Ticket Entailment is decidable

Vincent Padovani

Under consideration for publication in Math. Struct. in Comp. Science

Ticket Entailment is decidable

VINCENT PADOVANI

Equipe Preuves, Programmes et Systèmes

Université Paris VII - Denis Diderot

Case 7014

75205 PARIS Cedex 13

padovani@pps.jussieu.fr

Received 06/19/2010

We answer positively a question raised by Anderson and Belnap, by proving that the logic $T_{\to}$ of ticket entailment is decidable.

The pure calculus of entailment was introduced by Anderson and Belnap (Anderson and Belnap 1975) as part of a formal analysis of the notion of logical implication. The system $T_{\to}$ of *ticket entailment* is the implicational fragment of entailment based on modus ponens and the four following axiom schemes:

— $I : \phi \to \phi$

— $B : (\chi \to \psi) \to ((\phi \to \chi) \to (\phi \to \psi))$

— $B' : (\phi \to \chi) \to ((\chi \to \psi) \to (\phi \to \psi))$

— $W : (\phi \to (\phi \to \chi)) \to (\phi \to \chi)$

The four axioms already appear as early as 1956 in Ackermann's theory of "strenge Implikation" (Ackermann 1956; Anderson 1960) which according to Anderson and Belnap, provided the impetus for their study of the notions of relevance and necessity in logic (Anderson and Belnap 1975; Anderson *et al.* 1990).

The question of the decidability of $T_{\to}$ (the problem of deciding whether a given formula is derivable from the axioms of $T_{\to}$ and modus ponens) has remained unsolved since it was raised in the first volume of Anderson and Belnap's book, although proofs of the decidability and undecidability were given for several related systems (Anderson *et al.* 1990; Urquhart 1984). In 2004, a decidability result for a restricted class of formulas (the class of 1-*unary formulas* in which every maximal negative subformula is of arity at most 1) was proposed by Broda, Damas, Finger and Silva e Silva (Broda *et al.* 2004). The problem was also significantly investigated by Bimbó (Bimbó 2005). We prove in this paper that $T_{\to}$ is decidable.

Survey of the proof

We introduce in section 1 a set of simply typed terms similar to HRM-terms introduced in (Trigg *et al.* 1994) and prove that the set of types inhabited by these terms is exactly the set of all formulas derivable in the logic of Ticket entailement.

In section 2 what we call *blueprint* of a term M is the partial tree whose domain is the set of all addresses of subterms of M whose free variables are amongst the free variables of M, mapping each address to the type of the corresponding subterm. When a term M has the free variables $x_1, \ldots, x_n$, not all permutations π of $\{1, \ldots, n\}$ are such that $\lambda x_{\pi(1)}, \ldots x_{\pi(n)}.M$ is typable by a derivable formula - for instance $\lambda f\,x.(f\,x) : (\phi \to \psi) \to (\phi \to \psi)$ whereas $\lambda f\,x.(x\,f)$ is not typable, even if it is simply typable. Yet it is possible to effectively compute from the blueprint of M all such permutations. More precisely we introduce reduction rules which allows one to extract from the blueprint of a term M of type ϕ all sequences $(\chi_1, \ldots, \chi_k)$ for which there exists a term N yielded by a renaming of the variables of M and such that $\lambda y_1 \ldots y_k.N$ is a closed term of type $(\chi_1 \ldots \chi_k \to \phi)$.

In section 3 introduces the proof-search technique allowing one to decide whether a given formula is NF-inhabited. We associate with each formula ϕ an infinite family of labelled trees called term *shadows*. To each inhabitant M of ϕ corresponds a shadow of same domain as M in which each address a is labelled with a "compressed form" of the blueprint of the subterm at a in M. We define a relation on those compressed forms which allows one to safely "pump" the term M whenever satisfied by two labels, yielding an inhabitant of smaller size. Thus, as proven in section 4, to each inhabitant of ϕ of minimal size corresponds a *compact* shadow, a shadow for which there exists no such pair of labels. Finally, in section 5 we prove that for each formula ϕ, the set of all compact shadows associated with ϕ is a finite set effectively computable from ϕ.

1. Lambda calculus

Let $x_0, x_1, \ldots$ be different variables. We write $x_i < x_j$ when $i < j$. Throughout the paper, by *term* we always mean a term of pure lambda-calculus built over those variables. For each term M, we write $\mathsf{Free}(M)$ the least subsequence of $(x_i)_{i \in \mathbb{N}}$ in which every variable free in M occurs. Terms are not identified modulo α-conversion. We adopt however the usual convention according to which no variable is allowed to be bound more than once in any given term or simultaneously free and bound. The set of *well-labelled terms* is inductively defined by:

— each x_i is a well-labelled term,

— if M is well-labelled, then $\lambda x.M$ is well-labelled provided x is the greatest free variable of M,

— if M, N are well-labelled, then $(M\,N)$ is well-labelled provided: M is closed; or M, N are open terms and the greatest free variable of M is less than or equal to the greatest free variable of N.

Let $(\omega_i)_{i \in \mathbb{N}}$ be a sequence in which each ω_i is a formula occurring an infinite number of times. For each strictly increasing $X = (x_{i_1}, \ldots, x_{i_n})$ we let $\Omega(X) = (\omega_{i_1}, \ldots, \omega_{i_n})$. The judgment $M : \phi$ (in words, M is of type ϕ w.r.t the choice of $\omega_0, \omega_1, \ldots$) is inductively defined as follows:

— if $\Omega(x) = \phi$, then $x : \phi$,
— if $M : \chi$, $x : \phi$ and $\lambda x.M$ is well-labelled, then $\lambda x.M : \phi \to \chi$,
— if $M : \phi \to \chi$, $N : \phi$ and $(M\, N)$ is well-labelled, then $(M\, N) : \chi$.

Note that our definition ensures that each typable term has a unique type. We write NF the set of all typed terms in β-normal form. We call NF-*inhabitant of* ϕ every closed term $M \in \mathsf{NF}$ of type ϕ.

Lemma 1.1. If $M : \phi$ then ϕ is NF-inhabited.

Proof. The term M is a simply typable term, a fortiori normalisable. We leave as an exercise for the reader to check that $M\, \beta\, M'$ implies the existence of $M'' : \phi$ such that $M'' \equiv_\alpha M'$. □

Lemma 1.2. Let M be an NF-inhabitant of ϕ. The types of the subterms of M and of the variables free in M are subformulas of ϕ.

Proof. By an easy induction on M. □

1.1. *Equivalence between derivability in $T_\to$ and* NF*-inhabitation*

In the next lemmas by $\phi_1 \ldots \phi_n \to \psi$ we mean the formula $(\phi_1 \to (\ldots(\phi_n \to \psi)\ldots))$ if $n > 0$, the formula ψ if $n = 0$. We write $\vdash_T \phi$ the judgment "ϕ is derivable in $T_\to$".

Lemma 1.3. If $\vdash_T \phi$, then ϕ is NF-inhabited.

Proof. If $f < g < x$ and $h < x$, then $\lambda x.x$, $\lambda fgx.f(g\,x)$, $\lambda fgx.g(f\,x)$ and $\lambda h.(h\,x\,x)$ are well-labelled terms. For each axiom ϕ of ticket entailment the variables f, g, h, x can be chosen so that one of those terms is of type ϕ. By lemma 1.1, the set of NF-inhabited formulas is closed under modus ponens. □

Lemma 1.4. If $\vdash_T \chi \to \psi$, then $\vdash_T (\phi_1 \ldots \phi_n \to \chi) \to (\phi_1 \ldots \phi_n \to \psi)$ for all $\phi_1, \ldots, \phi_n$.

Proof. By induction on n, using B-axioms. □

Lemma 1.5. Suppose $(i_1, \ldots, i_n)$, $(j_1, \ldots, j_m)$, $(k_1, \ldots, k_p)$ are strictly increasing sequences of integers, $\{k_1, \ldots, k_p\} = \{i_1, \ldots, i_n, j_1, \ldots, j_m\}$, $n = 0$ or ($n > 0$, $m > 0$, $i_n \le j_m$). If

1 $\vdash_T \omega_{i_1} \ldots \omega_{i_n} \to (\chi \to \psi)$,
2 $\vdash_T \omega_{j_1} \ldots \omega_{j_m} \to \chi$,

then $\vdash_T \omega_{k_1} \ldots \omega_{k_p} \to \psi$.

Proof. By induction on $n + m$. The proposition is true when $n = m = 0$. Assume $n + m > 0$. Then $m > 0$.

Suppose ($n = 0$ and $m = 1$) or ($n > 0$ and $m > 1$ and $i_n \le j_{m-1}$). Then

(i) $\vdash_T (\chi \to \psi) \to ((\omega_{j_m} \to \chi) \to (\omega_{j_m} \to \psi))$
(ii) $\vdash_T (\omega_{i_1} \dots \omega_{i_n} \to (\chi \to \psi)) \to (\omega_{i_1} \dots \omega_{i_n} \to ((\omega_{j_m} \to \chi) \to (\omega_{j_m} \to \psi)))$
(iii) $\vdash_T \omega_{i_1} \dots \omega_{i_n} \to ((\omega_{j_m} \to \chi) \to (\omega_{j_m} \to \psi))$
where: (i) is a B-axiom; (ii) follows from (i) and lemma 1.4; (iii) follows from (ii), (1) and modus ponens. If $n = 0$ and $m = p = 1$ then $\vdash_T \omega_{k_1} \to \psi$ follows from (iii), (2) and modus ponens. Otherwise $k_p = j_m$ and $\{k_1, \dots, k_{p-1}\} = \{i_1, \dots, i_n, j_1, \dots, j_{m-1}\}$. By induction hypothesis $\vdash_T \omega_{k_1} \dots \omega_{k_{p-1}} \to (\omega_{j_m} \to \psi)$.

Suppose $n > 0$, $m > 1$ and $i_n > j_{m-1}$. Then
(iv) $\vdash_T (\omega_{j_m} \to \chi) \to ((\chi \to \psi) \to (\omega_{j_m} \to \psi))$
(v) $\vdash_T (\omega_{j_1} \dots \omega_{j_m} \to \chi) \to (\omega_{j_1} \dots \omega_{j_{m-1}} \to ((\chi \to \psi) \to (\omega_{j_m} \to \psi)))$
(vi) $\vdash_T \omega_{j_1} \dots \omega_{j_{m-1}} \to ((\chi \to \psi) \to (\omega_{j_m} \to \psi))$
(vii) $\vdash_T \omega_{n_1} \dots \omega_{n_q} \to (\omega_{j_m} \to \psi)$
where: (iv) is a B'-axiom; (v) follows from (iv) and lemma 1.4; (vi) follows from (v), (2) and modus ponens; $\{n_1, \dots, n_q\} = \{j_1, \dots, j_{m-1}, i_1, \dots, i_n\}$; (vii) follows from (vi), (1) and the induction hypothesis. If $j_m > i_n$, then $(n_1, \dots, n_q, j_m) = (k_1, \dots, k_p)$. Otherwise $j_m = i_n$, $n_q = i_n$, $(n_1, \dots n_q) = (k_1, \dots, k_p)$ and
(viii) $\vdash_T \omega_{k_1} \dots \omega_{k_{p-1}} \to (\omega_{i_n} \to (\omega_{i_n} \to \psi))$
(ix) $\vdash_T (\omega_{i_n} \to (\omega_{i_n} \to \psi)) \to (\omega_{i_n} \to \psi)$
(x) $\vdash_T (\omega_{k_1} \dots \omega_{k_{p-1}} \to (\omega_{i_n} \to (\omega_{i_n} \to \psi))) \to (\omega_{k_1} \dots \omega_{k_{p-1}} \to (\omega_{i_n} \to \psi))$
(xi) $\vdash_T \omega_{k_1} \dots \omega_{k_{p-1}} \to (\omega_{i_n} \to \psi)$
where: (viii) is (vii); (ix) is a W-axiom; (x) follows from (ix) and lemma 1.4; (xi) follows from (vii), (x) and modus ponens; (xi) is $\vdash_T \omega_{k_1} \dots \omega_{k_p} \to \psi$. □

Lemma 1.6. $\vdash_T \phi$ if and only if ϕ is NF-inhabited.

Proof. The left to right implication follows from lemma 1.3. An immediate induction on M shows that $M : \psi$, $\mathsf{Free}(M) = x_1, \dots, x_n$ and $x_1 : \chi_1, \dots, x_n : \chi_n$ implies $\vdash_T \chi_1 \dots \chi_n \to \psi$, using lemma 1.5 when M is an application. □

2. Blueprints

Let $(\mathbb{A}, \leq)$ be the set of all finite sequences of integers ordered by prefix ordering. Elements of $\mathbb{A}$ are called *addresses*. A *partial tree* is a function π whose domain is a set of addresses. We say that π is *rooted* if $\varepsilon \in \mathrm{dom}(\pi)$. For all $a \in \mathrm{dom}(\pi)$, the *relative depth of a in π* is the number of $b \in \mathrm{dom}(\pi)$ such that $b < a$. When the domain of π is a finite set, the *relative depth of* π is defined as 0 if π is of empty domain, the maximal relative depth of an address in π otherwise. For each address a, we let $\pi_{|a}$ denote the partial tree $c \mapsto \pi(a \cdot c)$ of domain $\{c \mid a \cdot c \in \mathrm{dom}(\pi)\}$. The following notations will be used to denote partial trees:

- $f(\pi_1, \dots, \pi_n)$ denotes the rooted partial tree π such that $\pi(\varepsilon) = f$ and $\pi_{|(i)} = \pi_i$ for each $i \in [1, \dots, n]$. When $n = 0$, the partial tree π may be written f instead of $f()$ if this notation is unambiguous.
- for every sequence $\overline{a} = (a_1, \dots, a_k)$ of pairwise incomparable addresses, $*_{\overline{a}}(\pi_1, \dots, \pi_k)$ denotes the partial tree π such that $\pi_{|a_i} = \pi_i$ for each $i \in [1, \dots, k]$. We let $*(\pi_1, \dots, \pi_k)$ denote the tree $*_{\overline{b}}(\pi_1, \dots, \pi_k)$ such that $\overline{b} = ((1), \dots, (k))$.

Let π, π' be partial trees. Let a be any address. We let $\pi[a \leftarrow \pi']$ denote the partial tree π'' such that $\pi''_{|a} = \pi'$ and $\pi''(b) = \pi(b)$ for all $b \in \mathrm{dom}(\pi)$ such that $a \not\leq b$.

A *tree domain* is a set $A \subseteq \mathbb{A}$ such that for all $a \in A$ and for every integer $i > 0$, if $a \cdot (i) \in A$, then $a \cdot (j) \in A$ for each $j \in \{1, \ldots, i\}$. A tree domain A is *finitely branching* if and only if for each $a \in A$, there exists an integer i such that $a \cdot (i)$ is undefined. We call *tree* every function whose domain is a tree domain.

2.1. *Blueprint of a term*

Let $\mathfrak{S}$ be the signature consisting of all formulas and all symbols of the form $@_\phi$ where ϕ is a formula, each formula being of null arity and each $@_\phi$ being of arity 2. We call *blueprint* every finite partial tree $\alpha : A \to \mathfrak{S}$ satisfying the following condition: for each $a \in A$, if $\alpha(a) = @_\phi$, then $\alpha_{|a\cdot(1)}$ and $\alpha_{|a\cdot(2)}$ are of non-empty domains.

We write $\emptyset_{\mathbb{B}}$ the blueprint of empty domain. For each $S \subseteq \mathfrak{S}$: we call *S-blueprint* every blueprint whose image is a subset of S; we write $\mathbb{B}(S)$ the set of all S-blueprints and $\mathbb{B}_\varepsilon(S)$ the set of all rooted S-blueprints.

In the remainder terms will be freely identified with trees. We identify: x with the tree mapping ε to x; $\lambda x.M$ with the tree τ mapping ε to λx such that $\tau_{|(1)}$ is the tree of M; $(M_1\, M_2)$ with the tree τ mapping ε to @ such that $\tau_{|(i)}$ is the tree of M_i for each $i \in \{1, 2\}$.

Definition 2.1. For all $M \in \mathsf{NF}$, the *stable part* of M is the set of all $a \in \mathrm{dom}(M)$ such that $\mathsf{Free}(M_{|a}) \subseteq \mathsf{Free}(M)$ and $M_{|a}$ is a variable or an application.

Remarks. It is easy to check that our conventions - no variable may be simultaneously free and bound in a term - ensure that the stable part of a term M does not depend on the choice of bound variables. Since M is in normal form, M is of empty stable part if and only if it is closed. If $\mathsf{Free}(M_{|a\cdot b}) \subseteq \mathsf{Free}(M)$ then $\mathsf{Free}(M_{|a\cdot b}) \subseteq \mathsf{Free}(M_{|a})$. Consequently if $a \cdot b$ is in the stable part of M, then b is in the stable part of $M_{|a}$.

Definition 2.2. For all $M \in \mathsf{NF}$, we call *blueprint of M* the function α mapping each a in the stable part of M to:
— ψ if $M_{|a}$ is a variable x of type ψ,
— $@_\psi$ if $M_{|a}$ is an application of type ψ.
We write $M \Vdash \alpha$ the judgment "M is of blueprint α".

Remarks. If $M = (M_1 M_2) \in \mathsf{NF}$, $M : \phi$, $M_1 \Vdash \alpha_1$, $M_2 \Vdash \alpha_2$, then each α_i is of non-empty domain and $(M_1 M_2) \Vdash @_\phi(\alpha_1, \alpha_2)$ - in other words the so-called blueprint of M is indeed a blueprint. If $M_{|b} \Vdash \beta$ and $M_{|b\cdot c} \Vdash \gamma$, then $\beta_{|c} = \gamma$. When $M = \lambda x.M_1$ the blueprint of M is of the form $*(\alpha)$ - the relation between α and the blueprint of M_1 in that case will be clarified by lemma 2.6.

2.2. *Blueprint reduction*

Definition 2.3. The judgment $\alpha \rhd^a_\phi \alpha'$ where α, α' are blueprints, a is an address and ϕ is a formula, is inductively defined as follows:

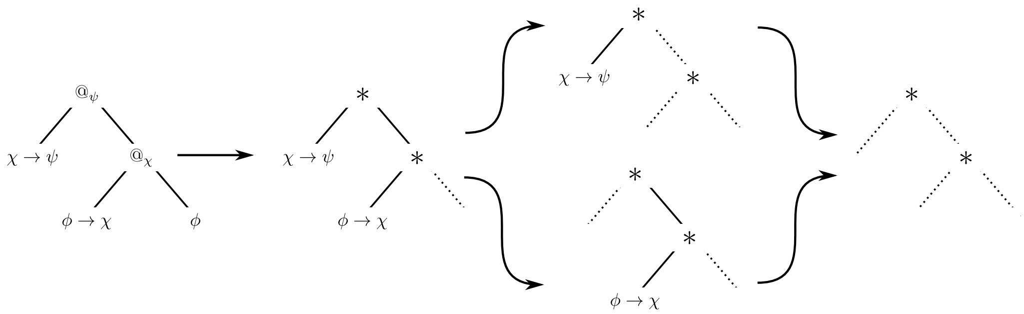

Fig. 1. Full reduction of a blueprint.

— $\phi \rhd_{\phi}^{\varepsilon} \emptyset_{\mathbb{B}}$,
— if $\beta_2 \rhd_{\phi}^{c} \beta_2'$, then $@_{\psi}(\beta_1, \beta_2) \rhd_{\phi}^{(2)\cdot c} *(\beta_1, \beta_2')$
— if $b = (b_1, \ldots, b_n)$, $\beta_i \rhd_{\phi}^{c} \beta_i'$, then $*_{\overline{b}}(\beta_1, \ldots, \beta_n) \rhd_{\phi}^{b_i \cdot c} *_{\overline{b}}(\beta_1, \ldots, \beta_{i-1}, \beta_i', \beta_{i+1}, \ldots, \beta_n)$.

We let $\rhd_{\phi}$ be the relation defined by: $\alpha \rhd_{\phi} \alpha' \Leftrightarrow \exists a\, (\alpha \rhd_{\phi}^{a} \alpha')$.

Remarks. The blueprint α' can be seen as α in which the formula ϕ at a is erased together with all @'s in the path to a. At each @ this path follows the left branch of @. When $\alpha \neq \emptyset_{\mathbb{B}}$ there exists necessarily a, ϕ, α' such that $\alpha \rhd_{\phi}^{a} \alpha'$. For instance (see figure 2.2):

$$
\begin{aligned}
— \quad @_{\psi}(\chi \to \psi, @_{\chi}(\phi \to \chi, \phi)) \quad &\rhd_{\phi}^{(2,2)} \quad *(\chi \to \psi, *(\phi \to \chi, \emptyset_{\mathbb{B}})) \\
&\rhd_{\phi\to\chi}^{(2,1)} \quad *(\chi \to \psi, *(\emptyset_{\mathbb{B}}, \emptyset_{\mathbb{B}})) \\
&\rhd_{\chi\to\psi}^{(1)} \quad *(\emptyset_{\mathbb{B}}, *(\emptyset_{\mathbb{B}}, \emptyset_{\mathbb{B}})) = \emptyset_{\mathbb{B}}
\end{aligned}
$$

$$
\begin{aligned}
— \quad @_{\psi}(\chi \to \psi, @_{\chi}(\phi \to \chi, \phi)) \quad &\rhd_{\phi}^{(2,2)} \quad *(\chi \to \psi, *(\phi \to \chi, \emptyset_{\mathbb{B}})) \\
&\rhd_{\chi\to\psi}^{(1)} \quad *(\emptyset_{\mathbb{B}}, *(\phi \to \chi, \emptyset_{\mathbb{B}})) \\
&\rhd_{\phi\to\chi}^{(2,1)} \quad *(\emptyset_{\mathbb{B}}, *(\emptyset_{\mathbb{B}}, \emptyset_{\mathbb{B}})) = \emptyset_{\mathbb{B}}
\end{aligned}
$$

Definition 2.4. For each blueprint α we write $\mathbb{F}(\alpha)$ the set of all sequences $(\phi_1, \ldots, \phi_n)$ such that $\alpha \rhd_{\phi_n}^{+} \ldots \rhd_{\phi_1}^{+} \emptyset$.

Remarks. Either $\alpha = \emptyset_{\mathbb{B}}$ and $\mathbb{F}(\alpha) = \{\varepsilon\}$; or $\alpha \neq \emptyset_{\mathbb{B}}$, all elements of $\mathbb{F}(\alpha)$ are non-empty sequences and $\mathbb{F}(\alpha)$ is the closure under contraction of the set of all (non-empty) sequences $(\phi_1, \ldots, \phi_n)$ such that $\alpha \rhd_{\phi_n} \ldots \rhd_{\phi_1} \emptyset$.

Definition 2.5. A *contraction* of a sequence F is either the sequence F or a sequence $G \cdot (f) \cdot H$ where $G \cdot (f) \cdot (f) \cdot H$ is a contraction of F. Given finite sequences $F_1, \ldots, F_n$ we call *shuffle* of $(F_1, \ldots, F_n)$ every sequence $F_1^1 \cdot \ldots \cdot F_n^1 \cdot \ldots \cdot F_1^p \cdot \ldots \cdot F_n^p$ such that $F_i^1 \cdot \ldots \cdot F_i^p = F_i$ for each i. For each tuple of sets of finite sequences $(\mathcal{F}_1, \ldots, \mathcal{F}_n)$ we write $\circledast(\mathcal{F}_1, \ldots, \mathcal{F}_n)$ the closure under contraction of the set of shuffles of elements of $\mathcal{F}_1, \times \ldots \times \mathcal{F}_n$. Given two finite sequences F_1, F_2 we call *right-shuffle* of (F_1, F_2) every sequence $F_1^1 \cdot F_2^1 \cdot \ldots \cdot F_1^p \cdot F_2^p$ where $F_i^1 \cdot \ldots F_i^p = F_i$ for each i and $F_2^p \neq \varepsilon$ if $F_1 \neq \varepsilon$.

For each pair of sets of finite sequences $(\mathcal{F}_1, \mathcal{F}_2)$ we write $\circledast(\mathcal{F}_1, \mathcal{F}_2)$ the closure under contraction of the set of right-shuffles of elements $\mathcal{F}_1 \times \mathcal{F}_2$.

Remarks. The following properties follow from our definitions and will be used without reference:

1 If $\alpha = \emptyset_{\mathbb{B}}$, then $\mathbb{F}(\alpha) = \{\varepsilon\}$.
2 If $\alpha = \phi$, then $\mathbb{F}(\alpha) = \{(\phi)\}$.
3 If $\alpha = *_{\overline{a}}(\beta_1, \ldots, \beta_k)$, then $\mathbb{F}(\alpha) = \circledast(\mathbb{F}(\beta_1), \ldots, \mathbb{F}(\beta_k))$.
4 If $\alpha = @_\phi(\alpha_1, \alpha_2)$, then $\mathbb{F}(\alpha) = \circledcirc(\mathbb{F}(\alpha_1), \mathbb{F}(\alpha_2))$.

2.3. *Abstraction vs blueprint reduction*

Recall that for every strictly increasing sequence of variables $X = (x_{i_1}, \ldots, x_{i_n})$, we let $\Omega(X)$ denotes the sequence of the types of $x_{i_1}, \ldots, x_{i_n}$. We now clarify the link between the blueprint α of a term M and the one of $\lambda x.M$.when both belong to NF.

The next lemma immediately implies $\Omega(\mathsf{Free}(M)) \in \mathbb{F}(\alpha)$. Lemma 2.7 states that for each sequence of formulas $F \in \Omega(\alpha)$ and for each sequence Y such that $\Omega(Y) = F$, one can rename the variables of M so that the yielded term N is an element of NF of blueprint α, of same type as M and such that $\mathsf{Free}(N) = Y$.

Lemma 2.6. For all $M \in \mathsf{NF}$ of type ϕ, of blueprint α, the following conditions are equivalent:

1 $\lambda x.M : \chi \to \phi$ and $\lambda x.M \Vdash \beta$.
2 x is the greatest free variable of M and there exists $\alpha', a_1, \ldots, a_n$ such that:
— $M^{-1}(x) = \{a_1, \ldots, a_n\}$,
— $\alpha \rhd_\chi^{a_1} \ldots \rhd_\chi^{a_n} \alpha'$,
— $\beta = *(\alpha')$.

Proof. Let ρ_M be the least partial function such that: $\rho_M(\varepsilon, \gamma) = \gamma$ for all blueprint γ; if $\rho_M(X, \gamma) = \delta$, $M^{-1}(x) = \{a_0, \ldots, a_n\}$ and $\delta \rhd_\chi^{a_0} \ldots \rhd_\chi^{a_n} \delta'$, then $\rho_M((x) \cdot X, \gamma) = \delta'$. Note that $M^{-1}(x) = \{a_0, \ldots, a_n\} = \{b_0, \ldots, b_n\}$, $\delta \rhd_\chi^{a_0} \ldots \rhd_\chi^{a_n} \delta'$ and $\delta \rhd_\chi^{b_0} \ldots \rhd_\chi^{b_n} \delta''$ implies $\delta' = \delta''$, consequently ρ_M is indeed a function. For each finite sequence of variables X, let $\mu_M(X, \alpha)$ be the restriction of α to $\mathrm{dom}(\alpha) \cap \{a \mid \mathsf{Free}(M_{|a}) \subseteq X\}$. We shall prove by induction on M that for all pairs (X, X') such that $\mathsf{Free}(M) = X \cdot X'$, we have $\mu_M(X, \alpha) = \rho_M(X', \alpha)$. In particular if $\mathsf{Free}(M) = X \cdot (x)$, the following property implies the lemma: the blueprint of $\lambda x.M$ is $*(\mu_M(X, \alpha))$ and $\rho_M((x), \alpha) = \mu_M(X, \alpha)$.

The case $X' = \varepsilon$ is immediate so we may as well assume that X' is a non-empty suffix of $\mathsf{Free}(M)$. The case $M = x$ follows immediately from our definitions.

Suppose $M = (M_1\, M_2)$, $M_1 : \phi_1$ $M_1 \Vdash \alpha_1$, $\phi_1 = \phi_2 \to \phi$, $M_2 : \phi_2$, $M_2 \Vdash \alpha_2$. There exists X_1, X_2, X_1', X_2' such that: $X_1 \cup X_2 = X$; $X_1' \cup X_2' = X'$; $\mathsf{Free}(M_i) = X_i \cdot X_i'$ for each $i \in \{1, 2\}$. We have $\alpha = @_\phi(\alpha_1, \alpha_2)$ and $\mu_M(X, \alpha) = *(\mu_{M_1}(X_1, \alpha_1), \mu_{M_2}(X_2, \alpha_2))$. By induction hypothesis $\mu_{M_i}(X_i, \alpha_i) = \rho_{M_i}(X_i', \alpha_i)$ for each i. The sequence X' is non-empty hence the last elements of X', X_2' are equal. As a consequence $\rho_M(X', \alpha) = *(\rho_{M_1}(X_1', \alpha_1), \rho_{M_2}(X_2', \alpha_2)) = \mu_M(X, \alpha)$.

Suppose $M = \lambda x.M_1 : \chi \to \psi_1,\ M_1 \Vdash \alpha_1$. By induction hypothesis $\mu_{M_1}(X, \alpha_1) = \rho_{M_1}(X' \cdot (x), \alpha_1) = \rho_{M_1}(X', \rho_{M_1}(x, \alpha_1)) = \rho_{M_1}(X', \mu(X \cdot X', \alpha_1)) = \rho_{M_1}(X', \alpha_{|(1)})$. Also $\mu_{M_1}(X, \alpha_1) = \mu_{M_1}(X, \mu_1(X \cdot X', \alpha_1)) = \mu_{M_1}(X, \alpha_{|(1)})$. Hence $\mu_{M_1}(X, \alpha_{|(1)}) = \rho_{M_1}(X', \alpha_{|(1)})$, therefore $\mu_{M_1}(X, \alpha) = \rho_{M_1}(X', \alpha)$. □

Lemma 2.7. For all $M \in \mathsf{NF}$ of blueprint α, for all Y such that $\Omega(Z) \in \mathbb{F}(\alpha)$, there exists N of same domain, of same blueprint and of same type as M such that $\mathsf{Free}(N) = Y$.

Proof. By an easy induction on M, using the implication (2) ⇒ (1) of lemma 2.6 when M is an abstraction. □

3. Proof-search

This section introduces the proof-search technique allowing one to decide whether a given formula is NF-inhabited. The two main definitions of this part are the ones of a *shadow* and of a *compact* shadow (definitions 3.6 and 3.8).

3.1. *Blueprint equivalence and transversal compression*

Definition 3.1. We let $\equiv$ be the least binary relation on blueprints such that:
— $\phi \equiv \phi$,
— if $\alpha_1 \equiv \beta_1$ and $\alpha_2 \equiv \beta_2$ then $@_\phi(\alpha_1, \alpha_1) \equiv @_\phi(\beta_1, \beta_2)$,
— if $|\overline{a}| = |\overline{b}| = n$ and $\alpha_i \equiv \beta_i$ for each $i \in [1, \ldots n]$, then $*_{\overline{a}}(\alpha_1, \ldots \alpha_n) \equiv *_{\overline{b}}(\beta_1, \ldots, \beta_n)$.

Remarks. Up to some extent this equivalence allows us to consider blueprints regardless of the exact values of their adresses. For instance $*_{\overline{a}}(\alpha_1, \ldots \alpha_n) \equiv *(\alpha_1, \ldots, \alpha_n) \equiv *(\alpha_n, \ldots, \alpha_1)$, also $*(*(\alpha, \beta), \gamma) \equiv *(\alpha, \beta, \gamma) \equiv *(\alpha, *(\beta, \gamma))$, etc. It is easy to check that $\alpha \equiv \beta$ implies $\mathbb{F}(\alpha) = \mathbb{F}(\beta)$ - this property will be used without reference.

Definition 3.2. For each non-null integer m, we let $\curvearrowleft_m$ be the binary relation on blueprints inductively defined as follows:
— if $\beta_1 \equiv \ldots \equiv \beta_{m+1}$,
then $*_{\overline{a}}(\gamma_1, \ldots, \gamma_k, \beta_1, \ldots, \beta_m) \curvearrowleft_m *_{\overline{a} \cdot b}(\gamma_1, \ldots, \gamma_k, \beta_1, \ldots, \beta_m, \beta_{m+1})$,
— if $\alpha \curvearrowleft_m \beta$ then:
- $@_\phi(\alpha, \gamma) \curvearrowleft_m @_\phi(\beta, \gamma)$,
- $@_\phi(\gamma, \alpha) \curvearrowleft_m @_\phi(\gamma, \beta)$,
- $*_{\overline{a}}(\alpha, \gamma_0, \ldots, \gamma_k) \curvearrowleft_m *_{\overline{a}}(\beta, \gamma_0, \ldots, \gamma_k)$.

We call *m-compression of β* every α such that $\alpha \curvearrowleft_m \beta$. The *width* of β is defined as the least m for which there is no α such that $\alpha \curvearrowleft_m \beta$. We write $\sqsubseteq_m$ the reflexive and transitive closure of the union of $\equiv$ and $\curvearrowleft_m$. We let $\sqsubseteq_m^{\max}$ denote the subset of the relation $\sqsubseteq_m$ of all pairs with a left-hand-side of width at most m.

Remarks. If β is of width m, then for all address a and for $\beta_{|a} = *_{\overline{a}}(\gamma_1, \ldots, \gamma_k)$ the sequence $(\gamma_1, \ldots, \gamma_k)$ contains no more than m blueprints $\equiv$-equivalent to γ_i for each i. Of course $\alpha \sqsubseteq_m \beta$ implies $\alpha \sqsubseteq_j \beta$ for all $j \in [1, \ldots, m]$ and clearly, $\alpha \curvearrowleft_m \beta$ implies $|\mathrm{dom}(\alpha)| < |\mathrm{dom}(\beta)|$ therefore $\curvearrowleft_m$ is well-founded.

Definition 3.3. For all $S \subseteq \mathfrak{S}$, for all $d \in \mathbb{N}$ and for all $m \in \mathbb{N}^*$:

— we let $\mathbb{B}(S, d, \infty)$ be the set of S-blueprints of relative depth at most d,
— we let $\mathbb{B}(S, d, m)$ be the set of all blueprints in $\mathbb{B}(S, d, \infty)$ of width at most m.

Lemma 3.4. For all finite $S \subseteq \mathfrak{S}$, for all $d \in \mathbb{N}$ and for all $m \in \mathbb{N}^*$:

1 The set $\mathbb{B}(S, d, m)/\equiv$ is a finite set.
2 A selector $\mathbb{R}(S, d, m)$ for $\mathbb{B}(S, d, m)/\equiv$ is effectively computable from (S, d, m).

Proof. We prove the two propositions simultaneously by induction on d. (A) For each $\alpha \equiv *(\phi_1, \ldots, \phi_k) \in \mathbb{B}(S, 0, m)$, let $\sigma(\alpha) = (\phi_1, \ldots, \phi_k)$. Clearly, for each $\phi \in S$, there are no more than m occurrences of ϕ in $\sigma(\alpha)$. For all $\alpha' \in \mathbb{B}(S, 0, m)$, we have $\alpha \equiv \alpha'$ if and only if $\sigma(\alpha)$ and $\sigma(\alpha')$ are equal up to permutation of their elements. As a consequence, $\mathbb{B}(S, 0, m)/\equiv$ is a finite set and we may define $\mathbb{R}(S, 0, m)$ as the set consisting in all blueprints of the form $*(\phi_1, \ldots, \phi_k)$ where each null arity symbol of S occurs at most m times in the sequence $(\phi_1, \ldots, \phi_k)$.

(B) Let $\mathcal{R}$ be the set of all blueprints of the form $@_\phi(\phi_1, \phi_2)$ where $@_\phi \in S$ and $(\alpha_1, \alpha_2) \in \mathbb{R}(S, d, m) \times \mathbb{R}(S, d, m)$. Let S be the set of all sequences over $\mathcal{R}$ in which every element occurs at most m times. We may define $\mathbb{R}(S, d + 1, m)$ as the set of all blueprints of the form $*(\beta_1, \ldots, \beta_k)$ where $(\beta_1, \ldots, \beta_k)$ is a sequence over $\mathcal{R}$ in which evey element occurs at most m times. $\square$

3.2. *Shadows*

Definition 3.5. For each integer d, for each formula ϕ, we let $\mathfrak{R}(\phi, d)$ be the set equal to $\{\emptyset_{\mathbb{B}}\}$ if $d = 0$, and otherwise equal to $\mathbb{R}(\Sigma_0, d, d \times p)$, where $\mathbb{R}$ is the function introduced in lemma 3.4, Σ_0 is the set of all subformulas of ϕ and all $@_\psi$ where ψ is a subformula of ϕ and p is the cardinal of the set of all subformulas of ϕ.

Definition 3.6. We call *ϕ-shadow* every tree Ξ satisyfing the following conditions:

— $\Xi(\varepsilon) = (\emptyset_{\mathbb{B}}, \phi)$,
— each node of Ξ is of arity at most 2,
— for each $a \in \mathrm{dom}(\Xi)$, let d_a be the number of $b < a$ such that the node of Ξ at b is unary; $\Xi(a)$ is of the form (γ, ψ) where ψ is a subformula of ϕ and $\gamma \in \mathfrak{R}(\phi, d_a)$

Definition 3.7. Let $\Uparrow$ be least reflexive and transitive relation on $\mathbb{B}$ satisfying the following condition: if $a, b \in \mathrm{dom}(\beta)$, $a < b$ and $\beta(a) = \beta(b)$, then $\beta[a \leftarrow \beta_{|b}] \Uparrow \beta$. We call *shadow ordering* the binary relation $\Subset$ on $\mathbb{B}$ defined by $\alpha \Subset \beta$ if and only if for all $F \in \mathbb{F}(\alpha)$ there exists $\beta' \Uparrow \beta$ such that $F \in \mathbb{F}(\beta')$.

Obviously $\Uparrow$ is a well-founded partial order and $\alpha \Uparrow \beta$ implies $|\mathrm{dom}(\alpha)| \leq |\mathrm{dom}(\beta)|$.

Definition 3.8. A shadow Ξ is *compact* if and only if there exists no a, b such that: $a < b$, the nodes of Ξ at a, b are of same arity, $\Xi(a) = (\gamma_a, \psi)$, $\Xi(b) = (\gamma_b, \psi)$ and $\gamma_a \Subset \gamma_b$.

4. Compact shadows and NF-inhabitation

We prove in this scetion that a formula ϕ is NF-inhabited if and only if there exists a compact ϕ-shadow of same domain as a NF-inhabitant of ϕ.

4.1. *Blueprint pumping vs term pumping*

Definition 4.1. Two terms $M, M' \in \mathsf{NF}$ are *of same kind* if and only they are both variables, or both applications, or both abstractions, and if they are of same type.

The next lemma shows that we can safely "pump" a term within its stable part in the following sense: if $M \Vdash \beta$, $a < b$ and $\beta(a) = \beta(b)$, then $M[a \leftarrow M_{|b}]$ is not in general a well-labelled term, yet there exists in NF a term M of same domain, of blueprint $\beta[a \leftarrow \beta_{|b}]$.

Lemma 4.2. Suppose $M : \phi$, $M \Vdash \beta$ and $\alpha \Uparrow \beta$. There exists a term $M' \in \mathsf{NF}$ of same kind as M, of blueprint α and such that $|\mathrm{dom}(M')| \leq |\mathrm{dom}(M)|$.

Proof. It suffices to consider the case of $\alpha = \beta[a \leftarrow \beta_{|b}]$ with $a, b \in \mathrm{dom}(\beta)$, $a < b$ and $\beta(a) = \beta(b)$. Recall that for all c, c', if $b = c \cdot c'$ and $M_{|c} \Vdash \gamma$, then $\gamma_{|c'} = \beta_{|b}$. We prove the existence of M' by induction on the length of a. The case $a = \varepsilon$ is immediate. Assume $a \neq \varepsilon$.

(1) Suppose $M = (M_1\, M_2)$, $M_1 \Vdash \beta_1$, $M_2 \Vdash \beta_2$, $a = (i) \cdot a_i$ and $b = (i) \cdot b_i$. By induction hypothesis there exists N_i of blueprint $\gamma_i = \beta_i[a_i \leftarrow \beta_{i|b_i}] = \beta_i[a_i \leftarrow \beta_{|b}]$, of same kind as M_i and such that $\mathrm{dom}(N_i) \leq \mathrm{dom}(M_i)$. Let $j = 1$ if $i = 2$, otherwise let $j = 2$. Let $(N_j, \gamma_j) = (M_j, \beta_j)$. By lemma 2.7 there exists M'_1, M'_2 such that $(M'_1 M'_2)$ is well labelled and each M'_i is a term of blueprint γ_i of same kind and same domain as N_i. Moreover we may take $M' = (M'_1\, M'_2)$.

(2) Suppose $M = \lambda x.M_1$, $M_1 \Vdash \beta_1$, $x : \chi$, $a = (1) \cdot a_1$ and $b = (1) \cdot b_1$. As $a, b \in \mathrm{dom}(\beta)$, we have also $a_1, a_2 \in \mathrm{dom}(\beta_1)$. By induction hypothesis there exists M'_1 of same kind as M_1, of blueprint $\alpha_1 = \beta_1[a_1 \leftarrow \beta_{1|b_1}]$ and such that $\mathrm{dom}(M'_1) \leq \mathrm{dom}(M_1)$. By lemma 2.6 there exists $\gamma_1, c_0, \ldots, c_n$ such that $\{c_0, \ldots, c_n\} = M_1^{-1}(x)$, $\beta_1 \rhd^{c_0}_{\chi} \ldots \rhd^{c_n}_{\chi} \gamma_1$ and $\beta = *(\gamma_1)$. Now, $a, b \in \mathrm{dom}(\alpha)$ implies that for each i: a_1 and c_i are incomparable addresses; b_1 and c_i are incomparable addresses. So $\beta_1[a_1 \leftarrow \beta_{1|b_1}] \rhd^{c_0}_{\chi} \ldots \rhd^{c_n}_{\chi} \gamma_1[a_1 \leftarrow \beta_{1|b_1}] = \beta[a \leftarrow \beta_{|b}]_{|(1)}$ and there exists in $\mathbb{F}(\alpha_1)$ a sequence of last element χ. By lemma 2.7 there exists a term N'_1 of same type and of same domain as M'_1 such that the greatest variable y free in N'_1 is of type χ. By lemma 2.6, $\lambda y.N'_1 \Vdash \beta[a \leftarrow \beta_{|b}]$ and we may take $M' = \lambda y.N'_1$. □

Lemma 4.3. If $\alpha \sqsubseteq_m \beta$, then:

1 $\mathbb{F}(\alpha) \subseteq \mathbb{F}(\beta)$.
2 For all $G \in \mathbb{F}(\beta)$, there exists in $\mathbb{F}(\alpha)$ a subsequence of G.
3 The set of all elements of $\mathbb{F}(\beta)$ of length at most m is a subset of $\mathbb{F}(\alpha)$.

Proof. We prove each property by induction on $|\mathrm{dom}(\beta)|$. Since $\gamma \equiv \gamma'$ implies $\mathbb{F}(\gamma) = \mathbb{F}(\gamma')$ and $|\mathrm{dom}(\gamma)| = |\mathrm{dom}(\gamma')|$, we may consider all blueprints up to $\equiv$.

(1) Since $\alpha \sqsubseteq_m \beta$ implies $\alpha \sqsubseteq_1 \beta$ it is sufficient to consider the case where α is $\equiv$-equivalent to some 1-compression of β. The base case $\beta \equiv *(\alpha, \alpha)$ is clear. The case

$\beta \equiv *(\beta', \gamma)$ and $\alpha \equiv *(\alpha', \gamma)$ with $\gamma \neq \emptyset_{\mathbb{B}}$ and $\alpha' \curvearrowleft_1 \beta'$ follow easily from the induction hypothesis, as well as the case $\beta \equiv @(\beta_1, \beta_2)$

(2) As in (1), it sufficient to consider the case where α is $\equiv$-equivalent to some 1-compression of β. In order to deal with the case of $\beta \equiv @(\beta_1, \beta_2)$, we need to prove a more precise property: if β is not empty, then for all $G \in \mathbb{F}(\beta)$, there exists in $\mathbb{F}(\alpha)$ a subsequence F of G such that the last element of F and G are equal. Again, the base case $\beta \equiv *(\alpha, \alpha)$ is clear and the other cases follow easily from the induction hypothesis.

(3) The case $\beta \equiv *(\beta', \gamma)$ and $\alpha \equiv *(\alpha', \gamma)$ with $\gamma \neq \emptyset_{\mathbb{B}}$ and $\alpha' \curvearrowleft_m \beta'$ follow easily from the induction hypothesis, as well as the case $\beta \equiv @(\beta_1, \beta_2)$. The base case is $\alpha \equiv *(\gamma_1, \ldots, \gamma_m)$, $\beta \equiv *(\gamma_1, \ldots, \gamma_m, \gamma_{m+1})$ where for some γ we have $\gamma \equiv \gamma_i$ for all i. Let $\mathcal{G} = \mathbb{F}(\gamma)$. For each integer k, let $\mathcal{G}^{(k)} = \circledast(\mathcal{G}_1, \ldots, \mathcal{G}_k)$ where $\mathcal{G}_i = \mathbb{F}(\gamma)$ for each i. Let $F = (\phi_1, \ldots, \phi_p) \in \mathbb{F}(\beta)$ such that $p \leq m$. For each $J \subseteq \{1, \ldots, p\}$, and for $(j_1, \ldots, j_q)$ equal to the strictly increasing enumeration of all elements of J, let $f(J) = (\phi_{j_1}, \ldots, \phi_{j_q})$. We have $F \in \mathbb{F}(\beta) = \mathcal{G}^{(m+1)}$, hence there exist $J_1, \ldots, J_{m+1}$ such that $J_1 \cup \ldots \cup J_{m+1} = \{1, \ldots, p\}$, and $f(J_i) \in \mathbb{F}(\gamma)$ for each $i \in [1, \ldots, m+1]$. For each $j \in [1, \ldots, p]$, let $k_j \in [1, \ldots, m+1]$ be such that $j \in J_{k_j}$. Then $J_{k_1} \cup \ldots \cup J_{k_p} = \{1, \ldots, p\}$, so $F \in \circledast(\{f(J_{k_1})\}, \ldots, \{f(J_{k_p})\}) \subseteq \mathcal{G}^{(p)} \subseteq \mathcal{G}^{(m)} = \mathbb{F}(\alpha)$. □

Lemma 4.4. If $\alpha \Uparrow \beta \sqsubseteq_1 \beta'$, then there exists α' such that $\alpha \sqsubseteq_1 \alpha' \Uparrow \beta'$.

Proof. (1) An immediate induction on the sum of the lengths of all addresses in $\mathrm{dom}(\beta')$ shows that if $\alpha = \beta[a \leftarrow \beta_{|b}]$ and $\beta \equiv \beta'$, then there exist (a', b') such that $\alpha \equiv \alpha' = \beta'[a' \leftarrow \beta'_{|b'}]$. Consequently an immediate induction on the length of the derivation of $\alpha \Uparrow \beta$ shows that the lemma holds if $\beta \equiv \beta'$.

(2) Another induction on the sum of the lengths of all addresses in $\mathrm{dom}(\beta')$ shows that $\alpha \Uparrow \beta \curvearrowleft_1 \beta'$ implies the existence of α' such that $\alpha \curvearrowleft_1 \alpha' \Uparrow \beta'$. The only non trivial case is $\beta' = *_{\overline{a} \cdot b}(\gamma_1, \ldots, \gamma_k, \beta_1, \beta_2)$, $\beta = *_{\overline{a}}(\gamma_1, \ldots, \gamma_k, \beta_1)$ with $\beta_1 \equiv \beta_2$ and $\alpha = *_{\overline{a}}(\delta_1, \ldots, \delta_k, \alpha_1)$ where $\alpha_1 \Uparrow \beta_1$ and $\delta_i \Uparrow \gamma_i$ for each i. By (1), $\alpha_1 \Uparrow \beta_1 \equiv \beta_2$ implies the existence of α_2 such that $\alpha_1 \equiv \alpha_2 \Uparrow \beta_2$. Hence $\alpha = *_{\overline{a}}(\delta_1, \ldots, \delta_k, \alpha_1) \curvearrowleft_1 *_{\overline{a} \cdot b}(\delta_1, \ldots, \delta_k, \alpha_1, \alpha_2) \Uparrow *_{\overline{a} \cdot b}(\gamma_1, \ldots, \gamma_k, \beta_1, \beta_2) = \beta'$.

(3) Using (1) and (2), the lemma follows by induction on the length of an arbitrary sequence $(\beta_0, \ldots, \beta_n)$ such that $\beta_0 = \beta$, $\beta_n = \beta'$ and $\beta_{i-1} \equiv \beta_i$ or $\beta_{i-1} \curvearrowleft_1 \beta_i$ for each $i \in [1, \ldots, n]$. □

Lemma 4.5. For all formula ϕ, we have $\vdash_T \phi$ if and only if there exists a compact ϕ-shadow of same domain as an NF-inhabitant of ϕ.

Proof. The right to left implication follows trivially from lemma 1.6. Suppose $\vdash_T \phi$. By lemmas 1.6 there exists in NF a closed M of type ϕ of minimal size. For each $a \in \mathrm{dom}(M)$:

— let α_a, ϕ_a be respectively the blueprint and the type of $M_{|a}$,

— let $(a_1, \ldots, a_m)$ be the sequence of all prefixes of a strictly increasing w.r.t $<$, let $(\lambda x_1, \ldots, \lambda x_n)$ be the subsequence $(M(a_1), \ldots, M(a_m))$ of all binders; we let $\Lambda(M, a) = (x_1, \ldots, x_n)$.

Without loss of generality we may assume that all $\Lambda(M,a)$ are strictly increasing sequences of variables, so that $\mathsf{Free}(M_{|a})$ is a subsequence of $\Lambda(M,a)$ for each a. Let p be the cardinal of the set of all subformulas of ϕ.

(1) Suppose there exists $a \in \mathrm{dom}(M)$ such that α_a is of relative depth $n > |\Lambda(M,a)| \times p$. Let $b_1, \ldots, b_n, c \in \mathrm{dom}(\alpha_a)$ such that $b_1 < \ldots < b_n < c$. For each i, let $X_i = \mathsf{Free}(M_{|a \cdot b_i})$, let ϕ_i be the type of $M_{|a \cdot b_i}$. We have $X_n \subseteq \ldots \subseteq X_1 \subseteq \Lambda(M,a)$. By lemma 1.2, each ψ_i is a subformula of ϕ. Hence there exists i, j such that $i < j$ and $(X_i, \psi_i) = (X_j, \psi_j)$, that is, $M_{|a \cdot b_i}$ and $M_{|a \cdot b_j}$ are applications of the same type and with the same free variables. The term $M' = M[a \cdot b_i \leftarrow M_{|a \cdot b_j}]$ is then NF-inhabitant of type ϕ_i such that $|\mathrm{dom}(M')| < |\mathrm{dom}(M)|$, a contradiction.

(2) According to (1) each α_a is of depth at most $|\Lambda(M,a)| \times p$, hence there exists for each a a blueprint $\gamma_a \in \mathfrak{R}(\phi, |\Lambda(M,a)|)$ such that $\gamma_a \sqsubseteq^{\max}_{|\Lambda(M,a)|} \alpha_a$. The function Ξ mapping each $a \in \mathrm{dom}(\Pi)$ to (γ_a, ϕ_a) is therefore a $(\phi, 0)$-shadow. Assume by way of contradiction that this shadow is not compact. There exists $a, b \in \mathrm{dom}(M)$ and γ_a, γ_b such that $a < b$, $M_{|a}$, $M_{|b}$ are of same kind, $\gamma_a \sqsubseteq^{\max}_{|\Lambda(M,a)|} \alpha_a$, $\gamma_b \sqsubseteq^{\max}_{|\Lambda(M,a\cdot b)|} \alpha_b$ and $\gamma_a \Subset \gamma_b$. Let $X_a = \mathsf{Free}(M_{|a})$. By lemma 2.6, $\Omega(X_a) \in \mathbb{F}(\alpha_a)$. We have $X_a \subseteq \Lambda(M,a)$, therefore $|\Omega(X_a)| \leq |\Lambda(M,a)|$. By lemma 4.3, $\Omega(X_a) \in \mathbb{F}(\gamma_a)$. By assumption there exists δ_b such that $\delta_b \Uparrow \gamma_b \sqsubseteq_1 \alpha_b$ and $\Omega(X_a) \in \mathbb{F}(\delta_b)$. By lemma 4.4 there exists α'_b such that $\delta_b \sqsubseteq_1 \alpha'_b \Uparrow \alpha_b$. By lemma 4.3, $\Omega(X_a) \in \mathbb{F}(\alpha'_b)$. The conjuction of lemmas 4.2 and 2.7 implies the existence of $N \in \mathsf{NF}$ of blueprint α'_b, of same kind as $M_{|b}$, such that $|\mathrm{dom}(N)| \leq |\mathrm{dom}(M_{|b})|$ and $\mathsf{Free}(N) = X_a$. Then $M' = M[a \leftarrow N]$ is an NF-inhabitant of ϕ such that $|\mathrm{dom}(M')| < |\mathrm{dom}(M)|$, a contradiction. ☐

5. Finitness of the set of compact ϕ-shadows

Our last aim will be to prove that for each formula ϕ, the set of all compact ϕ-shadows is a finite set effectively computable from ϕ. We shall prove that for each finite $S \subseteq \mathfrak{S}$ (in particular when S is the set of all subformulas of ϕ and all applications tagged with a subformula of ϕ), the relation $\Subset$ is an almost full relation (Bezem, Klop and de Vrijer 2003) on $\mathbb{B}(S)$. This result will be proven with the help of Melliès' Axiomatic Kruskal Theorem (Melliès 1998)

5.1. *Almost full relations and Higman's theorem*

Definition 5.1. Let $\mathcal{U}$ be an arbitrary set. An *almost full relation (AFR) on* $\mathcal{U}$ is a binary relation $\ll$ such that for every infinite sequence $(u_i)_{i \in \mathbb{N}}$ over $\mathcal{U}$, there exists i, j such that $i < j$ and $u_i \ll u_j$.

Proposition 5.2.

1 If $\ll$ and $\ll'$ are AFRs on $\mathcal{U}$, then $\ll \cap \ll'$ is an AFR on $\mathcal{U}$.

2 Suppose $\ll_{\mathcal{U}}$ is an AFR on $\mathcal{U}$ and $\ll_{\mathcal{V}}$ is an AFR on $\mathcal{V}$. Let $\ll_{\mathcal{U}\times\mathcal{V}}$ be the relation defined by $(U, V) \ll_{\mathcal{U}\times\mathcal{V}} (U', V')$ if and only if $U \ll_{\mathcal{U}} U'$ and $V \ll_{\mathcal{V}} V'$. Then $\ll_{\mathcal{U}\times\mathcal{V}}$ is an AFR on $\mathcal{U} \times \mathcal{V}$.

Proof. See (Melliès 1998). ☐

Definition 5.3. Let $\mathcal{U}$ be a set, let $\ll$ be a binary relation. We let $\mathbb{S}(\mathcal{U})$ denote the set of all finite sequences over $\mathcal{U}$. The relation $\ll_{\mathbb{S}}$ *induced by* $\ll$ *on* $\mathbb{S}(\mathcal{U})$ is defined by $(U_1, \dots, U_n) \ll_{\mathbb{S}} (V_1, \dots, V_m)$ if and only if there exists a strictly monotone function $\eta : \{1, \dots, n\} \to \{1, \dots, m\}$ such that $U_i \ll V_{\eta(i)}$ for each $i \in \{1, \dots, n\}$.

Theorem 5.4. (Higman) If $\ll$ is an AFR on $\mathcal{U}$, then $\ll_{\mathbb{S}}$ is an AFR on $\mathbb{S}(\mathcal{U})$.

Proof. See (Higman 1952; Kruskal 1972; Melliès 1998). □

5.2. *From rooted to unrooted blueprints*

Lemma 5.5. Let S be a finite subset of $\mathfrak{S}$. Let $S_@$ be the set of all binary symbols of S. For all $\beta \in \mathbb{B}$, for all $G \in \mathbb{F}(\beta)$, there exists $\alpha \Uparrow \beta$ of relative depth at most $\Sigma_{i=1}^{1+|S_@|} i$ such that $\mathbb{F}(\alpha)$ contains a subsequence of G.

Proof. Call *S-linearisation* every pair (γ, H) such that $\gamma \in \mathbb{B}(S)$ and $H \in \mathbb{F}(\gamma)$. Call *starting address for* (γ, H) every address b for which there exists ϕ, γ' such that $\gamma \rhd_\phi^b \gamma'$ and $H \in \circledcirc(\mathbb{F}(\gamma'), (\phi))$. Call *path to b in γ* the maximal sequence $(b_1, \dots, b_n, b_{n+1})$ over elements of $\mathrm{dom}(\gamma)$ such that $b_1 < \dots < b_n < b_{n+1} = b$.

Given an arbitrary S-linearisation (β, G), we prove simultaneously by induction on the sum of $|S_@|$ and the sum of the length of all addresses in $\mathrm{dom}(\beta)$ the two properties:

1 There exists an S-linearisation (γ, H) such that :
   (a) $\gamma \Uparrow \beta$ and H is a subsequence of G,
   (b) γ is of relative depth at most $1 + \Sigma_{i=1}^{|S_@|} i$

2 There exists an S-linearisation (α, F) such that :
   (a) $\alpha \Uparrow \beta$, F is a subsequence of G, and the last elements of F, G are equal,
   (b) for each starting address b of (α, F) of path $(b_1, \dots, b_n, b_{n+1})$, the values $\alpha(b_1), \dots, \alpha(b_n)$ are pairwise distinct,
   (c) for all c incomparable with each starting address for (α, F), $(\alpha_{|c})$ is of relative depth $1 + \Sigma_{i=1}^{|S_@|} i$

Note that the conjunction of (2.b) and (2.c) implies that every address d in α is of relative depth at most $|S_@| + 1 + \Sigma_{i=1}^{|S_@|} i = \Sigma_{i=1}^{1+|S_@|} i$. The cases $\beta = *_{\overline{a}}(\beta')$ with $a \neq \varepsilon$ and $\beta = *_{\overline{a}}(\beta_1, \dots, \beta_n)$ with $n > 1$ follow easily from the induction hypothesis. Suppose $\beta = @_\psi(\beta_1, \beta_2)$.

(1) Let d be an address of maximal length in $\beta^{-1}(@_\psi)$. Let $\delta = @_\psi(\delta_1, \delta_2) = \beta_{|d}$. By assumption ε is the only element of $\delta^{-1}(@_\psi)$. As $G \in \mathbb{F}(\beta)$, there exists in $\mathbb{F}(\delta)$ a subsequence G' of G, and $(G_1, G_2) \in \mathbb{F}(\delta_1) \times \mathbb{F}(\delta_2)$ such that $G' \in \circledcirc(\{G_1\}, \{G_2\})$. By induction hypothesis there exists an $(S - \{@_\psi\})$-realisation (H_1, γ_1) statisfying conditions (1.a), (1.b) w.r.t (δ_0, G_1), and an $(S - \{@_\psi\})$-realisation (γ_2, H_2) satisfying conditions (2.a), (2.b), (2.c) w.r.t (δ_2, G_2).

Let $\gamma = @_\psi(\gamma_1, \gamma_2)$. We have $\gamma \Uparrow \delta$ and $\beta(\varepsilon) = \delta(\varepsilon) = \gamma(\varepsilon)$, hence $\gamma \Uparrow \beta$. Each γ_i is of relative depth at most $\Sigma_{i=1}^{|S_@|} i$, therefore γ is of relative depth at most $1 + \Sigma_{i=1}^{|S_@|} i$. Now H_2 is a subsequence of G_2 of same last element, so there exists in $\circledcirc(\{H_1\}, \{H_2\}) \subseteq \mathbb{F}(@_\psi(\gamma_1, \gamma_2))$ a subsequence H of G'. Thus (γ, H) satisfies (1.a) and (1.b) w.r.t (β, G).

(2) As $G \in \mathbb{F}(\beta)$, there exists $G_1 \in \mathbb{F}(\beta_1), G_2 \in \mathbb{F}(\beta_2)$ such that $G \in \circledcirc(\{G_1\}, \{G_2\})$. By induction hypothesis there exists an S-linearisation (α_1, F_1) satisfying conditions (1.a), (1.b) w.r.t (β_1, G_1), and an S-linearisation (α_2, F_2) satisfying conditions (2.a), (2.b), (2.c) w.r.t (β_2, G_2).

Let $\alpha_0 = @_\psi(\alpha_1, \alpha_2)$. We have $\alpha_0 \Uparrow \beta$. Since F_2 and G_2 are of same last symbol and $\circledcirc(\{F_1\}, \{F_2\}) \subseteq \mathbb{F}(\alpha)$, there exists in $\mathbb{F}(\alpha)$ a subsequence F_0 of G, of same last element as G. Hence (α_0, F_0) satisfies (2.a). For all c incomparable with each starting address for (α_0, F_0), either $c = (1) \cdot c'$ and $c' \in \mathrm{dom}(\alpha_1)$, or $c = (2) \cdot c''$ and $c'' \in \mathrm{dom}(\alpha_2)$ is incomparable with each starting address in α_2. As a consequence, the choice of α_1, α_2 ensures that (α_0, F_0) satisfies (2.c).

If (α_0, F_0) satisfies (2.b), then we may take $(\alpha, F) = (\alpha_0, F_0)$. Otherwise some starting address b for (α_0, F_0) does not satisfy condition (2.b). Let $(b_1, \dots, b_n, b_{n+1})$ be the path to b in α. We have $b_1 = \varepsilon$, and for each $i > 0$, there exists d_i such that $b_i = (2) \cdot d_i$. The sequence $(d_2, \dots, d_{n+1})$ is then a path to $d = d_{n+1}$ in α_2, and d is a starting address for (α_2, F_2). The values $\alpha_2(d_2), \dots, \alpha_2(d_n)$ are pairwise distinct, so there must exists $i > 1$ such that $\alpha(b_i) = @_\psi$. Since b_i is in the path to b, there exists in $\mathbb{F}(\alpha_{2|d_i})$ a subsequence F'_0 of F_0 of same last element as F_0. For $\alpha'_0 = \alpha_0[\varepsilon \leftarrow \alpha_{2|d_i}]$, we have $\alpha'_0 \Uparrow \beta$ and $F'_0 \in \mathbb{F}(\alpha'_0)$. The existence of (α, F) follows then from the induction hypothesis. □

Definition 5.6. For each tuple (S, β, G, α) satisfying the conditions of lemma 5.5, we call *S-residual of β* each α_0 such that $\alpha_0 \sqsubseteq_1^{\max} \alpha$.

Lemma 5.7. Let S be a finite subset of $\mathfrak{S}$. Suppose:
— $\beta = *_{\overline{a}}(\beta_1, \dots, \beta_n) \in \mathbb{B}(S)$,
— $\beta' = *_{\overline{b}}(\beta'_1, \dots, \beta'_n, \beta'_{n+1}, \dots, \beta'_{n+k}) \in \mathbb{B}(S)$,
— $(\beta_1, \dots, \beta_n) \Subset_{\mathbb{S}} (\beta'_1, \dots, \beta'_n)$,
— the sets of S-residuals of β, β' are equal.

Then $\beta \Subset \beta'$.

Proof. For each $i \in [1, \dots, n]$, let $G_i \in \mathbb{F}(\beta_i)$. Let $G \in \circledast(\{G_1\}, \dots, \{G_n\})$. By assumption there exists for each $i \in [1, \dots, n]$ a $\delta_i \Uparrow \beta'_i$ such that $G_i \in \mathbb{F}(\delta_i)$. As a consequence $G \in \mathbb{F}(*(\delta_1, \dots, \delta_n))$. By lemma 5.5, the set of S-residuals of β is not empty. By assumption there exist α, α_0 and for each $i \in [1, \dots, n+k]$ a blueprint α'_i such that: $\alpha_0 \sqsubseteq_1 \alpha \Uparrow \beta$; $\mathbb{F}(\alpha)$ contains a subsequence F of G; $\alpha_0 \sqsubseteq_1 *_{\overline{b}}(\alpha'_1, \dots, \alpha'_{n+k}) \Uparrow \beta'$. By lemma 4.3, there exists in $\mathbb{F}(\alpha_0) \cap \mathbb{F}(*_{\overline{b}}(\alpha'_1, \dots, \alpha'_{n+k}))$ a subsequence of F. Hence, for each $i \in [1, \dots, n+k]$, there exists in $\mathbb{F}(\alpha'_i)$ a subsequence of G. Let $\delta = *_{\overline{b}}(\delta_1, \dots, \delta_n, \alpha'_{n+1}, \dots, \alpha'_{n+k})$. Then $\delta \Uparrow \beta'$, $G \in \mathbb{F}(*(\delta_1, \dots \delta_n))$, and for each j there exists in $\mathbb{F}(\alpha'_{n+j})$ a subsequence of G. As a consequence $G \in \mathbb{F}(\delta)$. □

Lemma 5.8. Let S be a finite subset of $\mathfrak{S}$. Let $\mathcal{B}_\varepsilon$ be a subset of $\mathbb{B}_\varepsilon(S)$. Let $\mathcal{B} = \{*_{\overline{a}}(\beta_1, \dots, \beta_n) \mid \forall i \in [1, \dots, n], \beta_i \in \mathcal{B}_\varepsilon\}$. If $\Subset$ is an AFR on $\mathcal{B}_\varepsilon$, then $\Subset$ is an AFR on $\mathcal{B}$.

Proof. For each $\gamma \in \mathcal{B}$, the set of S-residuals of γ is a subset of $\mathcal{R} = \mathbb{B}(\mathcal{S}, \Sigma_{i=1}^{1+|S_@|} i, 1)$ closed under $\equiv$. By lemma 3.4, the set $\mathcal{R}$ is finite up to $\equiv$. For each $\gamma = *_{\overline{a}}(\gamma_1, \dots, \gamma_n) \in \mathcal{B}$ where $\overline{a}$ is increasing w.r.t the lexicographic ordering of addresses, let $\sigma(\gamma) = (\gamma_1, \dots, \gamma_n)$. By theorem 5.4, $\Subset_{\mathbb{S}}$ is an AFR on the set of all $\{\sigma(\gamma) \mid \gamma \in \mathcal{B}\}$. Let $\ll$ be the relation on

$\mathcal{B}$ defined by $\gamma \ll \gamma'$ if and only if $\sigma(\gamma) \Subset_{\mathbb{S}} \sigma(\gamma')$ and the sets of S-residuals of γ, γ' are equal. By lemma 5.2.(1), $\ll$ is an AFR on $\mathcal{B}$. The conclusion follows from lemma 5.7. □

5.3. *Axiomatic Kruskal theorem and main key-lemma*

Definition 5.9. An *abstract decomposition system* is an 8-tuple

$$(\mathcal{T}, \mathcal{L}, \mathcal{V}, \preceq_{\mathcal{T}}, \preceq_{\mathcal{L}}, \preceq_{\mathcal{V}}, \stackrel{\cdot}{\longrightarrow}, \vdash)$$

where:

— $\mathcal{T}$ is a set of *terms* noted $t, u, \ldots$ equipped with a binary relation $\preceq_{\mathcal{T}}$,
— $\mathcal{L}$ is a set of *labels* noted $f, g, \ldots$ equipped with a binary relation $\preceq_{\mathcal{L}}$,
— $\mathcal{V}$ is a set of *vectors* noted $T, U, \ldots$ equipped with a binary relation $\preceq_{\mathcal{V}}$,
— $\stackrel{\cdot}{\longrightarrow}$ is a relation on $\mathcal{T} \times \mathcal{L} \times \mathcal{V}$, *e.g.* $t \stackrel{f}{\longrightarrow} T$
— $\vdash$ is a relation on $\mathcal{V} \times \mathcal{T}$, *e.g.* $T \vdash t$.

For each such system, we let $\rhd_{\mathcal{T}}$ be the binary relation on $\mathcal{T}$ defined by

$$t \rhd_{\mathcal{T}} u \Longleftrightarrow \exists (f, T) \in \mathcal{L} \times \mathcal{V}, \quad t \stackrel{f}{\longrightarrow} T \vdash u$$

An *elementary term* t is a term minimal w.r.t $\rhd_{\mathcal{T}}$, that is, a term for which there exists no u such that $t \rhd_{\mathcal{T}} u$.

Theorem 5.10. (Melliès) Suppose $(\mathcal{T}, \mathcal{L}, \mathcal{V}, \preceq_{\mathcal{T}}, \preceq_{\mathcal{L}}, \preceq_{\mathcal{V}}, \stackrel{\cdot}{\longrightarrow}, \vdash)$ satisfies the following properties:

— (Axiom I) There is no infinite chain $t_1 \rhd_{\mathcal{T}} t_2 \rhd_{\mathcal{T}} \ldots$
— (Axiom II) The relation $\preceq_{\mathcal{T}}$ is an AFR on the set of elementary terms.
— (Axiom III) For all t, u, u', f, U,
  if $t \preceq_{\mathcal{T}} u'$ and $u \stackrel{f}{\longrightarrow} U \vdash u'$, then $t \preceq_{\mathcal{T}} u$.
— (Axiom IV-bis) For all t, u, f, g, T, U,
  if $t \stackrel{f}{\longrightarrow} T$ and $u \stackrel{g}{\longrightarrow} U$ and $f \preceq_{\mathcal{L}} g$ and $T \preceq_{\mathcal{V}} U$, then $t \preceq_{\mathcal{T}} u$.
— (Axiom V) For all $\mathcal{W} \subseteq \mathcal{V}$, for $\mathcal{W}_{\vdash} = \{t \in \mathcal{T} \mid \exists T \in \mathcal{W}, T \vdash t\}$,
  if $\preceq_{\mathcal{T}}$ is an AFR on $\mathcal{W}_{\vdash}$, then $\preceq_{\mathcal{V}}$ is an AFR on $\mathcal{W}$.

If furthermore $\preceq_{\mathcal{L}}$ is an AFR on $\mathcal{L}$, then $\preceq_{\mathcal{T}}$ is an AFR on $\mathcal{T}$.

Proof. See (Melliès 1998). □

Lemma 5.11. For each finite $S \subseteq \mathfrak{S}$, the relation $\Subset$ is an AFR on $\mathbb{B}(S)$.

Proof. According to lemma 5.8, it is sufficient to prove that $\Subset$ is an AFR on $\mathbb{B}_{\varepsilon}(S)$. Let $(\mathcal{T}, \mathcal{L}, \mathcal{V}, \preceq_{\mathcal{T}}, \preceq_{\mathcal{L}}, \preceq_{\mathcal{V}}, \stackrel{\cdot}{\longrightarrow}, \vdash)$ be the abstract decomposition system defined as follows.

— The set $\mathcal{T}$ is $\mathbb{B}_{\varepsilon}(S)$; we let $\alpha \preceq_{\mathcal{T}} \beta$ if and only if there exists an address c such that $\alpha \Subset (\beta_{|c})$ and $\alpha(\varepsilon) = (\beta_{|c})(\varepsilon)$.
— The set $\mathcal{L}$ is the set of all elements of S of non null arity, the relation $\preceq_{\mathcal{L}}$ is the identity relation on this set.
— The set $\mathcal{V}$ is equal to $\mathbb{B}(S) \times \mathbb{B}(S)$.
  The relation $\preceq_{\mathcal{V}}$ is defined by $(\gamma_1, \gamma_1) \preceq_{\mathcal{V}} (\delta_1, \delta_2)$ if and only if $\gamma_1 \Subset \delta_1$ and $\gamma_2 \Subset \delta_2$.

— The relation $\stackrel{\cdot}{\longrightarrow}$ is defined by $\alpha \stackrel{@_\phi}{\longrightarrow} (\gamma_1, \gamma_2)$ if and only if $\alpha = @_\phi(\gamma_1, \gamma_2)$.

— The relation $\vdash$ is the least relation satisfying the following condition. If $V = (\gamma_1, \gamma_2)$, $i \in \{1, 2\}$ and $\gamma_i = *_{\overline{a}}(\alpha_1, \ldots, \alpha_n)$ then $V \vdash \alpha_j$ for each $j \in [1, \ldots, n]$.

(A) For all $\mathcal{T}' \subseteq \mathcal{T}$, the relation $\Subset$ is an AFR on $\mathcal{T}'$ if and only if $\preceq_{\mathcal{T}}$ is an AFR on $\mathcal{T}'$. Indeed, consider an arbitrary infinite sequence $\overline{\alpha}$ over $\mathcal{T}'$. This sequence contains an infinite subsequence $(\alpha)_{i\in\mathbb{N}}$ such that all $\alpha_i(\varepsilon)$ are equal. Clearly $\alpha_i \Subset \alpha_j$ implies $\alpha_i \preceq_{\mathcal{T}} \alpha_j$. Conversely, if $\alpha_i \preceq_{\mathcal{T}} \alpha_j$, then there exists c such that $\alpha_i \Subset \alpha_{j|c}$ and $\alpha_i(\varepsilon) = \alpha_j(c)$. For all $F \in \mathbb{F}(\alpha_i)$, there exists γ such that $\gamma \Uparrow \alpha_{j|c}$ and $F \in \mathbb{F}(\gamma)$. Now the relation $\Uparrow$ is such that $\gamma(\varepsilon) = \alpha_i(\varepsilon) = \alpha_j(\varepsilon) = \alpha_j(c)$, so $\gamma \Uparrow \alpha_{j|c} \Uparrow \alpha_j$. Hence $\alpha_i \Subset \alpha_j$.

(B) We now check that all axioms of theorem 5.10 are satisfied. Axiom I is clear. The set of elementary terms is the set all $\alpha \in \mathbb{B}_\varepsilon(S)$ such that $\mathrm{dom}(\alpha) = \{\varepsilon\}$. Since S is a finite set, the relation $\preceq_{\mathcal{T}}$ is of course an AFR on the set of elementary terms, that is, axiom II is satisfied. Axiom III is immediate. If $(\gamma_1, \gamma_2) \preceq_{\mathcal{V}} (\delta_1, \delta_2)$ then $\gamma_1 \Subset \delta_1$ and $\gamma_2 \Subset \delta_2$ implies $@_\psi(\gamma_1, \gamma_2) \Subset @_\psi(\delta_1, \delta_2)$, a fortiori $@_\psi(\gamma_1, \gamma_2) \preceq_{\mathcal{T}} @_\psi(\delta_1, \delta_2)$, hence Axiom IV-bis is satisfied. We now prove that Axiom V is satisfied. Let $\mathcal{W} \subseteq \mathcal{V}$, let $\mathcal{W}_\vdash = \{\beta \in \mathcal{T} \,|\, \exists(\gamma_1, \gamma_2) \in \mathcal{W}, (\gamma_1, \gamma_2) \vdash \beta\}$. Assuming $\preceq_{\mathcal{T}}$ is an AFR on $\mathcal{W}_\vdash$, we prove that $\preceq_{\mathcal{V}}$ is an AFR on $\mathcal{W}$. By (A), $\Subset$ is an AFR on $\mathcal{W}_\vdash$. Let $\mathcal{B} = \{*_{\overline{a}}(\beta_1, \ldots, \beta_n) | \forall i \in [1, \ldots, n], \beta_i \in \mathcal{W}_\vdash\}$. By lemma 5.8, the relation $\Subset$ is an AFR on $\mathcal{B}$. Moreover $\mathcal{W} \subseteq \mathcal{B} \times \mathcal{B}$. By lemma 5.2, $\preceq_{\mathcal{V}}$ is an AFR on $\mathcal{B} \times \mathcal{B}$, therefore an AFR on $\mathcal{W}$ □

Lemma 5.12. For each formula ϕ, the set of all compact ϕ-shadows is a finite set effectively computable from ϕ.

Proof. For each compact ϕ-shadow Ξ and for each address a such that a is a leaf in Ξ, call *step-continuation at a* of Ξ every compact ϕ-shadow Ξ' such that $\mathrm{dom}(\Xi') \subseteq \mathrm{dom}(\Xi) \cup \{a \cdot (1), a \cdot (2)\}$ and Ξ, Ξ' take the same value on $\mathrm{dom}(\Xi)$. Let $\rightsquigarrow$ be the relation defined by $\Xi \rightsquigarrow \Xi'$ if and only if Ξ' is a step continuation of Ξ. By proposition 3.4 and the fact that the set of subformulas is a finite set, for all Ξ, the set of all Ξ' such that $\Xi \rightsquigarrow \Xi'$, is a finite set, effectively computable from Ξ. Moreover the set $\mathcal{C}$ of all compact ϕ-shadows is clearly equal to the closure under $\rightsquigarrow$ of $\{(\varepsilon \mapsto (\emptyset_{\mathbb{B}}, \phi))\}$, hence it suffices to prove that $\mathcal{C}$ is a finite set. Assume by way of contradiction that $\mathcal{C}$ is infinite. Then there exists an infinite sequence $\Xi_1 \rightsquigarrow \Xi_2 \rightsquigarrow \ldots$ over $\mathcal{C}$. By König's lemma, $\Xi_\infty = \cup_{i>0} \Xi_i$ contains an infinite path $a_1, a_2, \ldots$. Now, each $\Xi_\infty(a_k)$ belongs to $\mathbb{B}(S_\phi) \times \mathcal{F}_\phi$ where $\mathcal{F}_\phi$ is the set of all subformulas of ϕ and S_ϕ is the union of $\mathcal{F}_\phi$ and the set of all binary elements of $\mathfrak{S}$ tagged with elements of $\mathcal{F}_\phi$. Since each Ξ_i is compact, there is no i, j, ψ such that $i < j$, $\Xi_\infty(a_i) = (\gamma_i, \psi)$, $\Xi_\infty(a_j) = (\gamma_j, \psi)$ and $\gamma_i \Subset \gamma_j$. A contradiction follows immediately from lemmas 5.2 and 5.11. □

Remarks. The proof of lemma 5.10 being non-constructive, lemma 5.12 gives no information about the complexity of our proof-search method.

6. From the shadows to the light

Theorem 6.1. Ticket entailment is decidable.

Proof. By lemmas 4.5 and 5.12. □

Acknowledgments

This work could not have been achieved without countless helpful comments and invaluable support from Paweł Urzyczyn, Paul-André Melliès and Pierre-Louis Curien.

References

Handbook of Mathematical Logic (1977). Edited by Barwise, J., Studies in Logic and Foundations of Mathematics, North-Holland.

Anderson, A. R., and Belnap Jr, N. D. (1975) *Entailment: The Logic of Relevance and Necessity, Vol. 1.* Princeton University Press.

Ackermann, W. (1956) Begrundung einer strengen Implikation. *J. Symb. Log.* **21** (2), 113–128.

Anderson, A. R. (1960) Entailment shorn of modality. *J. Symb. Log.* **25** (4), 388.

Anderson, A. R., Belnap Jr, N. D., and Dunn, J. M. (1990) *Entailment: The Logic of Relevance and Necessity, Vol. 2.* Princeton University Press.

Bimbó, K. (2005) Types of I-free hereditary right maximal terms. *Journal of Philosophical Logic* **34** (5–6), 607–620.

Broda, S., Damas, L., Finger, M., and Silva e Silva, P. S. (2004) The decidability of a fragment of $BB'IW$-logic. *Theor. Comput. Sci.* **318** (3), 373–408.

Trigg, P., Hindley, J. R., and Bunder, M. W. (1994) Combinatory abstraction using B, B' and friends. *Theor. Comput. Sci.* **135** (2), 405–422.

Melliès, P.-A. (1998) On a duality between Kruskal and Dershowitz theorems. In: Larsen, K. G, Skyum, S., Winskel, G. (Eds.), ICALP, *Lecture Notes in Computer Science* **1443**, 518–529, Springer-Verlag.

Higman, G. (1952) Ordering by divisibility in abstract algebra. *Proc. London Math. Soc.* **3** (2), 326–336.

Kruskal, J. B. (1972) The theory of well-quasi-ordering: A frequently discovered concept. *J. Comb. Theory, Ser. A* **13** (3), 297–305.

Routley, R., and Meyer, R. K. (1972) Semantics of entailment — III. *Journal of Philosophical Logic* **1**, 192–208.

Bezem, M., Klop, J.,W., de Vrijer, R., ("Terese") (2003) Term Rewriting Systems. *Cambridge Tracts in Theoretical Computer Science* **55**, Cambridge University Press.

Urquhart, A (1984) The undecidability of entailment and relevant implication. *J. Symb. Log.* **49** (4), 1059–1073.