



HAL
open science

Ticket Entailment is decidable

Vincent Padovani

► **To cite this version:**

| Vincent Padovani. Ticket Entailment is decidable. 2010. hal-00599342v4

HAL Id: hal-00599342

<https://hal.science/hal-00599342v4>

Preprint submitted on 19 Dec 2011 (v4), last revised 5 Jul 2012 (v6)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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 19 June 2010. Accepted 19 December 2011. Under revision.

We answer positively a question raised by Anderson and Belnap, by proving that the logic T_{\rightarrow} 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_{\rightarrow} of *Ticket Entailment* is the implicational fragment of entailment based on modus ponens and the four following axiom schemes:

- $I : \phi \rightarrow \phi$
- $B : (\chi \rightarrow \psi) \rightarrow ((\phi \rightarrow \chi) \rightarrow (\phi \rightarrow \psi))$
- $B' : (\phi \rightarrow \chi) \rightarrow ((\chi \rightarrow \psi) \rightarrow (\phi \rightarrow \psi))$
- $W : (\phi \rightarrow (\phi \rightarrow \chi)) \rightarrow (\phi \rightarrow \chi)$

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_{\rightarrow} (the problem of deciding whether a given formula is derivable from the axioms of T_{\rightarrow} 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).

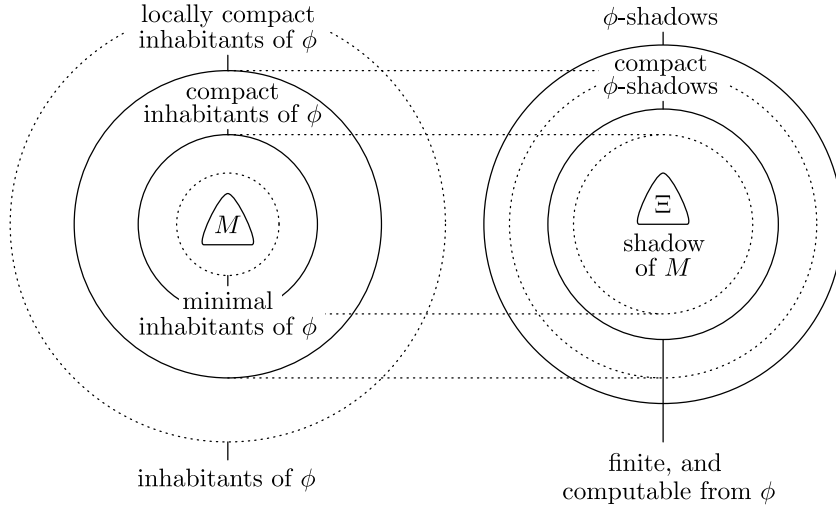


Fig. 1. Principle of the proof of decidability of type inhabitation for well-labelled terms.

We prove in this paper that T_{\rightarrow} is decidable. The proof appeals to a translation of the problem into a type inhabitation problem for *well-labelled terms*, a restricted class of terms of lambda-calculus (similar to the HMR-terms introduced in (Trigg *et al.* 1994)).

In Section 1, the problem of determining whether a formula ϕ is provable is shown to be equivalent to the question of determining the existence of an *inhabitant of ϕ* , that is, a simply-typed well-labelled term (in normal form) of type ϕ – this approach is not new (Bunder 1996; Broda *et al.* 2004).

The principle of the remainder of the proof is depicted on Figure 1. In Sections 2 and 3 we provide for each formula ϕ a partial characterisation of the inhabitants of ϕ in normal form and of minimal size. We show that all those terms belong to two larger sets of terms, the set of *compact* and *locally compact* inhabitants of ϕ .

In Section 4 we show how to associate, with each locally compact inhabitant M of a formula ϕ , a labelled tree called the *shadow* of M . This labelled tree is of same tree structure as M , allowing one to reconstruct M from its shadow only. We define for shadows the analogue of compactness for terms and show that the shadow of a compact term is itself compact.

Finally, in Section 5, we prove that for each formula ϕ the (empty, if ϕ is not provable) set of all compact shadows of inhabitants of ϕ is a finite set (hence the set of compact inhabitants of ϕ is also a finite set), effectively computable from ϕ . The proof appeals to Higman’s Theorem and Kruskal Theorem – more precisely, to Melliès’ Axiomatic Kruskal Theorem. The decidability of T_{\rightarrow} follows from this last key-result.

Preliminaries

The first section of this paper assumes a familiarity with pure and simply-typed lambda-calculus, and with the usual notions of α -conversion, β -reduction and β -normal form

(Barendregt 1984; Krivine 1993). The last three notions are not essential to our discussion, as we later focus exclusively on a particular set of simply-typed terms in β -normal form. Let us briefly recall the definitions and results used in Section 1.

The set of *terms of pure lambda-calculus* (λ -terms) is inductively defined by:

- every variable x is a λ -term,
- if M is a λ -term and x is a variable, then $(\lambda x M)$ is a λ -term,
- if M, N are λ -terms, then (MN) is a λ -term.

The second and third forms are called *abstractions* and *applications* respectively. The parentheses surrounding applications and abstractions are often omitted when unambiguous. We let $\lambda x_1 \dots x_n. MN_1 \dots N_p$ abbreviate $(\lambda x_1 (\dots (\lambda x_n (((MN_1) \dots) N_p)) \dots))$. For instance, $\lambda xy. x(xy)z$ stands for $(\lambda x (\lambda y ((x(xy))z)))$.

The *bound variables* of a term M are all x such that λx occurs in M . A variable x is *free* in a term M if and only:

- $M = x$,
- or $M = \lambda y. N$, $y \neq x$ and x is free in N ,
- or $M = NP$ and x is free in N or free in P .

A *closed* term is a term with no free variables. The *raw substitution of N for x in M* , written $M\langle x \leftarrow N \rangle$, is the term obtained by substituting N for every free occurrence of x in M (every occurrence of x that is not in the scope of a λx). We require that this substitution avoids variable capture (if a variable y is free in N , no free occurrence of x in M is allowed to be in the scope of a λy):

- if $y = x$, then $y\langle x \leftarrow N \rangle$ is equal to N , otherwise it is equal to y ,
- $(\lambda x. M)\langle x \leftarrow N \rangle = \lambda x. M$,
- if $y \neq x$ and y is free in N , then $(\lambda y. M)\langle x \leftarrow N \rangle$ is undefined,
- if $y \neq x$, y is not free in N and $M\langle x \leftarrow N \rangle = M'$, then $(\lambda y. M)\langle x \leftarrow N \rangle = \lambda y. M'$,
- if $M_1\langle x \leftarrow N \rangle = M'_1$ and $M_2\langle x \leftarrow N \rangle = M'_2$, then $(M_1 M_2)\langle x \leftarrow N \rangle = (M'_1 M'_2)$.

The α -*conversion* is the process of renaming bound variables in a term – again, avoiding variable capture. It is defined as the least binary relation \equiv_α such that:

- $x \equiv_\alpha x$,
- if $M \equiv_\alpha M'$, y is not free in M' and $M'\langle x \leftarrow y \rangle = M''$, then $(\lambda x. M) \equiv_\alpha (\lambda y. M'')$
- if $M_1 \equiv_\alpha M'_1$ and $M_2 \equiv_\alpha M'_2$, then $(M_1 M_2) \equiv_\alpha (M'_1 M'_2)$.

For instance $\lambda x. y \equiv_\alpha \lambda z. y \not\equiv_\alpha \lambda y. y$. A common practice (which we will *not* follow in our exposition) is to consider λ -terms up to α -conversion. The β -*reduction* is the least binary relation β satisfying:

- if $M \equiv_\alpha (\lambda x. N)P$ and $N\langle x \leftarrow P \rangle = N'$, then $M\beta N'$.
- if $M\beta M'$, then $(\lambda x. M)\beta(\lambda x. M')$, $(MN)\beta(M'N)$ and $(NM)\beta(NM')$.

In the first rule, x is not necessarily free in N , so we may have $N = N'$ – in particular, free variables may disappear in the process of reduction.

We write β^* for the reflexive and transitive closure of β . A term M is *in β -normal form* – or β -*normal* – if there is no M' such that $M\beta M'$. A term M is *normalising* if there is a normal N – called *normal form of M* – such that $M\beta^* N$. It is *strongly normalising* if there is no infinite sequence $M = M_0\beta M_1\beta M_2 \dots$

It is well-known that β -conversion enjoys the *Church-Rosser property*, that is, if $M\beta^*N$ and $M\beta^*N'$, then there exists two α -convertible P, P' such that $N\beta^*P$ and $N'\beta^*P'$. In consequence, if a term is normalising, then its normal form is unique up to α -conversion.

The judgment “assuming x_1, \dots, x_n are of types ψ_1, \dots, ψ_n , the term M is of type ϕ ”, written $\{x_1 : \psi_1, \dots, x_n : \psi_n\} \vdash M : \phi$, where $\psi_1, \dots, \psi_n, \phi$ are formulas of propositional calculus and x_1, \dots, x_n are distinct variables, is defined by:

- $\Gamma \vdash x : \psi$ for each $x : \psi \in \Gamma$,
- if $\Gamma \cup \{x : \phi\} \vdash M : \psi$, then $\Gamma \vdash \lambda x.M : \phi \rightarrow \psi$.
- if $\Gamma \vdash M : \phi \rightarrow \psi$ and $\Gamma \vdash N : \phi$, then $\Gamma \vdash (MN) : \psi$

The *simply-typable terms* are all M for which there exist Γ, ϕ such that $\Gamma \vdash M : \phi$. Note that Γ must contain all variables free in M , and may contain only those variables. The following properties are well-known:

- 1 (Strong normalisation) If $\Gamma \vdash M : \phi$, then M is strongly normalising.
- 2 (Subject reduction) If $\Gamma \vdash M : \phi$ and $M\beta N$, then $\Gamma \vdash N : \phi$.

1. From Ticket Entailment to simply-typed lambda-calculus

The axioms of T_{\rightarrow} are natural types for $\lambda f g x.f(gx)$, $\lambda f g x.g(fx)$, $\lambda x.x$, $\lambda h x.hxx$ (or for their respective counterparts in combinatory logic). To each theorem ϕ of T_{\rightarrow} corresponds a closed term M of type ϕ – an *inhabitant* of ϕ – built with applicative combinations of terms of those four forms. Subject reduction ensures that all reducts of M are also of type ϕ , and the strong normalisation property also ensures the existence of a normal form of M . The aim of this first section is to provide a full characterisation of simply-typable normal terms that are typable with theorems of Ticket Entailment, so as to transform the question of the provability of a formula ϕ in T_{\rightarrow} into a type inhabitation problem.

1.1. Lambda-calculus

Let $x_0, x_1 \dots$ be different variables. We write $x_i < x_j$ when $i < j$. Throughout the paper, by *term* we always mean a term of lambda-calculus built over those variables. For each term M , we write $\text{Free}(M)$ for the strictly increasing sequence of all variables free in M .

Terms are *not* identified modulo α -conversion – apart from Section 1, all terms will be in normal form. The Greek letters α, β will be used with new meaning at the beginning of Section 2. We adopt however the usual convention according to which two distinct λ 's may not bound the same variable in a term, and no variable can be simultaneously free and bound in the same term.

1.2. Well-labelled terms and simply-typed terms

Definition 1.1. The set of *well-labelled terms* is inductively defined by:

- 1 Each x_i is a well-labelled term.
- 2 If M is well-labelled and x is the greatest free variable of M then $\lambda x.M$ is well-labelled.
- 3 If M, N are well-labelled, and for every free variable x in M , there exists a free variable y in N such that $x \leq y$, then (MN) is well-labelled.

Well-labelled terms are similar to the HRM-terms introduced in (Trigg *et al.* 1994) with the aim of characterizing the translations in λ -calculus of terms of combinatory logic built over various partial bases of atomic combinators.

The second rule ensures that all well-labelled terms are λ_I -terms, that is, terms in which every subterm $\lambda x.M$ is such that x is free in M . The set of free variables of a well-labelled term is thus preserved under β -reduction. As we shall see in the proof of Lemma 1.5, the preservation of well-labelledness is also allowed, at the cost of appropriate bound variable renamings.

In the third rule, if N is closed then so is M . When M and N are non-closed terms, the greatest free variable of M is less than or equal to the greatest free variable of N . For instance, if $f < g < x$ and $h < x$, then $\lambda f g x.f(gx)$, $\lambda f g x.g(fx)$, $\lambda x.x$, $\lambda h x.hxx$ are well-labelled, whereas $\lambda y z.zy$ is not, no matter if $y < z$ or $y > z$.

Definition 1.2. Let $(x_i)_{i \in \mathbb{N}}$ be the strictly increasing sequence of all variables. Let $(\omega_i)_{i \in \mathbb{N}}$ be a sequence of formulas in which every formula occurs an infinite number of times. For each strictly increasing $X = (x_{i_1}, \dots, x_{i_n})$ we let $\Omega(X) = (\omega_{i_1}, \dots, \omega_{i_n})$.

Definition 1.3. The judgment $M : \phi$ (in words, M is of type ϕ w.r.t Ω) is defined by:

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

The function Ω will remain fixed throughout the paper: to each variable x corresponds a unique type. In consequence each typed term M has a unique type, which we call *the* type of M without any further reference to the choice of Ω . Note that every typed term is also well-labelled.

Definition 1.4. We write **NF** for the set of all typed terms in β -normal form. We call *NF-inhabitant of ϕ* every closed term $M \in \mathbf{NF}$ of type ϕ .

1.3. Preservation of well-labelledness under reduction and subformula property

Lemma 1.5. Suppose M is closed and $M : \phi$. Then ϕ is **NF**-inhabited.

Proof. (1) We leave to the reader the proof of this simple fact: for every variable y , and for every $N : \phi$, there exists $N' \equiv_\alpha N$ such that $N' : \phi$ and every variable bound in N' is strictly greater than y .

(2) We prove the following proposition by induction on P . Let P, Q be well-labelled typed terms. Suppose:

- x and Q are of the same type,
- $\text{Free}(P) = (z_1, \dots, z_k, x, z_{k+1}, \dots, z_{k+q})$,
- $\text{Free}(Q) = (y_1, \dots, y_p)$,
- if $k > 0$ and $p > 0$, then $z_k \leq y_p$,
- if $p > 0$ and $q > 0$, then $y_p < z_{k+1}$,
- if $p > 0$, then for all bound variable z of P we have $y_p < z$.

Then $P\langle x \leftarrow Q \rangle$ is defined, well-labelled and of the same type as P . The proposition is clear if $P = x$.

If $P = \lambda z.P'$, then $\text{Free}(P') = (z_1, \dots, z_k, x, z_{k+1}, \dots, z_{k+q}, z)$. If $p > 0$ and $q = 0$, then $y_p < z$. By induction hypothesis $R' = P'\langle x \leftarrow Q \rangle$ is defined, well-labelled and of the same type as P' . The variable z is still the greatest free variable of R' , and z is not free in Q . Hence $R = \lambda z.R'$.

Suppose $P = (P_1 P_2)$. For each $i \in \{1, 2\}$ we have: either x is not free in P_i and $R_i = P_i\langle x \leftarrow Q \rangle = P_i$, or by induction hypothesis $R_i = P_i\langle x \leftarrow Q \rangle$ is defined, well-labelled and of the same type as P_i . If $p = 0$ then $\text{Free}(P_1) = \text{Free}(R_1)$, $\text{Free}(P_2) = \text{Free}(R_2)$. If $p > 0$ then the greatest free variable of R_1 is less than or equal to y_p and the greatest free variable of R_2 is greater than or equal to y_p . In either case $(R_1 R_2)$ is well-labelled.

(3) Assume $N : \phi$ and N is not in normal form. We prove by induction on N the existence of $N' : \phi$ such that $N\beta N'$. If $N = \lambda x.P$, or if $N = (N_1 N_2)$ with N_1 or N_2 not in normal form, then the existence of N' follows from the induction hypothesis and the fact that β -reduction preserves the set of free variables of a well-labelled term. Otherwise $N = (\lambda x.P)Q$ where x is the greatest free variable of P . By (1) there exists $P_0 \equiv_\alpha P$ such that $P_0 : \phi$ and no bound variable of P' is less than or equal to a free variable of Q . The variable x is the greatest free variable of P' . By (2), the term $R = P_0\langle x \leftarrow Q \rangle$ is well-defined, well-labelled and of the type ϕ . Moreover $N\beta N'$.

(3) We prove the lemma. The term M is a simply-typable well-labelled term. The strong normalisation property implies the existence of a normal form N of M . The term N is still a closed term. By (1), there exists $N' \equiv_\alpha N$ such that $N' : \phi$, that is, ϕ is NF-inhabited, \square

Lemma 1.6. Let M be an NF-inhabitant of ϕ . The types of the subterms of M are subformulas of ϕ .

Proof. This lemma is the well-known subformula property of simply-typed lambda-calculus. An immediate induction on N shows that for every normal $N : \phi$ (not necessarily closed), the type of each subterm of N (including free and bound variables) is a subformula of ϕ or a subformula of a free variable of N . \square

1.4. Equivalence between provability in T_\rightarrow and NF-inhabitation

In the next lemmas by $\phi_1 \dots \phi_n \rightarrow \psi$ we mean the formula $(\phi_1 \rightarrow (\dots (\phi_n \rightarrow \psi) \dots))$ if $n > 0$, the formula ψ if $n = 0$. We write $\vdash_T \phi$ for the judgment “ ϕ is provable in T_\rightarrow ”.

Lemma 1.7. If $\vdash_T \phi$, then ϕ is NF-inhabited.

Proof. If $f < g < x$ and $h < x$, then $\lambda x.x$, $\lambda f g x.f(gx)$, $\lambda f g x.g(fx)$ and $\lambda h x.hxx$ 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 . The set of all formulas ϕ for which there exists a closed M of type ϕ is clearly closed under modus ponens. By Lemma 1.5, every such formula is NF-inhabited. \square

Lemma 1.8. If $\vdash_T \chi \rightarrow \psi$, then $\vdash_T (\phi_1 \dots \phi_n \rightarrow \chi) \rightarrow (\phi_1 \dots \phi_n \rightarrow \psi)$ for all ϕ_1, \dots, ϕ_n .

Proof. By induction on n , using B -axioms. \square

Lemma 1.9. Suppose $(i_1, \dots, i_n), (j_1, \dots, j_m), (k_1, \dots, k_p)$ are strictly increasing sequences of integers, $\{k_1, \dots, k_p\} = \{i_1, \dots, i_n, j_1, \dots, j_m\}$, $n = 0$ or $(n > 0, m > 0, i_n \leq j_m)$. If

- 1 $\vdash_T \omega_{i_1} \dots \omega_{i_n} \rightarrow (\chi \rightarrow \psi)$,
- 2 $\vdash_T \omega_{j_1} \dots \omega_{j_m} \rightarrow \chi$,

then $\vdash_T \omega_{k_1} \dots \omega_{k_p} \rightarrow \psi$.

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

Suppose $n = 0$. Then $(j_1, \dots, j_m) = (k_1, \dots, k_p)$. We have:

- (i) $\vdash_T (\chi \rightarrow \psi) \rightarrow ((\omega_{j_m} \rightarrow \chi) \rightarrow (\omega_{j_m} \rightarrow \psi))$
- (ii) $\vdash_T (\omega_{j_m} \rightarrow \chi) \rightarrow (\omega_{j_m} \rightarrow \psi)$

where: (i) is a B -axiom; (ii) follows from (i), (1) and modus ponens. If $m = 1$ then $\vdash_T \omega_{j_1} \rightarrow \psi$ follows from (ii), (2) and modus ponens. Otherwise $\vdash_T \omega_{j_1} \dots \omega_{j_m} \rightarrow \psi$ follows from (ii), (2) and the induction hypothesis.

We now assume $n > 0$. Suppose $m > 1$ and $i_n \leq j_{m-1}$. Then

- (iii) $\vdash_T (\chi \rightarrow \psi) \rightarrow ((\omega_{j_m} \rightarrow \chi) \rightarrow (\omega_{j_m} \rightarrow \psi))$
- (iv) $\vdash_T (\omega_{i_1} \dots \omega_{i_n} \rightarrow (\chi \rightarrow \psi)) \rightarrow (\omega_{i_1} \dots \omega_{i_n} \rightarrow ((\omega_{j_m} \rightarrow \chi) \rightarrow (\omega_{j_m} \rightarrow \psi)))$
- (v) $\vdash_T \omega_{i_1} \dots \omega_{i_n} \rightarrow ((\omega_{j_m} \rightarrow \chi) \rightarrow (\omega_{j_m} \rightarrow \psi))$

where: (iii) is a B -axiom; (iv) follows from (iii) and Lemma 1.8; (v) follows from (iv), (1) and modus ponens. We have $k_p = j_m$ and $\{k_1, \dots, k_{p-1}\} = \{i_1, \dots, i_n, j_1, \dots, j_{m-1}\}$. Since $i_n \leq j_{m-1}$, we have $\vdash_T \omega_{k_1} \dots \omega_{k_{p-1}} \rightarrow (\omega_{j_m} \rightarrow \psi)$ by (v), (2) and the induction hypothesis.

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

- (vi) $\vdash_T (\omega_{j_m} \rightarrow \chi) \rightarrow ((\chi \rightarrow \psi) \rightarrow (\omega_{j_m} \rightarrow \psi))$
- (vii) $\vdash_T (\omega_{j_1} \dots \omega_{j_m} \rightarrow \chi) \rightarrow (\omega_{j_1} \dots \omega_{j_{m-1}} \rightarrow ((\chi \rightarrow \psi) \rightarrow (\omega_{j_m} \rightarrow \psi)))$
- (viii) $\vdash_T \omega_{j_1} \dots \omega_{j_{m-1}} \rightarrow ((\chi \rightarrow \psi) \rightarrow (\omega_{j_m} \rightarrow \psi))$
- (ix) $\vdash_T \omega_{n_1} \dots \omega_{n_q} \rightarrow (\omega_{j_m} \rightarrow \psi)$

where: (vi) is a B' -axiom; (vii) follows from (vi) and Lemma 1.8; (viii) follows from (vii), (2) and modus ponens; $\{n_1, \dots, n_q\} = \{j_1, \dots, j_{m-1}, i_1, \dots, i_n\}$; (ix) follows from (viii), (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

- (x) $\vdash_T \omega_{k_1} \dots \omega_{k_{p-1}} \rightarrow (\omega_{i_n} \rightarrow (\omega_{i_n} \rightarrow \psi))$
- (xi) $\vdash_T (\omega_{i_n} \rightarrow (\omega_{i_n} \rightarrow \psi)) \rightarrow (\omega_{i_n} \rightarrow \psi)$
- (xii) $\vdash_T (\omega_{k_1} \dots \omega_{k_{p-1}} \rightarrow (\omega_{i_n} \rightarrow (\omega_{i_n} \rightarrow \psi))) \rightarrow (\omega_{k_1} \dots \omega_{k_{p-1}} \rightarrow (\omega_{i_n} \rightarrow \psi))$
- (xiii) $\vdash_T \omega_{k_1} \dots \omega_{k_{p-1}} \rightarrow (\omega_{i_n} \rightarrow \psi)$

where: (x) is (ix); (xi) is a W -axiom; (xii) follows from (xi) and Lemma 1.8; (xiii) follows from (x), (xii) and modus ponens; (xiii) is $\vdash_T \omega_{k_1} \dots \omega_{k_p} \rightarrow \psi$. \square

Lemma 1.10. For every formula ϕ , we have $\vdash_T \phi$ if and only if ϕ is NF-inhabited.

Proof. The left to right implication is Lemma 1.7. An immediate induction on M shows that $M : \psi$, $\text{Free}(M) = (x_1, \dots, x_n)$ and $x_1 : \chi_1, \dots, x_n : \chi_n$ implies $\vdash_T \chi_1 \dots \chi_n \rightarrow \psi$, using Lemma 1.9 when M is an application. \square

2. Stable parts and blueprints

The last lemma showed that the decidability of Ticket Entailment is equivalent to the decidability of NF-inhabitation. The remainder of the paper is devoted to the elaboration of a decision algorithm for this latter problem.

The question we shall examine throughout Sections 2 and 3 is the following: if an inhabitant is not of minimal size, is there any way to transform it (with the help of grafts and/or another compression of some sort) into a smaller inhabitant of same type? This question is difficult, because we are dealing with a lambda-calculus restricted with strong structural constraints (well-labelledness). There are however simple situations in which an inhabitant is obviously not minimal.

Consider an NF-inhabitant M and two subterms N, P of M such that P is a strict subterm of N . Suppose:

- N, P are applications of the same type or abstractions of the same type.
- $\text{Free}(N) = X = (x_1, \dots, x_n)$,
- $\text{Free}(P) = Y = (y_0^1, \dots, y_{p_1}^1, \dots, y_0^n, \dots, y_{p_n}^n)$
- $\Omega(X) = (\chi_1, \dots, \chi_n)$,
- $\Omega(Y) = (\chi_0^1, \dots, \chi_{p_1}^1, \dots, \chi_0^n, \dots, \chi_{p_n}^n)$,
- $\chi_j^i = \chi_i$ for each i, j ,

Then M is not an inhabitant of minimal size. Indeed, we may rename the free variables of P (letting $\rho(y_j^i) = x_i$) as to obtain a term P' of same size as P , of the same type and same free variables as N . If we replace N with P in M , the resulting term is a strictly smaller inhabitant.

This simple property is far from being enough to characterise the minimal inhabitants of a formula: there are indeed formulas with inhabitants of arbitrary size in which this situation never occurs. We obviously need a more flexible way to reduce the size of non-minimal inhabitants. In particular, we need a better understanding of our available freedom of action if we are to rename the free variables of a term – possibly occurrence by occurrence – and if we want to ensure that well-labelledness is preserved. This section is devoted to the proof of two key-lemmas that delimit this freedom.

- In Sections 2.1, 2.2 and 2.2 we show how to build from any term $M \in \text{NF}$ a partial tree labelled with formulas. This partial tree is called the *blueprint* of M . It can be seen as a synthesized version of M that contains all and only the information required to determine whether a (non-uniform) renaming of the free variables of M will preserve well-labelledness.
- In Sections 2.4 and 2.5 we introduce a rewriting relation on blueprints that allows one to “extract” sequences of formulas from a blueprint.
- In section 2.6 we prove our two key-lemmas. Lemma 2.15 clarifies the link between the blueprints of M and $\lambda x.M$ (provided both are in NF). It implies that the sequence

of the types of the free variables of M (that is, $\Omega(\text{Free}(M))$) can always be extracted from its blueprint. Lemma 2.17 shows that for *every* sequence of formulas $\bar{\phi}$ than can be extracted from the blueprint of M , there exists a (non-uniform) renaming of the free variables of M that will produce a term N of the same type and with the same blueprint as M , and such that $\Omega(\text{Free}(N)) = \bar{\phi}$.

As a continuation of our first example, let us examine the consequences of this last result. Consider again M, N, P as above, and suppose:

— the sequence $\Omega(\text{Free}(N))$ can be extracted from the blueprint of P .

This situation is a generalization of the preceding one (in our first example $\Omega(X)$ could also be extracted from the blueprint of P , see Definition 2.10). The term M is still not of minimal size. Indeed, we may use the second key-lemma to prove the existence of (non-uniform) renaming of the free variables of P that will produce a term P' of same type as P such that $\text{Free}(P') = \text{Free}(N)$. The term N can be replaced with P' in M .

2.1. Partial trees and trees

Definition 2.1. Let (\mathbb{A}, \leq) be the set of all finite sequences over the set \mathbb{N}_+ of non-null integers, ordered by prefix ordering. Elements of \mathbb{A} are called *addresses*. We call *partial tree* every function π whose domain is a set of addresses. For each partial tree π and for each address a , we let $\pi|_a$ denote the partial tree $c \mapsto \pi(a \cdot c)$ of domain $\{c \mid a \cdot c \in \text{dom}(\pi)\}$.

Definition 2.2. For all partial trees π, π' and for every address a , we let $\pi[a \leftarrow \pi']$ denote the partial tree π'' such that $\pi''|_a = \pi'$ and $\pi''(b) = \pi(b)$ for all $b \in \text{dom}(\pi)$ such that $a \not\leq b$.

Definition 2.3. A *tree domain* is a set $A \subseteq \mathbb{A}$ such that for all $a \in A$: every prefix of a is in A ; for every integer $i > 0$, if $a \cdot (i) \in A$, then $a \cdot (j) \in A$ for each $j \in \{1, \dots, i-1\}$. A tree domain A is *finitely branching* if and only if for each $a \in A$, there exists an $i > 0$ such that $a \cdot (i)$ is undefined. We call *tree* every function whose domain is a tree domain.

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 and such that $\tau|_{(1)}$ is the tree of M ; $(M_1 M_2)$ with the tree τ mapping ε to $@$ and such that $\tau|_{(i)}$ is the tree of M_i for each $i \in \{1, 2\}$.

2.2. Blueprints

Definition 2.4. Let \mathfrak{S} be the signature consisting of all formulas and all symbols of the form $@_\phi$ where ϕ is a formula. Each formula is considered as a symbol of null arity. Each $@_\phi$ is of arity 2.

We call *blueprint* every finite partial tree $\alpha : A \rightarrow \mathfrak{S}$ 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. A blueprint α is *rooted* if $\varepsilon \in \text{dom}(\alpha)$.

For each $\mathcal{S} \subseteq \mathfrak{S}$, we call *\mathcal{S} -blueprint* every blueprint whose image is a subset of \mathcal{S} . We write $\mathbb{B}(\mathcal{S})$ for the set of all \mathcal{S} -blueprints, $\mathbb{B}_\varepsilon(\mathcal{S})$ for the set of all rooted \mathcal{S} -blueprints.

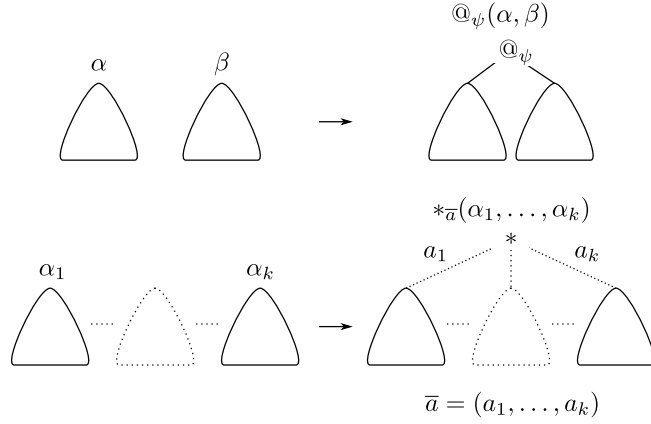


Fig. 2. Construction of blueprints, with the notations of Section 2.2. In the upper diagram, the blueprints α and β must be non-empty. Although $\alpha_1, \dots, \alpha_k$ are displayed from left to right, the sequence (a_1, \dots, a_k) needs not to be lexicographically ordered.

Definition 2.5. For every blueprint α and every address a , the *relative depth* of a in α is the number of $b \in \text{dom}(\alpha)$ such that $b < a$. The *relative depth* of α is defined as 0 if α is of empty domain, the maximal relative depth of an address in α otherwise.

In the remainder the following notations will be used to denote blueprints (see Figure 2):

- $\emptyset_{\mathbb{B}}$ denotes the blueprint of empty domain.
- we abbreviate $\varepsilon \mapsto \phi$ as ϕ .
- $@_\phi(\beta_1, \beta_2)$ denotes the (rooted) blueprint α such that $\alpha(\varepsilon) = \phi$, $\alpha|_{(1)} = \beta_1$, $\alpha|_{(2)} = \beta_2$.
- for every sequence $\bar{a} = (a_1, \dots, a_k)$ of pairwise incomparable addresses, $*_{\bar{a}}(\beta_1, \dots, \beta_k)$ denotes the blueprint α of minimal domain such that $\alpha|_{a_i} = \beta_i$ for each $i \in [1, \dots, k]$.
- we let $*(\beta_1, \dots, \beta_k)$ denote the blueprint $*_{\bar{b}}(\beta_1, \dots, \beta_k)$ such that $\bar{b} = ((1), \dots, (k))$.

For each blueprint α , the choice of $\bar{a}, \beta_1, \dots, \beta_k$ such that $\alpha = *_{\bar{a}}(\beta_1, \dots, \beta_k)$ is obviously not unique. Moreover the sequence of β_i may contain an arbitrary number of empty blueprints, hence the sequence \bar{a} may be of arbitrary length. Also, α can be rooted (if $k = 1$, $a_1 = \varepsilon$ and β_1 is rooted) or empty (if $k = 0$ or $\beta_1 = \dots = \beta_k = \emptyset_{\mathbb{B}}$). This ambiguity is not difficult to deal with, but will require a few precautions in our proofs by induction on blueprints.

2.3. Blueprint of a term

Definition 2.6. For all $M \in \text{NF}$, the *stable part* of M is the set of all $a \in \text{dom}(M)$ such that $\text{Free}(M|_a) \subseteq \text{Free}(M)$ and $M|_a$ is a variable or an application.

It is easy to check that our conventions (no variable is simultaneously free and bound in a term) ensure that the stable part of a term does not depend on the choice of variable names. Since M is in normal form, M is of empty stable part if and only if it is closed.

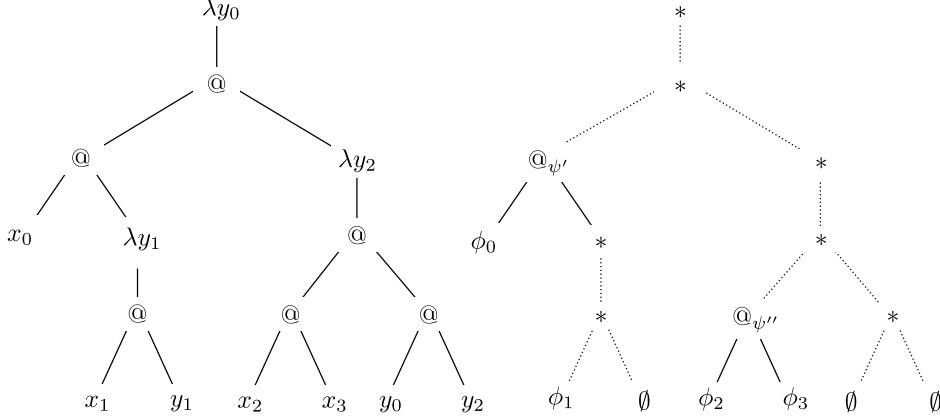


Fig. 3. An element of NF with its blueprint ($x_0 < x_1 < y_1$, $x_2 < x_3 < y_0 < y_2$, $x_1 < y_0 < y_2$).

Definition 2.7. For all $M \in \text{NF}$, 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 let $M \Vdash \alpha$ denote the judgment “ M is of blueprint α ”.

(See Figure 3) If $M = (M_1 M_2) \in \text{NF}$, $M : \phi$, $M_1 \Vdash \alpha_1$, $M_2 \Vdash \alpha_2$, 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. 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 2.15.

Lemma 2.8. For all $M \in \text{NF}$ and for all $a \cdot b \in \text{dom}(M)$:

- 1 If $\text{Free}(M|_{a \cdot b}) \subseteq \text{Free}(M)$ then $\text{Free}(M|_{a \cdot b}) \subseteq \text{Free}(M|_a)$.
- 2 If $M|_a \Vdash \alpha$ and $M|_{a \cdot b} \Vdash \beta$, then $\alpha|_b = \beta$.

Proof. The first proposition is a consequence of our bound variable convention (see Section 1.1): if $\text{Free}(M) = X$, $\text{Free}(M|_a) = X' \cup Y$ where $X' \subseteq X$ and X, Y are disjoint, then every element of $\text{Free}(M|_{a \cdot b})$ in X is also an element of X' . Thus if $a \cdot b$ is in the stable part of M , then b is also in the stable part of $M|_a$. The second proposition is equivalent to the first. \square

2.4. Extraction of the formulas of a blueprint

Definition 2.9. The judgment “ α' is the blueprint obtained by extracting the formula ϕ at the address a in the blueprint α ”, written $\alpha \triangleright_\phi^a \alpha'$, is inductively defined by:

- 1 $\phi \triangleright_\phi^\varepsilon \emptyset_{\mathbb{B}}$,
- 2 if $\alpha_2 \triangleright_\phi^a \alpha'_2$, then $@_\psi(\alpha_1, \alpha_2) \triangleright_\phi^{(2) \cdot a} *(\alpha_1, \alpha'_2)$

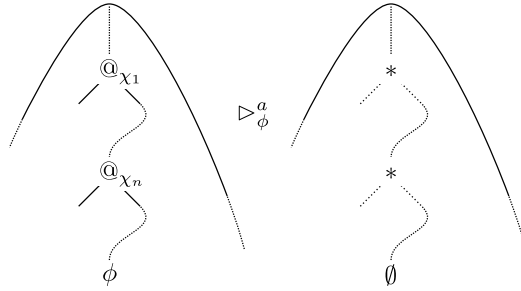


Fig. 4. Principle of blueprint reduction.

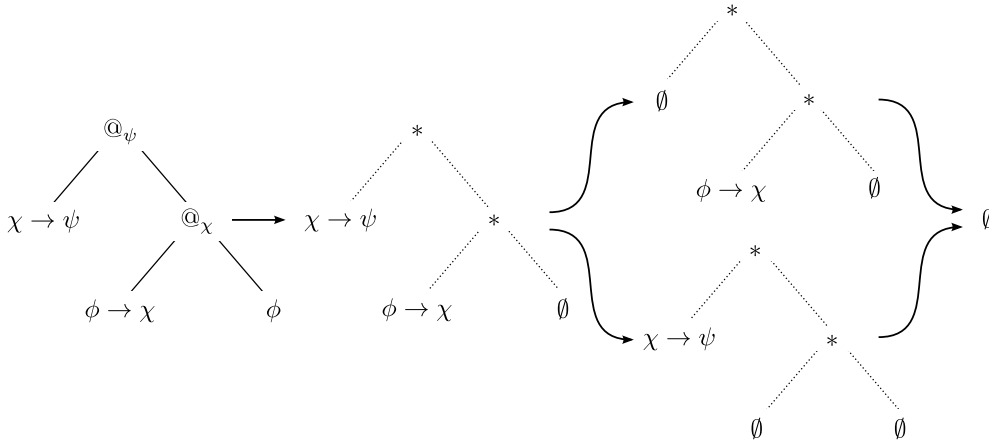


Fig. 5. Full reductions of $@_{\psi}(\chi \rightarrow \psi, @_{\chi}(\phi \rightarrow \chi, \phi))$ to $\emptyset_{\mathbb{B}}$.

3 if $\alpha \triangleright_{\phi}^a \alpha'$, then $*(b, c_1, \dots, c_n)(\alpha, \beta_1, \dots, \beta_n) \triangleright_{\phi}^{b \cdot a} *(b, c_1, \dots, c_n)(\alpha', \beta_1, \dots, \beta_n)$.

In (2) we assume of course that α_1 and α_2 are non-empty. In (3) in order to avoid circularity, we assume $b \neq \varepsilon$.

For instance (Figure 5):

$$\begin{aligned}
 \text{--- } @_{\psi}(\chi \rightarrow \psi, @_{\chi}(\phi \rightarrow \chi, \phi)) & \triangleright_{\phi}^{(2,2)} *(\chi \rightarrow \psi, *(\phi \rightarrow \chi, \emptyset_{\mathbb{B}})) \\
 & \triangleright_{\phi \rightarrow \chi}^{(2,1)} *(\chi \rightarrow \psi, *(\emptyset_{\mathbb{B}}, \emptyset_{\mathbb{B}})) \\
 & \triangleright_{\chi \rightarrow \psi}^{(1)} *(\emptyset_{\mathbb{B}}, *(\emptyset_{\mathbb{B}}, \emptyset_{\mathbb{B}})) = \emptyset_{\mathbb{B}} \\
 \text{--- } @_{\psi}(\chi \rightarrow \psi, @_{\chi}(\phi \rightarrow \chi, \phi)) & \triangleright_{\phi}^{(2,2)} *(\chi \rightarrow \psi, *(\phi \rightarrow \chi, \emptyset_{\mathbb{B}})) \\
 & \triangleright_{\chi \rightarrow \psi}^{(1)} *(\emptyset_{\mathbb{B}}, *(\phi \rightarrow \chi, \emptyset_{\mathbb{B}})) \\
 & \triangleright_{\phi \rightarrow \chi}^{(2,1)} *(\emptyset_{\mathbb{B}}, *(\emptyset_{\mathbb{B}}, \emptyset_{\mathbb{B}})) = \emptyset_{\mathbb{B}}
 \end{aligned}$$

When $\alpha \triangleright_{\phi}^a \alpha'$, 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 must follow the right branch

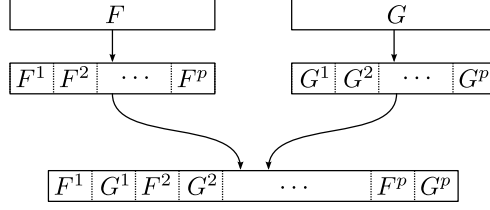


Fig. 6. A Shuffling of two sequences. The chunks of F and G need not to be of the same size – some of them can even be empty. All contractions of the resulting sequence belong to $\otimes(F, G)$. They also belong to $\odot(F, G)$ if F, G are non-empty and the last chunk of G is non empty.

of \odot . The constraints on the construction of blueprints imply the existence of at least one such path in every non-empty blueprint, even if it is not the blueprint of a term.

2.5. Sets of extractible sequences

Definition 2.10. For each formula ϕ , let \triangleright_ϕ be the relation defined by: $\alpha \triangleright_\phi \alpha'$ if and only if there exists a such that $\alpha \triangleright_\phi^a \alpha'$. Let \triangleright_ϕ^+ be the transitive closure of \triangleright_ϕ . For each α , we write $\mathbb{F}(\alpha)$ for the set of all sequences (ϕ_1, \dots, ϕ_n) such that $\alpha \triangleright_{\phi_1}^+ \dots \triangleright_{\phi_n}^+ \emptyset$.

The set $\mathbb{F}(\alpha)$ is what we called “set of extractible sequences of α ” in the introduction of Section 2. Note that $\mathbb{F}(\emptyset_{\mathbb{B}}) = \{\varepsilon\}$. If $\alpha \neq \emptyset_{\mathbb{B}}$, then all elements of $\mathbb{F}(\alpha)$ are non-empty sequences. We now introduce the notion of *shuffle* which will allow us to characterise $\mathbb{F}(\alpha)$ depending on the structure of α .

Definition 2.11. A *contraction* of a sequence F is either the sequence F or a sequence $G \cdot (f) \cdot (f) \cdot H$ where $G \cdot (f) \cdot (f) \cdot H$ is a contraction of F .

Definition 2.12. Given finite sequences F_1, \dots, F_n we call *shuffle* of (F_1, \dots, F_n) every sequence $F_1^1 \cdot \dots \cdot F_n^1 \cdot \dots \cdot F_1^p \cdot \dots \cdot F_n^p$ such that $F_i^1 \cdot \dots \cdot F_i^p = F_i$ for each i . For each tuple of sets of finite sequences $(\mathcal{F}_1, \dots, \mathcal{F}_n)$ we write $\otimes(\mathcal{F}_1, \dots, \mathcal{F}_n)$ for the closure under contraction of the set of shuffles of elements of $\mathcal{F}_1 \times \dots \times \mathcal{F}_n$.

Definition 2.13. Given two non-empty finite sequences F_1, F_2 , we call *right-shuffle* of (F_1, F_2) every sequence $F_1^1 \cdot F_2^1 \cdot \dots \cdot F_1^p \cdot F_2^p$ where $F_i^1 \cdot \dots \cdot F_i^p = F_i$ for each i and $F_2^p \neq \varepsilon$. For each pair of sets of non-empty finite sequences $(\mathcal{F}_1, \mathcal{F}_2)$ we write $\odot(\mathcal{F}_1, \mathcal{F}_2)$ for the closure under contraction of the set of right-shuffles of elements $\mathcal{F}_1 \times \mathcal{F}_2$.

The principle of (right-)shuffling is depicted on figure 6. 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 $\alpha = *_{\bar{\alpha}}(\beta_1, \dots, \beta_k)$, then $\mathbb{F}(\alpha) = \otimes(\mathbb{F}(\beta_1), \dots, \mathbb{F}(\beta_k))$.
- 4 If $\alpha = \odot_\phi(\alpha_1, \alpha_2)$, then $\mathbb{F}(\alpha) = \odot(\mathbb{F}(\alpha_1), \mathbb{F}(\alpha_2))$.

2.6. Abstraction vs. extraction

Recall that for every strictly increasing sequence of variables $X = (x_1, \dots, x_n)$, we write $\Omega(X)$ for the sequence of the types of x_1, \dots, x_n . We now clarify the link between the blueprint α of a term M and the one of $\lambda x.M$ (see Figure 7).

Lemma 2.14. Suppose $\{a_1, \dots, a_p\} = \{b_1, \dots, b_p\}$, and:

- $\alpha \triangleright_{\chi}^{a_1} \dots \triangleright_{\chi}^{a_p} \beta$,
- $\alpha \triangleright_{\chi}^{b_1} \dots \triangleright_{\chi}^{b_p} \beta'$.

Then $\beta = \beta'$.

Proof. By an easy induction on α . □

Lemma 2.15. For all $M \in \text{NF}$ of type ϕ , of blueprint α , the following conditions are equivalent:

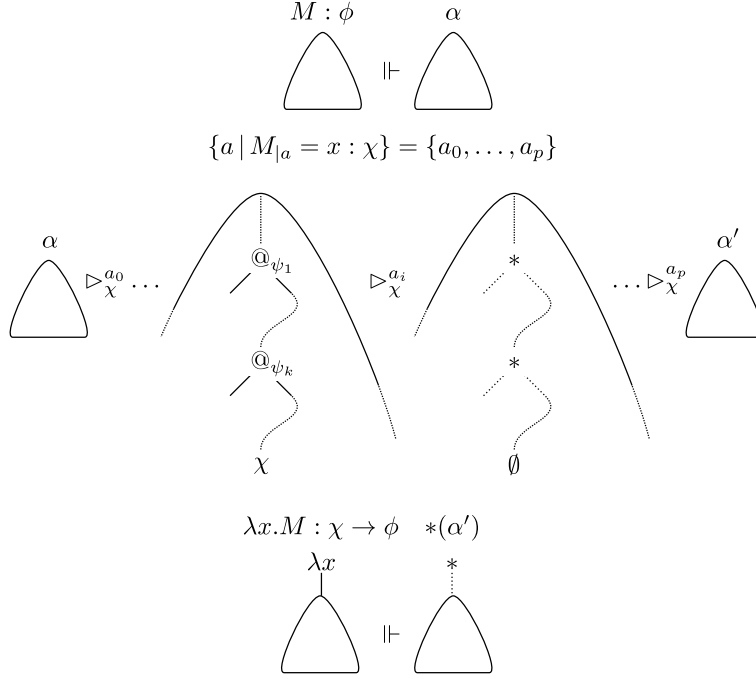
- 1 We have $\lambda x.M : \chi \rightarrow \phi$ and $\lambda x.M \Vdash \beta$.
- 2 The variable x is the greatest free variable of M and there exist α', a_1, \dots, a_p such that:
 - $\{a \mid M|_a = x\} = \{a_0, \dots, a_p\}$,
 - $\alpha \triangleright_{\chi}^{a_0} \dots \triangleright_{\chi}^{a_p} \alpha'$,
 - $\beta = *(\alpha')$.

Proof. (A) For each $N \in \text{NF}$, let ρ_N be the least partial function such that: $\rho_N(\varepsilon, \gamma) = \gamma$ for every blueprint γ ; if $\rho_N(Y, \gamma) = \delta$, $\{b \mid N|_b = y\} = \{b_0, \dots, b_m\}$ and $\delta \triangleright_{\chi}^{b_0} \dots \triangleright_{\chi}^{b_m} \delta'$, then $\rho_M((y) \cdot Y, \gamma) = \delta'$. By Lemma 2.14, if $\{b \mid N|_b = y\} = \{b_0, \dots, b_m\} = \{c_0, \dots, c_m\}$, $\delta \triangleright_{\chi}^{b_0} \dots \triangleright_{\chi}^{b_m} \delta'$ and $\delta \triangleright_{\chi}^{c_0} \dots \triangleright_{\chi}^{c_m} \delta''$, then $\delta' = \delta''$, thus ρ_N is indeed a function. For each finite sequence of variables Z and for each blueprint γ , we let $\mu_N(Z, \gamma)$ be the restriction of γ to $\text{dom}(\gamma) \cap \{b \mid \text{Free}(N|_b) \subseteq Z\}$.

We shall prove by induction on N that if N is of blueprint γ , then for all pairs (Y, Z) such that $\text{Free}(N) = Y \cdot Z$, we have $\mu_N(Y, \gamma) = \rho_N(Z, \gamma)$. The case $Z = \varepsilon$ is immediate so we may as well assume that Z is a non-empty suffix of $\text{Free}(N)$. The case of N equal to a variable follows immediately from our definitions.

Suppose $N = (N_1 N_2)$, $N_1 : \psi_1 N_1 \Vdash \gamma_1$, $\psi_1 = \psi_2 \rightarrow \psi$, $N_2 : \psi_2, N_2 \Vdash \gamma_2$. There exist Y_1, Y_2, Z_1, Z_2 such that: $Y_1 \cup Y_2 = Y$; $Z_1 \cup Z_2 = Z$; $\text{Free}(N_i) = Y_i \cdot Z_i$ for each $i \in \{1, 2\}$. We have $\gamma = @_{\psi}(\gamma_1, \gamma_2)$ and $\mu_N(Y, \gamma) = *(\mu_{N_1}(Y_1, \gamma_1), \mu_{N_2}(Y_2, \gamma_2))$. By induction hypothesis $\mu_{N_i}(Y_i, \gamma_i) = \rho_{N_i}(Z_i, \gamma_i)$ for each i . The sequence Z is non-empty hence the last elements of Z, Z_2 are equal. Assume $Z = Z' \cdot (y)$ and $Z_2 = Z'_2 \cdot (y)$. If y is not the last element of Z_1 then:

$$\begin{aligned}
\rho_N(Z, \gamma) &= \rho_N(Z, @_{\psi}(\gamma_1, \gamma_2)) \\
&= \rho_N(Z_1 \cup Z'_2, *(\gamma_1, \rho_{N_2}((y), \gamma_2))) \\
&= *(\rho_{N_1}(Z_1, \gamma_1), \rho_{N_2}(Z'_2, \rho_{N_2}((y), \gamma_2))) \\
&= *(\rho_{N_1}(Z_1, \gamma_1), \rho_{N_2}(Z'_2 \cdot (y), \gamma_2)) \\
&= *(\rho_{N_1}(Z_1, \gamma_1), \rho_{N_2}(Z_2, \gamma_2))
\end{aligned}$$

Fig. 7. How the blueprint of M evolves into the blueprint of $\lambda x.M$

Otherwise, $Z_1 = Z'_1 \cdot (y)$ and we have:

$$\begin{aligned}
\rho_N(Z, \gamma) &= \rho_N(Z, @_{\psi}(\gamma_1, \gamma_2)) \\
&= \rho_N(Z'_1 \cup Z'_2, *(\rho_{N_1}((y), \gamma_1), \rho_{N_2}((y), \gamma_2))) \\
&= *(\rho_{N_1}(Z'_1, \rho_{N_1}((y), \gamma_1)), \rho_{N_2}(Z'_2, \rho_{N_2}((y), \gamma_2))) \\
&= *(\rho_{N_1}(Z'_1 \cdot (y), \gamma_1), \rho_{N_2}(Z'_2 \cdot (y), \gamma_2)) \\
&= *(\rho_{N_1}(Z_1, \gamma_1), \rho_{N_2}(Z_2, \gamma_2))
\end{aligned}$$

In either case $\rho_M(Z, \gamma) = *(\rho_{M_1}(Z_1, \gamma_1), \rho_{M_2}(Z_2, \gamma_2)) = *(\mu_{M_1}(Z_1, \gamma_1), \mu_{M_2}(Z_2, \gamma_2)) = \mu_M(X, \gamma)$.

Suppose $N = \lambda y.N_1 : \chi \rightarrow \psi_1$, $N_1 \Vdash \gamma_1$. By induction hypothesis $\mu_{N_1}(Y, \gamma_1) = \rho_{M_1}(Z \cdot (y), \gamma_1) = \rho_{N_1}(Z, \rho_{N_1}(y, \gamma_1)) = \rho_{N_1}(Z, \mu(Y \cdot Z, \gamma_1)) = \rho_{N_1}(Z, \gamma_{|(1)})$. Also $\mu_{N_1}(Y, \gamma_1) = \mu_{N_1}(Y, \mu_1(Y \cdot Z, \gamma_1)) = \mu_{N_1}(Y, \gamma_{|(1)})$. Hence $\mu_{N_1}(Y, \gamma_{|(1)}) = \rho_{N_1}(Z, \gamma_{|(1)})$, therefore $\mu_{N_1}(Y, \gamma) = \rho_{M_1}(Z, \gamma)$.

(B) We now prove the lemma. If (1) or (2), then x is the greatest variable of M , that is, $\text{Free}(M)$ is of the form $X \cdot (x)$. The blueprint of $\lambda x.M$ is by definition $*(\mu_M(X, \alpha))$. By (A), $\rho_M((x), \alpha)$ is defined and equal to $\mu_M(X, \alpha)$. Hence there exist c_1, \dots, c_p such that $\{c \mid M|_c = x\} = \{c_1, \dots, c_p\}$, $\alpha \triangleright_{\chi}^{c_1} \dots \triangleright_{\chi}^{c_p} \rho_M((x), \alpha) = \mu_M(X, \alpha)$. If (1) then $\beta = *(\mu_M(X, \alpha)) = *(\rho_M((x), \alpha))$, and we can take $(a_1, \dots, a_p) = (c_1, \dots, c_p)$, $\alpha' = \rho_M((x), \alpha)$. If (2) then by Lemma 2.14, $\alpha' = \rho_M((x), \alpha) = \mu_M(X, \alpha)$, hence $*(\alpha')$ is indeed the blueprint of $\lambda x.M$. \square

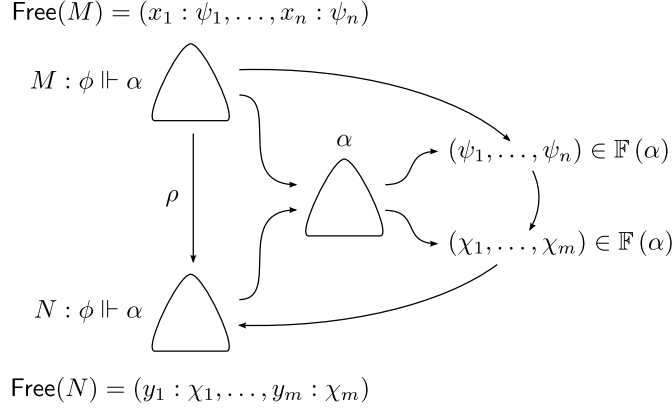


Fig. 8. A non-uniform renaming of the variables of M , based on an alternate extraction of the formulas of its blueprint.

2.7. Blueprints and renamings

Lemma 2.16. For all $M \in \text{NF}$ of blueprint α , we have $\Omega(\text{Free}(M)) \in \mathbb{F}(\alpha)$.

Proof. Let $(x_1, \dots, x_n) = \text{Free}(M)$. Let $(\psi_1, \dots, \psi_n) = \Omega(\text{Free}(M)) \in \mathbb{F}(\alpha)$. For each $i \in [0, \dots, n]$, let α_i be the blueprint of $M_i = \lambda x_{i+1} \dots x_n. M$. By Lemma 2.15 there exists for each $i > 0$ a sequence of addresses $(a_0^i, \dots, a_{p_i}^i)$ such that

$$\alpha_i \triangleright_{\psi_i}^{a_0^i} \dots \triangleright_{\psi_i}^{a_{p_i}^i} \alpha_{i-1|1}$$

For each $i > 0$, the blueprint α_i is of the form $*_{c_i}(\gamma_i)$ where b_i be the sequence $(1, \dots, 1)$ of length $n - i$, hence each a_j^i is of the form $c_i \cdot b_j^i$. Moreover:

$$\gamma_i \triangleright_{\psi_i}^{b_0^i} \dots \triangleright_{\psi_i}^{b_{p_i}^i} \gamma_{i-1}$$

Hence $\alpha = \gamma_n \triangleright_{\psi_n}^{a_0^n} \dots \triangleright_{\psi_n}^{a_{p_n}^n} \dots \triangleright_{\psi_1}^{a_0^1} \dots \triangleright_{\psi_1}^{a_{p_1}^1} \gamma_0 = \emptyset_{\mathbb{B}}$ □

Thus the full sequence of the types of the free variables of M can be extracted from its blueprint. The next lemma shows that we can do the opposite (Figure 8): for each sequence $\bar{\chi}$ in $\mathbb{F}(\alpha)$, there exists a term N with the same type, same tree structure and same blueprint as M , and such that the sequence of types of the free variables of N is equal to $\bar{\chi}$.

Lemma 2.17. Let $M \in \text{NF}$ be a term of blueprint α . Suppose

$$\alpha \triangleright_{\chi_m}^{a_0^m} \dots \triangleright_{\chi_m}^{a_{p_m}^m} \dots \triangleright_{\chi_1}^{a_0^1} \dots \triangleright_{\chi_1}^{a_{p_1}^1} \emptyset_{\mathbb{B}}$$

Then for every strictly increasing sequence of variables $Y = (y_1, \dots, y_m)$ such that $\Omega(Y) = (\chi_1, \dots, \chi_m)$, there exists N of same domain, of same blueprint and of same type as M such that $\text{Free}(N) = Y$ and $\{a \mid N|_a = y_i\} = \{a_1^i, \dots, a_{p_i}^i\}$ for each i .

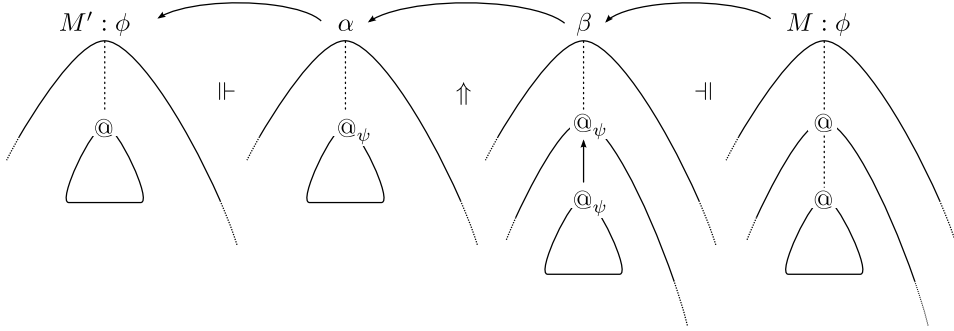


Fig. 9. How the compression of terms is able to follow the compression of blueprints.

Proof. By induction on M . The proposition is clear if M is a variable. The case of $M = (M_1 M_2)$ follows easily from the induction hypothesis. Suppose $M = \lambda x.M_1 : \phi \rightarrow \psi$ with $M_1 \Vdash \gamma$. Let $Y' = (y_1, \dots, y_m, x)$. By Lemma 2.15.(1 \Rightarrow 2) there exists b_1, \dots, b_p such that $\{b_1, \dots, b_p\} = \{b \mid M|_b = x\}$ and $\gamma \triangleright_{\phi}^{b_0} \dots \triangleright_{\phi}^{b_p} \gamma' = \alpha|_1$. Now,

$$\alpha \triangleright_{\chi_m}^{a_0^m} \dots \triangleright_{\chi_m}^{a_{p_m}^m} \dots \triangleright_{\chi_1}^{a_0^1} \dots \triangleright_{\chi_1}^{a_{n_{p1}}^1} \emptyset_{\mathbb{B}}$$

implies that each a_j^i is of the form $(1) \cdot c_j^i$. Furthermore

$$\gamma \triangleright_{\phi}^{b_0} \dots \triangleright_{\phi}^{b_p} \triangleright_{\chi_m}^{c_0^m} \dots \triangleright_{\chi_m}^{c_{p_m}^m} \dots \triangleright_{\chi_1}^{c_0^1} \dots \triangleright_{\chi_1}^{c_{p1}^1} \emptyset_{\mathbb{B}}$$

By induction hypothesis there exists N_1 of same domain, of same blueprint and of same type as M_1 such that $\text{Free}(N_1) = Y'$, $\{b \mid N_1|_b = x\} = \{b_0, \dots, b_p\}$ and $\{a \mid N_1|_a = y_i\} = \{c_0^i, \dots, c_{p_i}^i\}$ for each i . By Lemma 2.15.(2 \Rightarrow 1), $\lambda x.N_1 \Vdash \alpha$. Hence we may take $N = \lambda x.N_1$. \square

3. Compact terms

We go on with our study of the properties of minimal inhabitants. Section 3.1 is just a simple remark on the relative depths of their blueprints, and an easy consequence of the subformula property (Lemma 1.6): if M is a minimal NF-inhabitant of ϕ , then for all addresses a in M the blueprint of $M|_a$ is of relative depth at most $k \times p$, where:

- k is the number of λ in the path from the root to M to a ,
- p is the number of subformulas of ϕ .

We call *locally compact* every NF-inhabitant satisfying this condition. In Section 3.2 we introduce the notion of *vertical compression* of a blueprint. A (strict) vertical compression of β is obtained by taking any address b in β , then by grafting $\beta|_b$ at any address $a < b$ such that $\beta(a) = \beta(b)$. The vertical compressions of β are all blueprints obtained by applying this transformation to β zero or more times. The key-properties of those compressions is the following (see Figure 9):

- If M is of blueprint β and α is a vertical compression of β , the compression of β into α can be mimed by a compression of M into a well-labelled term, in the following

sense. Assuming $\alpha = \beta[a \leftarrow \beta|_b]$ (the base case), the term $Q = M[a \leftarrow M|_b]$ is *not* in general well-labelled. However, *there exists* a term M' with the same domain as Q and of same type as M . Moreover (because $\beta(a) = \beta(b)$) M' is an application if M is an application, an abstraction if M is an abstraction (because $a < b$ and $\beta(a) = \beta(b)$, it cannot be a variable)

Let us again consider a NF-inhabitant M and two addresses a, b such that $a < b$, $M|_a$ and $M|_b$ are applications of the same type or abstractions of the same type. Suppose:

- there exists a vertical compression α' of the blueprint of $M|_b$ such that the sequence $\Omega(\text{Free}(M|_a))$ can be extracted from α' .

This situation is a generalisation of the last example in the introduction of Section 2 (in which α' was equal to the blueprint of $M|_b$, thereby a trivial compression of this blueprint). The term M is not minimal. Indeed, the key-property above implies the existence of a term N of blueprint α' whose size is not greater than the size of $M|_b$, and such that $N, M|_b, M|_a$ are applications of the same type or abstractions of the same type. By Lemma 2.17, there exists a term P of same type and of same domain as N such that $\text{Free}(P) = \text{Free}(M|_a)$. The graft of P at a yields then an inhabitant of strictly smaller size.

We will call *compact* all inhabitants in which the preceding situation does not occur. All inhabitants of minimal size are of course compact. As we shall see in Section 5, we will not need a sharper characterisation of minimal inhabitants. For every formula ϕ , the set of compact inhabitants of ϕ is actually a *finite* set, and our decision method will merely consist in the exhaustive computation of their domains.

3.1. Depths of the blueprints of minimal inhabitants

Definition 3.1. Two terms $M, M' \in \text{NF}$ are *of same kind* if and only if they are both variables, or both applications, or both abstractions, and if they are of same type.

Definition 3.2. For all formula ϕ , we write $\text{Sub}(\phi)$ the set of all subformulas of ϕ .

Definition 3.3. Let $M \in \text{NF}$. Let a be any address in M . Let (a_1, \dots, a_k) be the strictly increasing sequence of all prefixes of a . Let $(\lambda x_1, \dots, \lambda x_n)$ be the subsequence $(M(a_1), \dots, M(a_k))$ of all labels of the form λx . We write $\Lambda(M, a)$ for (x_1, \dots, x_n) .

When M is an NF-inhabitant of ϕ , we say that M is *locally compact* if for all addresses a in M , the blueprint of $M|_a$ of relative depth at most $|\Lambda(M, a)| \times |\text{Sub}(\phi)|$.

Lemma 3.4. Let M be any NF-inhabitant of ϕ . If M is not locally compact, then there exist two addresses b, b' such that $b < b'$, $M|_b$ and $M|_{b'}$ are of same kind, and $\text{Free}(M|_b) = \text{Free}(M|_{b'})$.

Proof. For each address a in $\text{dom}(M)$, let α_a be the blueprint of $M|_a$ and let $X_a = \text{Free}(M|_a)$. Assume an α_a is of relative depth $n > |\Lambda(M, a)| \times |\text{Sub}(\phi)|$. There exists $b_1, \dots, b_{n+1} \in \text{dom}(\alpha_a)$ such that $b_1 < \dots < b_n < b_{n+1}$. ? By Lemma 2.8 we have $X_{a \cdot b_n} \subseteq \dots \subseteq X_{a \cdot b_1} \subseteq \Lambda(M, a)$. By Lemma 1.6, each $\phi_{a \cdot b_i}$ is a subformula of ϕ . Hence

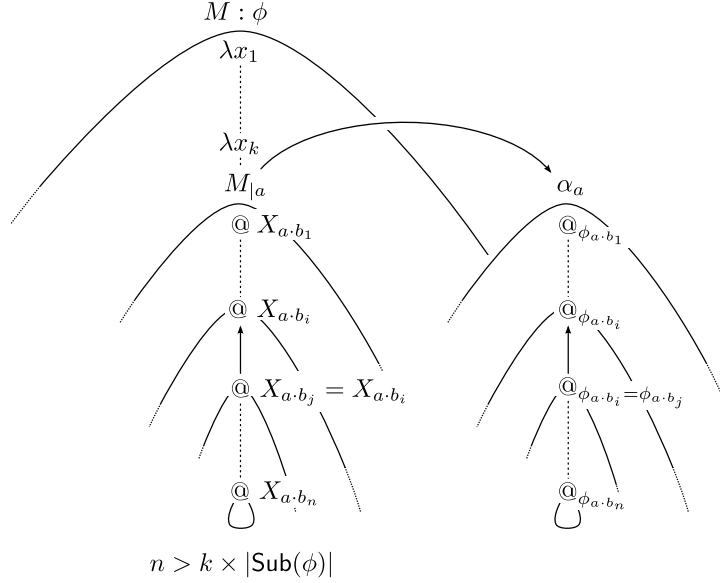


Fig. 10. Proof of Lemma 3.4.

there exist i, j such that $i < j$ and $(X_{a.b_i}, \phi_{a.b_i}) = (X_{a.b_j}, \phi_{a.b_j})$, that is, $M|_{a.b_i}$ and $M|_{a.b_j}$ are applications of the same type and with the same free variables (Figure 10). \square

As an immediate corollary of this result, every NF-inhabitant of minimal size is also locally compact: indeed, if M is not locally compact, then Lemma 3.4 will provide two addresses b, b' such that the subterm at b in M can be replaced with the subterm at b' , the resulting term being an NF-inhabitant of same type and of strictly smaller size.

3.2. Vertical compression of a blueprint

Definition 3.5. Let \uparrow be least reflexive and transitive binary relation on blueprints satisfying the following: if $a, b \in \text{dom}(\beta)$, $a < b$ and $\beta(a) = \beta(b)$, then $\beta[a \leftarrow \beta|_b] \uparrow \beta$.

Lemma 3.6. Suppose $M \in \text{NF}$, $M : \phi$, $M \Vdash \beta$ and $\alpha \uparrow \beta$. There exists a term $M' \in \text{NF}$ of same kind as M , of blueprint α and such that $|\text{dom}(M')| \leq |\text{dom}(M)|$.

Proof. It suffices to consider the case of $\alpha = \beta[a \leftarrow \beta|_b]$ with $a, b \in \text{dom}(\beta)$, $a < b$ 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 . If $a = \varepsilon$ then M is necessarily an application and $\beta(\varepsilon) = \beta(b) = @_\phi$, hence $M|_b$ is an application of type ϕ , and we can take $M' = M|_b$. 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 $\text{dom}(N_i) \leq \text{dom}(M_i)$. Let $j = 1$ if $i = 2$, otherwise let $j = 2$. Let $(N_j, \gamma_j) = (M_j, \beta_j)$. Let $X = (x_1, \dots, x_n)$ be the strictly increasing sequence

of all variables that are free or bound in N_2 . Let $Y = (y_1, \dots, y_n)$ be a strictly increasing sequence of variables such that $\Omega(X) = \Omega(Y)$ and y_1 is greater than or equal to the greatest variable of N_1 . Call N'_2 the term obtained by replacing each x_i by y_i in N_2 . We can take $M' = (N_1 N'_2)$.

(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 $a, b \in \text{dom}(\beta)$, we have also $a_1, b_1 \in \text{dom}(\beta_1)$. 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 $\text{dom}(M'_1) \leq \text{dom}(M_1)$. By Lemma 2.15 there exist $\gamma_1, c_0, \dots, c_n$ such that $\{c_0, \dots, c_n\} = \{c \mid M|_c = x\}$, $\beta_1 \triangleright_\chi^{c_0} \dots \triangleright_\chi^{c_n} \gamma_1$ and $\beta = *(\gamma_1)$. Now, $a, b \in \text{dom}(\alpha)$ implies that for each i : a_1 and c_i are incomparable addresses; b_1 and c_i are incomparable addresses. So $\alpha_1 = \beta_1[a_1 \leftarrow \beta_1|_{b_1}] \triangleright_\chi^{c_0} \dots \triangleright_\chi^{c_n} \gamma_1[a_1 \leftarrow \beta_1|_{b_1}] = \beta[a \leftarrow \beta|_b]_{|(1)} = \alpha|_1$. By Lemma 2.17 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 and $\{c \mid N_1|_c = y\} = \{c_0, \dots, c_n\}$. By Lemma 2.15 ($2 \Rightarrow 1$), $\lambda y.N_1 \Vdash \alpha$, and we may take $M' = \lambda y.N_1$. \square

Definition 3.7. A term $M \in \text{NF}$ is *compact* when there are no a, b, α' such that $a < b$, $M|_a$ and $M|_b$ are of same kind, $M|_b \Vdash \alpha_b$, $\alpha' \uparrow \alpha_b$ and $\Omega(\text{Free}(M|_a)) \in \mathbb{F}(\alpha')$.

Lemma 3.8. Every NF-inhabitant of minimal size is compact. Every compact NF-inhabitant of ϕ is locally compact.

Proof. Let M be any NF-inhabitant of ϕ .

(1) Assume M is not compact. Let a, b be such that $a < b$, $M|_a$ and $M|_b$ are of same kind, $M|_b \Vdash \alpha_b$, $\alpha' \uparrow \alpha_b$, $\text{Free}(M|_a) = X_a$ and $\Omega(X_a) \in \mathbb{F}(\alpha')$ (see Figure 11). By Lemma 3.6 there exists a term $N \in \text{NF}$ of blueprint α' , of same kind as $M|_b$ and such that $|\text{dom}(N)| \leq |\text{dom}(M|_b)|$. By Lemma 2.17 there exists $P \in \text{NF}$ of blueprint α' , of same kind as N , such that $\text{dom}(P) = \text{dom}(N)$ and $\text{Free}(P) = X_a$. The term $M[a \leftarrow P]$ is then an NF-inhabitant of ϕ of smaller size.

(2) Suppose M meets conditions of Lemma 3.4. By Lemma 2.15, the blueprint $\alpha_{b'}$ of $M|_{b'}$ satisfies $\Omega(\text{Free}(M|_b)) = \Omega(\text{Free}(M|_{b'})) \in \mathbb{F}(\alpha'_{b'})$. As the relation \uparrow is reflexive, M is not compact. \square

4. Shadows

So far we have isolated two properties shared by all minimal inhabitants (Lemma 3.8). We shall now exploit them so as to design a decision method for the inhabitation problem.

In Section 4.1 and 4.2 we show how to associate each locally compact inhabitant M of a formula ϕ with a tree of same domain as M , the *shadow* of M . At each address a this tree is labelled with a triple of the form $(\bar{\chi}_a, \gamma_a, \phi_a)$ where ϕ_a is the type of $M|_a$, the sequence $\bar{\chi}_a$ is $\Omega(\text{Free}(M|_a))$, and γ_a is a “transversal compression” of the blueprint α_a of $M|_a$ (Definitions 4.1 and 4.2). The blueprint γ_a at a can be seen as a synthesized version of α_a of same relative depth but of smaller “width”, and such that $\bar{\chi}_a \in \mathbb{F}(\gamma_a) \subseteq \mathbb{F}(\alpha_a)$.

Each tree prefix of the shadow of M belongs to a finite set effectively computable from ϕ and the domain of this prefix. In particular, one can compute all possible values for

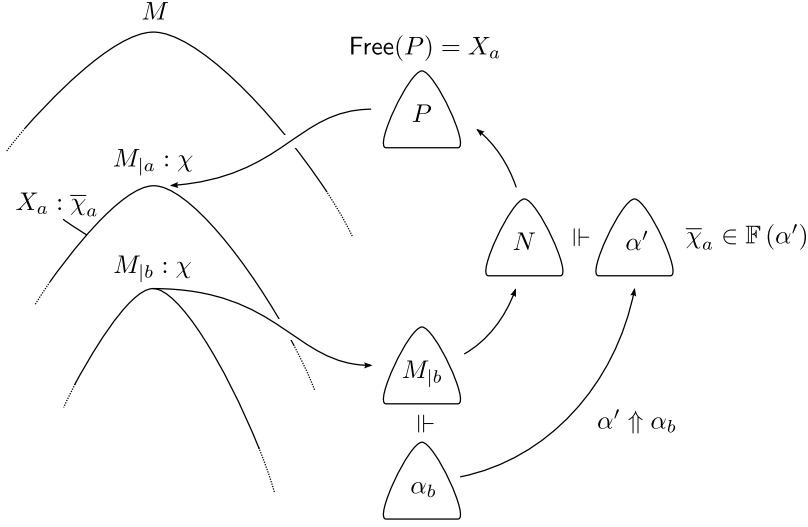


Fig. 11. Proof of Lemma 3.8, part (1).

its labels, regardless of the full knowledge of M – or even without the knowledge of the existence of M . The key-property satisfied by this shadow at every address a is:

— for each $\gamma' \uparrow \gamma_a$, there exists $\alpha' \uparrow \alpha_a$ such that $\mathbb{F}(\gamma') \subseteq \mathbb{F}(\alpha')$.

This property is sufficient to detect the non-compactness of M for a pair of addresses (a, b) only from the knowledge of $\bar{\chi}_a, \phi_a, \gamma_b, \phi_b$ and the arity of the nodes at a and b . Indeed, suppose $a < b$, $\phi_a = \phi_b$ and the nodes at a, b are of same arity (1, or 2). Now, assume:

— there exists $\gamma' \uparrow \gamma_b$ such that $\bar{\chi}_a \in \mathbb{F}(\gamma')$.

Then $M|_a$ and $M|_b$ are of same kind and there exists $\alpha' \uparrow \alpha_b$ such that $\bar{\chi}_a = \Omega(\text{Free}(M|_a)) \in \mathbb{F}(\gamma') \subseteq \mathbb{F}(\alpha')$, therefore M is not compact.

In Section 4.2, what we call *shadow* is a tree $a \mapsto (\bar{\chi}_a, \gamma_a, \phi_a)$ of a certain shape, no matter if this tree is the shadow of a term or not. This shadow is *compact* if there is no pair (a, b) as above. Of course, the shadow of a compact term is always compact in this sense.

In Section 5 we will prove that for every formula ϕ , the set of shadows of compact inhabitants of ϕ is a finite set effectively computable from ϕ (hence the same holds for the set of compact inhabitants of ϕ). In other words we will prove the decidability of Ticket Entailment.

4.1. Blueprint equivalence and transversal compression

Definition 4.1. We let \equiv be the least binary relation on blueprints such that:

- 1 $\emptyset_{\mathbb{B}} \equiv \emptyset_{\mathbb{B}}$,
- 2 $\phi \equiv \phi$,

- 3 if $\alpha_1 \equiv \beta_1, \alpha_2 \equiv \beta_2$, then $@_\phi(\alpha_1, \alpha_2) \equiv @_\phi(\beta_1, \beta_2)$,
- 4 if $|\bar{a}| = |\bar{b}| = n$ and $\alpha_i \equiv \beta_i$ for each $i \in [1, \dots, n]$, then $*_{\bar{a}}(\alpha_1, \dots, \alpha_n) \equiv *_{\bar{b}}(\beta_1, \dots, \beta_n)$.

In (3), we assume $\alpha_1, \alpha_2, \beta_1, \beta_2$ non-empty. In (4), we assume that the elements of each sequence \bar{a}, \bar{b} are pairwise incomparable addresses.

To some extent this equivalence allows us to consider blueprints regardless of the exact values of addresses. For instance $*_{\bar{a}}(\alpha_1, \dots, \alpha_n) \equiv *(\alpha_1, \dots, \alpha_n) \equiv *(\alpha_n, \dots, \alpha_1)$, 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 4.2. For each $m \in \mathbb{N}$, we let \curvearrowright_m be the least binary relation such that:

- 1 if $\gamma_1 \equiv \dots \equiv \gamma_m \equiv \gamma_{m+1} \neq \emptyset_{\mathbb{B}}$, then $*_{\bar{a}}(\gamma_1, \dots, \gamma_m) \curvearrowright_m *_{\bar{a} \cdot (b)}(\gamma_1, \dots, \gamma_m, \gamma_{m+1})$,
- 2 if $\alpha = *_{\bar{a}}(\alpha_1, \dots, \alpha_n), \beta = *_{\bar{b}}(\beta_1, \dots, \beta_p)$ and $\alpha \curvearrowright_m \beta$, then:
 - (a) $@_\phi(\alpha, \gamma) \curvearrowright_m @_\phi(\beta, \gamma)$,
 - (b) $@_\phi(\gamma, \alpha) \curvearrowright_m @_\phi(\gamma, \beta)$,
 - (c) $*_{\bar{a}}(\alpha_1, \dots, \alpha_n, \gamma) \curvearrowright_m *_{\bar{b}}(\beta_1, \dots, \beta_p, \gamma)$.

We call *m-compression of β* every α such that $\alpha \curvearrowright_m \beta$. The *width* of β is defined as the least $m \in \mathbb{N}$ for which there is no α such that $\alpha \curvearrowright_m \beta$.

Again the elements of $\bar{a} \cdot (b)$ must be pairwise incomparable addresses, and α, β, γ must be non-empty.

Note that for all non-empty β , we have $\emptyset_{\mathbb{B}} \curvearrowright_0 \beta$, hence the empty blueprint is the only blueprint of null width. If β is of width $m > 0$, then for all addresses a , for $\beta|_a = *_{\bar{a}}(\gamma_1, \dots, \gamma_k)$ and for each $\gamma_i \neq \emptyset_{\mathbb{B}}$, the sequence $(\gamma_1, \dots, \gamma_k)$ contains no more than m blueprints \equiv -equivalent to γ_i . For instance, if ϕ, ψ, χ are distinct formulas, $*(\phi, \phi, \phi, \psi, \psi, \chi)$ is of width 3, $*(\omega, @_\omega(*(\phi, \psi), \phi), @_\omega(*(\psi, \phi), \phi))$ is of width 2, etc.

Definition 4.3. For each $m \in \mathbb{N}$, we write \sqsubseteq_m for the reflexive and transitive closure of the union of \equiv and \curvearrowright_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 .

For instance, if ϕ, ψ, χ are distinct formulas:

$$\emptyset_{\mathbb{B}} \sqsubseteq_0^{\max} *(\psi, \chi, \phi) \sqsubseteq_1^{\max} *(\chi, \phi, \phi, \psi, \psi) \sqsubseteq_2^{\max} *(\phi, \phi, \phi, \psi, \psi, \chi)$$

Of course $\alpha \sqsubseteq_m \beta$ implies $\alpha \sqsubseteq_j \beta$ for all $j \in [1, \dots, m]$ and clearly, $\alpha \curvearrowright_m \beta$ implies $|\text{dom}(\alpha)| < |\text{dom}(\beta)|$, therefore \curvearrowright_m is well-founded.

Definition 4.4. For all $\mathcal{S} \subseteq \mathfrak{S}$, for all $d \in \mathbb{N}$ and for all $m \in \mathbb{N}$:

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

Lemma 4.5. For all finite $\mathcal{S} \subseteq \mathfrak{S}$, for all $d \in \mathbb{N}$ and for all $m \in \mathbb{N}$:

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

Proof. (1) Let $\mathbb{B}_\varepsilon(\mathcal{S}, d, m)$ be the set of all rooted blueprints in $\mathbb{B}(\mathcal{S}, d, m)$. Assuming $\mathbb{B}_\varepsilon(\mathcal{S}, d, m)/\equiv$ is a finite set and a selector $\mathbb{R}_\varepsilon(\mathcal{S}, d, m)$ for $\mathbb{B}_\varepsilon(\mathcal{S}, d, m)/\equiv$ is effectively computable from (\mathcal{S}, d, m) , we prove that $\mathbb{B}(\mathcal{S}, d, m)/\equiv$ and $\mathbb{B}_\varepsilon(\mathcal{S}, d+1, m)/\equiv$ are finite sets and show how to compute a selector for each set.

Let $(\alpha_1, \dots, \alpha_k)$ be an enumeration of $\mathbb{R}_\varepsilon(\mathcal{S}, d, m)$. Let Σ_d be the set of all functions from $\{1, \dots, k\}$ to $\{0, \dots, m\}$. For each $\beta \in \mathbb{B}(\mathcal{S}, d, m)$ there exists \bar{b} and $\beta_1, \dots, \beta_n \in \mathbb{B}_\varepsilon(\mathcal{S}, d, m)$ such that $\beta = *_{\bar{b}}(\beta_1, \dots, \beta_n)$. We let σ_β be the function mapping each $i \in [1, \dots, k]$ to the number of occurrences of an element \equiv -equivalent to α_i in the sequence $(\beta_1, \dots, \beta_n)$. Clearly $\sigma_\alpha \in \Sigma_d$ and furthermore for all $\beta' \in \mathbb{B}(\mathcal{S}, d, m)$ we have $\beta \equiv \beta'$ if and only if $\sigma_\beta = \sigma_{\beta'}$, hence $\mathbb{B}(\mathcal{S}, d, m)$ is a finite set.

For each $\tau \in \Sigma_d$, let $\rho_\tau = *(\alpha_1^1, \dots, \alpha_1^{\tau(1)}, \dots, \alpha_k^1, \dots, \alpha_k^{\tau(k)})$ where each α_i^j is equal to α_i . We have $\rho_\tau \in \mathbb{B}(\mathcal{S}, d, m)$ and $\sigma(\rho_\tau) = \tau$, that is, if $\tau, \tau' \in \Sigma_d$ and $\tau \neq \tau'$, then $\rho_\tau \not\equiv \rho_{\tau'}$. Hence we may define $\mathbb{R}(\mathcal{S}, d, m)$ as $\{\rho_\tau \mid \tau \in \Sigma_d\}$.

The finiteness of $\mathbb{B}_\varepsilon(\mathcal{S}, d+1, m)/\equiv$ follows immediately from the finiteness of $\mathbb{B}(\mathcal{S}, d, m)$ and the fact that if $\beta = @_\phi(\beta_1, \beta_2)$ and $\beta' = @_\psi(\beta'_1, \beta'_2)$ are elements of $\mathbb{B}_\varepsilon(\mathcal{S}, d+1, m)$, then $\beta_1, \beta_2, \beta'_1, \beta'_2$ are non-empty elements of $\mathbb{B}(\mathcal{S}, d, m)$ and furthermore $\beta \equiv \beta'$ if and only if $\beta_1 \equiv \beta'_1$ and $\beta_2 \equiv \beta'_2$. The same property allows us to define $\mathbb{R}_\varepsilon(\mathcal{S}, d+1, m)$ as the set of all blueprints of the form $@_\phi(\gamma_1, \gamma_2)$ where $@_\phi \in S$ and each γ_i is a non-empty element of $\mathbb{R}(\mathcal{S}, d, m)$.

(2) The lemma follows by induction on d , using (1) and the facts that: $\mathbb{B}_\varepsilon(\mathcal{S}, 0, 0)$ is empty (hence $\mathbb{B}(\mathcal{S}, d, 0) = \{\emptyset_{\mathbb{B}}\}$ for all d); if $m \in \mathbb{N}_+$, then $\mathbb{B}_\varepsilon(\mathcal{S}, 0, m)$ is the finite set of all formulas of \mathcal{S} . \square

4.2. Shadow of a term

Definition 4.6. Let ϕ be a formula. Let \mathcal{S}_ϕ be the union of $\text{Sub}(\phi)$ and the set of all $@_\psi$ such that $\psi \in \text{Sub}(\phi)$ (see Definition 3.2). For each integer k , for each formula ϕ , we let $\mathfrak{R}(\phi, k) = \mathbb{R}(\mathcal{S}_\phi, k \times |\text{Sub}(\phi)|, k)$, where \mathbb{R} is the function introduced in Lemma 4.5.(2).

Definition 4.7. A *shadow* is a tree in which each node is of arity at most 2 and is labelled with a triple of the form $(\bar{\chi}, \gamma, \psi)$, where $\bar{\chi}$ is a sequence of formulas, γ is a blueprint and ψ is a formula.

We call ϕ -*shadow* every shadow Ξ satisfying the two following conditions. We have $\Xi(\varepsilon) = (\varepsilon, \emptyset_{\mathbb{B}}, \phi)$. For each $a \in \text{dom}(\Xi)$, let k_a be the number of $b < a$ such that the node of Ξ at b is unary, and let $(\bar{\chi}_a, \gamma_a, \psi_a) = \Xi(a)$. Then:

- $\bar{\chi}_a$ is a sequence of subformulas of ϕ of length at most d_a ,
- $\gamma_a \in \mathfrak{R}(\phi, k_a)$,
- $\bar{\chi}_a \in \mathbb{F}(\gamma_a)$
- ψ_a is a subformula of ϕ .

Definition 4.8. Let M be a locally compact NF-inhabitant of ϕ . For each $a \in \text{dom}(M)$:

- let $\bar{\chi}_a = \Omega(\text{Free}(M|_a))$,
- let α_a be the blueprint of $M|_a$,
- let $\gamma_a \in \mathfrak{R}(\phi, |\Lambda(M, a)|)$ be such that $\gamma_a \sqsubseteq_{|\Lambda(M, a)|}^{\max} \alpha_a$,

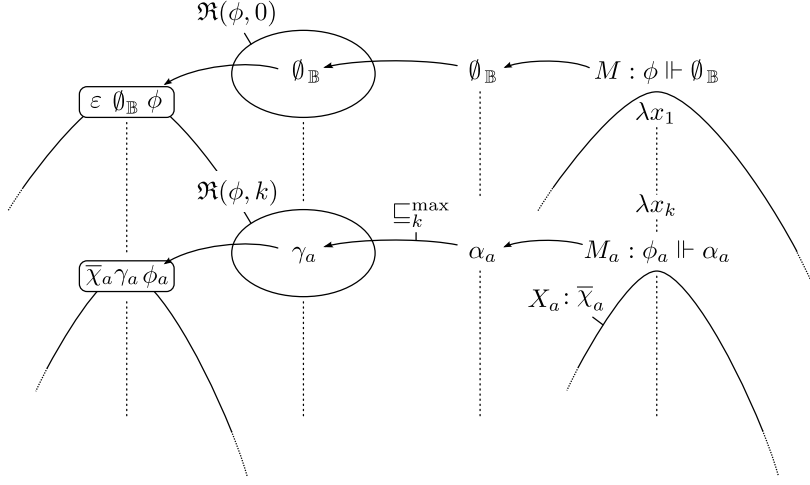


Fig. 12. A compact inhabitant and its shadow.

— let ϕ_a be the type of $M|_a$.

The tree Ξ mapping each $a \in \text{dom}(M)$ to $(\bar{\chi}_a, \gamma_a, \phi_a)$ will be called *the shadow of M* .

Recall that if M is a locally compact NF-inhabitant of ϕ , then for each address a in M , the blueprint α_a of $M|_a$ is of relative depth at most than $|\Lambda(M, a)| \times |\text{Sub}(\phi)|$. Every maximal $|\Lambda(M, a)|$ -compression of α_a produces a shadow α'_a of same relative depth and of width at most $|\Lambda(M, a)|$, to which some element of $\mathfrak{R}(\phi, |\Lambda(M, a)|)$ is equivalent, thus the shadow of M is well-defined. Note that there is possibly more than one choice for γ_a (although it not the case since \mathbb{R} is a selector and one can actually prove that $\gamma \sqsubseteq_m^{\max} \alpha$ and $\gamma' \sqsubseteq_m^{\max} \alpha$ implies $\gamma \equiv \gamma'$, but this property is irrelevant to our discussion). We assume though that *some* γ_a is chosen for each address a in M .

Obviously the shadow of M satisfies the first, second and fourth conditions in the definition of ϕ -shadows above – in the next section, we prove that it satisfies also the third.

4.3. Compact shadows and compact inhabitants

Definition 4.9. A shadow Ξ is *compact* if and only if there are no a, b such that: $a < b$, the nodes of Ξ at a, b are of same arity, $\Xi(a) = (\bar{\chi}_a, \gamma_a, \psi)$, $\Xi(b) = (\bar{\chi}_b, \gamma_b, \psi)$ and there exists $\gamma' \uparrow \gamma_b$ such that $\bar{\chi}_a \in \mathbb{F}(\gamma')$.

Compare this definition with the definition of compactness for term (Definition 3.7). With the help of three auxiliary lemmas, we now prove the key-lemma of Section 4: if M is a compact inhabitant – a fortiori locally compact by Lemma 3.8 – then the shadow of M is a compact ϕ -shadow.

Lemma 4.10. 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 $|\text{dom}(\beta')|$ shows that if $\alpha = \beta[a \leftarrow \beta|_b]$ and

$\beta \equiv \beta'$, then there exist a', b' such that $a' < b'$ and $\alpha \equiv \alpha' = \beta'[a' \leftarrow \beta']_{|b'}$. As a consequence, 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 $|\text{dom}(\beta')|$ shows that if $\alpha \uparrow \beta \curvearrowright_1 \beta'$, then there exists α' such that $\alpha \curvearrowright_1 \alpha' \uparrow \beta'$. The only non trivial case is $\alpha = *_{(a_1)}(\alpha_1)$, $\beta = *_{(a_1)}(\beta_1)$ with $\alpha_1 \uparrow \beta_1$ and $\beta' = *_{(a_1, a_2)}(\beta_1, \beta_2)$ with $\beta_1 \equiv \beta_2$. Since $\alpha_1 \uparrow \beta_1 \equiv \beta_2$, there exists by (1) an α_2 such that $\alpha_1 \equiv \alpha_2 \uparrow \beta_2$. Hence $\alpha = *_{(a_1)}(\alpha_1) \curvearrowright_1 *_{(a_1, a_2)}(\alpha_1, \alpha_2) \uparrow *_{(a_1, a_2)}(\beta_1, \beta_2) = \beta'$.

(3) Using (1) and (2), the lemma follows by induction on the length of an arbitrary sequence $(\beta_0, \dots, \beta_n)$ such that $\beta_0 = \beta$, $\beta_n = \beta'$ and $\beta_{i-1} \equiv \beta_i$ or $\beta_{i-1} \curvearrowright_1 \beta_i$ for each $i \in [1, \dots, n]$. \square

Lemma 4.11. If $\alpha \sqsubseteq_1 \beta$, then $\mathbb{F}(\alpha) \subseteq \mathbb{F}(\beta)$.

Proof. By induction on $|\text{dom}(\beta)|$. Since $\gamma \equiv \gamma'$ implies $\mathbb{F}(\gamma) = \mathbb{F}(\gamma')$ and $|\text{dom}(\gamma)| = |\text{dom}(\gamma')|$, it suffices to consider the case where α is a 1-compression of β . The case $\alpha = *_{(a_1)}(\alpha_1)$ and $\beta = *_{(a_1, a_2)}(\alpha_1, \alpha_2)$ is clear. The remaining cases follow easily from the induction hypothesis. \square

Lemma 4.12. If $\alpha \sqsubseteq_m \beta$, then the set of all elements of $\mathbb{F}(\beta)$ of length at most m is a subset of $\mathbb{F}(\alpha)$.

Proof. By induction on $|\text{dom}(\beta)|$. Again, we examine only the case $\alpha \curvearrowright_m \beta$. The proposition is trivially true if $m = 0$. Suppose $m > 0$. The only non-trivial case is $\alpha \equiv *_{\bar{a}}(\gamma_1, \dots, \gamma_m)$ and $\beta \equiv *_{\bar{a}}(\gamma_1, \dots, \gamma_m, \gamma_{m+1})$ with $\gamma_i \equiv \gamma$ for all i . Let $\Phi = \mathbb{F}(\gamma)$. For each integer k , let $\Phi^{(k)} = \otimes(\Phi_1, \dots, \Phi_k)$ where $\Phi_i = \mathbb{F}(\gamma)$ for each i . Let $\bar{\phi} = (\phi_1, \dots, \phi_p) \in \mathbb{F}(\beta)$ be such that $p \leq m$. For each $J \subseteq \{1, \dots, p\}$, let (j_1, \dots, j_q) be the strictly increasing enumeration of all elements of J and let $f(J) = (\phi_{j_1}, \dots, \phi_{j_q})$. We have $\bar{\phi} \in \mathbb{F}(\beta) = \Phi^{(m+1)}$, hence there exist J_1, \dots, J_{m+1} such that $J_1 \cup \dots \cup J_{m+1} = \{1, \dots, p\}$, and $f(J_i) \in \mathbb{F}(\gamma)$ for each $i \in \{1, \dots, m+1\}$. For each $j \in \{1, \dots, p\}$, let k_j be any element of $\{1, \dots, m+1\}$ such that $j \in J_{k_j}$. Then $J_{k_1} \cup \dots \cup J_{k_p} = \{1, \dots, p\}$, so $\bar{\phi} \in \otimes(\{f(J_{k_1})\}, \dots, \{f(J_{k_p})\}) \subseteq \Phi^{(p)} \subseteq \Phi^{(m)} = \mathbb{F}(\alpha)$. \square

Lemma 4.13. Let M be a locally compact NF-inhabitant of ϕ . The shadow of M is a ϕ -shadow. If M is compact, then this shadow is also compact.

Proof. The first proposition follows immediately from the definition of the shadow of M , Lemma 1.6 and Lemma 4.12. Let Ξ be shadow of M . Assume Ξ is not compact. There exist $a, b \in \text{dom}(\Xi) = \text{dom}(M)$ such that $\Xi(a) = (\bar{\chi}_a, \gamma_a, \psi)$, $\Xi(b) = (\bar{\chi}_b, \gamma_b, \psi)$, the nodes at a, b in Ξ are of same arity, and there exists $\gamma' \uparrow \gamma_b$ such that $\bar{\chi}_a \in \mathbb{F}(\gamma')$. We have $M|_a, M|_b$ of same kind. Let α_a, α_b be the blueprints of $M|_a, M|_b$. Since $\gamma_b \sqsubseteq_{|\Lambda(M, a, b)|}^{\max} \alpha_b$, we have $\gamma' \uparrow \gamma_b \sqsubseteq_1 \alpha_b$. By Lemma 4.10 there exists α' such that $\gamma' \sqsubseteq_1 \alpha' \uparrow \alpha_b$. By Lemma 4.11, we have $\bar{\chi}_a = \Omega(\text{Free}(M|_a)) \in \mathbb{F}(\gamma') \subseteq \mathbb{F}(\alpha')$, hence M is not compact. \square

5. Finiteness 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 .

In definition 5.1, we introduce a last binary relation \in on blueprints. The key-lemma of this section (Lemma 5.14) shows that whenever $\mathcal{S} \subseteq \mathfrak{S}$ is a finite set (in particular when \mathcal{S} is the set of all subformulas of ϕ and all $\textcircled{\ast}$'s tagged with a subformula of ϕ), the relation \in is an almost full relation (Bezem, Klop and de Vrijer 2003) on the set of all \mathcal{S} -blueprints: there is no infinite sequence $\gamma_1, \gamma_2, \dots$ over $\mathbb{B}(\mathcal{S})$ such that $\gamma_i \notin \gamma_{i+1+k}$ for all i, k . This result will be proven with the help of Melliès' Axiomatic Kruskal Theorem (Melliès 1998). The finiteness of the set of compact ϕ -shadows follows from this key-lemma with the help of König's Lemma (Lemma 5.15). The ability to compute these shadows follows directly from their definition.

By lemma 4.13, a consequence of this result is also the finiteness for each ϕ of the set of all compact NF-inhabitants of ϕ , although our decision method is based on the computation of *shadows* of compact terms rather than a direct computation of those terms. It is worth mentioning that the proof of Theorem 5.13 is non-constructive and that it gives no information about the complexity of our proof-search method.

5.1. Almost full relations and Higman's theorem

Definition 5.1. We let \in be the relation on blueprints defined by $\alpha \in \beta$ if and only if for all $\bar{\alpha} \in \mathbb{F}(\alpha)$, there exists $\gamma \uparrow \beta$ such that $\bar{\alpha} \in \mathbb{F}(\gamma)$.

Definition 5.2. 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 exist i, j such that $i < j$ and $u_i \ll u_j$.

The main aim of Section 5 will be to prove a last key-lemma from which will easily infer the decidability of Ticket Entailment: for each finite $\mathcal{S} \subseteq \mathfrak{S}$, the relation \in is an AFR on $\mathbb{B}(\mathcal{S})$.

Proposition 5.3.

- 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). This result appears in the proof of Theorem 1, Step 4 (p.523) as a corollary of Lemma 4 (p.520) □

Definition 5.4. 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 $\eta : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ such that $U_i \ll V_{\eta(i)}$ for each $i \in \{1, \dots, n\}$.

Theorem 5.5. (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

Melliès' Axiomatic Kruskal Theorem allows one to conclude that a relation is an AFR (a “well binary relation” in (Melliès 1998)) as long as it satisfies a set of five properties or “axioms” (six in the original version of the theorem – see the remarks of Melliès at the end of its proof explaining why five axioms suffice). The details of those axioms will be given in Section 5.3.

Four of those five axioms are relatively easy to check. The remaining axiom is more problematical. This rather technical section is entirely devoted to the proof of Lemma 5.11, which will ensure that this last axiom is satisfied. We want to prove:

Let \mathcal{S} be a finite subset of \mathfrak{S} . Let \mathcal{B}_ε be a subset of $\mathbb{B}_\varepsilon(\mathcal{S})$.

Let $\mathcal{B} = \{\bar{\alpha}(\beta_1, \dots, \beta_n) \mid \forall i \in [1, \dots, n], \beta_i \in \mathcal{B}_\varepsilon\}$.*

If \Subset is an AFR on \mathcal{B}_ε , then \Subset is an AFR on \mathcal{B} .

Recall that $\mathbb{B}_\varepsilon(\mathcal{S})$ stands for the set of all rooted \mathcal{S} -blueprints. We want to be able to extend the property that \Subset is an AFR on a given set of rooted blueprints to the set all blueprints that have those rooted blueprints at their minimal addresses.

Higman's theorem suffices to show that $\Subset_{\mathfrak{S}}$ (Definition 5.4) is an AFR on the set of finite sequences over \mathcal{B}_ε . However, if consider an infinite sequence over \mathcal{B} and transform each blueprint $*\bar{\alpha}(\beta_1, \dots, \beta_n)$ into $(\beta_1, \dots, \beta_n)$, the theorem will only provide two sequences $(\beta_1, \dots, \beta_n)$, $(\beta'_1, \dots, \beta'_{n+k})$ and a subsequence $(\beta_{i_1}, \dots, \beta_{i_n})$ of the latter such that $\beta_j \Subset \beta'_{i_j}$ for each $j \in [1, \dots, n]$. Letting $\{j_{n+1}, \dots, j_{n+k}\} = \{1, \dots, n+k\} - \{j_1, \dots, j_n\}$, this is sufficient to ensure $*\bar{\alpha}(\beta_1, \dots, \beta_n) \Subset *_{\bar{b}}(\beta'_{i_1}, \dots, \beta'_{i_n})$, but not in general $*\bar{\alpha}(\beta_1, \dots, \beta_n) \Subset *_{\bar{b}}(\beta'_{j_1}, \dots, \beta'_{j_n}, \beta'_{j_{n+1}}, \dots, \beta'_{j_{n+k}})$. The question is: what should we do with $\beta'_{j_{n+1}}, \dots, \beta'_{j_{n+k}}$?

To bypass this difficulty we show how for each blueprint $\beta \in \mathbb{B}(\mathcal{S})$, one can extract from the set of all vertical compressions of β a complete set of “followers” of β of minimal size (Lemma 5.7). This set $\{\alpha_1, \dots, \alpha_p\}$ has the property that for each $\bar{\phi} \in \mathbb{F}(\beta)$, there exists at least one α_i such that $\mathbb{F}(\alpha_i)$ contains a *subsequence* of $\bar{\phi}$ – but not necessarily $\bar{\phi}$ itself. The relative depth of each α_i does not depends on the relative depth on β , but only on \mathcal{S} : it is at most $\sum_{i=1}^{1+|\mathcal{S}_{\text{@}}|} i$, where $\mathcal{S}_{\text{@}}$ is the set of all binary symbols in \mathcal{S} . The lemma is then proven in four steps.

First, observe that the set of all $\alpha \uparrow \beta$ of relative depth at most $\sum_{i=1}^{1+|\mathcal{S}_{\text{@}}|} i$ is a complete set of followers. If we consider the set of all γ such that $\gamma \sqsubseteq_1^{\max} \alpha$ for at least one such α , we obtain a (possibly infinite) set closed under \equiv and finite up to \equiv . We call it the set of \mathcal{S} -residuals of β .

Second, we prove that the set of \mathcal{S} -residuals of β is a complete set of followers of β in the same sense, that is, for each $\bar{\phi} \in \mathbb{F}(\beta)$ there exists an \mathcal{S} -residual γ of β such that $\mathbb{F}(\alpha_i)$ contains a subsequence of $\bar{\phi}$ (Lemma 5.9).

Third, we prove that if $\beta = *\bar{\alpha}(\beta_1, \dots, \beta_n)$, $\beta' = *_{\bar{b}}(\beta'_1, \dots, \beta'_n, \beta'_{n+1}, \dots, \beta'_{n+k})$ are such that $\beta_i \Subset \beta'_i$ for each $i \in [1, \dots, n]$, and if furthermore β, β' have the same set of \mathcal{S} -residuals, then $\beta \Subset \beta'$ (Lemma 5.10).

The last step is the proof of the lemma itself. There are only a finite number of possible values for the set of residuals of each \mathcal{S} -blueprint, hence from any infinite sequence over

\mathcal{B} , one is able to extract an infinite sequence of blueprints with the same set of residuals. The conclusion follows from the third step and Higman's theorem.

Definition 5.6. For every $\mathcal{S} \subseteq \mathfrak{S}$, we let $\mathcal{S}_\circlearrowleft$ denote the set of all binary symbols in \mathcal{S} .

Lemma 5.7. Let \mathcal{S} be a finite subset of \mathfrak{S} . For all $\beta \in \mathbb{B}(\mathcal{S})$, for all $\bar{\psi} \in \mathbb{F}(\beta)$, there exists $\alpha \uparrow \beta$ of relative depth at most $\sum_{i=1}^{1+|\mathcal{S}_\circlearrowleft|} i$ such that $\mathbb{F}(\alpha)$ contains a subsequence of $\bar{\psi}$.

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

Given an arbitrary \mathcal{S} -linearisation $(\beta, \bar{\psi})$, we prove simultaneously by induction on $|\text{dom}(\beta)|$ the following properties:

- 1 There exists an \mathcal{S} -linearisation $(\gamma, \bar{\chi})$ such that:
 - (a) $\gamma \uparrow \beta$ and $\bar{\chi}$ is a subsequence of $\bar{\psi}$,
 - (b) γ is of relative depth at most $1 + \sum_{i=1}^{|\mathcal{S}_\circlearrowleft|} i$.
- 2 There exists an \mathcal{S} -linearisation $(\alpha, \bar{\phi})$ such that:
 - (a) $\alpha \uparrow \beta$, $\bar{\phi}$ is a subsequence of $\bar{\psi}$, and the last elements of $\bar{\phi}, \bar{\psi}$ are equal,
 - (b) for each starting address b of $(\alpha, \bar{\phi})$ 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 $(\alpha, \bar{\phi})$, $(\alpha|_c)$ is of relative depth $1 + \sum_{i=1}^{|\mathcal{S}_\circlearrowleft|} i$.

Note that the conjunction of (2.b) and (2.c) implies that every address d in α is of relative depth at most $|\mathcal{S}_\circlearrowleft| + 1 + \sum_{i=1}^{|\mathcal{S}_\circlearrowleft|} i = \sum_{i=1}^{1+|\mathcal{S}_\circlearrowleft|} i$. The cases $\beta = *_{\bar{a}}(\beta')$ with $a \neq \varepsilon$ and $\beta = *_{\bar{a}}(\beta_1, \dots, \beta_n)$ 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 $\bar{\psi} \in \mathbb{F}(\beta)$, there exist $\bar{\psi}_0 \in \mathbb{F}(\delta)$, $\bar{\psi}_1 \in \mathbb{F}(\delta_1)$, $\bar{\psi}_2 \in \mathbb{F}(\delta_2)$ such that $\bar{\psi}_0$ is a subsequence $\bar{\psi}$ and $\bar{\psi}_0 \in \circlearrowleft(\{\bar{\psi}_1\}, \{\bar{\psi}_2\})$. By induction hypothesis there exists an $(\mathcal{S} - \{@\psi\})$ -linearisation $(\gamma_1, \bar{\chi}_1)$ satisfying conditions (1.a), (1.b) w.r.t $(\delta_0, \bar{\psi}_1)$, and an $(\mathcal{S} - \{@\psi\})$ -linearisation $(\gamma_2, \bar{\chi}_2)$ satisfying conditions (2.a), (2.b), (2.c) w.r.t $(\delta_2, \bar{\psi}_2)$.

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 $\sum_{i=1}^{|\mathcal{S}_\circlearrowleft|} i$, therefore γ is of relative depth at most $1 + \sum_{i=1}^{|\mathcal{S}_\circlearrowleft|} i$. Now $\bar{\chi}_2$ is a subsequence of $\bar{\psi}_2$ with the same last element, so there exists in $\circlearrowleft(\{\bar{\chi}_1\}, \{\bar{\chi}_2\}) \subseteq \mathbb{F}(@_\psi(\gamma_1, \gamma_2))$ a subsequence $\bar{\chi}$ of $\bar{\psi}_0$. Thus $(\gamma, \bar{\chi})$ satisfies (1.a) and (1.b) w.r.t $(\beta, \bar{\psi})$.

(2) As $\bar{\psi} \in \mathbb{F}(\beta)$, there exist $\bar{\psi}_1 \in \mathbb{F}(\beta_1)$, $\bar{\psi}_2 \in \mathbb{F}(\beta_2)$ such that $\bar{\psi} \in \circlearrowleft(\{\bar{\psi}_1\}, \{\bar{\psi}_2\})$. By induction hypothesis there exists an \mathcal{S} -linearisation $(\alpha_1, \bar{\phi}_1)$ satisfying conditions (1.a), (1.b) w.r.t $(\beta_1, \bar{\psi}_1)$, and an \mathcal{S} -linearisation $(\alpha_2, \bar{\phi}_2)$ satisfying conditions (2.a), (2.b), (2.c) w.r.t $(\beta_2, \bar{\psi}_2)$.

Let $\alpha_0 = @_\psi(\alpha_1, \alpha_2)$. We have $\alpha_0 \uparrow \beta$. The last elements of $\bar{\phi}_2, \bar{\psi}_2$ are equal, and

$\circledast(\{\bar{\phi}_1\}, \{\bar{\phi}_2\}) \subseteq \mathbb{F}(\alpha)$. Hence there exists in $\mathbb{F}(\alpha)$ a subsequence $\bar{\phi}_0$ of $\bar{\psi}$ with the same last element as $\bar{\psi}$. Thus $(\alpha_0, \bar{\phi}_0)$ satisfies (2.a).

For all c incomparable with each starting address for $(\alpha_0, \bar{\phi}_0)$, either $c = (1) \cdot c'$ and $c' \in \text{dom}(\alpha_1)$, or $c = (2) \cdot c''$ and $c'' \in \text{dom}(\alpha_2)$ is incomparable with each starting address in α_2 . As a consequence, the choice of α_1, α_2 ensures that $(\alpha_0, \bar{\phi}_0)$ satisfies (2.c).

If $(\alpha_0, \bar{\phi}_0)$ satisfies (2.b), then we may take $(\alpha, \bar{\phi}) = (\alpha_0, \bar{\phi}_0)$. Otherwise some starting address b for $(\alpha_0, \bar{\phi}_0)$ 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 $(\alpha_2, \bar{\phi}_2)$. The values $\alpha_2(d_2), \dots, \alpha_2(d_n)$ are pairwise distinct, so there must exist $i > 1$ such that $\alpha(b_i) = \textcircled{\ast}$. Since b_i is in the path to b , there exists in $\mathbb{F}(\alpha_{2|d_i})$ a subsequence $\bar{\phi}'_0$ of $\bar{\phi}_0$ of same last element as $\bar{\phi}_0$. For $\alpha'_0 = \alpha_0[\varepsilon \leftarrow \alpha_{2|d_i}]$, we have $\alpha'_0 \uparrow \beta$ and $\bar{\phi}'_0 \in \mathbb{F}(\alpha'_0)$. The existence of $(\alpha, \bar{\phi})$ follows then from the induction hypothesis. \square

Definition 5.8. Let \mathcal{S} be a finite subset of \mathfrak{S} . For all $\beta \in \mathbb{B}(\mathcal{S})$, for all $\alpha \uparrow \beta$ or relative depth at most $\sum_{i=1}^{1+|\mathcal{S}|} i$ and for all $\alpha_0 \sqsubseteq_1^{\text{max}} \alpha$, the blueprint α_0 will be called an \mathcal{S} -residual of β .

Note that the set of \mathcal{S} -residuals of β is $\{\emptyset_{\mathbb{B}}\}$ if $\beta = \emptyset_{\mathbb{B}}$. Otherwise, it is an infinite set: even if $\beta = \phi$, the set of residuals of β is the \equiv -equivalence class of β and contains all blueprints of the form $*_{\bar{\pi}}(\phi)$ (recall that \equiv is a subset of \sqsubseteq_1 , see Definition 4.3).

Lemma 5.9. Let \mathcal{S} be a finite subset of \mathfrak{S} . For all $\beta \in \mathbb{B}(\mathcal{S})$ and for all $\bar{\psi} \in \mathbb{F}(\beta)$, there exists an \mathcal{S} -residual α_0 of β such that $\mathbb{F}(\alpha_0)$ contains a subsequence of $\bar{\psi}$.

Proof. (1) Let γ, δ be arbitrary blueprints. Suppose $\gamma \sqsubseteq_1 \delta$. We shall prove that for all $\bar{\phi} \in \mathbb{F}(\delta)$, there exists in $\mathbb{F}(\gamma)$ a subsequence of $\bar{\phi}$. As in the proof of Lemma 4.12, we may consider $\delta \equiv *(\gamma, \gamma)$ as our base case. In order to deal with the case $\delta = \textcircled{\ast}_{\phi}(\delta_1, \delta_2)$, we need to prove a slightly more precise property: if δ is not empty, then for all $\bar{\phi} \in \mathbb{F}(\delta)$, there exists in $\mathbb{F}(\gamma)$ a subsequence $\bar{\psi}$ of $\bar{\phi}$ such that the last elements of $\bar{\phi}, \bar{\psi}$ are equal. The case $\delta \equiv *(\gamma, \gamma)$ is clear. Other cases follow easily from the induction hypothesis.

(2) We prove the lemma. By Lemma 5.7 and by definition of an \mathcal{S} -residual, there exist α_0, α such that $\alpha_0 \sqsubseteq_1 \alpha \uparrow \beta$, $\mathbb{F}(\alpha)$ contains a subsequence of $\bar{\psi}$ and α_0 is an \mathcal{S} -residual. It follows from (1) that $\mathbb{F}(\alpha_0)$ contains a subsequence of $\bar{\psi}$. \square

Lemma 5.10. Let \mathcal{S} be a finite subset of \mathfrak{S} . Suppose:

- $\beta = *_{\bar{\pi}}(\beta_1, \dots, \beta_n) \in \mathbb{B}(\mathcal{S})$,
- $\beta' = *_{\bar{\pi}'}(\beta'_1, \dots, \beta'_n, \beta'_{n+1}, \dots, \beta'_{n+k}) \in \mathbb{B}(\mathcal{S})$,
- $\beta_i \in \beta'_i$ for each $i \in \{1, \dots, n\}$,
- the sets of \mathcal{S} -residuals of β and β' are equal.

Then $\beta \in \beta'$.

Proof. Let $\bar{\phi} \in \mathbb{F}(\beta)$. There exists for each $i \in [1, \dots, n]$ a sequence $\bar{\phi}_i \in \mathbb{F}(\beta_i)$ such that $\bar{\phi} \in \textcircled{\ast}(\{\bar{\phi}_1\}, \dots, \{\bar{\phi}_n\})$. By assumption there exists for each $i \in [1, \dots, n]$ an $\alpha_i \uparrow \beta'_i$ such that $\bar{\phi}_i \in \mathbb{F}(\alpha_i)$. As a consequence $\bar{\phi} \in \mathbb{F}(*(\alpha_1, \dots, \alpha_n))$.

By Lemma 5.9 there exists an \mathcal{S} -residual γ_0 of β such that $\mathbb{F}(\gamma_0)$ contains a subsequence

$\bar{\psi}$ of $\bar{\phi}$. By assumption γ_0 is also an \mathcal{S} -residual of β' , hence there exists $\gamma'_1, \dots, \gamma'_{n+k}, \bar{b}$ such that $\gamma_0 \sqsubseteq_1 *_{\bar{b}}(\gamma'_1, \dots, \gamma'_{n+k}) \uparrow \beta'$. By Lemma 4.11, we have $\bar{\psi} \in \mathbb{F}(*_{\bar{b}}(\gamma'_1, \dots, \gamma'_{n+k}))$. Hence for each $i \in [1, \dots, n+k]$, there exists in $\mathbb{F}(\gamma'_i)$ a subsequence of $\bar{\psi}$, which is also a subsequence of $\bar{\phi}$. Now, let $\alpha = *_{\bar{b}}(\alpha_1, \dots, \alpha_n, \gamma'_{n+1}, \dots, \gamma'_{n+k})$. Then $\alpha \uparrow \beta'$, $\bar{\phi} \in \mathbb{F}(*(\alpha_1, \dots, \alpha_n))$, and for each $j \in [1, \dots, k]$ there exists in $\mathbb{F}(\gamma'_{n+j})$ a subsequence of $\bar{\phi}$. As a consequence $\bar{\phi} \in \mathbb{F}(\alpha)$. \square

Lemma 5.11. Let \mathcal{S} be a finite subset of \mathfrak{S} . Let \mathcal{B}_ε be a subset of $\mathbb{B}_\varepsilon(\mathcal{S})$. Let $\mathcal{B} = \{*\bar{\alpha}(\beta_1, \dots, \beta_n) \mid \forall i \in [1, \dots, n], \beta_i \in \mathcal{B}_\varepsilon\}$. If \Subset is an AFR on \mathcal{B}_ε , then \Subset is an AFR on \mathcal{B} .

Proof. Let $\mathcal{R} = \mathbb{B}(\mathcal{S}, \Sigma_{i=1}^{1+|\mathcal{S}_{\text{@}}|} i, 1)$ (see Definition 4.4). By Lemma 4.5.(1) the set \mathcal{R}/\equiv is finite. For each $\beta \in \mathcal{B}$, let $\rho(\beta)$ be the set of \mathcal{S} -residuals of β . We have $\rho(\beta) \subseteq \mathcal{R}$. Moreover $\rho(\beta)$ is closed under \equiv (as \equiv is a subset of \sqsubseteq_1 , see Definition 4.3). Hence $\rho(\beta)/\equiv \subseteq \mathcal{R}/\equiv$, therefore $\{\rho(\beta) \mid \beta \in \mathcal{B}\}/\equiv$ is a finite set.

For each $\beta = *\bar{\alpha}(\beta_1, \dots, \beta_n) \in \mathcal{B}$ where $\bar{\alpha}$ is increasing w.r.t the lexicographic ordering of addresses and $\beta_1, \dots, \beta_n \in \mathcal{B}_\varepsilon$, let $\sigma(\beta) = (\beta_1, \dots, \beta_n)$. Since $\{\rho(\beta) \mid \beta \in \mathcal{B}\}/\equiv$ is finite, every infinite sequence over \mathcal{B} contains an infinite subsequence of blueprints with the same set of \mathcal{S} -residuals. By assumption \Subset is an AFR on \mathcal{B}_ε . By theorem 5.5, $\Subset_{\mathfrak{S}}$ is an AFR on the set of all $\{\sigma(\beta) \mid \beta \in \mathcal{B}\}$.

Thus for every infinite sequence $(\beta_i)_{i \in \mathbb{N}}$ over \mathcal{B} there exists i, j such that $i < j$, $\sigma(\beta_i) \Subset_{\mathfrak{S}} \sigma(\beta_j)$ and β_i, β_j have the same set of residuals. For $\sigma(\beta_i) = (\beta_1^i, \dots, \beta_n^i)$ and $\sigma(\beta_j) = (\beta_1^j, \dots, \beta_n^j)$, there exists a subsequence $(\beta_{l_1}^i, \dots, \beta_{l_n}^i)$ of $\sigma(\beta_j)$ such that $\beta_1^i \Subset_{\mathfrak{S}} \beta_{l_1}^i, \dots, \beta_n^i \Subset_{\mathfrak{S}} \beta_{l_n}^i$. There exists also l_{n+1}, \dots, l_{n+k} and two sequences \bar{a} and \bar{b} such that $\beta_i = *\bar{a}(\beta_1^i, \dots, \beta_n^i)$ and $\beta_j = *\bar{b}(\beta_{l_1}^j, \dots, \beta_{l_{n+k}}^j)$. By Lemma 5.10 we have $\beta_i \Subset \beta_j$. \square

5.3. Axiomatic Kruskal theorem and main key-lemma

Definition 5.12. An *abstract decomposition system* is an 8-tuple

$$(\mathcal{T}, \mathcal{L}, \mathcal{V}, \preceq_{\mathcal{T}}, \preceq_{\mathcal{L}}, \preceq_{\mathcal{V}}, \xrightarrow{\quad}, \vdash)$$

where:

- \mathcal{T} is a set of *terms* noted t, u, \dots equipped with a binary relation $\preceq_{\mathcal{T}}$,
- \mathcal{L} is a set of *labels* noted f, g, \dots equipped with a binary relation $\preceq_{\mathcal{L}}$,
- \mathcal{V} is a set of *vectors* noted T, U, \dots equipped with a binary relation $\preceq_{\mathcal{V}}$,
- $\xrightarrow{\quad}$ is a relation on $\mathcal{T} \times \mathcal{L} \times \mathcal{V}$, e.g. $t \xrightarrow{f} T$
- \vdash is a relation on $\mathcal{V} \times \mathcal{T}$, e.g. $T \vdash t$.

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

$$t \triangleright_{\mathcal{T}} u \iff \exists (f, T) \in \mathcal{L} \times \mathcal{V}, \quad t \xrightarrow{f} T \vdash u$$

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

Theorem 5.13. (Melliès) Suppose $(\mathcal{T}, \mathcal{L}, \mathcal{V}, \preceq_{\mathcal{T}}, \preceq_{\mathcal{L}}, \preceq_{\mathcal{V}}, \xrightarrow{\quad}, \vdash)$ satisfies the following properties:

- (Axiom I) There is no infinite chain $t_1 \triangleright_{\mathcal{T}} t_2 \triangleright_{\mathcal{T}} \dots$.
- (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 $u \xrightarrow{f} U \vdash u'$, then $t \preceq_{\mathcal{T}} u$.
- (Axiom IV-bis) For all t, u, f, g, T, U ,
if $t \xrightarrow{f} T$ and $u \xrightarrow{g} U$ 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 5.14. For each finite $\mathcal{S} \subseteq \mathfrak{S}$, the relation \Subset is an AFR on $\mathbb{B}(\mathcal{S})$.

Proof. According to Lemma 5.11 it is sufficient to prove that \Subset is an AFR on $\mathbb{B}_{\varepsilon}(\mathcal{S})$. Let $(\mathcal{T}, \mathcal{L}, \mathcal{V}, \preceq_{\mathcal{T}}, \preceq_{\mathcal{L}}, \preceq_{\mathcal{V}}, \xrightarrow{\bullet}, \vdash)$ be the abstract decomposition system defined as follows.

- The set \mathcal{T} is $\mathbb{B}_{\varepsilon}(\mathcal{S})$; 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 \mathcal{S} of non null arity, the relation $\preceq_{\mathcal{L}}$ is the identity relation on this set.
- The set \mathcal{V} is equal to $\mathbb{B}(\mathcal{S}) \times \mathbb{B}(\mathcal{S})$.
The relation $\preceq_{\mathcal{V}}$ is defined by $(\alpha_1, \alpha_2) \preceq_{\mathcal{V}} (\beta_1, \beta_2)$ if and only if $\alpha_1 \Subset \beta_1$ and $\alpha_2 \Subset \beta_2$.
- The relation $\xrightarrow{\bullet}$ is defined by $\alpha \xrightarrow{\textcircled{\phi}} (\beta_1, \beta_2)$ if and only if $\alpha = \textcircled{\phi}(\beta_1, \beta_2)$.
- The relation \vdash is the least relation satisfying the following condition. If $V = (\alpha_1, \alpha_2)$, $i \in \{1, 2\}$, $\beta_1, \dots, \beta_n \in \mathbb{B}_{\varepsilon}(\mathcal{S})$ and $\alpha_i = *_{\bar{\alpha}}(\beta_1, \dots, \beta_n)$, then $V \vdash \beta_j$ for each $j \in [1, \dots, n]$.

Note that the elements of \mathcal{V} are pairs of blueprints that may be rootless. However if $V \vdash \beta$, then the blueprint β is always a rooted blueprint, thus the relation \vdash is indeed a subset of $\mathcal{V} \times \mathcal{T}$.

(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 $\bar{\alpha}$ 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 5.13 are satisfied. Axiom I is clear. The set of elementary terms is the set of all blueprints consisting into a single formula of \mathcal{S} . 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 $(\alpha_1, \alpha_2) \preceq_{\mathcal{V}} (\beta_1, \beta_2)$ then $\alpha_1 \Subset \beta_1$ and $\alpha_2 \Subset \beta_2$, hence $\textcircled{\psi}(\alpha_1, \alpha_2) \Subset \textcircled{\psi}(\beta_1, \beta_2)$, a fortiori $\textcircled{\psi}(\alpha_1, \alpha_2) \preceq_{\mathcal{T}} \textcircled{\psi}(\beta_1, \beta_2)$, hence Axiom IV-bis is satisfied. We now prove that Axiom V is satisfied. Let $\mathcal{W} \subseteq \mathcal{V}$, let $\mathcal{W}_{\vdash} = \{\beta \in \mathcal{T} \mid \exists (\alpha_1, \alpha_2) \in \mathcal{W}, (\alpha_1, \alpha_2) \vdash \beta\}$. 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) the relation \Subset is an AFR on \mathcal{W}_{\vdash} . Let $\mathcal{B} = \{*\bar{\alpha}(\beta_1, \dots, \beta_n) \mid \forall i \in [1, \dots, n], \beta_i \in \mathcal{W}_{\vdash}\}$. We have $\mathcal{W}_{\vdash} \subseteq \mathbb{B}_{\varepsilon}(\mathcal{S})$. By Lemma 5.11

the relation \in is an AFR on \mathcal{B} . Moreover $\mathcal{W} \subseteq \mathcal{B} \times \mathcal{B}$. By Proposition 5.3.(2) the relation $\preceq_{\mathcal{V}}$ is an AFR on $\mathcal{B} \times \mathcal{B}$, therefore an AFR on \mathcal{W} . \square

Lemma 5.15. 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 $\Xi' \neq \Xi$ such that $\text{dom}(\Xi') \subseteq \text{dom}(\Xi) \cup \{a \cdot (1), a \cdot (2)\}$ and Ξ, Ξ' take the same values on $\text{dom}(\Xi)$. Let \rightsquigarrow be the relation defined by $\Xi \rightsquigarrow \Xi'$ if and only if Ξ' is a step continuation of Ξ . By Lemma 4.5 and the fact that the set of subformulas of ϕ 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 $\{(\varepsilon \mapsto (\varepsilon, \emptyset_{\mathbb{B}}, \phi))\}$, hence it suffices to prove that \mathcal{C} is a finite set. Assume by way of contradiction that \mathcal{C} is infinite. By König's Lemma there exists an infinite sequence $\Xi_1 \rightsquigarrow \Xi_2 \rightsquigarrow \dots$ over \mathcal{C} . The tree $\Xi_{\infty} = \bigcup_{i>0} \Xi_i$ is then an infinite compact ϕ -shadow. Hence there exists an infinite chain of addresses $a_1 < a_2 < \dots$ such that all a_i are nodes of same arity in Ξ_{∞} , labelled with the same subformula of ϕ . If $i < j$ and a_i, a_j are labelled with $(\bar{x}_i, \gamma_i, \psi), (\bar{x}_j, \gamma_j, \psi)$, then we cannot have $\gamma_i \in \gamma_j$, as $\bar{x}_i \in \mathbb{F}(\gamma_j)$ and Ξ_{∞} is compact. A contradiction follows from Lemma 5.14. \square

6. From the shadows to the light

Theorem 6.1. Ticket Entailment is decidable.

Proof. The following propositions are equivalent:

- the formula ϕ is provable in T_{\rightarrow} ,
- the formula ϕ is NF-inhabited (Lemma 1.10),
- there exists a compact NF-inhabitant of ϕ (Lemma 3.8)
- there exists a compact ϕ -shadow of same tree domain as an NF-inhabitant of ϕ (Lemmas 3.8 and 4.13).

By Lemma 5.15, the set of compact ϕ -shadows is effectively computable from ϕ . For each shadow in this set, the subformula property (Lemma 1.6) allows one to decide whether there exists an NF-inhabitant of ϕ of same domain. \square

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

- Anderson, A. R., and Belnap Jr, N. D. (1975) *Entailment: The Logic of Relevance and Necessity, Vol. 1*. Princeton University Press.
- Ackermann, W. (1956) Begründung 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.
- Barendregt, H., *The Lambda Calculus: Its Syntax and Semantics*, Studies in Logic and the Foundations of Mathematics, 103 (Revised ed.), North Holland.
- Handbook of Mathematical Logic* (1977). Edited by Barwise, J., Studies in Logic and Foundations of Mathematics, North-Holland.
- Bezem, M., Klop, J.W., de Vrijer, R., (“Terese”) (2003) Term Rewriting Systems. *Cambridge Tracts in Theoretical Computer Science* **55**, Cambridge 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.
- Bunder, M.W., (1996) Lambda Terms Definable as Combinators. *Theor. Comput. Sci.* **169** (1), 3–21.
- Higman, G. (1952) Ordering by divisibility in abstract algebra. *Proc. London Math. Soc.* **3** (2), 326–336.
- Krivine, J.-L. (1993) *Lambda-calculus, types and models*. Masson.
- 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.
- 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.
- Trigg, P., Hindley, J. R., and Bunder, M. W. (1994) Combinatory abstraction using B , B' and friends. *Theor. Comput. Sci.* **135** (2), 405–422.
- Urquhart, A (1984) The undecidability of entailment and relevant implication. *J. Symb. Log.* **49** (4), 1059–1073.