentation in the language $\mathcal{L}_{og}$. Let $\mathcal{H}_{=0}$ be the subgroup of $\mathrm{Ab}(G)$ generated by $R_{=0}$, and $\mathcal{P}_{\geq 0}$ the additive monoid in $\mathrm{Ab}(G)$ generated by $R_{\geq 0} \cup R_{>0}$. A collapse of the presentation $\mathcal{H}$ in the theory of proto-ordered groups produces an equality in G*

$$s + q + i = 0$$

with $s \in R_{>0}$, $q \in \mathcal{P}_{\geq 0}$ and $i \in \mathcal{H}_{=0}$.

Lemma 5.3 *Let $\mathcal{H} = (G; R_{=0}, R_{\geq 0}, R_{>0})$ be a presentation in the language $\mathcal{L}_{og}$, $p \in \mathrm{Ab}(G)$ and y a new variable.*

a) If the presentation $\mathcal{H} \cup (p = 0)$ collapses in the theory of proto-ordered groups, then so does the presentation $\mathcal{H} \cup (p \geq 0,\ -p \geq 0)$.

b) If the presentations $\mathcal{H} \cup (p \geq 0)$ and $\mathcal{H} \cup (-p \geq 0)$ collapse in the theory of proto-ordered groups, then so does the presentation $\mathcal{H}$.

c) If the presentations $\mathcal{H} \cup (p > 0)$ and $\mathcal{H} \cup (p = 0)$ collapse in the theory of proto-ordered groups, then so does the presentation $\mathcal{H} \cup (p \geq 0)$.

d) If the presentation $\mathcal{H} \cup (ny - p = 0)$ collapses in the theory of proto-ordered groups, then so does the presentation $\mathcal{H}$.

Proposition 5.4 *The theories of proto-ordered groups, ordered groups and divisible ordered groups collapse simultaneously.*

Proposition 5.5 (non-constructive formal Positivstellensatz) *Let H be an abelian group, $R_{=0}$, $R_{\geq 0}$ and $R_{>0}$ three families of elements of H. Let $\mathcal{H}_{=0}$ be the subgroup of H generated by $R_{=0}$, and $\mathcal{P}_{\geq 0}$ the additive monoid in H generated by $R_{\geq 0} \cup R_{>0}$. Then the following properties are equivalent:*

i) There exist $s \in R_{>0}$, $q \in \mathcal{P}_{\geq 0}$ and $i \in \mathcal{H}_{=0}$ with $s + q + i = 0$ in H

ii) There exists no homomorphism $\phi : H \to L$ with L a divisible ordered group, $\phi(a) = 0$ for $a \in R_{=0}$, $\phi(p) \geq 0$ for $p \in R_{\geq 0}$ and $\phi(s) > 0$ for $s \in R_{>0}$.

iii) There exists no ordering of any quotient group H/H_0 with $R_{=0} \subset H_0$, $R_{>0} + H_0 \subset (H/H_0)^{>0}$ and $R_{\geq 0} + H_0 \subset (H/H_0)^{\geq 0}$.

Decision algorithm and constructive Positivstellensatz

The next theorem is easily obtained by a close inspection of a decision algorithm for testing emptiness in the theory of divisible ordered groups.

Theorem 5.6 *Let H be an ordered group, D its divisible ordered closure, and $R_{=0}, R_{\geq 0}, R_{>0}$ three finite families of $H\{x_1, x_2, \cdots, x_m\} = H\{x\}$. The system of sign conditions $[u(x) > 0, q(x) \geq 0, j(x) = 0]$ for $u \in R_{>0}$, $q \in R_{\geq 0}$, $j \in R_{=0}$ is impossible in D^n if and only if the presentation $\mathcal{DG}(H) \cup (\{x_1, x_2, \cdots, x_m\}; R_{=0}, R_{\geq 0}, R_{>0})$ collapses in the theory of divisible ordered groups.*

Proof: (sketch)

Call x the variable you want to eliminate in an existential assertion for a system of signs conditions. Call y the other variables considered as parameters. Write every sign condition in form $nx = t(y)$ with $n \in \mathbf{Z}^{\geq 0}$ and $t(y) \in H\{y\}$, or $nx > t(y)$ with $n \in \mathbf{Z}$ and $t(y) \in H\{y\}$, or $nx \geq t(y)$ with $n \in \mathbf{Z}$ and $t(y) \in H\{y\}$. Any sign condition is equivalent to the same one multiplied by a positive integer.

If there is one sign condition of the first type and $n > 0$, multiply all other conditions by n and then substitute nx by the value given by the first sign condition. So you get an equivalent system with x in only the first equality. The existence of x in D is equivalent to the other conditions without x.

In the other case, you may assume w.l.o.g. that you have, for all sign conditions with $n \neq 0$ the same absolute value for n. For example you have the system $(t_1 \geq nx, t_2 \geq nx, t_3 > nx, nx \geq t_4, nx > t_5)$ (S) (and other conditions without x). The existence of an x in D verifying (S) is equivalent to a big disjunction of systems "without x", each disjunct saying in what order are the t_i. E.g. one of these disjuncts is $(t_1 \geq t_2, t_2 \geq t_3, t_3 > t_5, t_5 \geq t_4)$. Clearly there is a covering of $\mathcal{DG}(H) \cup (\{y, x\}; R_{=0}, R_{\geq 0}, R_{>0})$ in the theory of divisible ordered groups corresponding to this equivalence.

So eliminating one variable after the other, you get a covering where every leaf contains only conditions in H. If the system is impossible you have a collapse of the presentation in the theory of divisible ordered groups. In the other case you may construct a point in D^m corresponding to a leaf of your tree. □

Then, gluing theorem 5.6, proposition 5.4 and proposition 5.2 we get the "baby Positivstellensatz".

Theorem 5.7 *Let H be an ordered group, D its divisible ordered closure, and $R_{=0}, R_{\geq 0}, R_{>0}$ three finite families of $H\{x_1, x_2, \cdots, x_n\} = H\{x\}$. Let $\mathcal{H}_{=0}$ be the subgroup of $H\{x\}$ generated by $R_{=0}$, and $\mathcal{P}_{\geq 0}$ the additive monoid in $H\{x\}$ generated by $R_{\geq 0} \cup R_{>0} \cup H^{>0}$.*

The system of sign conditions $[u(x) > 0, q(x) \geq 0, j(x) = 0]$ for $u \in R_{>0}$, $q \in R_{\geq 0}$, $j \in R_{=0}$ is impossible in D^n if and only if there is an equality in $H\{x\}$

$$s + q + i = 0$$

with $s \in R_{>0} \cup H^{>0}$, $q \in \mathcal{P}_{\geq 0}$ and $i \in \mathcal{H}_{=0}$.

We give now a variant.

Theorem 5.8 *Let H be an ordered group, D its divisible ordered closure, and $R_{=0}, R_{\geq 0}, R_{>0}$ three finite families of $H\{x_1, x_2, \cdots, x_n\} = H\{x\}$ and $p \in H\{x\}$. Let $\mathcal{H}_{=0}$ be the subgroup of $H\{x\}$ generated by $R_{=0}$, and $\mathcal{P}_{\geq 0}$ the additive monoid in $H\{x\}$ generated by $R_{\geq 0} \cup R_{>0} \cup H^{>0}$.*

Let $\mathcal{S} \subset D^n$ the "semialgebraic" set $\{x \in D^n; u(x) > 0, q(x) \geq 0, j(x) = 0$ for $u \in R_{>0}$, $q \in R_{\geq 0}$, $j \in R_{=0}\}$.

a) p is positive on $\mathcal{S}$ if and only if there is an equality in $H\{x\}$

$$s + q + i = mp$$

with $s \in R_{>0} \cup H^{>0}$, $q \in \mathcal{P}_{\geq 0}$, $i \in \mathcal{H}_{=0}$ and m a nonnegative integer.

b) Assume $\mathcal{S}$ to be nonempty, then p is nonnegative on $\mathcal{S}$ if and only if there is an equality in $H\{x\}$

$$q + i = mp$$

with $q \in \mathcal{P}_{\geq 0}$, $i \in \mathcal{H}_{=0}$ and m a positive integer.

c) Assume $\mathcal{S}$ to be nonempty, then p is null on $\mathcal{S}$ if and only if there are two equalities in $H\{x\}$

$$q + i = mp \qquad \text{and} \qquad -q' + i' = mp$$

with $q, q' \in \mathcal{P}_{\geq 0}$, $i, i' \in \mathcal{H}_{=0}$ and m a positive integer.

d) p is nonzero on $\mathcal{S}$ if and only if there is an equality in $H\{x\}$

$$s + q + i = mp$$

with $s \in R_{>0} \cup H^{>0}$, $q \in \mathcal{P}_{\geq 0}$, $i \in \mathcal{H}_{=0}$ and m an integer.

Finally we give an algebraic theory, the theory of *quasi-ordered groups* which proves the same facts as theories of ordered groups and ordered divisible groups.

Axioms are those of proto-ordered groups and the following simplification axioms.

$$\begin{array}{rll} x \geq 0,\ -x \geq 0 & \vdash\ x = 0 & S(1)_{og} \\ nx \geq 0 & \vdash\ x \geq 0 & S_n(2)_{og} \\ nx > 0 & \vdash\ x > 0 & S_n(3)_{og} \end{array}$$

Remark 5.9 Previous results are closely related to well known theorems in linear programming over $\mathbf{Q}$. E.g., applying theorem 5.7 with $H = \mathbf{Q}$ and $R_{=0} = \emptyset$ we get the Motzkin's transposition theorem (see [31] corollary 7.1k p.94). Similarly, when $H = \mathbf{Q}$ and $R_{=0} = R_{>0} = \emptyset$ we get a variant of Farka's lemma (see [31] corollary 7.1e p.89).

References

[1] Bastiani A., Ehresmann C.: *Categories of sketched structures.* Cahiers de topologie et geometrie differentielle 13 (2), 1972. 4

[2] Bochnak J., Coste M., Roy M.-F.: *Géometrie Algébrique Réelle.* Springer-Verlag. Ergeb. M. n 11. 1987.

[3] Coppey L., Lair C.: *Leçons de théorie des esquisses (I).* Diagramme **12**. Paris, 1984 4

[4] Coppey L., Lair C.: *Leçons de théorie des esquisses (II).* Diagramme **19**. Paris, 1988 4

[5] Coquand T., Persson H.: *Valuations and Dedekind's Prague Theorem.* To appear in J. Pure Appl. Algebra. 37

[6] Della Dora J., Dicrescenzo C., Duval D.: *About a new method for computing in algebraic number fields.* In Caviness B.F. (Ed.): EUROCAL '85. Lecture Notes in Computer Science 204, 289–290. Springer 1985. 4

[7] Dicrescenzo C., Duval D.: *Algebraic extensions and algebraic closure in Scratchpad.* In Gianni P., (Ed.): Symbolic and Algebraic Computation. Lecture Notes in Computer Science 358, 440–446. Springer 1989. 4

[8] Duval, D.: *Simultaneous computations in fields of arbitrary characteristic.* In Kaltofen E., Watt S.M. (Eds.): Computers and Mathematics, 321– 326. Springer 1989. 4

[9] Duval D., Gonzalez-Vega L.: *Dynamic evaluation and real closure.* Symbolic computation, new trends and developments (Lille, 1993). Math. Comput. Simulation **42** (1996), 551–560. 4

[10] Duval D., Reynaud J.-C.: *Esquisses et Calcul.* Annales Universite Caen. Vol VII (1989-1990) p 15-83. (J. Dehornoy, editeur) 4

[11] Duval D., Reynaud J.-C.: *Sketches and Computation (Part I) Basic Definitions and Static Evaluation.* Mathematical Structures in Computer Science **4** (1994) 185–238. 4

[12] Duval D., Reynaud J.-C.: *Sketches and Computation (Part II) Dynamic Evaluation and Applications.* Mathematical Structures in Computer Science **4** (1994) 239–271. 4

[13] Duval D., Senechaud P.: *Sketches and Parametrization.* Theoretical Computer Science, **123** (1) (1994) 117–130 4

[14] Ehresmann C.: *Esquisses et types de structures algébriques.* Bulletin de l'Institut Polytechnique Iasi 14, 1968. 4

[15] Gomez-Diaz T.: *Examples of using dynamic constructible closure.* Symbolic computation, new trends and developments (Lille, 1993). Math. Comput. Simulation **42** (1996), 375–383. 4, 18

[16] Joyal A.: *Théorème de Chevalley-Tarski et remarque sur l'algèbre constructive.* Cahiers de Topologie et Géométrie Différentielle **16** (1975) 256–258 17

[17] Kuhlmann F.-V., Lombardi H., Perdry H.: *Dynamic computations inside the algebraic closure of a valued field.* Preprint 2000 33

[18] Lombardi H.: *Théorème effectif des zéros réel et variantes.* Publications Mathématiques Besançon. Théorie des Nombres, 88–89. Fascicule 1. English abridged version: Effective real nullstellensatz and variants. p. 263- 288 in Effective Methods in Algebraic Geometry. Ed. Mora T., Traverso C. Birkhauser 1991. Progress in Math. n 94. 21

[19] Lombardi H.: *Une borne sur les degrés pour le Théoreme des zéros réel effectif.* p 323–345. In: Real Algebraic Geometry. Proceedings, Rennes 1991, Lecture Notes in Mathematics n 1524. Eds.: Coste M., Mahe L., Roy M.-F. (Springer-Verlag, 1992). 27

[20] Lombardi H.: *Relecture constructive de la théorie d'Artin- Schreier.* Annals of Pure and Applied Logic **91**, (1998), 59–92. 3

[21] Lombardi H.: *Le contenu constructif d'un principe local- global avec une application à la structure d'un module projectif de type fini.* Publications Mathématiques de Besançon. Théorie des nombres. Fascicule 94–95 & 95–96, 1997. 3

[22] Lombardi H.: *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Preprint 1998. 3

[23] Lombardi H.: *Platitude, localisation et anneaux de Prüfer : une approche constructive.* Preprint 1999. 3

[24] Lombardi H.: *Constructions cachées en algèbre abstraite (1) Relations de dépendance intégrale.* Preprint 1999. 3

[25] Lombardi H., Coquand T.: *Constructions cachées en algèbre abstraite (3) Dimension de Krull, Going Up, Going Down,. . . .* In preparation. 3

[26] Lombardi H., Quitté C.: *Constructions cachées en algèbre abstraite (2) Théorème de Horrocks, du local au global.* Preprint 1999. 3

[27] Lombardi H., Roy M.-F.: *Théorie constructive élémentaire des corps ordonnés.* Publications Mathématiques de Besançon, Théorie des Nombres, 1990-1991. English abridged version: Constructive elementary theory of ordered fields. p. 249-262. in Effective Methods in Algebraic Geometry. Ed. Mora T., Traverso C. Birkhauser 1991. Progress in Math. n 94. 19, 26, 27

[28] Makkai M., Reyes G.: *First order categorical logic.* Lecture Notes in Mathematics 611, Springer 1977. 10

[29] Mines R., Richman F., Ruitenburg W.: *A Course in Constructive Algebra.* Springer-Verlag. Universitext. 1988. 19, 21

[30] Prestel A., Ripoli C.: *Integral valued rational functions on valued fields.* Manuscripta Math. **73**, 437–452 (1991) 3, 37

[31] Schrijver A. : *Theory of integer and linear programming.* John Wiley. New-York. (1985) 41

[32] Stengle, G.: *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry.* Math. Ann. 207, 87-97 (1974) 21

[33] Troelstra, A., Schwichtenberg, H.: *Basic proof theory.* Cambridge Tracts in Theoretical Computer Science, 43. Cambridge University Press, Cambridge, 1996. 9

[34] Weispfenning, V.: *Quantifier elimination and decision procedures for valued fields.* In Müller, G.H., Richter, M.M. (Eds.): Models and Sets. Lecture Notes in Math. 1103, 419–472. Springer 1984. 33