A Generalization of Equational Proof Theory

Olivier Bournez

LORIA & INRIA,
615 rue du Jardin Botanique, BP 101,
54602 Villers-lès-Nancy Cedex, Nancy, France.
Olivier.Bournez@loria.fr

Abstract. Recently rule based languages focussed on the use of rewriting as a modeling tool which results in making specifications executable. To extend the modeling capabilities of rule based languages, we explored in a previous work the possibility of making the rule applications subject to probabilistic choices, and started to study the generalization of the results in the rewriting community about abstract reduction systems to systems with probabilistic choices.

This paper presents a new contribution on this line by presenting a generalization of classical equational proof theory. We obtain a nice proof theory which is sound and complete, and which has initial models.

1 Introduction

Term rewriting has been developed since the last thirty years, leading to a deep and solid corpus of knowledge about the rewrite relation induced by a set of rewrite rules: see [1, 12] for example for an introduction. More recently, rule based languages focussed on the use of rewriting as a modeling tool, which results in making the out-coming specification executable in a very efficient way [10]. Such languages enlighten the fundamental role of rewrite strategies, either for computation or for deduction.

To extend the modeling capabilities of rule based languages, we explored in a previous work the possibility of making the rule application subject to probabilistic choices [3]. We introduced the notion of probabilistic strategy, and showed that it provides a natural and nice framework to model and prototype systems with probabilistic choices [3]. This was demonstrated on several examples, dealing with classical toy problems as well as for the prototyping of randomized algorithms [3].

Dealing with rewriting with probabilistic firing of rules leads to numerous theoretical problems about the understanding of the underlying theoretical notions and results. In our previous work, we started to discuss what could be the generalization of the classical definitions in rewriting community for systems with probabilistic firing of rules. Indeed, in [3], we introduce a notion of probabilistic abstract reduction system, and introduce notions such as almost-sure termination or confluence, probabilistic termination or confluence, and we give some generalizations of the results known in the classical setting: see [3] for the details.

In this paper, we try to go to next step which is to understand what could be the generalization of the notion of equational proof theory.

It turns out that the theory that we obtain, which was originally motivated by probabilities, is actually closer to fuzzy logic, and could actually be called fuzzy equational proof theory: see [7] for an introduction to deductive systems in fuzzy logic.

Many papers have been devoted to the question of understanding the links between logic and probabilities: see for example [15, 2, 8, 15, 6, 5, 9, 13, 16]. Among them, some focus particularly on the links between fuzzy logic and probabilities: see for example [8, 11, 14]. However, one may understand that fuzzy logic and probability theory are à priori distinct since these two theories are different and can prove different things: see [4, 8] for discussions.

However, we think that this work can help to understand the proof theory of systems with randomized choices, or at least with fuzziness.

In Section 2, we fix some way of measuring derivations. In Section 3, we recall some basic usual notions of classical equational proof theory. In Section 4, we introduce the notion of valued relation, that we also call $*$-relation. In Section 5, we introduce the rewrite relation induced by a set of valued identities. This relation is characterized as the smallest $*$-similarity relation, closed by substitution, and closed by Σ-operations in Section 6. We introduce valued equational proof theory in Section 7. We define its models in Section 8. Sections 9 and 10 prove that valued equational proof theory is respectively sound and complete. Finally, we conclude in Section 11.

Note that the plan and the organization of this paper follows closely the presentation of the classical settings in [1].

2 Measuring derivations

We will first need to have a way to put a measure (or according to the the fuzzy logic view a "truth degree") on rewrite steps. We propose to do it abstractly, by defining the notion of operation.

Definition 1 (Operation). *Let Π be a complete lattice: Π is a set with some partial order $\leq$ on it, such that any finite subset $A \subseteq \Pi$ has a maximum denoted by $\max(A)$, and such that any subset $A \subseteq \Pi$ has a least upper bound denoted by $\sup(A)$. Such a set must[1] have a minimal element $\mathbf{0}$ and a maximal element $\mathbf{1}$.*

A operation on Π is an associative and commutative function from $\Pi \times \Pi$ to Π.

Sometimes, we will need to avoid bad ones (our good operations corresponds to the notion of t-norm in fuzzy logic: see for example [7]).

Definition 2 (Good operation). *An operation is good if furthermore:*

1. $x \leq x'$ and $y \leq y'$ implies $x * y \leq x' * y'$;

---

[1] Consider $\mathbf{0} = \sup\{x | \forall y \in \Pi, x \leq y\}$ and $\mathbf{1} = \sup(\Pi)$.

2. $x * \mathbf{1} \leq x$ for all x;
3. $\mathbf{0} * x = \mathbf{0}$ for all x.

For example, one can take:

Example 1 (Counting rewrite steps). $\Pi = \mathbb{N} \cup \{+\infty\}$, $\mathbf{0} = +\infty$, $\mathbf{1} = 0$, $x \leq y$ true iff y is less or equal to x, and $x * y$ defined as $x + y$: that will correspond in what follows to counting the number of rewrite steps in a derivation.

Example 2 (Product logic). $\Pi = [0,1]$, $\mathbf{0} = 0$, $\mathbf{1} = 1$ and $x * y$ defined as xy: that will correspond in what follows to evaluation of the truth degree of a derivation in product logic.

Example 3 (Lukasiewicz logic). $\Pi = [0,1]$, $\mathbf{0} = 0$, $\mathbf{1} = 1$, and $x * y$ defined as $max(x + y - 1, 0)$: that will correspond in what follows to evaluation of the truth degree of a derivation in Lukasiewicz Logic.

3   Signature, Terms, Positions, Substitutions

We now recall some classical definitions in rewriting community: see for example [1, 12].

Definition 3 (Signature). *A signature Σ is a set of function symbols, where each $f \in \Sigma$ is associated with a non-negative integer n, the arity of f. For every $n \geq 0$, we denote by $\Sigma^{(n)}$ the set of elements of Σ of arity n. A constant symbol is an element of $\Sigma^{(0)}$.*

Definition 4 (Terms). *Let Σ be a signature, and X a set of variables with $\Sigma \cap X = \emptyset$. The set $T(\Sigma, X)$ of Σ-terms over X is inductively defined as:*

1. *$X \subseteq T(\Sigma, X)$;*
2. *for all $n \geq 0$, for all $f \in \Sigma^{(n)}$, and all $t_1, \ldots, t_n \in T(\Sigma, X)$, we have $f(t_1, \ldots, t_n) \in T(\Sigma, X)$.*

For example, $t = f(e, f(x, i(x)))$ is a term over signature $\Sigma = \{f, i, e\}$ and $X = \{x\}$.

Definition 5 (Positions). *Let $s \in T(\Sigma, X)$ be a term over signature Σ.*

1. *The set of positions of a term s is the set $Pos(s)$ of strings over the alphabet of positive integers, which is inductively defined as follows:*
   (a) for $x \in X$, $Pos(x) = \{\epsilon\}$, where ϵ is the empty word;
   (b) for $n \geq 0$, $f \in \Sigma^{(n)}$, $s_1, \ldots, s_n \in T(\Sigma, X)$, $Pos(f(s_1, \ldots, s_n)) = \{\epsilon\} \cup \bigcup_{i=1}^{n} \{ip | p \in Pos(s_i)\}$.
2. *The sub-term of s at a position $\rho \in Pos(s)$, denoted by $s_{/\rho}$ is defined by induction on the length of ρ by: for all $n \geq 0$, $f \in \Sigma^{(n)}$, $s, s_1, \ldots, s_n \in T(\Sigma, X)$*
   (a) $s_{/\epsilon} = s$;

(b) $f(s_1, \ldots, s_n)_{/i\rho} = s_{i/\rho}$.

3. $s[t]_\rho$ *denotes the term that is obtained by replacing* $s_{/\rho}$ *by* t *in* s, *that is, for all* $n \geq 0$, $f \in \Sigma^{(n)}, s, s_1, \ldots, s_n \in T(\Sigma, X)$,

    (a) $s[t]_\epsilon = t$;

    (b) $f(s_1, \ldots, s_n)[t]_{i\rho} = f(s_1, \ldots, s_i[t]_\rho, \ldots, s_n)$.

For the above example, we have $Pos(t) = \{\epsilon, 1, 2, 21, 22, 221\}$, $t_{/22} = i(x)$, $t[i(e)]_{22} = f(e, f(x, i(e)))$.

Definition 6 (Substitution). *Let* Σ *be a signature, and* X *a set of variables with* $\Sigma \cap X = \emptyset$. *A* $T(\Sigma, X)$-*substitution, or simply substitution, is a function* $\sigma : X \to T(\Sigma, X)$ *such that* $\sigma(x) \neq x$ *for only finitely many* x.

Any $T(\Sigma, X)$-*substitution can be extended in a unique way to a mapping* $\sigma' : T(\Sigma, X) \to T(\Sigma, X)$ *defined as follows:*

1. $\sigma'(x) = \sigma(x)$ *for* $x \in X$;
2. $\sigma'(f(s_1, \ldots, s_n)) = f(\sigma(s_1), \ldots, \sigma(s_n))$ *for all* $n \geq 0, f \in \Sigma^{(n)}, s_1, \ldots, s_n \in T(\Sigma, X)$.

From now, as it is usually done, we will not distinguish between substitutions and their extensions.

On our previous example, if we take substitution $\sigma(x) = i(f(e, e))$, we have $\sigma(t) = f(e, f(i(f(e, e)), i(i(f(e, e)))))$.

Lemma 1. *For any terms* $s, t \in T(\Sigma, X)$, *for any substitution* σ, *and for any position* $\rho \in Pos(s)$, *we have:*

1. $\sigma(s)_{/\rho} = \sigma(s_{/\rho})$
2. $\sigma(s[t]_\rho) = (\sigma(s)[\sigma(t)]_\rho$

Proof. Easy induction on the length of ρ.

Definition 7 (Identity). *Let* Σ *be a signature and* V *a countably infinite set of variables disjoint from* Σ.

A Σ-*identity, or simply identity, is given by a multi-pair* $\{s, t\}$ *with* $s \in T(\Sigma, V)$ *and* $t \in T(\Sigma, V)$. *Such an identity will be written as* $s \approx t$.

4 Valued-relations

We assume from now that some operation $*$ on some set Π is fixed.

In this section, we introduce the notion of valued relation, that we will also call $*$-operation.

Definition 8 (Valued relation R). *Let* A *be a countable set.*

A valued relation (or $*$-*relation)* R *on* A *is a function from* $A \times A \to \Pi$.

This is a clear generalization of the classical notion of binary relation: to a classical binary relation R_c on A corresponds the valued relation R defined by $R(a, b) = \mathbf{1}$ if $R_c(a, b)$, $\mathbf{0}$ otherwise.

Definition 9 (Relations R^n). *Let R be a $*$-relation on A. Let $n \geq 0$ be some integer.*

$*$-relation R^n is defined by induction on $n \geq 0$ as follows:

1. *R^0 is the identity relation: for all $a, b \in A$, $R(a, b)$ is $\mathbf{1}$ if $b = a$, $\mathbf{0}$ otherwise;*
2. *R^1 is $*$-relation R;*
3. *R^n is defined for all $a, b \in A$ by*

$$R^n(a, c) = \sup\{R^{n-1}(a, b) * R(b, c) | b \in A\}$$

Definition 10 (Relations R^{-1}). *Let R be a $*$-relation on A. $*$-relation R^{-1} is defined for all $a, b \in A$ by*

$$R^{-1}(a, b) = R(b, a).$$

Definition 11 (Comparing $*$-relations). *Let R_1, R_2 be two $*$-relations on A. We say that R_1 is included in R_2, denoted by $R_1 \subseteq R_2$, if for all $a, b \in A$,*

$$R_1(a, b) \leq R_2(a, b).$$

Definition 12 (Union of $*$-relations).

1. *Let R_1, R_2 be two $*$-relations on A.*
   The union of R_1 and R_2, denoted by $R_1 \cup R_2$ is the $*$-relation defined for all $a, b \in A$ by
   $$R_1 \cup R_2(a, b) = \max\{R_1(a, b), R_2(a, b))\};$$
2. *Let $(R_i)_{i \in \mathbb{N}}$ be a family of $*$-relations on A.*
   The union of the $(R_i)_{i \in \mathbb{N}}$, denoted by $\bigcup_{i \in \mathbb{N}} R_i$ is the $*$-relation defined for all $a, b \in A$ by
   $$(\bigcup_{i \in \mathbb{N}} R_i)(a, b) = \sup\{R_i(a, b) | i \in \mathbb{N}\}.$$

We are now ready to give the generalization of the notion of equivalence relation in the classical setting (we call it "similarity relation" according to fuzzy logic terminology: see for example [7]):

Definition 13 ($*$-similarity relation). *Let R be a $*$-relation on A.*
R is said to be a $*$-similarity relation iff

1. *it is reflexive: $Id \subseteq R$;*
2. *it is symmetric: $R^{-1} \subseteq R$;*
3. *it is transitive: $R^2 \subseteq R$.*

As in the classical settings, one can easily prove:

Proposition 1 (Reflexive transitive closure of a $*$-relation). *Let R be a symmetric $*$-relation on A.*
The $*$-relation R^* defined by

$$R^* = \bigcup_{i \in \mathbb{N}} R^i,$$

called the transitive reflexive closure of R, is the smallest (for inclusion) $*$-similarity relation which contains R.

5   Rewriting relation induced by a set of valued identities

We now introduce the rewrite relation induced by a set of valued identities. We first define what a valued identity is:

Definition 14 (∗-identities). *Let Σ be a signature and V a countably infinite set of variables disjoint from Σ.*

A ∗-Σ-identity, or simply ∗- identity, or valued identity, is a Σ-identity $s \approx t$ plus some $p \in \Pi$. p is called the cost of the ∗-identity.

Such a ∗-identity will be written as $s \approx_p t$.

We can now define:

Definition 15 (Reduction relation $\to^E$). *Let E be a finite set of ∗-Σ-identities. The reduction relation $\to^E$: $T(\Sigma, X) \times T(\Sigma, X) \to \Pi$ is the ∗-relation on $T(\Sigma, X)$ defined as (we write $s \to_p^E t$ as a synonym for $(s \to^E t) = p$):*

1. *$s \to_p^E t$ if there exists a ∗-identity $l \approx_p r$ in E, ρ a position of s, and σ a substitution such that $s_{/\rho} = \sigma(l)$, $t = s[\sigma(r)]_\rho$, and p maximal with this property;*
2. *$s \to_{\mathbf{0}}^E t$ otherwise.*

Definition 16 (Relation $\leftrightarrow^E$, $\leftrightarrow^{E*}$). *Let E be a finite set of ∗-Σ-identities. The ∗-relation $\leftrightarrow^E$ is defined as $\to^E \cup (\to^E)^{-1}$.*

The ∗-relation $\leftrightarrow^{E*}$ is defined as the reflexive transitive closure of $\leftrightarrow^E$.

6   Characterizing the induced rewriting relation

We now show that $\leftrightarrow^{E*}$ can be characterized as the smallest ∗-similarity relation on $T(\Sigma, V)$ which contains E, is closed by substitution, and closed by Σ-operations.

We need first some new definitions:

Definition 17 (Closure by substitution). *Let $\equiv$ be some ∗-relation on $T(\Sigma, X)$.*

Relation $\equiv$ is closed under substitution iff, for all $s, t \in T(\Sigma, X)$, and for all substitution σ,

$$s \equiv t \leq \sigma(s) \equiv \sigma(t).$$

Definition 18 (Compatibility with Σ-operations). *Let $\equiv$ be some ∗-relation on $T(\Sigma, X)$.*

Relation $\equiv$ is compatible with Σ-operations iff, for all $n \geq i \geq 0$, $f \in \Sigma^{(n)}$ and $s_1, \ldots, s_{i-1}, s, t, s_{i+1}, \ldots, s_n \in T(\Sigma, X)$, we have

$$s \equiv t \leq f(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n) \equiv f(s_1, \ldots, s_{i-1}, t, s_{i+1}, \ldots, s_n).$$

Definition 19 (Closure by Σ-operations). *Let $\equiv$ be some $*$-relation on $T(\Sigma, X)$.*

Relation $\equiv$ is closed by Σ-operations iff, for all $n \geq 0$, $f \in \Sigma^{(n)}$ and $s_1, \ldots, s_n, t_1, \ldots, t_n \in T(\Sigma, X)$, we have

$$(s_1 \equiv t_1) * (s_2 \equiv t_2) * \ldots * (s_n \equiv t_n) \leq f(s_1, \ldots, s_n) \equiv f(t_1, \ldots, t_n).$$

Definition 20 (Compatibility with Σ-contexts). *Let $\equiv$ be some $*$-relation on $T(\Sigma, X)$.*

Relation $\equiv$ is compatible with Σ-contexts if, for all $s, s', t \in T(\Sigma, X)$ and for all position ρ, we have

$$s \equiv s' \leq t[s]_\rho \equiv t[s']_\rho.$$

Proposition 2. *Let E be a finite set of $*$-Σ-identities. The reduction relation $\to^E$ is closed under substitutions and compatible with Σ-operations.*

Proof. Assume that $s \to_p^E t$ with $p > \mathbf{0}$. Then there exists a $*$-Σ-identity $l \approx_p r$ in E, ρ a position of s, and σ' a substitution such that $s_{/\rho} = \sigma'(l)$, $t = s[\sigma'(r)]_\rho$.

From Lemma 1, we have $\sigma(s)_{/\rho} = \sigma(s_{/\rho}) = \sigma(\sigma'(l))$ and $\sigma(t) = \sigma(s[\sigma'(r)]_\rho) = \sigma(s)[\sigma\sigma'(r)]_\rho$. From definition of $\to^E$, we get $p = s \to^E t \leq \sigma(s) \to^E \sigma(t)$.

In a same vein, let $n \geq 0$, $f \in \Sigma^{(n)}$ and $s_1, \ldots, s_n \in T(\Sigma, X)$. We have $f(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n)_{/i.\rho} = \sigma'(l)$ and $f(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n)[\sigma'(r)]_{i.\rho} = f(s_1, \ldots, s_{i-1}, s[\sigma'(r)]_\rho, s_{i+1}, \ldots, s_n) = f(s_1, \ldots, s_{i-1}, t, s_{i+1}, \ldots, s_n)$. From definition of $\to^E$ we get $p = s \to^E t \leq f(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n) \to^E f(s_1, \ldots, s_{i-1}, t, s_{i+1}, \ldots, s_n)$.

We get $s \to^E t \leq \sigma(s) \to^E \sigma(t)$ and $s \to^E t \leq f(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n) \to^E f(s_1, \ldots, s_{i-1}, t, s_{i+1}, \ldots, s_n)$ when $p > \mathbf{0}$, and since this clearly also holds for $p = \mathbf{0}$ (recall that $\mathbf{0}$ is a minimal element of Π), this holds for all $p \in \Pi$.

Proposition 3. *Assume that $*$ satisfies $\mathbf{0} * x = \mathbf{0}$ for all x, and $x * y \leq x' * y'$ whenever $x \leq x'$ and $y \leq y'$.*

Then $\leftrightarrow^{E*}$ is closed under substitutions and compatible with Σ-operations.

Proof. An easy generalization of the previous proof shows that for all $n \geq 0$, $(\leftrightarrow^E)^n$ is closed under substitutions and compatible with Σ-operations. Taking sup over n over both sides of the inequalities $s(\leftrightarrow^E)^n t \leq \sigma(s)(\leftrightarrow^E)^n \sigma(t)$ and $s(\leftrightarrow^E)^n t \leq f(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n)(\leftrightarrow^E)^n f(s_1, \ldots, s_{i-1}, t, s_{i+1}, \ldots, s_n)$ yields the result.

Proposition 4. *Let $\equiv$ be some $*$-relation on $T(\Sigma, V)$.*

Relation $\equiv$ is compatible with Σ-operations iff it is compatible with Σ-contexts.

Proof. Indirect sense is obvious. Direct sense, is easy by an easy induction on the length of position ρ.

Proposition 5. *Let $\equiv$ be some $*$- relation on $T(\Sigma, V)$.*

Assume that $*$ satisfies $x \leq x'$ and $y \leq y'$ implies $x * y \leq x' * y'$ and $x * \mathbf{1} \leq x$ for all x.

Assume that $\equiv$ is reflexive and transitive.

Relation $\equiv$ is compatible with Σ-operations iff it is closed under Σ-operations.

Proof. Direct sense is easy using transitivity. Indirect sense is easy using reflexivity and $x * \mathbf{1} \leq x$ for all x.

The main theorem of this section is:

Theorem 1. *Let E be a finite set of $*$-Σ-identities.*
Assume that $*$ is good.
Relation $\leftrightarrow^{E*}$ is the smallest (for inclusion) $*$-relation on $T(\Sigma, V)$ which contains E, is a $*$-similarity relation, is closed by substitution, and is closed by Σ-operations.

Proof. $\leftrightarrow^{E*}$ is an $*$-similarity relation from Proposition 1. It is also closed by substitution and compatible with Σ-operations by Proposition 3. from Proposition 5, it is closed under Σ-operations. Furthermore, it contains E.

Conversely, assume that $\equiv$ is a $*$-similarity relation, closed by substitution, and by Σ-operations. If we prove that $\rightarrow^{E}\subseteq\equiv$ we are done, since that implies $\leftrightarrow^{E}\subseteq\equiv\ \cup\ \equiv^{-1}\subseteq\equiv$, and from Proposition 1, that in turn implies $\leftrightarrow^{E*}\subseteq\equiv$. Assume that $s \rightarrow^{E}_{p} t$ for some $s, t \in T(\Sigma, x), p \in \Pi$. There exists a $*$-identity $l \approx_p r$ in E, ρ a position of s, and σ a substitution such that $s_{/\rho} = \sigma(l)$, $t = s[\sigma(r)]_{\rho}$. Since $\equiv$ contains E, from $l \approx_p r \in E$, we deduce $l \rightarrow^{E} r \leq l \equiv r$. Closure by substitution yields $p = l \rightarrow^{E} r \leq \sigma(l) \equiv \sigma(r)$. Closure by Σ-operations yields by Proposition 5 compatibility with Σ-operations, and hence compatibility with Σ-contexts. We obtain $l \rightarrow^{E} r \leq \sigma(l) \equiv \sigma(r) \leq s = s[\sigma(l)]_{\rho} \equiv s[\sigma(r)]_{\rho} = t$, and hence $\rightarrow^{E}\subseteq\equiv$.

7 $*$-equational logic

The previous theorem says that $\leftrightarrow^{E*}$ can be obtained by starting with the $*$-relations of E, and then closing by reflexivity, symmetry, transitivity, substitution, and Σ-operations.

Describing this closing process as inference rules, leads to $*$-equational logic.

Definition 21 ($*$-equational logic).
$*$-equational logic is the logic obtained using the following inference rules:

$$\frac{(s \approx_q t) \in E}{E \vdash s \approx_q t}$$

$$\frac{}{E \vdash s \approx_{\mathbf{1}} s}$$

$$\frac{E \vdash s \approx_q t}{E \vdash t \approx_q s}$$

$$\frac{E \vdash s \approx_q t \quad E \vdash t \approx_r u}{E \vdash s \approx_{q*r} u}$$

$$\frac{E \vdash s \approx_q t}{E \vdash \sigma(s) \approx_q \sigma(t)}$$

$$\frac{E \vdash s_1 \approx_{q_1} t_1 \ E \vdash s_n \approx_{q_n} t_n}{E \vdash f(s_1, \ldots, s_n) \approx_{q_1 * q_2 \ldots * q_n} f(t_1, \ldots, t_n)}$$

We can then introduce the notion of provability degree of some Σ-identity:

Definition 22 (Provability degree). *Let $s, t \in T(\Sigma, X)$ be two Σ-terms. The provability degree of $s \approx t$, denoted by $|s \approx t|$, is defined as*

$$|s \approx t| = \sup\{p | E \vdash s \approx_p t\}$$

The results of previous section can then be restated as:

Theorem 2. *Let E be a finite set of $*$-Σ-identities.*
   Assume that $*$ is good.
   For all $s, t \in T(\Sigma, X)$,

$$|s \approx t| = \leftrightarrow^{E*} (s, t).$$

8   Algebras

We are now going to talk about algebras and models (we still follow the presentation of (classical) equational proof theory of [1]).
   From now, we assume that some *good* operation $*$ on a complete lattice Π is fixed.

Definition 23 (Σ-algebra). *Let Σ be a signature. A Σ-algebra $\mathcal{A}$ consists of*

1. *a carrier set A;*
2. *a mapping that associate to each function symbol $f \in \Sigma^{(n)}$ a function $f^A : A^n \to A$;*
3. *a $*$-congruence $=^A$ on A: that is to say, a $*$-similarity relation $=^A$ which is compatible with the interpretations of all function symbols of $\mathcal{A}$. That means that for all $n \geq 0$, $f \in \Sigma^{(n)}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$, we have (for $a, b \in A$, we note $a =^A b$ for $=^A (a, b)$):*

$$(a_1 =^A b_1) * \ldots * (a_n =^A b_n) \leq (f^A(a_1, \ldots, a_n) =^A f^A(b_1, \ldots, b_n)).$$

We can now give the definition of an homomorphism between two Σ-algebras (when $=^A$ is some $*$-congruence on A, and $p \in \Pi$ is some value, we note $a =^A_p b$ as a synonym for $=^A (a, b) = p$):

Definition 24 (Homomorphism). *Let Σ be a signature, and $\mathcal{A}, \mathcal{B}$ be two Σ-algebras.*
   A Σ-homomorphism $\phi : \mathcal{A} \to \mathcal{B}$ is a mapping $\phi : A \to B$ such that for all $n \geq 0$, $f \in \Sigma^{(n)}$, and $a, b, a_1, \ldots, a_n \in A$, we have:

1. *$\phi(f^A(a_1, \ldots, a_n)) =^B_1 f^B(\phi(a_1), \ldots, \phi(a_n))$;*
2. *$a =^A_1 b$ implies $\phi(a) =^B_1 \phi(b)$.*

Lemma 2 (Composition of homomorphisms). *Let Σ be a signature, and $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be three Σ-algebras.*

The composition of a Σ-homomorphism $\phi : \mathcal{A} \to \mathcal{B}$ and a Σ-homomorphism $\psi : \mathcal{B} \to \mathcal{C}$ is a Σ-homomorphism $\psi \circ \phi : \mathcal{A} \to \mathcal{C}$.

Proof. For all $n \geq 0$, $f \in \Sigma^{(n)}$, and $a_1, \ldots, a_n \in A$, we have $\phi(f^A(a_1, \ldots, a_n)) =_{\mathbf{1}}^{B} f^B(\phi(a_1), \ldots, \phi(a_n))$. We obtain $\psi \circ \phi(f^A(a_1, \ldots, a_n)) =_{\mathbf{1}}^{C} \psi(f^B(\phi(a_1), \ldots, \phi(a_n)))$. We deduce $\psi \circ \phi(f^A(a_1, \ldots, a_n)) =_{\mathbf{1}}^{C} f^C(\psi \circ \phi(a_1), \ldots, \psi \circ \phi(a_n))$ from $\psi \circ \phi(f^A(a_1, \ldots, a_n)) =_{\mathbf{1}}^{C} \psi(f^B(\phi(a_1), \ldots, \phi(a_n)))$ and $f^C(\psi \circ \phi(a_1), \ldots, \psi \circ \phi(a_n)) =_{\mathbf{1}}^{C} \psi(f^B(\phi(a_1), \ldots, \phi(a_n)))$ using transitivity and $\mathbf{1} * \mathbf{1} = \mathbf{1}$.

Assume that $a =_{\mathbf{1}}^{A} b$. We have $\phi(a) =_{\mathbf{1}}^{B} \phi(b)$, and then $\psi(\phi(a)) =_{\mathbf{1}}^{C} \psi(\phi(b))$.

We then introduce the Crisp term algebra.

Definition 25 (Crisp Term Algebra). *Let Σ be a signature and X a countable set of variables disjoint from X.*

The Crisp Σ-term algebra $\mathcal{T}_{=}(\Sigma, X)$ has $T(\Sigma, X)$ as carrier set, $=$ as $*$-relation on it (that is to say $=^{\mathcal{T}_{=}(\Sigma, X)} (s, t) = \mathbf{1}$ if $s = t$ and $\mathbf{0}$ otherwise), and interprets the function symbols $f \in \Sigma^{(n)}$ as follows:

$$f^{\mathcal{T}_{=}(\Sigma, X)}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n).$$

The following remark will be useful:

Lemma 3 (Substitution versus Homomorphisms). *Let Σ be a signature and X a set of variables disjoint from X. A substitution σ is an homomorphism from the Crisp Term Algebra $\mathcal{T}_{=}(\Sigma, X)$ to itself.*

We have all the ingredients to define the notion of validity of a valued identity:

Definition 26 (Validity of an identity). *A $*$-Σ-identity $s \approx_p t$ holds in a Σ-algebra $\mathcal{A}$, denoted by $\mathcal{A} \models s \approx_p t$ iff, for all Σ-homomorphism $\phi : \mathcal{T}_{=}(\Sigma, X) \to \mathcal{A}$, we have $p \leq=^{A} (\phi(s), \phi(t))$.*

We obtain the notion of model of a set of valued identities:

Definition 27 (Model of a set of $*$-Σ-identities). *Let Σ be a signature and E a finite set of $*$-Σ-identities. A Σ-algebra $\mathcal{A}$ is a model of E, denoted by $\mathcal{A} \models E$, iff every $*$-Σ-identity of E holds in $\mathcal{A}$.*

9   Soundness of $*$-equational proof theory

In this section, we prove that $*$-equational proof theory is sound. To do so, we introduce the notion of truth degree of an identity.

Definition 28 (Truth degree of an identity). *Let Σ be a signature and E a finite set of $*$-Σ-identities. Let $s, t \in T(\Sigma, X)$ be two terms.*

The truth degree of identity $s \approx t$, denoted by $\|s \approx t\|$, is defined as

$$\|s \approx t\| = \inf\{p | \mathcal{A} \models s \approx_p t \text{ for some } \Sigma\text{-algebra } \mathcal{A} \text{ with } \mathcal{A} \models E\}$$

Soundness of $*$-equational proof theory can then be expressed by:

Proposition 6 (Soundness). *Assume that $*$ is good.*

Then $*$-equational proof theory is sound: for any finite set E of $*$-Σ-identities, for any terms $s, t \in T(\Sigma, X)$, we have

$$|s \approx t| \leq \|s \approx t\|.$$

Proof. If we prove that for any Σ-algebra $\mathcal{A}$ with $\mathcal{A} \models E$, and for all rules of $*$-equational theory the conclusion follows from the premise, we are done: taking supremum (over proofs) of $\{p | E \vdash s \approx_p t\}$ and infimum (over Σ-algebras) of $\{p | \mathcal{A} \models s \approx_p t, \mathcal{A} \models E\}$ yields the required inequality.

Since $\mathcal{A} \models E$, we have $\mathcal{A} \models s \approx_q t$ for all $s \approx_q t \in E$. From reflexivity of $=^A$, we have $\phi(s) =^A_1 \phi(s)$ for all Σ-homomorphism $\phi : \mathcal{T}_=(\Sigma, X) \to \mathcal{A}$, and hence $\mathcal{A} \models s \approx_1 s$. From symmetry of $=^A$, $\mathcal{A} \models s \approx_q t$ clearly implies $\mathcal{A} \models t \approx_q s$. Now $\mathcal{A} \models s \approx_p t$ and $\mathcal{A} \models t \approx_q u$ implies that $\mathcal{A} \models s \approx_{q*r} u$: since $=^A$ is transitive, for any Σ-homomorphism $\phi : \mathcal{T}_=(\Sigma, X) \to \mathcal{A}$ we have $=^A (\phi(s), \phi(t))* =^A (\phi(t), \phi(u)) \leq =^A (\phi(s), \phi(u))$. Now, since $*$ is good, from $p \leq =^A (\phi(s), \phi(t))$ and $q \leq =^A (\phi(t), \phi(u))$ we deduce $p * q \leq =^A (\phi(s), \phi(t))* =^A (\phi(t), \phi(u)) \leq =^A (\phi(s), \phi(u))$. $\mathcal{A} \models s \approx_q t$ implies $\mathcal{A} \models \sigma(s) \approx_q \sigma(t)$ for all substitution σ: indeed, for any Σ-homomorphism $\phi : \mathcal{T}_=(\Sigma, X) \to \mathcal{A}$ we have $\mathcal{A} \models \phi(\sigma(s)) \approx_q \phi(\sigma(t))$ since by Lemma 2 and Lemma 3 $\phi \circ \sigma$ is a particular Σ-homomorphism $\phi : \mathcal{T}_=(\Sigma, X) \to \mathcal{A}$. Now $\mathcal{A} \models s_1 \approx_{q_1} t_1$ $\ldots \mathcal{A} \models s_n \approx_{q_1} t_n$ implies $\mathcal{A} \models f(s_1, \ldots, s_n) \approx_{q_1 * q_2 * \ldots * q_n} f(t_1, \ldots, t_n)$. Indeed, by hypothesis for any Σ-homomorphism $\phi : \mathcal{T}_=(\Sigma, X) \to \mathcal{A}$ we have $q_1 \leq =^A (\phi(s_1), \phi(t_1))$, $\ldots$, $q_n \leq =^A (\phi(s_n), \phi(t_n))$. From the goodness of $*$ we get $q_1 * \ldots * q_n \leq =^A (\phi(s_1), \phi(t_1)) * \ldots * =^A (\phi(s_n), \phi(t_n))$ which is less than $=^A (\phi(f(s_1, \ldots, s_n)), \phi(f(t_1, \ldots, t_n)))$ because $=^A$ is a congruence. $\qquad\blacksquare$

10 Completeness of $*$-equational proof theory

We now prove completeness of $*$-equational proof theory.

First, we need to consider the term algebra with other $*$-congruence relation than equality $=$.

Definition 29 ($\equiv$-Term Algebra). *Let Σ be a signature and X a set of variables disjoint from X.*

Let $\equiv$ be some $*$-congruence relation on $T(\Sigma, X)$.

The Σ-term algebra associated to $\equiv$, denoted by $\mathcal{T}_\equiv(\Sigma, X)$, has $T(\Sigma, X)$ as carrier set, $\equiv$ as $*$-congruence on it, and interprets the function symbols $f \in \Sigma^{(n)}$ as follows:

$$f^{\mathcal{T}_\equiv(\Sigma, X)}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n).$$

In other words, the crisp Σ-term algebra $\mathcal{T}_=(\Sigma, X)$ is the Σ-term algebra associated to equality $=$.

We can now observe:

Proposition 7 (Provability congruence). *Let E be a finite set of $*$-Σ-identities. Assume that $*$ is good and is a continuous function.*

The $*$-relation on $T(\Sigma, X)$ defined by

$$(s \equiv t) = |s \approx t|$$

for all $s, t \in T(\Sigma, X)$ is a $*$-congruence relation.

This $*$-congruence will be called the provability congruence.

Proof. For all $s \in T(\Sigma, X)$, from $E \vdash s \approx_{\mathbf{1}} s$, we get $|s \approx s| \geq \mathbf{1}$. We have $|t \approx s| = |s \approx t|$ for all $s, t \in T(\Sigma, X)$, since one can swap the role of t and s in any $*$-equational proof. Let $\epsilon > \mathbf{0}$. For any $\delta > \mathbf{0}$, there exists a proof $E \vdash s \approx_p t$ for some $p \geq |s \approx t| - \delta$, and a proof $E \vdash s \approx_q t$ for some $q \geq |t \approx u| - \delta$. From the transitivity rule of $*$-equational theory, we have $E \vdash s \approx_r u$ for $r = p * q$, and so $|s \approx u| \geq r$. Since $*$ is a continuous function, one can choose δ so that $r = p * q \geq |s \approx t| * |t \approx u| - \epsilon$. This yields $|s \approx u| \geq |s \approx t| * |t \approx u| - \epsilon$. Since this is true for all $\epsilon > \mathbf{0}$, we must have $|s \approx u| \geq |s \approx t| * |t \approx u|$. Let $n \geq 0$, $f \in \Sigma^{(n)}$ and $a_1, \ldots, a_n, b_1, \ldots, b_n \in T(\Sigma, X)$. Let $\epsilon > \mathbf{0}$. For all δ, and $1 \leq i \leq n$, there exists a proof of $E \vdash a_i \approx_{p_i} b_i$ with $p_i \geq |a_i \approx b_i| - \delta$. From the congruence rule of $*$-equational theory, we have $E \vdash f(a_1, \ldots, a_n) \approx_q f(b_1, \ldots, b_n)$, with $q = p_1 * \ldots * p_n$, and hence $|f(a_1, \ldots, a_n) \approx f(b_1, \ldots, b_n)| \geq p_1 * \ldots * p_n = q$. Observing that have $(|a_1 \approx b_1| - \delta) * \ldots * (|a_n \approx b_n| - \delta) \leq p_1 * \ldots * p_n = q$, and since $*$ is continuous, one can choose δ such that this q satisfies $q \geq |a_1 \approx b_1| * \ldots * |a_n \approx b_n| - \epsilon$. Since this is true for all $\epsilon > \mathbf{0}$, we must have $|f(a_1, \ldots, a_n) \approx f(b_1, \ldots, b_n)| \geq |a_1 \approx b_1| * \ldots * |a_n \approx b_n|$.

We now introduce some new binary relation:

Proposition 8 (Relation $\cong$). *Let $\mathcal{A}$ be a Σ-algebra.*

The (classical) binary relation on A defined by

$$x \cong y \ \text{iff} \ =^A (x, y) = \mathbf{1}$$

1. *is an equivalence relation;*
2. *is compatible with the interpretation of all function symbols of $\mathcal{A}$: for all $n \geq 0$, $f \in \Sigma^{(n)}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$, we have $a_1 \cong b_1$, $\ldots$, $a_n \cong b_n$ implies $f^A(a_1, \ldots, a_n) \cong f^A(b_1, \ldots, b_n)$);*
3. *is compatible with the $*$-congruence relation of $\mathcal{A}$: for all $a_1, a_2, b_1, b_2 \in A$, we have $a_1 \cong b_1$, $a_2 \cong b_2$ implies $=^A (a_1, a_2) ==^A (b_1, b_2)$.*

Proof. Point 1. follows from reflexivity, symmetry, and transitivity of $=^A$. Point 2. follows from $*$-congruence of $=^A$. Point 3. follows from transitivity of $=^A$.

To any Σ-algebra one can associate its quotient through the previous relation:

Definition 30 (Quotient algebra). *Let $\mathcal{A}$ be a Σ-algebra. The Σ-algebra whose carrier set is $A/\cong$, the equivalence classes of A with respect to the previous relation $\cong$, whose $*$-similarity relation is*

$$=^{A/\cong} ([s]/\cong, [t]/\cong) ==^A (s, t)$$

, and whose interpretation for all $n \geq 0$, $f \in \Sigma^{(n)}$, $a_1, \ldots, a_n \in A$ is given by

$$f^{A/\cong}([a_1]/\cong, \ldots, [a_n]/\cong) = [f^A(a_1, \ldots, a_n)]/\cong$$

is called the quotient algebra of A trough $\cong$, denoted by $A/\cong$.

We can now define a particular model, called the initial model, defined as the quotient of Σ-term algebra associated to the provability congruence through $\cong$.

Definition 31 (Initial model). *Let Σ be a signature, and E be a finite set of $*$-Σ-valued identities.*

Let $\mathcal{T}_{\equiv}(\Sigma, X)$ be the Σ-term algebra associated to the provability congruence.

The quotient of this Σ-term algebra through the corresponding $\cong$ is called the initial model of E, and is denoted by $\mathcal{I}_E$. Formally,

$$\mathcal{I}_E = (\mathcal{T}_{\equiv}(\Sigma, X))/\cong .$$

The following result is easy:

Lemma 4. *Any Σ-homomorphism $\phi : \mathcal{T}_=(\Sigma, X) \to \mathcal{T}_{\equiv}(\Sigma, X)/\cong$ can be written as $\psi \circ \sigma$ where $\sigma : \mathcal{T}_=(\Sigma, X) \to \mathcal{T}_=(\Sigma, X)$ is a substitution, and ψ is the canonical endomorphism $\psi : \mathcal{T}_=(\Sigma, X) \to \mathcal{T}_{\equiv}(\Sigma, X)/\cong : \psi(x) = [x]/\cong$ for all x.*

Proof. Exercice.

We can then prove completeness:

Theorem 3 (Completeness). *Assume that $*$ is good and is a continuous function.*

$*$-equational theory is complete. For any finite set E of $*$-Σ-identities, for any terms $s, t \in T(\Sigma, X)$, we have

$$\|s \approx t\| \leq |s \approx t|.$$

Proof. It is sufficient to observe that the initial model $\mathcal{I}_E$ is a model of the $*$-Σ-identities of E, since this is a particular Σ-algebra.

Let $s, t \in T(\Sigma, X)$ be two terms with $s \approx_p t \in E$. We must show that for all Σ-homomorphism $\phi : \mathcal{T}_=(\Sigma, X) \to \mathcal{I}_E$, we have $p \leq |\phi(s) \approx \phi(t)|$, to get $\mathcal{I}_E \models s \approx_p t$. From Lemma 4, such a Σ-homomorphism ϕ can be written as $\psi \circ \sigma$ where σ is a substitution and ψ is the canonical endomorphism from $\mathcal{T}_=(\Sigma, X)$ to $\mathcal{T}_{\equiv}(\Sigma, X)/\cong$. Since $s \approx_p t \in E$, we have $E \vdash s \approx_p t$. From the rules of $*$-equational proof theory, we then have then $E \vdash \sigma(s) \approx_p \sigma(t)$. This yields $|\sigma(s) \approx \sigma(t)| \geq p$. We then have from definitions, $=^{\mathcal{I}_E} (\psi \circ \sigma(s), \psi \circ \sigma(t)) ==^{\mathcal{T}_{\equiv}(\Sigma, X)} (\sigma(s), \sigma(t)) = |\sigma(s) \approx \sigma(t)| \geq p$.

To summary, we have:

Theorem 4 (Soundness and completeness of ∗-equational theory). *Assume that ∗ is good and is a continuous function.*

∗-equational theory is sound and complete.

For any finite set E of $∗$-Σ-identities, for any terms $s, t \in T(\Sigma, X)$,

$$|s \approx t| = \|s \approx t\|.$$

Observe that $\mathcal{I}_E$ corresponds correctly to the usual notion of initial model in the sense that:

Proposition 9 (Initiality of $\mathcal{I}_E$). *For any finite set E of $∗$-Σ-identities, for all $s, t \in T(\Sigma, X)$, $p \in \Pi$,*

$$\mathcal{I}_E \models s \approx_p t \text{ iff } E \models s \approx_p t.$$

11 Conclusion

In this paper, we have introduced ∗-equational proof theory. We proved that this theory is sound and complete, as soon as ∗ is a continuous t-norm. Furthermore, we proved that ∗-equational proof theory has a notion of natural initial model.

Future work may include understanding techniques for solving equational problems (see for example [1]) in such theories, or for understanding the frontier between effectiveness and non-effectiveness.

Clearly this work can be related to soundness and completeness results for some particular fuzzy logics: see [7] for a tutorial about deductive systems in fuzzy logic. Our work can been seen as a consequence of known results about soundness and completeness for particular fuzzy logics, as classical equational proof theory can be seen as a consequence of the soundness and completeness of classical first-order logic. Observe however, that we have a notion of initial model, like what happens in the classical equational proof theory settings, and unlike what happens in the (classical) general first-order proof theory settings.

Note that this work was originally motivated by understanding rewriting in presence of probabilities. It turns out that we obtain a theory for understanding rewriting in presence of fuzziness. Future work includes to understand if a notion of rewriting when (true) probabilities are used can exist: see [15, 2, 8, 15, 6, 5, 9, 13, 16] for discussions and problems about mixing logic and probabilities.

References

1. Franz Baader and Tobias Nipkow. *Term Rewriting and all That*. Cambridge University Press, 1998.
2. F. Bacchus. *Representing and reasoning with probabilistic knowledge*. MIT-Press, 1990.
3. Olivier Bournez and Claude Kirchner. Probabilistic rewrite strategies: Applications to ELAN. In Sophie Tison, editor, *Rewriting Techniques and Applications*, volume 2378 of *Lecture Notes in Computer Science*, pages 252–266. Springer-Verlag, July 22-24 2002.

4. D. Dubois and H. Prade. Fuzzy sets and probability: Misunderstanding, bridges and gaps. In *Proceedings of the second IEEE International Conference on Fuzzy Systems*, pages 1059–1068, 1993.

5. H. Gaifman and M. Snir. Probabilities over rich languages, testing and randomness. *The journal of symbolic logic*, 47(3):495–548, 1982.

6. P. Hajek and T. Havraknek. *Mechanizing Hypothesis Formation (Mathematical Foundations for a General Theory)*. Springer-Verlag, Berlin - Heidelberg - New York, 1978.

7. Petr Hajek and Lluis Godo. Deductive systems of fuzzy logic (a tutorial). Technical report, `http://www.uivt.cas.cz/~hajek/`, 2002.

8. Petr Hajek, Lluis Godo, and Francesc Esteva. Fuzzy logic and probability. In *Proceedings of the Eleventh Annual Conference on Uncertainty in Artificial Intelligence (UAI'95)*, August 1995.

9. J.Y. Halpern. An analysis of first order logics of probability. In *Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI'89)*, pages 1375–1381, 1989.

10. Hélène Kirchner and Pierre-Etienne Moreau. Promoting rewriting to a programming language: A compiler for non-deterministic rewrite programs in associative-commutative theories. *Journal of Functional Programming*, 11(2):207–251, 2001. Report LORIA A01-R-007.

11. G. Klir and T.A Folger. *Fuzzy Sets, Uncertainty and Information*. Prentice-Hall International, 1988.

12. Jan Willem Klop. Term rewriting systems. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science*, volume 2, chapter 1, pages 1–117. Oxford University Press, Oxford, 1992.

13. N.J. Nilsson. Probabilistic logic. *Artificial Intelligence*, 28(1):71–87, 1986.

14. L. Sadeh. Is probability theory theory sufficient for dealing with uncertainty in ai: a negative view. In *Proceedings of Uncertainty in Artificial Intelligence*, pages 103–115, 1986.

15. D. Scott and P. Krauss. *Assigning Probabilities to Logical Formulas*. North-Holland, Amsterdam, 1966.

16. N. Wilson and S. Moral. A logical view of probability. In *Proceedings of the 11th European Conference on Artificial Intelligence (ECAI'94)*, pages 386–390, 1994.