VERIFICATION OF PTIME REDUCIBILITY FOR SYSTEM F TERMS: TYPE INFERENCE IN DUAL LIGHT AFFINE LOGIC.

VINCENT ATASSI[†], PATRICK BAILLOT[†], AND KAZUSHIGE TERUI[‡]

LIPN, Université Paris 13 / CNRS , France
e-mail address: vincent.atassi@lipn.univ-paris13.fr

LIPN, Université Paris 13 / CNRS , France
e-mail address: patrick.baillot@lipn.univ-paris13.fr

National Institute of Informatics, Tokyo, Japan
e-mail address: terui@nii.ac.jp

ABSTRACT. In a previous work we introduced Dual Light Affine Logic ($DLAL$) ([BT04]) as a variant of Light Linear Logic suitable for guaranteeing complexity properties on lambda-calculus terms: all typable terms can be evaluated in polynomial time by beta reduction and all Ptime functions can be represented. In the present work we address the problem of typing lambda-terms in second-order $DLAL$. For that we give a procedure which, starting with a term typed in system F, determines whether it is typable in $DLAL$ and outputs a concrete typing if there exists any. We show that our procedure can be run in time polynomial in the size of the original Church typed system F term.

1. INTRODUCTION

Several works have studied programming languages with intrinsic computational complexity properties. This line of research, Implicit computational complexity (ICC), is motivated both by the perspective of automated complexity analysis, and by foundational goals, in particular to give natural characterisations of complexity classes, like Ptime or Pspace. Different calculi have been used for this purpose coming from primitive recursion, lambda-calculus, rewriting systems (*e.g.* [BC92, MM00, LM93])... A convenient way to see these systems is in general to describe them as a subset of programs of a larger language satisfying certain criteria: for instance primitive recursive programs satisfying safe/ramified recursion

conditions, rewriting systems admitting a termination ordering and quasi interpretation, etc. . .

Inference. To use such ICC systems for programming purpose it is natural to wish to automatize the verification of the criterion. This way the user could stick to a simple programming language and the compiler would check whether the program satisfies the criterion, in which case a complexity property would be guaranteed.

In general this decision procedure involves finding a certain *witness*, like a type, a proof or a termination ordering. Depending on the system this witness might be useful to provide more precise information, like an actual bound on the running time, or a suitable strategy to evaluate the program. It might be used as a certificate guaranteeing a particular quantitative property of the program.

Light linear logic. In the present work we consider the approach of Light linear logic (LLL) ([Gir98]), a variant of Linear logic which characterises polynomial time computation, within the proofs-as-programs correspondence. It includes higher-order and polymorphism, and can be extended to a naive set theory ([Ter04a]), in which the provably total functions correspond to the class of polynomial time functions.

The original formulation of LLL by Girard was quite complicated, but a first simplification was given by Asperti with Light Affine Logic (LAL) ([AR02]). Both systems have two modalities (one more than Linear logic) to control duplication. There is a forgetful map to system F terms (polymorphic types) obtained by erasing some information (modalities) in types; if an LAL typed term t is mapped to an F-typed term M we also say that t is a *decoration* of M.

So an LAL program can be understood as a system F program, together with a typing guarantee that it can be evaluated in polynomial time once that program is written and evaluated in the right syntax (see below). As system F is a reference system for the study of polymorphically typed functional languages and has been extensively studied, this seems to offer a solid basis to LAL.

However LAL itself is still difficult to handle and following the previous idea for the application of ICC methods, we would prefer to use plain lambda-calculus as a front-end language, without having to worry about the handling of modalities, and instead to delegate the LAL typing part to a type inference engine. The study of this approach was started in [Bai02]. For it to be fully manageable however several conditions should be fulfilled:

(1) a suitable way to execute the lambda-terms with the expected complexity bound,
(2) an efficient type inference,
(3) a typed language which is expressive enough so that a reasonable range of programs is accepted.

The language LAL presents some drawback for the first point, because the LAL typed terms need to be evaluated with a specific graph syntax, *proof-nets*, in order to satisfy the polynomial bound, and plain beta reduction can lead to exponential blow-up. In a previous work ([BT04]) we addressed this issue by defining a subsystem of LAL, called Dual Light Affine Logic ($DLAL$). It is defined with both linear and non-linear function types. It is complete for Ptime just as LAL and its main advantage is that it is also Ptime sound w.r.t. beta reduction: a $DLAL$ term admits a bound on the length of all its beta reduction sequences. Hence $DLAL$ stands as a reasonable substitute for plain LAL for typing issues.

Concerning point 2, as type inference for system F is undecidable ([Wel99]) we don't try to give a fully-fledged type inference algorithm from untyped terms. Instead, to separate the polymorphic part issue from the proper $DLAL$ part one, we assume the initial program

already typed in F. Either the system F typing work is left to the user, or one could use a partial algorithm for system F typing for this preliminary phase.

So the contribution of the present work is to define an efficient algorithm to decide if a system F term can be decorated in a $DLAL$ typed term. This was actually one of the original motivations for defining $DLAL$. We show here that decoration can be performed in polynomial time. This is obtained by taking advantage of intuitions coming from proof-nets, but it is presented in a standard form with a first phase consisting in generating constraints expressing typability and a second phase for constraints solving. One difficulty is that the initial presentation of the constraints involves disjunctions of linear constraints, for which there is no obvious Ptime bound. Hence we provide a specific resolution strategy.

The complete algorithm is already implemented in ML, in a way that follows closely the specification given in the article. It is modular and usable with any linear constraints solver. The code is commented, and available for public download (Section 7). With this program one might thus write terms in system F and verify if they are Ptime and obtain a time upper bound. It should in particular be useful to study further properties of $DLAL$ and to experiment with reasonable size programs.

The point 3 stressed previously about expressivity of the system remains an issue which should be explored further. Indeed the $DLAL$ typing discipline will in particular rule out some nested iterations which might in fact be harmless for Ptime complexity. This is related to the line of work on the study of intensional aspects of Implicit computational complexity ([MM00, Hof03]).

However it might be possible to consider some combination of $DLAL$ with other systems which could allow for more flexibility, and we think a better understanding of $DLAL$ and in particular of its type inference, is a necessary step in that direction.

Related work. Inference problems have been studied for several ICC systems (*e.g.* [Ama05], [HJ03]). Elementary linear logic (EAL, [Gir98, DJ03]) in particular is another variant of Linear logic which characterises Kalmar elementary time and has applications to optimal reduction. Type inference for propositional EAL (without second-order) has been studied in [CM01],[CRdR03],[CDLRdR05] and [BT05] which gives a polynomial time procedure. Type inference for LAL was also investigated, in [Bai02, Bai04]. To our knowledge the present algorithm is however the first one for dealing with polymorphic types in an EAL-related system, and also the first one to infer light types in polynomial time.

This article is an extended version of the paper [ABT06]. Its main novelties are the following ones:

- it is self-contained and complete proofs are provided for the theorems;
- a new section has been added discussing the problem of type inference with data-type domain specification (Section 6);
- the section on the implementation of the algorithm and examples of type inference (Section 7) has been developed, with in particular more examples like the predecessor and polynomials.

2. FROM SYSTEM F TO $DLAL$

The language $\mathcal{L}_F$ of system F types is given by:

$$T, U ::= \alpha \mid T \to U \mid \forall \alpha.T .$$

We assume that a countable set of term variables $x^T, y^T, z^T, \ldots$ is given for each type T. The terms of system F are built as follows (here we write M^T to indicate that the term M has type T):

$$x^T \quad (\lambda x^T.M^U)^{T \to U} \quad ((M^{T \to U})N^T)^U \quad (\Lambda \alpha.M^U)^{\forall \alpha.U} \quad ((M^{\forall \alpha.U})T)^{U[T/\alpha]},$$

with the proviso that when building a term $\Lambda \alpha.M$, α does not occur free in the types of free term variables of M (the *eigenvariable condition*). The set of free variables of M is denoted $FV(M)$.

It is well known that there is no sensible resource bound (i.e. time/space) on the execution of system F terms in general. On the other hand, we are practically interested in those terms which can be executed in polynomial time. However the class $\mathcal{P}$ of such terms is neither recursively enumerable nor co-recursively enumerable. This can be verified for instance in the following way, by reduction of the problem of solvability of Diophantine equations. For each Diophantine equation $P(x) = 0$, build a lambda term M_P such that, when a binary word w is given, $M_P(w)$ returns ϵ if $P(x) = 0$ has an integer solution n with $-|w| \leq n \leq |w|$, and returns a word of length $2^{|w|}$ otherwise. Then $M_P \in \mathcal{P}$ iff $P(x) = 0$ has an integer solution. There is also a complementary reduction, establishing our claim. Actually a stronger result is shown in [BMM07]: the class $\mathcal{P}$ is Σ_2^0-complete.

So we are naturally led to the study of sufficiently large subclasses of $\mathcal{P}$. The system $DLAL$ gives such a class in a purely type-theoretic way.

The language $\mathcal{L}_{DLAL}$ of $DLAL$ types is given by:

$$A, B ::= \alpha \mid A \multimap B \mid A \Rightarrow B \mid \S A \mid \forall \alpha.A .$$

We note $\S^0 A = A$ and $\S^{k+1}A = \S\S^k A$. The erasure map $(.)^-$ from $\mathcal{L}_{DLAL}$ to $\mathcal{L}_F$ is defined by:

$$(\S A)^- = A^-, \quad (A \multimap B)^- = (A \Rightarrow B)^- = A^- \to B^-,$$

and $(.)^-$ commutes with the other connectives. We say $A \in \mathcal{L}_{DLAL}$ is a *decoration* of $T \in \mathcal{L}_F$ if $A^- = T$.

A *declaration* is a pair of the form $x^T : B$ with $B^- = T$. It is often written as $x : B$ for simplicity. A *judgement* is of the form $\Gamma; \Delta \vdash M : A$, where M is a system F term, $A \in \mathcal{L}_{DLAL}$ and Γ and Δ are disjoint sets of declarations. The intuition is that the (free) variables in Γ are duplicable (non-linear), while the ones in Δ are not (they are linear). When Δ consists of $x_1 : A_1, \ldots, x_n : A_n$, $\S\Delta$ denotes $x_1 : \S A_1, \ldots, x_n : \S A_n$. The type assignment rules are given on Figure 1. Here, we assume that the substitution $M[N/x]$ used in ($\S$ e) is *capture-free*. Namely, no free type variable α occurring in N is bound in $M[N/x]$. We write $\Gamma; \Delta \vdash_{DLAL} M : A$ if the judgement $\Gamma; \Delta \vdash M : A$ is derivable.

Examples of concrete programs typable in $DLAL$ are given in Section 7.

Recall that binary words, in $\{0,1\}^*$, can be given in system F the type:

$$W_F = \forall \alpha.(\alpha \to \alpha) \to (\alpha \to \alpha) \to (\alpha \to \alpha) .$$

A corresponding type in $DLAL$, containing the same terms, is given by:

$$W_{DLAL} = \forall \alpha.(\alpha \multimap \alpha) \Rightarrow (\alpha \multimap \alpha) \Rightarrow \S(\alpha \multimap \alpha) .$$

$$\frac{}{; x^{A^-} : A \vdash x^{A^-} : A} \text{ (Id)}$$

$$\frac{\Gamma; x^{A^-} : A, \Delta \vdash M : B}{\Gamma; \Delta \vdash \lambda x^{A^-}.M : A \multimap B} \text{ } (\multimap \text{ i}) \qquad \frac{\Gamma_1; \Delta_1 \vdash M : A \multimap B \quad \Gamma_2; \Delta_2 \vdash N : A}{\Gamma_1, \Gamma_2; \Delta_1, \Delta_2 \vdash (M)N : B} \text{ } (\multimap \text{ e})$$

$$\frac{x^{A^-} : A, \Gamma; \Delta \vdash M : B}{\Gamma; \Delta \vdash \lambda x^{A^-}.M : A \Rightarrow B} \text{ } (\Rightarrow \text{ i}) \qquad \frac{\Gamma; \Delta \vdash M : A \Rightarrow B \quad ; z : C \vdash N : A}{\Gamma, z : C; \Delta \vdash (M)N : B} \text{ } (\Rightarrow \text{ e}) \text{ (*)}$$

$$\frac{\Gamma_1; \Delta_1 \vdash M : A}{\Gamma_1, \Gamma_2; \Delta_1, \Delta_2 \vdash M : A} \text{ (Weak)} \qquad \frac{x_1 : A, x_2 : A, \Gamma; \Delta \vdash M : B}{x : A, \Gamma; \Delta \vdash M[x/x_1, x/x_2] : B} \text{ (Cntr)}$$

$$\frac{; \Gamma, \Delta \vdash M : A}{\Gamma; \S\Delta \vdash M : \S A} \text{ (\S i)} \qquad \frac{\Gamma_1; \Delta_1 \vdash N : \S A \quad \Gamma_2; x : \S A, \Delta_2 \vdash M : B}{\Gamma_1, \Gamma_2; \Delta_1, \Delta_2 \vdash M[N/x] : B} \text{ (\S e)}$$

$$\frac{\Gamma; \Delta \vdash M : A}{\Gamma; \Delta \vdash \Lambda\alpha.M : \forall\alpha.A} \text{ } (\forall \text{ i}) \text{ (**)} \qquad \frac{\Gamma; \Delta \vdash M : \forall\alpha.A}{\Gamma; \Delta \vdash (M)B^- : A[B/\alpha]} \text{ } (\forall \text{ e})$$

(*) $z : C$ can be absent.
(**) α does not occur free in Γ, Δ.

Figure 1: Typing system F terms in $DLAL$

The *depth* $d(A)$ of a $DLAL$ type A is defined by:

$$\begin{array}{rclcrcl}
d(\alpha) & = & 0, & & d(\forall\alpha.B) & = & d(B), \\
d(A \multimap B) & = & max(d(A), d(B)), & & d(\S A) & = & d(A) + 1, \\
d(A \Rightarrow B) & = & max(d(A) + 1, d(B)). & & & &
\end{array}$$

A type A is said to be Π_1 if it does not contain a negative occurrence of $\forall$; like for instance W_{DLAL}.

The fundamental properties of $DLAL$ are the following [BT04]:

Theorem 2.1.

(1) *For every function* $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ *in* $\text{DTIME}[n^k]$, *there exists a closed term* M *of type* $W_{DLAL} \multimap \S^d W_{DLAL}$ *with* $d = O(\log k)$ *representing* f.

(2) *Let* M *be a closed term of system F that has a* Π_1 *type* A *in DLAL. Then* M *can be normalized in* $O(|M|^{2^d})$ *steps by* β-*reduction, where* $d = d(A)$ *and* $|M|$ *is the structural size of* M. *Moreover, the size of any intermediary term occurring in normalization is also bounded by* $O(|M|^{2^d})$.

Although $DLAL$ does not capture all Ptime *algorithms* $\mathcal{P}$, the result 1 guarantees that $DLAL$ is at least expressive enough to represent all Ptime *functions*. In fact, $DLAL$ is as expressive as LAL even at the level of algorithms, because there exists a generic translation from LAL to $DLAL$ given by:

$$(!A)^o = \forall\alpha.((A^o \Rightarrow \alpha) \multimap \alpha), \qquad (.)^o \text{ commutes with other connectives than } !.$$

See the full version of [BT04] (forthcoming) for details.

The result 2 on the other hand implies that if we ignore the embedded types occurring in M, the normal form of M can be computed in polynomial time (*by ordinary* β-*reduction*; that is the difference from LAL).

Now, let $M^{W_F \to W_F}$ be a system F typed term and suppose that we know that it has a $DLAL$ type $W_{DLAL} \multimap \S^d W_{DLAL}$ for some $d \geq 0$. Then, by the consequence of the above theorem, we know that the term M is Ptime. In fact, given a binary word $w \in \{0,1\}^*$, consider its Church coding $\underline{w}$ of type W_{DLAL}. Then we have that $(M)\underline{w}$ has type $\S^d W_{DLAL}$, and can thus be evaluated in $O(|\underline{w}|^{2^{d+1}})$ steps. Thus by assigning a $DLAL$ type to a given system F term, one can *statically verify* a polynomial time bound for its execution.

In order to use $DLAL$ for resource verification of system F terms, we address the following problem:

Problem 2.2 (*DLAL* typing)**.** Given a closed term M^T of system F, determine if there is a decoration A of T such that $\vdash_{DLAL} M : A$.

(Here the closedness assumption is only for readability.)

In the sequel, we show that there is a polynomial time algorithm for solving the $DLAL$ typing problem.

3. Localization of $DLAL$ type inference

To solve the $DLAL$ typing problem, the main obstacle is that the typing rules of $DLAL$ are not syntax-directed. In particular, the rule (§ i) does not correspond to any constructs of system F terms, and the rule (§ e) involves term substitution. These features make local reasoning on types impossible.

To overcome the difficulty, we introduce (following [AR02]) an intermediary syntax which is more informative than system F terms, but not more informative than $DLAL$ derivations themselves (in 3.1). In particular, it has explicit constructs for (§ i). In addition, we replace the global typing rules of $DLAL$ (which involve substitution) with some local typing rules and a set of conditions (in 3.3 and 3.4). We then show that our local typing rules and conditions exactly characterise system F terms typable in $DLAL$ (in 3.5).

3.1. **Pseudo-terms.** We begin with introducing an intermediary syntax, which consists of $DLAL\star$ types and pseudo-terms.

First we decompose $A \Rightarrow B$ into $!A \multimap B$. The language $\mathcal{L}_{DLAL\star}$ of $DLAL\star$ types is given by:

$$A \quad ::= \quad \alpha \mid D \multimap A \mid \forall \alpha.A \mid \S A \; ,$$
$$D \quad ::= \quad A \mid !A \; .$$

There is a natural map $(.)^\star$ from $\mathcal{L}_{DLAL}$ to $\mathcal{L}_{DLAL\star}$ such that $(A \Rightarrow B)^\star = !A^\star \multimap B^\star$ and commutes with the other operations. The erasure map $(.)^-$ from $\mathcal{L}_{DLAL\star}$ to $\mathcal{L}_F$ can be defined as before. A $DLAL\star$ type is called a *bang type* if it is of the form $!A$, and otherwise called a *linear type*. In the sequel, A, B, C stand for linear types, and D for either bang or linear types.

We assume there is a countable set of term variables $x^D, y^D, z^D, \ldots$ for each $D \in \mathcal{L}_{DLAL\star}$. The *pseudo-terms* are defined by the following grammar:

$$t, u ::= x^D \mid \lambda x^D.t \mid (t)u \mid \Lambda \alpha.t \mid (t)A \mid \S t \mid \bar{\S} t \; ,$$

where A is a linear type and D is an arbitrary one. The idea is that $\S$ corresponds to the main door of a $\S$-box (or a !-box) in *proof-nets* ([Gir87, AR02]) while $\bar{\S}$ corresponds to auxiliary doors. But note that there is no information in the pseudo-terms to link occurrences of $\S$ and $\bar{\S}$ corresponding to the same box, nor distinction between $\S$-boxes and !-boxes.

There is a natural erasure map from pseudo-terms to system F terms, which we will also denote by $(.)^-$, consisting in removing all occurrences of $\S, \bar{\S}$, replacing x^D with x^{D^-} and $(t)A$ with $(t)A^-$. When $t^- = M$, t is called a *decoration* of M.

Let t be a pseudo-term and u be a subterm of t. We say that u is a *door-extreme subterm* of t if the following holds: if u is of the form $u = \S u'$ or $u = \bar{\S}u'$ then $\S u$ and $\bar{\S}u$ are not subterms of t.

As an example consider $t = (x \; \S\S y)$. Its door-extreme subterms are $\{t, \; x, \; \S\S y, \; y\}$, and $\S y$ is a subterm of t but not a door-extreme subterm.

For our purpose, it is sufficient to consider the class of *regular* pseudo-terms, given by:

$$u \quad ::= \quad x^D \mid \lambda x^D.t \mid (t)t \mid \Lambda\alpha.t \mid (t)A \;,$$
$$t \quad ::= \quad \S^m u \;,$$

where m is an arbitrary value in $\mathbb{Z}$ and $\S^m t$ denotes $\S \cdots \S t$ (m times) if $m \geq 0$, and $\bar{\S} \cdots \bar{\S}t$ ($-m$ times) if $m < 0$. In other words, a pseudo-term is regular if and only if it does not contain any subterm of the form $\S\bar{\S}u$ or $\bar{\S}\S u$.

3.2. **Pseudo-terms and proof-nets.** In this section we illustrate the links between pseudo-terms and proof-nets. It is independent of the sequel and can be skipped without problem.

The translation $(.)^\star$ from $DLAL$ to LAL gives a mapping on derivations; therefore a $DLAL$ type derivation corresponds to an LAL proof and thus to a proof-net ([AR02]). To facilitate the reading we will use here a 'syntax-tree like' representation for intuitionistic LAL proof-nets.

As an example consider the following term:

$$M = (\lambda f.(f)((f) \; x))((\lambda h.h) \; g) \;.$$

It can be given the typing $x : \S\alpha \vdash M : \S\alpha$, with the derivation of Fig. 2. The corresponding (intuitionistic) proof-net is given on Fig. 4. For readers more familiar with the classical representation of proof-nets (in the style of *e.g.* [AR02]), the corresponding representation is given on Fig. 3.

$$\dfrac{\dfrac{\dfrac{; f_2 : \alpha \multimap \alpha \vdash f_2 : \alpha \multimap \alpha \qquad ; x : \alpha \vdash x : \alpha}{\dfrac{; f_2 : \alpha \multimap \alpha, x : \alpha \vdash (f_2) \; x : \alpha \qquad\qquad ; f_1 : \alpha \multimap \alpha \vdash f_1 : \alpha \multimap \alpha}{\dfrac{; f_1 : \beta, f_2 : \beta, x : \alpha \vdash (f_1) \; ((f_2) \; x) : \alpha}{\dfrac{f_1 : \beta, f_2 : \beta; x : \S\alpha \vdash (f_1) \; ((f_2) \; x) : \S\alpha}{\dfrac{f : \beta; x : \S\alpha \vdash (f) \; ((f) \; x) : \S\alpha}{; x : \S\alpha \vdash \lambda f.(f) \; ((f) \; x) : \beta \Rightarrow \S\alpha}}}}}{} \qquad \dfrac{\dfrac{; h : \beta \vdash h : \beta}{\dfrac{; \vdash \lambda h.h : \beta \multimap \beta \qquad ; g : \beta \vdash g : \beta}{; g : \beta \vdash (\lambda h.h) \; g : \beta}}}{}}{g : \beta; x : \S\alpha \vdash (\lambda f.(f) \; ((f) \; x))((\lambda h.h) \; g) : \S\alpha}$$

where $\beta = \alpha \multimap \alpha$.

Figure 2: Example: $DLAL$ derivation for M.

The pseudo-term corresponding to the previous derivation is:

$$t = (\lambda f.\S(\bar{\S}f)((\bar{\S}f) \; \bar{\S}x))\S((\lambda h.h) \; \bar{\S}g) \;.$$
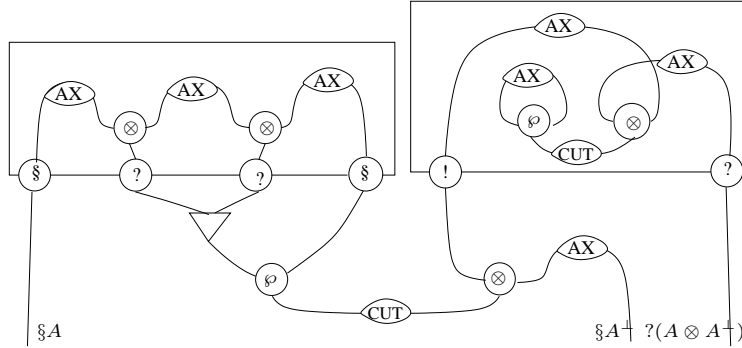
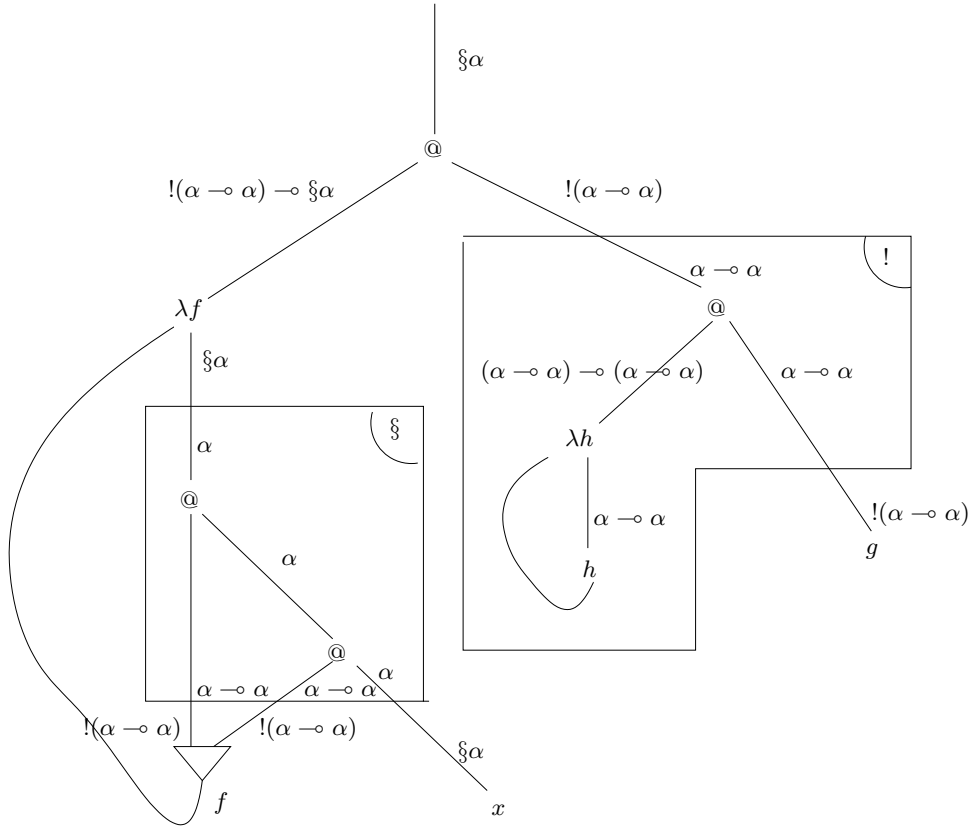Figure 3: Classical Proof-Net corresponding to the example.

Figure 4: Example of Proof-Net.

It is represented graphically on Fig. 5: to $\S$ and $\bar{\S}$ correspond respectively opening and closing doors.

In a proof-net, a box can be thought of as an opening door connected to a certain number (possibly none) of closing doors. If in the proof-net of Fig. 4 we disconnect opening doors from closing doors we get the graph of Fig. 5, corresponding to the pseudo-term.

Figure 5: Example: graph corresponding to pseudo-term.

Our method for type inference relies on a procedure for deciding if a pseudo-term comes from a $DLAL$ derivation. This essentially corresponds to deciding if a pseudo-term corresponds to a proof-net, that is to say in particular deciding whether opening and closing doors can be matched in such a way to yield a correct distribution of boxes.

3.3. **Local typing condition.** We now describe a way to assign types to pseudo-terms in a locally compatible way. A delicate point in $DLAL$ is that it is sometimes natural to associate *two* types to one variable x. For instance, we have $x : A ; \vdash_{DLAL} x : \S A$ in $DLAL$, and this can be read as $x : !A \vdash x : \S A$ in terms of $DLAL\star$ types. We thus distinguish between the *input types*, which are inherent to variables, and the *output types*, which are inductively assigned to all pseudo-terms. The condition (i) below is concerned with the output types. In the sequel, D° denotes $\S A$ if D is of the form $!A$, and otherwise denotes D itself.

A pseudo-term t satisfies the *local typing condition* if the following holds:

(i) one can inductively assign a *linear* type to each subterm of t in the following way (here the notation $t : A$ indicates that t has the output type A):

$$\frac{}{x^D : D^\circ} \quad \frac{t : B}{\lambda x^D.t : D \multimap B} \quad \frac{t : D \multimap B \quad u : A \quad D^\circ = A}{(t)u : B}$$

$$\frac{t : A}{\S t : \S A} \quad \frac{t : \S A}{\bar{\S} t : A} \quad \frac{t : A}{\Lambda\alpha.t : \forall\alpha.A} \quad \frac{t : \forall\alpha.A}{(t)B : A[B/\alpha]}$$

(ii) when a variable x occurs more than once in t, it is typed as $x^{!A}$,
(iii) t satisfies the eigenvariable condition. Namely, for any subterm of the form $\Lambda\alpha.u$ and any free term variable x^D in u, α does not occur free in D.

We also say that t is *locally typed*.

The local typing rules are syntax-directed, and assign a unique type to each pseudo-term whenever possible. Notice that there is a type mismatch between D and A in the application rule when D is a bang type. This mismatch will be settled by the *bang condition* below.

3.4. **Boxing conditions.** It is clear that local typability is not a sufficient condition for typability in $DLAL$, as it does not ensure that doors $\S, \bar{\S}$ are well placed so that boxes can be built around them. Moreover, it does not distinguish $\S$- and !- boxes. We therefore impose additional conditions on locally typed pseudo-terms.

We consider words over the language $\mathcal{L} = \{\S, \bar{\S}\}^*$ and $\leq$ the prefix ordering. If t is a pseudo-term and u is an occurrence of subterm in t, let $\mathsf{doors}(t, u)$ be the word inductively defined as follows. If $t = u$, let $\mathsf{doors}(t, u) = \epsilon$. Otherwise:

$$\begin{aligned}
\mathsf{doors}(\S t, u) &= \S :: (\mathsf{doors}(t, u)), \\
\mathsf{doors}(\bar{\S} t, u) &= \bar{\S} :: (\mathsf{doors}(t, u)), \\
\mathsf{doors}(\lambda y^D.t_1, u) &= \mathsf{doors}(\Lambda\alpha.t_1, u) = \mathsf{doors}((t_1)A, u) = \mathsf{doors}(t_1, u), \\
\mathsf{doors}((t_1)t_2, u) &= \mathsf{doors}(t_i, u), \text{ where } t_i \text{ is the subterm containing } u.
\end{aligned}$$

That is to say, $\mathsf{doors}(t, u)$ collects the modal symbols $\S, \bar{\S}$ occurring on the path from the root to the node u in the term tree of t. We define a map $s : \mathcal{L} \to \mathbb{Z}$ by:

$$\begin{aligned}
s(\epsilon) &= 0, \\
s(\S :: l) &= 1 + s(l), \\
s(\bar{\S} :: l) &= -1 + s(l).
\end{aligned}$$

A word $l \in \mathcal{L}$ is *weakly well-bracketed* if $\forall l' \leq l, s(l') \geq 0$, and is *well-bracketed* if this condition holds and moreover $s(l) = 0$: think of $\S$ and $\bar{\S}$ resp. as opening and closing brackets.

Bracketing condition. Let t be a pseudo-term. We say that t satisfies the *bracketing condition* if:

(i) for any occurrence of free variable x in t, $\mathsf{doors}(t, x)$ is well-bracketed;
(ii) for any occurrence of an abstraction subterm $\lambda x.v$ of t:
  (ii.a) $\mathsf{doors}(t, \lambda x.v)$ is weakly well-bracketed, and
  (ii.b) for any occurrence of x in v, $\mathsf{doors}(v, x)$ is well-bracketed.

This condition is sufficient to rule out the canonical morphisms for dereliction and digging, which are not valid in $DLAL$ (nor in EAL):

$$\lambda x^{\S A}.\bar{\S} x : \S A \multimap A, \qquad \lambda x^{\S A}.\S x : \S A \multimap \S\S A .$$

Since $\mathsf{doors}(\bar{\bar{\S}}x, x) = \bar{\bar{\S}}$ and $\mathsf{doors}(\S x, x) = \S$, they do not satisfy the bracketing condition (ii.b).

Remark 3.1. On the graph representation of pseudo-terms, conditions (i), (ii.a) and (ii.b) can be visualised as conditions of bracketing holding on certain paths of the graph: for instance condition (ii.b) means that any (top-down) path from a λx binder to an edge corresponding to an occurrence of x is well-bracketed (considering the opening and closing doors). For instance the pseudo-term graph of Fig. 5 satisfies these conditions; we show on the Figure two paths γ_1, γ_2 that have to be well-bracketed according to (ii.b).

Bang condition. Let t be a locally typed pseudo-term. A subterm u is called a *bang subterm* of t if it occurs as $(t')u$ in t for some $t' : !A \multimap B$. We say that t satisfies the *bang condition* if for any bang subterm u of t,

(i) u contains at most one occurrence of free variable $x^{!C}$, and it has a bang type $!C$.

(ii) for any subterm v of u such that $v \neq u$ and $v \neq x$, $s(\mathsf{doors}(u, v)) \geq 1$.

This condition is sufficient to rule out the canonical morphisms for monoidalness $!A \otimes !B \multimap !(A \otimes B)$ and $\S A \multimap !A$ which are not valid in LAL (the following terms and types are slightly more complicated since $\mathcal{L}_{DLAL\star}$ does not explicitly contain a type of the form $A \multimap !B$):

$$\lambda x^{!(A \multimap B)}.\lambda y^{!B \multimap C}.\lambda z^{!A}.(y)\S((\bar{\S}x)\bar{\S}z) \,, \qquad \lambda x^{\S A}.\lambda y^{!A \multimap B}.(y)\S(\bar{\S}x) \,.$$

In the first pseudo-term, the bang subterm $\S((\bar{\S}x)\bar{\S}z)$ contains more than one free variable. In the second pseudo-term, the bang subterm $\S(\bar{\S}x)$ has a free variable x with a linear type. Hence they both violate the bang condition (i).

Remark 3.2. Note that the bracketing and bang conditions imply that, if u is a bang subterm of t and x is a free variable in u, then we have:

$$s(\mathsf{doors}(u, x)) = 0.$$

Indeed, we know that there is a subterm w of t such that $\mathsf{doors}(w, x)$ is well-bracketed (w is of the form $\lambda x.v$, or $w = t$ if x is free in t). Therefore $s(\mathsf{doors}(w, u)) \geq 0$ and $s(\mathsf{doors}(w, x)) = 0$, so $s(\mathsf{doors}(u, x)) \leq 0$. Let u' be the smallest subterm of u strictly containing x. We have $s(\mathsf{doors}(u, u')) \geq 1$ and $-1 \leq s(\mathsf{doors}(u', x)) \leq 1$, so $s(\mathsf{doors}(u, x)) = 0$.

Remark 3.3. The intuition behind the Bang condition might be easier to understand on the graph representation of pseudo-terms. The idea is that in a proof-net, the argument of a non-linear application should be enclosed in a box, with at most one free variable, as in the Example of Fig. 4. This is enforced on the pseudo-term by Bang conditions (i) and (ii). Condition (ii) indeed forces the root of the argument of the application to start with an opening door, and this opening door can only be matched by a closing door on the edge corresponding to the free variable x.

Λ-Scope condition. The previous conditions, bracketing and bang, would be enough to deal with boxes in the propositional fragment of $DLAL$. For handling second-order quantification though, we need a further condition to take into account the sequentiality enforced by the quantifiers. For instance consider the following two formulas (the second one is known as *Barcan's formula*):

$$(1) \ \S \forall \alpha.A \multimap \forall \alpha.\S A \,, \qquad (2) \ \forall \alpha.\S A \multimap \S \forall \alpha.A \,.$$

Assuming α occurs free in A, formula (1) is provable while (2) is not. Observe that we can build the following pseudo-terms which are locally typed and have respectively type (1) and (2):

$$t_1 = \lambda x^{\S\forall\alpha.A}.\Lambda\alpha.\S((\bar{\S}x)\alpha) , \qquad t_2 = \lambda x^{\forall\alpha.\S A}.\S\Lambda\alpha.\bar{\S}((x)\alpha) .$$

Both pseudo-terms satisfy the previous conditions, but t_2 does not correspond to a $DLAL$ derivation.

Let u be a locally typed pseudo-term. We say that u *depends on* α if the type of u contains a free variable α. We say that a locally typed pseudo-term t satisfies the Λ-*scope condition* if: for any subterm $\Lambda\alpha.u$ of t and for any subterm v of u that depends on α, $\mathsf{doors}(u,v)$ is weakly well-bracketed.

Coming back to our example: t_1 satisfies the Λ-scope condition, but t_2 does not, because $(x)\alpha$ depends on α and nevertheless $\mathsf{doors}(\bar{\S}((x)\alpha),(x)\alpha) = \bar{\S}$ is not weakly well-bracketed.

We now give a reformulation of the Bang condition (ii), which will be useful later:

Lemma 3.4. *Assume t is a regular pseudo-term that satisfies the Bracketing condition and that u is a bang subterm of t. Then the Bang condition (ii) holds for u iff:*

for any door-extreme subterm v of u such that $v \neq u$, $v \neq x$, $s(\mathsf{doors}(u,v)) \geq 1$; and $s(\mathsf{doors}(u,x)) = 0$.

Proof. The 'only-if' direction follows from the fact that each door-extreme subterm is a subterm, and from Remark 3.2.

To show the 'if' direction, let v be a subterm of u such that $v \neq u$, $v \neq x$. If v is a door-extreme subterm then $s(\mathsf{doors}(u,v)) \geq 1$. Otherwise there are two door-extreme subterms v_1, v_2 of u such that:

- $v_1 \subseteq v \subseteq v_2$, where $\subseteq$ denotes the subterm relation,
- v_1 is an immediate distinct door-extreme subterm of v_2.

We have:

$$\text{either} \quad s(\mathsf{doors}(u,v_2)) > s(\mathsf{doors}(u,v)) > s(\mathsf{doors}(u,v_1)),$$
$$\text{or} \quad s(\mathsf{doors}(u,v_2)) < s(\mathsf{doors}(u,v)) < s(\mathsf{doors}(u,v_1)).$$

Moreover we know that $s(\mathsf{doors}(u,v_2)) \geq 1$ and $s(\mathsf{doors}(u,v_1)) \geq 0$ (because if $v_1 = x$ then $s(\mathsf{doors}(u,v_1)) = 0$, and otherwise $s(\mathsf{doors}(u,v_1)) \geq 1$). Therefore we have $s(\mathsf{doors}(u,v)) \geq 1$. $\qquad\square$

3.5. **Correctness of the conditions.** So far we have introduced four conditions on pseudo-terms: local typing, bracketing, bang and Λ-scope. Let us call a regular pseudo-term satisfying these conditions *well-structured*. It turns out that the well-structured pseudo-terms exactly correspond to the $DLAL$ typing derivations.

Lemma 3.5. *Let M_0 be a system F term. If*

$$x_1 : A_1, \ldots, x_m : A_m; \ y_1 : B_1, \ldots, y_n : B_n \vdash_{DLAL} M_0 : C,$$

then there is a decoration t of M_0 with type $C^\star$ and with free variables $x_1^{!A_1^\star}, \ldots, x_m^{!A_m^\star}$, $y_1^{B_1^\star}, \ldots, y_n^{B_n^\star}$ which is well-structured.

Proof. One can build a (possibly non-regular) decoration M_0^+ of M_0 by induction on the derivation. Depending on the last typing rule used (see Figure 1), M_0^+ takes one of the following forms:

(Id)	$x^{A^\star}$		
$(\multimap$ i$)$	$\lambda x^{A^\star}.M^+$	$(\multimap$ e$)$	$(M^+)N^+$
$(\Rightarrow$ i$)$	$\lambda x^{!A^\star}.M^+$	$(\Rightarrow$ e$)$	$(M^+)\S N^+[\bar{\S}z^{!C^\star}/z]$
(Weak)	M^+	(Cntr)	$M^+[x/x_1, x/x_2]$
$(\forall$ i$)$	$\Lambda\alpha.M^+$	$(\forall$ e$)$	$(M^+)B^\star$
$(\S$ i$)$	$\S M^+[\bar{\S}x_i^{!A_i^\star}/x_i, \bar{\S}y_j^{\S B_j^\star}/y_j]$	$(\S$ e$)$	$M^+[N^+/x]$,

where M^+ in $(\S$ i$)$ has free variables $x_1^{A_1}, \ldots, x_m^{A_m}, y_1^{B_1}, \ldots, y_n^{B_n}$.

It is easy to verify that M_0^+ admits local typing with the output type $C^\star$ and has the free variables $x_1^{!A_1^\star}, \ldots, x_m^{!A_m^\star}, y_1^{B_1^\star}, \ldots, y_n^{B_n^\star}$.

Moreover, one can show by induction on the derivation that M_0^+ satisfies the bracketing, bang and Λ-scope conditions. Let us just remark:

- The rules $(\multimap$ i$)$ and $(\Rightarrow$ i$)$ introduce new abstraction terms $\lambda x^{A^\star}.M^+$ and $\lambda x^{!A^\star}.M^+$, respectively. The bracketing condition (ii.b) for them follows from the bracketing condition (i) for M^+.

- The rule $(\Rightarrow$ e$)$ introduces a new bang term $\S N^+[\bar{\S}z^{!C^\star}/z]$. It satisfies the bang condition (i) because N contains at most one linear variable z. The condition (ii) holds because N^+ satisfies the bracketing condition, and thus we have $\mathsf{doors}(N^+, u) \geq 0$ for any subterm occurrence u.

  Observe also that the bracketing condition is maintained because the $\S$ added before N^+ and the $\bar{\S}$ added before the variable z match each other, so z remains well-bracketed, and condition (i) is preserved; since we add a $\S$ on N, condition (ii.a) is maintained as well; and as bounded variables of N are left unmodified, (ii.b) is obviously still verified.

  We also have to make sure that the substitution of $\bar{\S}z$ for z does not violate the Λ-scope condition. It follows from the eigenvariable condition for N, which ensures that z does not depend on any bound type variable.

- The rule (Cntr) conforms to the local typing condition (ii).

- The rule $(\forall$ i$)$ introduces a new type abstraction $\Lambda\alpha.M^+$. The Λ-scope condition for it follows from the bracketing condition for M^+.

- The rule $(\S$ i$)$ clearly preserves the bracketing condition. It is also clear that the substitution involved does not cause violation of the bang condition (as x_i's and y_j's have linear types in M^+, and thus do not appear in any bang term), and the Λ-scope condition (as x_i's and y_j's do not depend on any bound type variable due to the eigenvariable condition).

- The rule $(\S$ e$)$ involves substitution. The term $M^+[N^+/x]$ satisfies the Λ-scope condition since substitution is capture-free, and thus no free type variable in N^+ becomes bound in $M^+[N^+/x]$.

Finally, the required regular pseudo-term t is obtained from M_0^+ by applying the following rewrite rules as many times as possible:

$$\bar{\S}\S u \longrightarrow u, \qquad \S\bar{\S}u \longrightarrow u.$$

It is clear that all the conditions are preserved by these rewritings. $\qquad\square$

To show the converse direction, the following Lemma plays a crucial role:

Lemma 3.6 (Boxing). *If $\S t : \S A$ is a well-structured pseudo-term, then there exist pseudo-terms $v : A$, $u_1 : \S B_1$, ..., $u_n : \S B_n$, unique (up to renaming of v's free variables) such that:*

   (1) *$FV(v) = \{x_1^{B_1}, \ldots, x_n^{B_n}\}$ and each x_i occurs exactly once in v,*
   (2) *$\S t = \S v[\bar{\S} u_1/x_1, \ldots, \bar{\S} u_n/x_n]$ (substitution is assumed to be capture-free),*
   (3) *$v, u_1, \ldots, u_n$ are well-structured.*

Proof. Given $\S t$, assign an index to each occurrence of $\S$ and $\bar{\S}$ in $\S t$ to distinguish occurrences (we assume that the outermost $\S$ has index 0). By traversing from the root of the syntactic tree, one can find closing brackets $\bar{\S}_1, \ldots, \bar{\S}_n$ that match the opening bracket $\S_0$ in $\S_0 t$. Replace each $\bar{\S}_i u_i : B_i$ with a fresh and distinct free variable $x_i^{B_i}$ ($1 \le i \le n$), and let $\S v$ be the resulting pseudo-term. This way one can obtain $v, u_1, \ldots, u_n$, such that condition (2) holds.

Strictly speaking, it has to be checked that the substitution does not cause capture of type or term variables. Let us consider the case of type variables: suppose that u_i contains a subterm s that depends on a bound variable α of $\S v$. Then $\S_0 t$ contains a subterm of the form $\Lambda \alpha. v'[\bar{\S}_i u_i[s]/x_i]$. However, $\mathsf{doors}(v'', s)$ with $v'' = v'[\bar{\S}_i u_i[s]/x_i]$ cannot be weakly well-bracketed because $\bar{\S}_i$ has to match the outermost opening bracket $\S_0$. This contradicts the Λ-scope condition for $\S_0 t$. Hence the case of type variable capture is solved. A similar argument using the bracketing condition shows that the substitutions do no cause term variable capture either.

As to condition (1), we claim that v does not contain a free variable other than $x_1, \ldots, x_n$. If there is any, say y, then it is also a free variable of t, thus the bracketing condition for $\S_0 t$ implies that $\mathsf{doors}(\S_0 t, y)$ is well-bracketed, and thus there is a closing bracket that matches $\S_0$ in the path from $\S_0 t$ to y. That means that y belongs to one of u_1, ..., u_n, not to v. A contradiction.

Let us now check condition (3). As to the bracketing condition for v, observe that $s(\mathsf{doors}(\S_0 t, \bar{\S}_i u_i)) = 1$ for each $1 \le i \le n$. Therefore, $s(\mathsf{doors}(\S_0 v, x_i)) = 1$, and hence $s(\mathsf{doors}(v, x_i)) = 0$. This shows that v satisfies the bracketing condition (i). (ii.a) and (ii.b) are easy. As for u_i ($1 \le i \le n$), notice that $s(\mathsf{doors}(\S_0 t, u_i)) = 0$. This means that for any subterm occurrence u' of u_i, we have $s(\mathsf{doors}(u_i, u')) = s(\mathsf{doors}(\S_0 t, u'))$. Therefore, the bracketing condition for u_i reduces to that for $\S_0 t$.

The Λ-scope condition for $v, u_1, \ldots, u_n$ easily reduces to that for $\S_0 t$.

As to the local typing condition, the only nontrivial point to check is whether v satisfies the eigenvariable condition. Suppose that x_i depends on a variable α which is bound in v. Then $\S_0 t$ contains a subterm of the form $\Lambda \alpha. v'[\bar{\S}_i u_i/x_i]$ and u_i depends on α. However, $\mathsf{doors}(v'', u_i)$ with $v'' = v'[\bar{\S}_i u_i/x_i]$ cannot be weakly well-bracketed because $\bar{\S}_i$ should match the outermost opening bracket $\S_0$. This contradicts the Λ-scope condition for $\S_0 t$.

To show the bang condition for v (it is clear for $u_1, \ldots, u_n$), suppose that v contains a bang subterm v'. We claim that v' does not contain variables $x_1, \ldots, x_n$. If it contains any, say x_i, then $\S_0 t$ contains $v'' = v'[\bar{\S}_i u_i/x_i]$ and the bang condition for $\S_0 t$ implies that $s(\mathsf{doors}(v'', \bar{\S}_i u_i)) \ge 1$. On the other hand, we clearly have $s(\mathsf{doors}(\S_0 t, v'')) \ge 1$ because v'' contains the closing bracket $\bar{\S}_i$ that matches $\S_0$. As a consequence, we have $s(\mathsf{doors}(\S_0 t, \bar{\S}_i u_i)) \ge 2$. This means that $\bar{\S}_i$ does not match $\S_0$, a contradiction. As a consequence, v' does not contain $x_1, \ldots, x_n$. So v' occurs in $\S_0 t$, and therefore satisfies the bang condition. $\square$

Now we can prove:

Theorem 3.7. *Let M be a system F term. Then*

$$x_1 : A_1, \ldots, x_m : A_m; \ y_1 : B_1, \ldots, y_n : B_n \vdash_{DLAL} M : C$$

if and only if there is a decoration t of M with type $C^\star$ and with free variables $x_1^{!A_1^\star}, \ldots, x_m^{!A_m^\star}$, $y_1^{B_1^\star}, \ldots, y_n^{B_n^\star}$ which is well-structured.

Proof. The 'only-if' direction has already been proved. As for the 'if' direction, we prove the following: if a pseudo-term $t : C^\star$ is well-structured and $FV(t) = \{x_1^{!A_1^\star}, \ldots, x_m^{!A_m^\star}, y_1^{B_1^\star}, \ldots, y_n^{B_n^\star}\}$ for some $DLAL$ types $A_1, \ldots, A_m, B_1, \ldots, B_n$, then we have $\Gamma; \Delta \vdash_{DLAL} t^- : C$, where $\Gamma = x_1 : A_1, \ldots, x_m : A_m$ and $\Delta = y_1 : B_1, \ldots, y_n : B_n$. The proof proceeds by induction on the size of t.

- When $t = x_i^{!A_i^\star}$ for some $1 \leq i \leq m$, $C^\star$ must be $\S A_i^\star$ by local typing, and we have $\Gamma; \Delta \vdash_{DLAL} x_i : \S A_i$. Likewise, if $t = y_j^{B_j^\star}$ for some $1 \leq j \leq n$, we have $\Gamma; \Delta \vdash_{DLAL} y_j : B_j$.
- When $t = \lambda z^{!A_0^\star}.u : !A_0^\star \multimap C_0^\star$, $u : C_0^\star$ is also well-structured; observe in particular that the bracketing condition for t implies the same for u. By induction hypothesis, we have $z : A_0, \Gamma; \Delta \vdash_{DLAL} u^- : C_0$, and hence

$$\Gamma; \Delta \vdash_{DLAL} \lambda z^{A_0^-}.u^- : A_0 \Rightarrow C_0.$$

  The case when z has a linear type is similar.
- When $t = \Lambda\alpha.u : \forall\alpha.C_0^\star$, $u : C_0^\star$ is also well-structured. Hence one can argue as above; notice in particular that the eigenvariable condition on t ensures that one can apply the rule ($\forall$ i) to u^-.
- When $t = (u)B^\star : C_0^\star[B^\star/\alpha]$, $u : \forall\alpha.C_0^\star$ is well-structured, and the induction hypothesis yields $\Gamma; \Delta \vdash_{DLAL} u^- : \forall\alpha.C_0$. We therefore obtain $\Gamma; \Delta \vdash_{DLAL} (u^-)B^- : C_0[B/\alpha]$.
- It is impossible to have $t = \bar{\S}u$, because it clearly violates the bracketing condition.
- When $t = \S t' : \S C_0^\star$, the Boxing Lemma gives us well-structured terms $v : C_0^\star$, $u_1 : \S C_1^\star$, $\ldots$, $u_k : \S C_k^\star$ such that
  (1) $FV(v) = \{z_1^{C_1^\star}, \ldots, z_k^{C_k^\star}\}$ and each z_i occurs exactly once in v,
  (2) $\S t' = \S v[\bar{\S}u_1/z_1, \ldots, \bar{\S}u_k/z_k]$.
  By the induction hypothesis, we have

$$; z_1 : C_1, \ldots, z_k : C_k \vdash_{DLAL} v^- : C_0 \qquad \text{and} \qquad \Gamma; \Delta_i \vdash_{DLAL} u_i^- : \S C_i$$

  for $1 \leq i \leq k$, where $(\Delta_1, \ldots, \Delta_k)$ is a partition of Δ such that each Δ_i contains the free variables occurring in u_i. Hence by rules ($\S$ i), ($\S$ e) and (Cntr), we obtain

$$\Gamma; \Delta \vdash_{DLAL} v^-[u_1^-/z_1, \ldots, u_k^-/z_k] : \S C_0.$$

- When $t = (t')t''$ and t'' is not a bang subterm, one can argue as above. When t'' is a bang subterm, t' and t'' are typed as $t' : !A^\star \multimap C^\star$ and $t'' : \S A^\star$. They are well-structured, and moreover:
  (i) t'' contains at most one free variable $x_i^{!A_i^\star}$, which is among $\{x_1, \ldots, x_m\}$,
  (ii) for any subterm v of t'' such that $v \neq t''$ and $v \neq x_i$, $s(\text{doors}(u, v)) \geq 1$.

By the induction hypothesis on t' (and by the fact that t'' does not contain any variable of linear type), we have

$$\Gamma; \Delta \vdash_{DLAL} (t')^- : A \Rightarrow C.$$

On the other hand, the condition (ii) above entails that t'' is either the variable x_i or of the form $\S u$. In the former case, $A^\star = A_i^\star$ and we have:

$$\frac{\Gamma; \Delta \vdash (t')^- : A \Rightarrow C \quad ; x_i : A \vdash x_i : A}{\Gamma; \Delta \vdash (t')^- x_i : C}.$$

In the latter case, we can apply the Boxing Lemma. Then the conditions (i) and (ii) entail that there is a well-structured term $v : A^\star$ with a free variable z such that $t'' = \S u = \S v[\bar{\S} x_i / z]$. Notice here that z has a linear type $A_i^\star$, and by renaming, one can assume w.l.o.g. that $z = x_i$ in v. Therefore, we obtain:

$$\frac{\Gamma; \Delta \vdash (t')^- : A \Rightarrow C \quad ; x_i : A_i \vdash v^- : A}{\Gamma; \Delta \vdash (t')^- v^- : C}.$$

$\square$

As a consequence of Theorem 3.7, our $DLAL$ typing problem (Problem 2.2) boils down to:

Problem 3.8 (decoration). Given a system F term M, determine if there exists a decoration t of M which is well-structured.

4. Parameterization and constraints generation

To solve the decoration problem (Problem 3.8), one needs to explore an infinite set of decorations. This can be effectively done by introducing an abstract kind of types and terms with symbolic parameters (in 4.1), and expressing the conditions for such abstract terms to be materialized by boolean and integer constraints over those parameters (in 4.2 and in 4.3).

4.1. **Parameterized terms and instantiations.** Let us begin with introducing a term syntax with parameters. We use two sorts of parameters: *integer parameters* $\mathbf{n}, \mathbf{m}, \ldots$ meant to range over $\mathbb{Z}$, and *boolean parameters* $\mathbf{b_1}, \mathbf{b_2}, \ldots$ meant to range over $\{0, 1\}$. We also use *linear combinations of integer parameters* $\mathbf{c} = \mathbf{n_1} + \cdots + \mathbf{n_k}$, where $k \geq 0$ and each $\mathbf{n_i}$ is an integer parameter. In case $k = 0$, it is written as $\mathbf{0}$.

The set of *parameterized types* (*p-types* for short) is defined by:

$$
\begin{aligned}
F &\quad ::=\quad \alpha \mid D \multimap A \mid \forall \alpha. A \,, \\
A &\quad ::=\quad \S^{\mathbf{c}} F \,, \\
D &\quad ::=\quad \S^{\mathbf{b},\mathbf{c}} F \,.
\end{aligned}
$$

where $\mathbf{b}$ is a boolean parameter and $\mathbf{c}$ is a linear combination of integer parameters. Informally speaking, the parameter $\mathbf{c}$ in $\S^{\mathbf{b},\mathbf{c}} F$ stands for the number of modalities ahead of the type, while the boolean parameter $\mathbf{b}$ serves to determine whether the first modality, if any, is $\S$ or $!$. In the sequel, A, B, C stand for *linear p-types* of the form $\S^{\mathbf{c}} F$, and D for *bang p-types* of the form $\S^{\mathbf{b},\mathbf{c}} F$, and E for arbitrary p-types.

When A is a linear p-type $\S^{\mathbf{c}}F$, $B[A/\alpha]$ denotes a p-type obtained by replacing each $\S^{\mathbf{c}'}\alpha$ in B with $\S^{\mathbf{c}'+\mathbf{c}}F$ and each $\S^{\mathbf{b},\mathbf{c}'}\alpha$ with $\S^{\mathbf{b},\mathbf{c}'+\mathbf{c}}F$. When $D = \S^{\mathbf{b},\mathbf{c}}F$, D° denotes the linear p-type $\S^{\mathbf{c}}F$.

We assume that there is a countable set of variables $x^D, y^D, \ldots$ for each bang p-type D. The *parameterized pseudo-terms* (*p-terms* for short) $t, u \ldots$ are defined by the following grammar:

$$u \quad ::= \quad x^D \mid \lambda x^D.t \mid (t)t \mid \Lambda\alpha.t \mid (t)A ,$$
$$t \quad ::= \quad \S^{\mathbf{m}}u .$$

We denote by $par^{bool}(t)$ the set of boolean parameters of t, and by $par^{int}(t)$ the set of integer parameters of t. An *instantiation* $\phi = (\phi^b, \phi^i)$ for a p-term t is given by two maps $\phi^b : par^{bool}(t) \to \{0,1\}$ and $\phi^i : par^{int}(t) \to \mathbb{Z}$. The map ϕ^i can be naturally extended to linear combinations $\mathbf{c} = \mathbf{n_1} + \cdots + \mathbf{n_k}$ by $\phi^i(\mathbf{c}) = \phi^i(\mathbf{n_1}) + \cdots + \phi^i(\mathbf{n_k})$. An instantiation ϕ is said to be *admissible* for a p-type E if for any linear combination $\mathbf{c}$ occurring in E, we have $\phi^i(\mathbf{c}) \geq 0$, and moreover whenever $\S^{\mathbf{b},\mathbf{c}}F$ occurs in E, $\phi^b(\mathbf{b}) = 1$ implies $\phi^i(\mathbf{c}) \geq 1$. When ϕ is admissible for E, a type $\phi(E)$ of $DLAL\star$ is obtained as follows:

$$\phi(\S^{\mathbf{c}}F) \;=\; \S^{\phi^i(\mathbf{c})}\phi(F), \qquad \phi(\S^{\mathbf{b},\mathbf{c}}F) \;=\; \S^{\phi^i(\mathbf{c})}\phi(F) \qquad \text{if } \phi^b(\mathbf{b}) = 0,$$
$$=\; !\S^{\phi^i(\mathbf{c})-1}\phi(F) \qquad \text{otherwise,}$$

and ϕ commutes with the other connectives. An instantiation ϕ for a p-term t is said to be *admissible* for t if it is admissible for all p-types occurring in t. When ϕ is admissible for t, a regular pseudo-term $\phi(t)$ can be obtained by replacing each $\S^{\mathbf{m}}u$ with $\S^{\phi^i(\mathbf{m})}u$, each x^D with $x^{\phi(D)}$, and each $(t)A$ with $(t)\phi(A)$.

As for pseudo-terms there is an erasure map $(.)^-$ from p-terms with their p-types to system F terms consisting in forgetting modalities and parameters.

A *free linear decoration* (*free bang decoration*, resp.) of a system F type T is a linear p-type (bang p-type, resp.) E such that (i) $E^- = T$, (ii) each linear combination $\mathbf{c}$ occurring in E is a single integer parameter $\mathbf{m}$, and (iii) the parameters occurring in E are mutually distinct. Two free decorations $\overline{T}_1$ and $\overline{T}_2$ are said to be *disjoint* if the set of parameters occurring in $\overline{T}_1$ is disjoint from the set of parameters in $\overline{T}_2$.

The *free decoration* $\overline{M}$ of a system F term M (which is unique up to renaming of parameters) is obtained as follows: first, to each type T of a variable x^T used in M, we associate a free bang decoration $\overline{T}$, and to each type U occurring as $(N)U$ in M, we associate a free linear decoration $\overline{U}$ with the following proviso:

(i) one and the same $\overline{T}$ is associated to all occurrences of the same variable x^T;

(ii) otherwise mutually disjoint free decorations $\overline{T}_1, \ldots, \overline{T}_n$ are associated to different occurrences of T.

$\overline{M}$ is now defined by induction on the construction of M:

$$\overline{x^T} \;=\; \S^{\mathbf{m}}x^{\overline{T}}, \qquad \overline{\lambda x^T.M} \;=\; \S^{\mathbf{m}}\lambda x^{\overline{T}}.\overline{M}, \qquad \overline{(M)N} \;=\; \S^{\mathbf{m}}((\overline{M})\overline{N}),$$
$$\overline{\Lambda\alpha.M} \;=\; \S^{\mathbf{m}}\Lambda\alpha.\overline{M}, \qquad \overline{(M)T} \;=\; \S^{\mathbf{m}}((\overline{M})\overline{T}),$$

where all newly introduced parameters $\mathbf{m}$ are chosen to be fresh. The key property of free decorations is the following:

Theorem 4.1. *Let M be a system F term and t be a regular pseudo-term. Then t is a decoration of M if and only if there is an admissible instantiation ϕ for $\overline{M}$ such that $\phi(\overline{M}) = t$.*

Proof. We first prove that for any system F type T, any free linear (bang, resp.) decoration E of T and any linear (bang, resp.) $DLAL\star$ type E_0, we have $E_0^- = T$ iff there is an admissible instantiation ϕ for E such that $\phi(E) = E_0$. This can be proved by induction on T.

Then the Theorem can be shown by induction on M. □

Hence our decoration problem (Problem 3.8) boils down to:

Problem 4.2 (instantiation). Given a system F term M, determine if there exists an admissible instantiation ϕ for $\overline{M}$ such that $\phi(\overline{M})$ is well-structured.

For that we will need to be able to state the four conditions (local typing, bracketing, bang, and Λ-scope) on p-terms; they will yield some constraints on parameters. In the sequel, we will speak of *linear inequations*, meaning in fact both linear equations and linear inequations.

4.2. **Local typing constraints.** First of all, we need to express the unifiability of two p-types E_1 and E_2. We define a set $\mathcal{U}(E_1, E_2)$ of constraints by

$$
\begin{aligned}
\mathcal{U}(\alpha, \alpha) &= \emptyset, \\
\mathcal{U}(D_1 \multimap A_1, D_2 \multimap A_2) &= \mathcal{U}(D_1, D_2) \cup \mathcal{U}(A_1, A_2), \\
\mathcal{U}(\forall \alpha.A_1, \forall \alpha.A_2) &= \mathcal{U}(A_1, A_2), \\
\mathcal{U}(\S^{\mathbf{c_1}} F_1, \S^{\mathbf{c_2}} F_2) &= \{\mathbf{c_1} = \mathbf{c_2}\} \cup \mathcal{U}(F_1, F_2), \\
\mathcal{U}(\S^{\mathbf{b_1}, \mathbf{c_1}} F_1, \S^{\mathbf{b_2}, \mathbf{c_2}} F_2) &= \{\mathbf{b_1} = \mathbf{b_2}, \mathbf{c_1} = \mathbf{c_2}\} \cup \mathcal{U}(F_1, F_2).
\end{aligned}
$$

It is undefined otherwise. It is straightforward to observe:

Lemma 4.3. *Let E_1, E_2 be two linear (bang, resp.) p-types such that $E_1^- = E_2^-$. Then $\mathcal{U}(E_1, E_2)$ is defined. Moreover, when ϕ is an admissible instantiation for E_1 and E_2, we have $\phi(E_1) = \phi(E_2)$ if and only if ϕ is a solution of $\mathcal{U}(E_1, E_2)$.*

Proof. By induction on E_1. □

For any p-type E, define

$$\mathsf{Adm}(E) = \{\mathbf{c} \geq \mathbf{0} : \mathbf{c} \text{ occurs in } E\} \cup \{\mathbf{b} = \mathbf{1} \Rightarrow \mathbf{c} \geq \mathbf{1} : \S^{\mathbf{b}, \mathbf{c}} F \text{ occurs in } E\}.$$

Then ϕ is admissible for E if and only if ϕ is a solution of $\mathsf{Adm}(E)$.

Now consider the free decoration $\overline{M}$ of a system F typed term M. We assign to each subterm t of $\overline{M}$ a *linear* p-type B and a set $\mathcal{M}$ of constraints (indicated as $t : B : \mathcal{M}$) as on Figure 6. Notice that any linear p-type is of the form $\S^{\mathbf{c}} F$. Moreover, since t comes from a system F typed term, we know that t has a p-type $\S^{\mathbf{c}}(D \multimap B)$ when t occurs as $(t)u$, and $\S^{\mathbf{c}}(\forall \alpha.B)$ when t occurs as $(t)A$. In the former case, we have $(D^\circ)^- = A^-$, so that $\mathcal{U}(D^\circ, A)$ used in the application rule is always defined. As a consequence, for any M a unique p-type and a unique set of constraints $\mathcal{M}(\overline{M})$ are obtained. Finally, observe that $\overline{M}$ satisfies the eigenvariable condition.

Let $\mathsf{Ltype}(\overline{M})$ be $\mathcal{M}(\overline{M}) \cup \{\mathbf{b} = \mathbf{1} : x^{\S^{\mathbf{b}, \mathbf{c}} F} \text{ occurs more than once in } \overline{M}\}$.

Lemma 4.4. *Let M be a system F term and ϕ be an instantiation for $\overline{M}$. Then ϕ is admissible for $\overline{M}$ and $\phi(\overline{M})$ satisfies the local typing condition if and only if ϕ is a solution of $\mathsf{Ltype}(\overline{M})$.*

$$\frac{}{x^D : D^\circ : \mathsf{Adm}(D)} \qquad \frac{t : \S^{\mathbf{c}}F : \mathcal{M}}{\S^{\mathbf{m}}t : \S^{\mathbf{m}+\mathbf{c}}F : \mathcal{M} \cup \{\mathbf{m} + \mathbf{c} \geq \mathbf{0}\}}$$

$$\frac{t : A : \mathcal{M}}{\lambda x^D.t : \S^{\mathbf{0}}(D \multimap A) : \mathcal{M} \cup \mathsf{Adm}(D)} \qquad \frac{t : \S^{\mathbf{c}}(D \multimap B) : \mathcal{M}_1 \quad u : A : \mathcal{M}_2}{(t)u : B : \mathcal{M}_1 \cup \mathcal{M}_2 \cup \{\mathbf{c} = \mathbf{0}\} \cup \mathcal{U}(D^\circ, A)}$$

$$\frac{t : A : \mathcal{M}}{\Lambda\alpha.t : \S^{\mathbf{0}}\forall\alpha.A : \mathcal{M}} \qquad \frac{t : \S^{\mathbf{c}}(\forall\alpha.B) : \mathcal{M}}{(t)A : B[A/\alpha] : \mathcal{M} \cup \{\mathbf{c} = \mathbf{0}\} \cup \mathsf{Adm}(A)}$$

Figure 6: Local typing and $\mathcal{M}(t)$ constraints.

4.3. **Boxing constraints.** We consider the words over integer parameters $\mathbf{m}$, $\mathbf{n}$ ..., whose set we denote by $\mathcal{L}_p$. Let t be a p-term and u an occurrence of subterm of t. We define, as for pseudo-terms, the word $\mathsf{doors}(t, u)$ in $\mathcal{L}_p$ as follows. If $t = u$, let $\mathsf{doors}(t, u) = \epsilon$. Otherwise:

$$\begin{aligned}
\mathsf{doors}(\S^{\mathbf{m}}t, u) &= \mathbf{m} :: (\mathsf{doors}(t, u)), \\
\mathsf{doors}(\lambda y^D.t_1, u) &= \mathsf{doors}(\Lambda\alpha.t_1, u) = \mathsf{doors}((t_1)A, u) = \mathsf{doors}(t_1, u), \\
\mathsf{doors}((t_1)t_2, u) &= \mathsf{doors}(t_i, u) \text{ where } t_i \text{ is the subterm containing } u.
\end{aligned}$$

The sum $s(l)$ of an element l of $\mathcal{L}_p$ is a linear combination of integer parameters defined by:

$$s(\epsilon) = \mathbf{0}, \qquad s(\mathbf{m} :: l) = \mathbf{m} + s(l).$$

For each list $l \in \mathcal{L}_p$, define $\mathsf{wbracket}(l) = \{s(l') \geq \mathbf{0} \mid l' \leq l\}$ and $\mathsf{bracket}(l) = \mathsf{wbracket}(l) \cup \{s(l) = \mathbf{0}\}$.

Given a system F term M, we consider the following sets of constraints:

Bracketing constraints. $\mathsf{Bracket}(\overline{M})$ is the union of the following sets:
(i) for each occurrence of free variable x in $\overline{M}$, $\mathsf{bracket}(\mathsf{doors}(\overline{M}, x))$;
(ii) for each occurrence of an abstraction subterm $\lambda x.v$ of $\overline{M}$:
    (ii.a) $\mathsf{wbracket}(\mathsf{doors}(\overline{M}, \lambda x.v))$,
    (ii.b) for any occurrence of x in v, $\mathsf{bracket}(\mathsf{doors}(v, x))$.

Bang constraints. A subterm u that occurs in $\overline{M}$ as $(t)u$ with $t : \S^{\mathbf{c}'}(\S^{\mathbf{b},\mathbf{c}}F \multimap B)$ is called a *bang subterm* of $\overline{M}$ with the *critical parameter* $\mathbf{b}$. Now $\mathsf{Bang}(\overline{M})$ is the union of the following sets: for each bang subterm u of $\overline{M}$ with a critical parameter $\mathbf{b}$,
(i) $\{\mathbf{b} = \mathbf{0}\}$ if u has strictly more than one occurrence of free variable, and
    $\{\mathbf{b} = \mathbf{1} \Rightarrow \mathbf{b}' = \mathbf{1}\}$ if u has exactly one occurrence of free variable $x^{\S^{\mathbf{b}',\mathbf{c}'}F'}$.
(ii) $\{\mathbf{b} = \mathbf{1} \Rightarrow s(\mathsf{doors}(u, v)) \geq \mathbf{1} \ : \ v \text{ subterm of } u \text{ such that } v \neq u \text{ and } v \neq x\} \cup$
    $\{\mathbf{b} = \mathbf{1} \Rightarrow s(\mathsf{doors}(u, x)) = \mathbf{0}\}$.
    (where x is the free occurrence of variable in u, if there is one, otherwise the second set in the union is removed)

Remark 4.5. Note that if t is a p-term and ϕ is an instantiation, the pseudo-term $\phi(t)$ might have more subterms than t. In fact subterms of the p-term t are in correspondence with *door-extreme subterms* of the regular pseudo-term $\phi(t)$.

For instance if $t = \S^{\mathbf{m}}x$ and $\phi(\mathbf{m}) = 2$, the subterms of t and $\phi(t)$ are respectively $\{\S^{\mathbf{m}}x, x\}$ and $\{\S^2 x, \S x, x\}$. The door-extreme subterms of $\phi(t)$ are $\{\S^2 x, x\}$.

This is why we had to add in the Bang constraints (ii) the condition $\{\mathbf{b} = \mathbf{1} \Rightarrow s(\mathsf{doors}(u, x)) = \mathbf{0}\}$.

Λ-**Scope constraints**. $\mathsf{Scope}(\overline{M})$ is the union of the following sets:

(i) $\mathsf{wbracket}(\mathsf{doors}(u, v))$ for each subterm $\Lambda\alpha.u$ of $\overline{M}$ and for each subterm v of u that depends on α.

We denote $\mathsf{Const}(\overline{M}) = \mathsf{Ltype}(\overline{M}) \cup \mathsf{Bracket}(\overline{M}) \cup \mathsf{Bang}(\overline{M}) \cup \mathsf{Scope}(\overline{M})$.

Remark 4.6. Instead of using p-terms, the parameters and constraints might be visualized on pseudo-terms graphs. Using our running example of Fig. 5 we can decorate it with parameters $\mathbf{m_i}$: see Fig. 7. Each $\mathbf{m_i}$ stands for a possible sequence of doors: if it is instantiated with $k \geq 0$ (resp. $k \leq -1$) then this will correspond to k (resp. $(-k)$) opening (resp. closing) doors. Then, for instance, the Bracketing constraints correspond to conditions on the parameters occurring along certain paths of the graph (as indicated in Remark 3.1). As an example the Bracketing constraint (ii.b) for the binder λf and the two free occurrences of f gives here $\{\mathbf{m_3} \geq 0,\ \mathbf{m_3}+\mathbf{m_4} = 0,\ \mathbf{m_3}+\mathbf{m_5} \geq 0,\ \mathbf{m_3}+\mathbf{m_5}+\mathbf{m_6} = 0\}$.
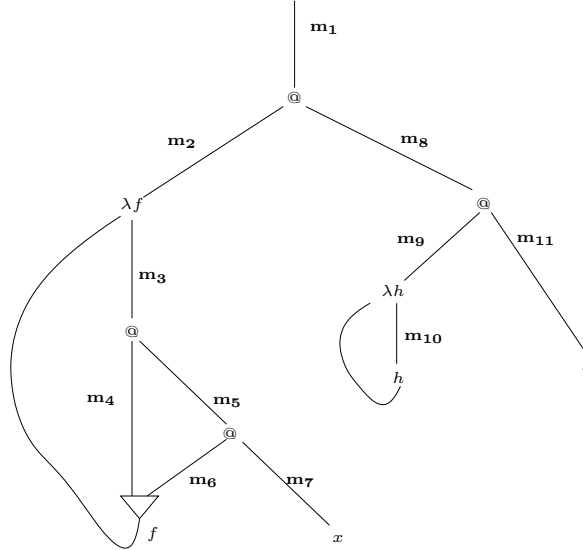
Figure 7: Example of parameterized pseudo-term graph.

Theorem 4.7. *Let M be a system F term and ϕ be an instantiation for $\overline{M}$. Then: ϕ is admissible for M and $\phi(\overline{M})$ is well-structured if and only if ϕ is a solution of $\mathsf{Const}(\overline{M})$.*

Moreover, the number of (in)equations in $\mathsf{Const}(\overline{M})$ is quadratic in the size of M.

Proof. Clearly, the above constraints are almost direct parameterizations of the corresponding conditions given in the previous section. Let us just examine the bang condition.

Suppose that $\phi(\overline{M})$ satisfies the bang condition. For each (parameterized) bang subterm u with the critical parameter $\mathbf{b}$ in $\overline{M}$, one of the following two happens:

- $\phi(u)$ is not a bang subterm of $\phi(\overline{M})$ (in the sense of the previous section). Namely, $\phi(\mathbf{b}) = 0$. In this case, ϕ is a solution of the equation $\mathbf{b} = \mathbf{0}$, and also of $\mathbf{b} = \mathbf{1} \Rightarrow \mathbf{b'} = \mathbf{1}$ if u has a free variable $x^{\S^{\mathbf{b'},\mathbf{c'}}F'}$.
- $\phi(u)$ is a bang subterm of $\phi(\overline{M})$. Namely, $\phi(\mathbf{b}) = 1$. In this case, u contains at most one variable by the bang condition. Hence the equation $\mathbf{b} = \mathbf{0}$ does not belong to

$\mathsf{Bang}(\overline{M})$. Moreover, if u has a free variable $x^{\S^{\mathbf{b}',\mathbf{c}'}F'}$, $\phi(x)$ must have a bang type and so $\phi(\mathbf{b}') = 1$. Hence ϕ is a solution of $\mathbf{b} = \mathbf{1} \Rightarrow \mathbf{b}' = \mathbf{1}$.

It is straightforward to observe that ϕ is a solution of the equations in (ii), by using Remark 3.2. Therefore, ϕ is a solution of $\mathsf{Bang}(\overline{M})$.

Now suppose the converse and let u be a (parameterized) bang subterm with the critical parameter $\mathbf{b}$ in $\overline{M}$. Suppose also that $\phi(u)$ is a bang subterm of $\phi(\overline{M})$. This means that $\phi(\mathbf{b}) = 1$. Since ϕ is supposed to be a solution of $\mathsf{Bang}(\overline{M})$, u must contain at most one free variable, say $x^{\S^{\mathbf{b}',\mathbf{c}'}F'}$. Moreover, we have $\phi(\mathbf{b}') = 1$, which means that $\phi(x)$ has a bang type in $\phi(\overline{M})$. Therefore, $\phi(\overline{M})$ satisfies the bang condition (i). As ϕ satisfies the conditions in (ii) and $\phi(\mathbf{b}) = 1$ we get that $\phi(u)$ satisfies the condition in Lemma 3.4, hence by this Lemma we obtain that $\phi(u)$ satisfies the bang condition (ii). $\square$

5. Solving the constraints

Having described a way to collect a set of constraints from a given system F term, there just remains to give a fast algorithm to solve them. Our method proceeds as follows: first solve the boolean constraints, which corresponds to determine which !-boxes are necessary (in 5.1), and then solve the integer constraints, which corresponds to complete the decoration by finding a suitable box structure (in 5.2).

5.1. Solving boolean constraints.

We split $\mathsf{Const}(\overline{M})$ into three disjoint sets $\mathsf{Const}^b(\overline{M})$, $\mathsf{Const}^i(\overline{M})$, $\mathsf{Const}^m(\overline{M})$:

- A *boolean constraint* $\mathbf{s} \in \mathsf{Const}^b(\overline{M})$ consists of only boolean parameters. $\mathbf{s}$ is of one of the following forms:

$$\begin{array}{llll} \mathbf{b_1} = \mathbf{b_2} & \text{(in } \mathsf{Ltype}(\overline{M})\text{)}, & \mathbf{b} = \mathbf{1} & \text{(in } \mathsf{Ltype}(\overline{M})\text{)}, \\ \mathbf{b} = \mathbf{0} & \text{(in } \mathsf{Bang}(\overline{M})\text{)}, & \mathbf{b} = \mathbf{1} \Rightarrow \mathbf{b}' = \mathbf{1} & \text{(in } \mathsf{Bang}(\overline{M})\text{)}. \end{array}$$

- A *linear constraint* $\mathbf{s} \in \mathsf{Const}^i(\overline{M})$ deals with integer parameters only. A linear constraint $\mathbf{s}$ is of one of the following forms:

$$\begin{array}{ll} \mathbf{c_1} = \mathbf{c_2} & \text{(in } \mathsf{Ltype}(\overline{M})\text{)}, \\ \mathbf{c} \geq \mathbf{0} & \text{(in } \mathsf{Ltype}(\overline{M}), \mathsf{Bracket}(\overline{M}), \mathsf{Scope}(\overline{M})\text{)}, \\ \mathbf{c} = \mathbf{0} & \text{(in } \mathsf{Ltype}(\overline{M}) \text{ and } \mathsf{Bracket}(\overline{M})\text{)}. \end{array}$$

- A *mixed constraint* $\mathbf{s} \in \mathsf{Const}^m(\overline{M})$ contains a boolean parameter and a linear combination and is of the following form:

$$\begin{array}{ll} \mathbf{b} = \mathbf{1} \Rightarrow \mathbf{c} = \mathbf{0} & \text{(in } \mathsf{Bang}(\overline{M})\text{)}, \\ \mathbf{b} = \mathbf{1} \Rightarrow \mathbf{c} \geq \mathbf{1} & \text{(in } \mathsf{Ltype}(\overline{M}) \text{ and } \mathsf{Bang}(\overline{M})\text{)}. \end{array}$$

We first try to find a solution of $\mathsf{Const}^b(\overline{M})$, and then proceed to the other constraints. This does not cause loss of generality, because $\mathsf{Const}^b(\overline{M})$ admits a *minimal* solution whenever solvable. Let us consider the set of instantiations on boolean parameters and the extensional order $\leq$ on these maps: $\psi^b \leq \phi^b$ if for any $\mathbf{b}$, $\psi^b(\mathbf{b}) \leq \phi^b(\mathbf{b})$.

Lemma 5.1. *There is a polynomial time algorithm to decide whether $\mathsf{Const}^b(\overline{M})$ has a solution or not. Moreover, the algorithm returns a minimal solution whenever there exists any.*

Proof. Our algorithm is based on the standard resolution procedure. Let $\mathcal{B} := \mathsf{Const}^b(\overline{M})$. Apply repeatedly the following steps until reaching a fixpoint:

- if $\mathbf{b_1} = \mathbf{b_2} \in \mathcal{B}$ and $\mathbf{b_1} = \mathbf{i} \in \mathcal{B}$ with $\mathbf{i} \in \{\mathbf{0}, \mathbf{1}\}$, then let $\mathcal{B} := \mathcal{B} \cup \{\mathbf{b_2} = \mathbf{i}\}$;
- if $\mathbf{b_1} = \mathbf{b_2} \in \mathcal{B}$ and $\mathbf{b_2} = \mathbf{i} \in \mathcal{B}$ with $\mathbf{i} \in \{\mathbf{0}, \mathbf{1}\}$, then let $\mathcal{B} := \mathcal{B} \cup \{\mathbf{b_1} = \mathbf{i}\}$;
- if $(\mathbf{b} = \mathbf{1} \Rightarrow \mathbf{b'} = \mathbf{1}) \in \mathcal{B}$ and $\mathbf{b} = \mathbf{1} \in \mathcal{B}$, then let $\mathcal{B} := \mathcal{B} \cup \{\mathbf{b'} = \mathbf{1}\}$.

It is obvious that this can be done in a polynomial number of steps and that the resulting system $\mathcal{B}$ is equivalent to $\mathsf{Const}^b(\overline{M})$.

Now, if $\mathcal{B}$ contains a pair of equations: $\mathbf{b} = \mathbf{0}, \mathbf{b} = \mathbf{1}$, then it is inconsistent, and hence $\mathsf{Const}^b(\overline{M})$ does not have a solution. Otherwise, define the boolean instantiation ψ^b by

$$\begin{aligned} \psi^b(\mathbf{b}) &:= 1 \quad \text{if } \mathbf{b} = \mathbf{1} \in \mathcal{B}; \\ &:= 0 \quad \text{otherwise.} \end{aligned}$$

It is clear that ψ^b is a solution of $\mathcal{B}$. In particular, observe that any constraint of the form $(\mathbf{b} = \mathbf{1} \Rightarrow \mathbf{b'} = \mathbf{1})$ in $\mathcal{B}$ is satisfied by ψ^b. Moreover any solution ϕ^b of $\mathcal{B}$ satisfies $\psi^b \leq \phi^b$. Therefore, ψ^b is a minimal solution of $\mathsf{Const}^b(\overline{M})$. $\square$

5.2. **Solving integer constraints.** When ϕ^b is a boolean instantiation, $\phi^b\mathsf{Const}^m(\overline{M})$ denotes the set of linear constraints defined as follows:

- for any constraint of the form $(\mathbf{b} = \mathbf{1} \Rightarrow \mathcal{I})$ in $\mathsf{Const}^m(\overline{M})$, where $\mathcal{I}$ is a linear (in)equation (of the form $\mathbf{c} \geq \mathbf{1}$ or $\mathbf{c} = \mathbf{0}$), $\mathcal{I}$ belongs to $\phi^b\mathsf{Const}^m(\overline{M})$ if and only if $\phi^b(\mathbf{b}) = 1$.

Then we clearly have:

(*) (ϕ^b, ϕ^i) is a solution of $\mathsf{Const}(\overline{M})$ if and only if ϕ^b is a solution of $\mathsf{Const}^b(\overline{M})$ and ϕ^i is a solution of $\phi^b\mathsf{Const}^m(\overline{M}) \cup \mathsf{Const}^i(\overline{M})$.

Lemma 5.2. $\mathsf{Const}(\overline{M})$ *admits a solution if and only if it has a solution $\psi = (\psi^b, \psi^i)$ such that ψ^b is the minimal solution of $\mathsf{Const}^b(\overline{M})$.*

Proof. Suppose that $\mathsf{Const}(\overline{M})$ admits a solution (ϕ^b, ϕ^i). Then by the previous Lemma, there is a minimal solution ψ^b of $\mathsf{Const}^b(\overline{M})$. Since $\psi^b \leq \phi^b$, we have $\psi^b\mathsf{Const}^m(\overline{M}) \subseteq \phi^b\mathsf{Const}^m(\overline{M})$. Since ϕ^i is a solution of $\phi^b\mathsf{Const}^m(\overline{M}) \cup \mathsf{Const}^i(\overline{M})$ by (*) above, it is also a solution of $\psi^b\mathsf{Const}^m(\overline{M}) \cup \mathsf{Const}^i(\overline{M})$. This means that (ψ^b, ϕ^i) is a solution of $\mathsf{Const}(\overline{M})$. $\square$

Coming back to the proof-net intuition, Lemma 5.2 means that given a syntactic tree of term there is a most general (minimal) way to place !-boxes (and accordingly ! subtypes in types), that is to say: if there is a *DLAL* decoration for this tree then there is one with precisely this minimal distribution of !-boxes.

Now notice that $\psi^b\mathsf{Const}^m(\overline{M}) \cup \mathsf{Const}^i(\overline{M})$ is a linear inequation system, for which a polynomial time procedure for searching a rational solution is known ([Kac79, Kar84]).

Lemma 5.3. $\psi^b\mathsf{Const}^m(\overline{M}) \cup \mathsf{Const}^i(\overline{M})$ *has a solution in $\mathbb{Q}$ if and only if it has a solution in $\mathbb{Z}$.*

Proof. Clearly the set of solutions is closed under multiplication by a positive integer. $\square$

Theorem 5.4. *Let M be a system F term. Then one can decide in time polynomial in the cardinality of $\mathsf{Const}(\overline{M})$ whether $\mathsf{Const}(\overline{M})$ admits a solution.*

Proof. First decide if there is a solution of $\mathsf{Const}^b(\overline{M})$, and if it exists, let ψ^b be the minimal one (Lemma 5.1). Then apply the polynomial time procedure to decide if $\psi^b\mathsf{Const}^m(\overline{M}) \cup \mathsf{Const}^i(\overline{M})$ admits a solution in $\mathbb{Q}$. If it does, then we also have an integer solution (Lemma 5.3). Otherwise, $\mathsf{Const}(\overline{M})$ is not solvable. $\square$

By combining Theorems 3.7, 4.1, 4.7 and 5.4, we conclude that the $DLAL$ typing problem (Problem 2.2) can be solved in polynomial time:

Theorem 5.5. *Given a system F term M^T, it is decidable in time polynomial in the size of M whether there is a decoration A of T such that $\vdash_{DLAL} M : A$.*

6. Data-types and typing with domain specification

6.1. **Data-types.** Now that we have a type inference procedure, we can reexamine the data-types in system F and the corresponding types in $DLAL$.

Consider for instance the system F type for unary integers:

$$N_F = \forall\alpha.(\alpha \to \alpha) \to (\alpha \to \alpha) \ .$$

We denote by $\underline{k}$ the Church integer for k.

If we apply the type inference procedure to the Church integer $\underline{2}$, we obtain the following family of parameterized types with constraints as result:

$$\begin{cases} A = \S^{\mathbf{n_1}}\forall\alpha.\S^{\mathbf{n_2}}[\S^{\mathbf{b_3},\mathbf{n_3}}(\S^{\mathbf{b_4},\mathbf{n_4}}\alpha \multimap \S^{\mathbf{n_5}}\alpha) \multimap \S^{\mathbf{n_6}}(\S^{\mathbf{b_7},\mathbf{n_7}}\alpha \multimap \S^{\mathbf{n_8}}\alpha)] \\ \mathbf{b_3 = 1, \ b_4 = 0} \\ \mathbf{n_4 = n_5, \ n_7 = n_8,} \\ \mathbf{n_3 + n_4 = n_6 + n_7} \\ \mathbf{n_i \geq 0, \ n_j \geq b_j} \text{ for } 1 \leq i \leq 8 \text{ and } j = 3, 4, 7. \end{cases}$$

It is easy to check that conversely, any solution to this system gives a type suitable for all Church integers. We denote by $\mathcal{N}(A)$ this set of constraints. If D is a free bang decoration of N_F, we define $\mathcal{N}(D) = \mathcal{N}(D^\circ)$.

Observe that the type $N_{DLAL} = \forall\alpha.(\alpha \multimap \alpha) \Rightarrow \S(\alpha \multimap \alpha)$ is obtained by a solution of this system $(\phi(\mathbf{n_3}) = \phi(\mathbf{n_6}) = 1, \ \phi(\mathbf{n_i}) = 0$ for $i \neq 3, 6, \ \phi(\mathbf{b_7}) = 0)$ but it is not the only one. For instance the following types are also suitable $DLAL$ types for Church integers:

- $N'_{DLAL} = \forall\alpha.(\alpha \multimap \alpha) \Rightarrow (\S\alpha \multimap \S\alpha)$,
  obtained with ϕ_0 defined as the previous ϕ, but for $\phi_0(\mathbf{n_6}) = 0, \ \phi_0(\mathbf{n_7}) = \phi_0(\mathbf{n_8}) = 1$.
- $\S\forall\alpha.\S^2(\S\alpha \multimap \S\alpha) \Rightarrow \S(\S^3\alpha \multimap \S^3\alpha)$,
  obtained with $\phi_1(\mathbf{n_i}) = 1$ for $i = 1, 4, 5, 6$; $\phi_1(\mathbf{n_i}) = 3$ for $i = 3, 7, 8$; $\phi_1(\mathbf{n_2}) = 0$, $\phi_1(\mathbf{b_7}) = 0$.

In the same way we can characterise the $DLAL$ types for the Church representations of binary words, with a linear free decoration A of the system F type W_F and the following set of constraints $\mathcal{W}(A)$.

$$\begin{cases} A = \S^{\mathbf{n_1}}\forall\alpha.\S^{\mathbf{n_2}}[\S^{\mathbf{b_3,n_3}}(\S^{\mathbf{b_4,n_4}}\alpha \multimap \S^{\mathbf{n_5}}\alpha) \multimap \S^{\mathbf{n_6}}[\S^{\mathbf{b_7,n_7}}(\S^{\mathbf{b_8,n_8}}\alpha \multimap \S^{\mathbf{n_9}}\alpha) \multimap \S^{\mathbf{n_{10}}}(\S^{\mathbf{b_{11},n_{11}}}\alpha \multimap \S^{\mathbf{n_{12}}}\alpha)]] \\ \mathbf{b_3 = b_7 = 1, \quad b_4 = b_8 = b_{11} = 0} \\ \mathbf{n_4 = n_5, \ n_8 = n_9, \ n_{11} = n_{12},} \\ \mathbf{n_3 + n_4 = n_6 + n_7 + n_8,} \\ \mathbf{n_7 + n_8 = n_{10} + n_{11},} \\ \mathbf{n_i \geq 0, \ n_j \geq b_j} \text{ for } 1 \leq i \leq 12 \text{ and } j = 3,4,7,8,11. \end{cases}$$

6.2. **Typing with domain specification.** Actually the $DLAL$ typability of a term $M^{W_F \to W_F}$ of system F is *not* sufficient to ensure that M is Ptime computable. To illustrate this point, we consider for simplicity unary Church integers and terms of type $N_F \to N_F$. Observe that the following term of system F has type $N_F \to N_F$ and represents the exponentiation function (2^n) over unary integers:

$$exp = \lambda n.\Lambda\beta.(n \ \beta \to \beta)(\underline{2} \ \beta).$$

Thus the term exp does not represent a Ptime function but... it is typable in $DLAL$, with for instance the type:

$$\forall\alpha.[(\alpha \Rightarrow \S\alpha) \multimap (\alpha \Rightarrow \S\alpha)] \multimap \forall\beta.[(\beta \multimap \beta) \Rightarrow \S(\beta \multimap \beta)].$$

The trick here is that this $DLAL$ type does not allow the term exp to be applied to all Church integers. Indeed the only closed terms of type $\forall\alpha.[(\alpha \Rightarrow \S\alpha) \multimap (\alpha \Rightarrow \S\alpha)]$ are $\underline{0}$ and $\underline{1}$. So we do obtain a Ptime term but over a restricted, finite domain ...

In general we are therefore not just interested in mere typability but in typability with meaningful types. Indeed we generally want the terms to be typable in $DLAL$ in such a way that they can be applied to arguments of certain data-types (unary integers, lists...). This can be enforced by adding some specification about the domain of the function.

Let M be a system F term of type T. We call a *domain specification* of M a list $Dom = \langle(x_1,s_1),\ldots,(x_k,s_k)\rangle$ such that for each i:

- x_i is a bound variable of M,
- $s_i \in \{\mathbf{N}, \mathbf{W}\}$,
- if $s_i = \mathbf{N}$ (resp. $s_i = \mathbf{W}$), then x_i is of type N_F (resp. W_F) in M.

For instance for the previous example of term exp we can take $Dom = \{(n, \mathbf{N})\}$.

Here we restrict to N_F, W_F for simplicity, but this definition could be extended to other data-types of system F such as lists, binary trees ...

Now we consider the free decoration $\overline{M}$. Let $\mathsf{DomConst}(\overline{M}, Dom)$ be the union of $\mathcal{N}(D_i)$ (resp. $\mathcal{W}(D_i)$) for all bound variables $x_i^{D_i}$ such that $(x_i, \mathbf{N})$ (resp. $(x_i, \mathbf{W})$) is in Dom.

Finding a $DLAL$ type for M such that, in the resulting $DLAL$ typed term, each x_i from Dom can be instantiated with a Church integer or binary word, is thus equivalent to finding a solution of $\mathsf{Const}(\overline{M})$ which also satisfies $\mathsf{DomConst}(\overline{M}, Dom)$. In the previous example of exp and the domain specification Dom, there is not any such solution.

We have:

Theorem 6.1. *Let M be a System F term and Dom be a domain specification. One can decide in time polynomial in the cardinality of $\mathsf{Const}(\overline{M}) \cup \mathsf{DomConst}(\overline{M}, Dom)$ whether it admits a solution.*

Proof. It is sufficient to observe that the constraints in $\mathcal{N}(D)$ (where D is a decoration of N_F or W_F) also satisfy the properties used to prove Lemma 5.1, Lemma 5.2 and Lemma 5.3.

Note that for Lemma 5.3 for instance the argument would not be valid anymore (at least in an obvious way) if we added constraints of the form $\mathbf{n} = 1$ or $\mathbf{n} \leq 1$. $\qquad\square$

Therefore one can perform $DLAL$ decoration for system F terms in polynomial time even with domain specification.

7. IMPLEMENTATION AND EXAMPLES

7.1. **Overview.** We designed an implementation of the type inference algorithm. The program is written in functional CAML and is quite concise (less than 1500 lines). A running program not only shows the actual feasibility of our method, but is also a great facility for building examples, and thus might allow for a finer study of the algorithm.

Data types as well as functions closely follow the previous description of the algorithm: writing the program in such a way tends to minimise the number of bugs, and speaks up for the robustness of the whole proof development.

The program consists of several successive parts:

(1) Parsing phase: turns the input text into a concrete syntax tree. The input is a system F typing judgement, in a Church style syntax with type annotations at the binders. It is changed into the de Bruijn notation, and parameterized with fresh parameters. Finally, the abstract tree is decorated with parameterized types at each node.

(2) Constraints generation: performs explorations on the tree and generates the boolean, linear and mixed constraints.

(3) Boolean constraints resolution: gives the minimal solution of the boolean constraints, or answers negatively if the set admits no solution.

(4) Constraints printing: builds the final set of linear constraints.

We use a solver employing the simplex algorithm to solve the linear constraints. It runs in $O(2^n)$, which comes in contrast with the previous result of polynomial time solving, but has proven to be the best in practice.

We now have to define the objective function that we will give to the solver. Basically, to minimize the resulting complexity bound, we should have an objective function which minimizes the nesting depth of the boxes of the typed term. To achieve this, we would have to minimize the maximum of the sums of door parameters from the root to each node (this corresponds to the depth of the proof-net, which yields the bound of Theorem 2.1). This clearly calls for a minimax objective function. Unfortunately, this does not fit into the linear programming setting that we are currently using: our objective function can only be a ponderated sum of variables.

So, we chose to simply put as objective function the sum of door parameters. A little trick is needed in order to handle the case of variables which are not of positive domain, and could lead to the absence of an optimal solution. Once this special case is handled, the solver always gives sensible results in practice.

The program, together with some examples, is available at:

`http://www-lipn.univ-paris13.fr/~atassi/`

7.2. Two examples: reversing of list and predecessor.

7.2.1. *List reversing.* Let us consider the reversing function on binary words. It can be defined by a single higher-order iteration on the type W_F, with the untyped term $\lambda w.\lambda so.\lambda si.(w)\ step_0\ step_1\ base$, with :

- base term: $base = \lambda z.z$,
- step terms: $step_0 = \lambda a.\lambda x.(a)(so)x$, $step_1 = \lambda a.\lambda x.(a)(si)x$.

We obtain as system F term the following one, denoted **rev**:

$$\lambda l^W.\Lambda\beta.\lambda so^{\beta\to\beta}.\lambda si^{\beta\to\beta}.(l\ (\beta\to\beta))$$
$$\lambda a^{\beta\to\beta}.\lambda x^\beta.(a)(so)x$$
$$\lambda a^{\beta\to\beta}.\lambda x^\beta.(a)(si)x\ (\Lambda\alpha.\lambda z^\alpha.z)\beta\ .$$

As discussed in Section 6.2 to obtain a meaningful typing we need to force the domain of the term to be that of binary words. For that a simple way is to apply the term to a particular argument, for instance: $\Lambda\alpha.\lambda so^{\alpha\to\alpha}.\lambda si^{\alpha\to\alpha}.\lambda x^\alpha.(si)(so)(si)(so)x$, representing the word $\underline{\mathbf{1010}}$. Since **rev** involves higher-order functionals and polymorphism, it is not so straightforward to tell, just by looking at the term structure, whether it works in polynomial time or not.

Given **rev(1010)** as input (coded by ASCII characters), our program produces 204 (in)equations on 79 variables. After constraint solving, we obtain the result:

$$(\lambda l^W.\Lambda\beta.\lambda so^{!(\beta\multimap\beta)}.\lambda si^{!(\beta\multimap\beta)}.$$
$$\S(\bar{\S}((l\ (\beta\multimap\beta))$$
$$\S\lambda a^{\beta\multimap\beta}.\lambda x^\beta.(a)(\bar{\S}so)x$$
$$\S\lambda a^{\beta\multimap\beta}.\lambda x^\beta.(a)(\bar{\S}si)x)$$
$$(\Lambda\alpha.\lambda z^\alpha.z)\beta)$$
$$\Lambda\alpha.\lambda so^{!\alpha\to\alpha}.\lambda si^{\alpha\to\alpha}.\S\lambda x^\alpha.(\bar{\S}si)(\bar{\S}so)(\bar{\S}si)(\bar{\S}so)\ .x\ .$$

It corresponds to the natural depth-1 typing of the term **rev**, with conclusion type $W_{DLAL}\multimap W_{DLAL}$. The solution ensures polynomial time termination, and in fact its depth guarantees normalization in a quadratic number of β-reduction steps.

7.2.2. *Predecessor on unary integers.* We now turn to another example which illustrates the use of polymorphism: the predecessor function on unary integers.

We consider a slight simplification of the term given by Asperti ([Asp98]). The simplification is not needed for typability, but is just chosen to facilitate readability.

For that we consider:

- pairs represented in the following way: $< P, Q > :\ \lambda z.(z)\ P\ Q$,
- terms for projection and an application combinator for pairs:

$$\begin{aligned} fst &= \lambda x.\lambda y.x, \\ snd &= \lambda x.\lambda y.y, \\ appl &= \lambda x.\lambda y.(x)y\ . \end{aligned}$$

We will do an iteration on type N_F, with:

- base term: $< I, x >$ (where $I = \lambda x.x$),
- step term: $\lambda p. < f, (p)\ appl >$.

The untyped term will then be $\lambda n.((n)\ step\ base)\ snd$.

Let us specify the system F typing of the subterms:

- $< P, Q > = \lambda z^{(\beta \to \beta) \to (\beta \to \beta)}.(z) \ P^{\beta \to \beta} \ Q^{\beta} : ((\beta \to \beta) \to (\beta \to \beta)) \to \beta,$
- $snd, appl : (\beta \to \beta) \to \beta \to \beta,$
- $step = \lambda p^{((\beta \to \beta) \to (\beta \to \beta)) \to \beta}.\lambda z^{(\beta \to \beta) \to (\beta \to \beta)}.(z) \ f^{\beta \to \beta} \ (p) \ appl^{(\beta \to \beta) \to (\beta \to \beta)} :$
  $(((\beta \to \beta) \to (\beta \to \beta)) \to \beta) \to (((\beta \to \beta) \to (\beta \to \beta)) \to \beta),$
- $base = \lambda z^{(\beta \to \beta) \to (\beta \to \beta)}.(z) \ I^{\beta \to \beta} \ x : ((\beta \to \beta) \to (\beta \to \beta)) \to \beta .$

The overall F-typed term for predecessor, denoted **pred** is thus:

$$\lambda n^{\forall \alpha.(\alpha \to \alpha) \to (\alpha \to \alpha)}.\Lambda\beta.\lambda f^{\beta \to \beta}.\lambda x^{\beta}.$$

$$($$

$$\quad (n \ ((\beta \to \beta) \to (\beta \to \beta)) \to \beta)$$

$$\quad \lambda p^{((\beta \to \beta) \to (\beta \to \beta)) \to \beta}.\lambda z^{(\beta \to \beta) \to (\beta \to \beta)}.(z) \ f^{\beta \to \beta} \ (p) \ appl^{(\beta \to \beta) \to (\beta \to \beta)}$$

$$\quad \lambda z^{(\beta \to \beta) \to (\beta \to \beta)}.(z) \ \lambda a^{\beta}.a \ x)$$

$$)$$

$$\lambda x^{\beta \to \beta}.\lambda y^{\beta}.y .$$

Observe that this term is linear (as Asperti's original one). Again, to force a meaningful typing we apply the term **pred** to a Church integer argument, here the integer $\underline{2}$.

The program then produces 220 equations, for 130 parameters. The solver produces a solution, yielding the following type for the subterm **pred**:

$$(\forall\alpha.(\alpha \multimap \alpha) \Rightarrow \S(\alpha \multimap \alpha)) \multimap (\forall\alpha.(\alpha \multimap \alpha) \Rightarrow \S(\alpha \multimap \alpha)),$$

which corresponds to the $N_{DLAL} \multimap N_{DLAL}$ type.

7.3. **Experiments with larger examples: polynomials.** In order to test our type inference program with larger examples it is interesting to consider a family of system F terms of increasing size. The family of terms representing polynomial functions over unary integers is a natural candidate for this goal, since in particular it is important for the encoding of polynomial time Turing machines in the system ([AR02, BT04]).

Therefore we wrote a CAML program which given a polynomial P outputs a system F term representing P and with type $N_F \to N_F$, that can then be fed to the $DLAL$ type inference program.

There is however a subtlety that needs to be stressed. Recall that in order to represent polynomial functions in LAL or $DLAL$ with suitable types it is necessary to use type cœrcions ([AR02, BT04]). These cœrcions are needed just for typing reasons, and not for computational ones. However, if we consider the system F terms underlying the LAL or $DLAL$ terms for polynomials the cœrcions are still present and correspond to explicit subterms.

So if we want our system F terms representing polynomials to be typable in $DLAL$ we need to anticipate on the need for cœrcions. Therefore our program generating system F terms for polynomials is guided by the encoding of polynomials in $DLAL$, in particular it takes into account the placement of subterms for cœrcions (even if the terms are not yet typed with modalities during this phase). It should be stressed that this increases considerably the size of the resulting term: in practice inside the resulting term the subpart accounting for the management of cœrcions is larger than the subpart performing a computational task... This makes however a good test for our type inference program, since the typing is not trivial and will put into use a large number of parameters and constraints.

In the following we will:

- describe the encoding of polynomials used,
- report on experiments of our type inference program on terms of this family.

Encoding of polynomials.

We recall from [BT04] the rules for cœrcions on type N_{DLAL} derivable in $DLAL$:

$$\frac{n : N_{DLAL}; \Delta \vdash t : A}{; m : N_{DLAL}, \S\Delta \vdash C_1[t] : \S A} \text{ (Coerc-1)}$$

$$\frac{\Gamma; n : \S N_{DLAL}, \Delta \vdash t : A}{\Gamma; m : N_{DLAL}, \Delta \vdash C_2[t] : A} \text{ (Coerc-2)}$$

where $C_1[.]$ and $C_2[.]$ are contexts, which contain as free variables some variables of the environments:

$$\begin{aligned} C_1[x] &= (m(\lambda g.\lambda p.(g \ (succ \ p))))(\lambda n.x)\underline{0}, \\ C_2[x] &= (\lambda n.x)(m \ succ \ \underline{0}) \ . \end{aligned}$$

succ is the usual term for successor.

Similarly we define the term $coerc = \lambda n.(n) \ succ \ \underline{0}$, which can be given in $DLAL$ any type $N_{DLAL} \multimap \S^k N_{DLAL}$ with $k \geq 0$.

Multiplication can be represented by the (untyped) term $mult = \lambda n.\lambda m.u$ with $u = ((m) \ \lambda k.\lambda f.\lambda x.(n) \ f \ (k) \ f \ x) \ \underline{0}$. It can be given in $DLAL$ the type $N_{DLAL} \Rightarrow N_{DLAL} \multimap \S N_{DLAL}$.

Now, in order to give multiplication any type: $\S^k N_{DLAL} \multimap \S^k N_{DLAL} \multimap \S^{k+2} N_{DLAL}$ with $k \geq 0$ we can use cœrcions:

$$\frac{\dfrac{\dfrac{...}{n : N_{DLAL}; m : N_{DLAL} \vdash u : \S N_{DLAL}}}{\dfrac{; n_2 : N_{DLAL}, m : \S N_{DLAL} \vdash C_1[u] : \S^2 N_{DLAL}}{\dfrac{; n_2 : N_{DLAL}, m_2 : N_{DLAL} \vdash C_2[C_1[u]] : \S^2 N_{DLAL}}{; n_2 : \S^k N_{DLAL}, m_2 : \S^k N_{DLAL} \vdash C_2[C_1[u]] : \S^{k+2} N_{DLAL}} \text{ \S-i } \times k}} \text{Coerc-2}} \text{Coerc-1}$$

Note that there is here a small abuse of notation as now the free variable of $C_1[.]$ is called n_2 (similarly for $C_2[.]$).

We will associate to each polynomial P of $\mathbb{N}[X]$ a system F term t_P of type $N_F \to N_F$ representing it, and which is typable in $DLAL$. We first describe the encoding of monomials.

We define the term t_{X^n} by induction on n:

$$t_{X^0} = \lambda x.\underline{1} \ , \quad t_{X^1} = \lambda x.x \ , \quad t_{X^{n+1}} = \lambda x.C_1[(\lambda n_2.\lambda m_2.C_2[C_1[u]]) \ (t_{X^n}) \ x \ (coerc) \ x],$$

for $n \geq 1$.

The term t_{X^n} can be given in $DLAL$ the type $N_{DLAL} \multimap \S^{4n} N_{DLAL}$. Actually a better encoding of monomials could be given, with a lower depth, but we stick here to this one for simplicity. To show that t_{X^n} can be typed with $N_{DLAL} \multimap \S^{4n} N_{DLAL}$ note that: it is easy to observe for t_{X^0} and t_{X^1}, and supposing it for t_{X^n} we get for $t_{X^{n+1}}$ (N in this derivation stands for N_{DLAL}):

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cdots}{\vdash \lambda n_2.\lambda m_2.C_2[C_1[u]] : \S^{4n}N \multimap \S^{4n}N \multimap \S^{4n+2}N} \quad \cfrac{\cdots}{; x_1 : N \vdash (t_{X^n})x_1 : \S^{4n}N}}{; x_1 : N \vdash (\lambda n_2.\lambda m_2.C_2[C_1[u]]) \, (t_{X^n}) \, x_1 : \S^{4n}N \multimap \S^{4n+2}N} \,\S\, i \times 4n \quad \cfrac{\cdots}{; x_2 : N \vdash (coerc) \, x_2 : \S^{4n}N}}{; x_1 : N, x_2 : N \vdash (\lambda n_2.\lambda m_2.C_2[C_1[u]]) \, (t_{X^n}) \, x_1 \, (coerc) \, x_2 : \S^{4n+2}N}}{x_1 : N, x_2 : N; \vdash (\lambda n_2.\lambda m_2.C_2[C_1[u]]) \, (t_{X^n}) \, x_1 \, (coerc) \, x_2 : \S^{4n+3}N} \S i}{x : N; \vdash ((\lambda n_2.\lambda m_2.C_2[C_1[u]]) \, (t_{X^n}) \, x \, (coerc) \, x : \S^{4n+3}N} \,contr}{; x : N \vdash C_1[(\lambda n_2.\lambda m_2.C_2[C_1[u]]) \, (t_{X^n}) \, x \, (coerc) \, x] : \S^{4n+4}N} \,coerc\text{-}1}{\vdash \lambda x.C_1[(\lambda n_2.\lambda m_2.C_2[C_1[u]]) \, (t_{X^n}) \, x \, (coerc) \, x] : N \multimap \S^{4(n+1)}N} \,\multimap i$$

Now, once t_{X^n} has been defined it is easy to represent monomials with coefficient, $\alpha_n X^n$ and, using the term for addition and cœrcions again, arbitrary polynomials: $\sum_{i=1}^{j} \alpha_{n_i} X^{n_i}$.

Experiments of type inference.

We used the program for generating system F terms representing polynomials and denoted $\mathbf{t_P}$ to test our $DLAL$ type inference program. We give the results of the experiments on a few examples, in the array of Figure 8. Again we stress that the large size of $\mathbf{t_P}$, even for small polynomials, is due to the cœrcions (for instance the encoding of x^5 without cœrcions produces a term of size 322 — which is not typable however) and to the fact that all types are written explicitly in the term, since it is written in a Church style syntax.

In the array the following quantities are reported:

- the size of $\mathbf{t_P}$ is the number of symbols of the term;
- the column **# Par** stands for the number of parameters in the resulting parameterized term,
- the time (in seconds) for generating the set of linear constraints is divided in two parts:
  - **GEN** is the time taken by the program for parsing the input, generating the whole constraints and solving the boolean part,
  - **SIMPL** is the time taken to simplify the set of constraints (this is a preprocessing before using the solver).
- **# Cons** is the cardinal of the set of of linear constraints generated by the program,
- **Sol** is the time taken by the solver (LPsol) to solve the set of constraints.

Recall that $N'_{DLAL} = \forall \alpha.(\alpha \multimap \alpha) \Rightarrow \S\alpha \multimap \S\alpha$. We think that the fact that we obtain a N'_{DLAL} type instead of N_{DLAL} on the right-hand-side is not significative here: we could force obtention of a N_{DLAL} type instead by techniques similar to that of domain specification of Section 6 (adding a constraint of the form $p = 0$).

Note that the type obtained is slightly smaller (containing fewer $\S$ and of smaller depth) than the one described above: we obtain the type $N_{DLAL} \multimap \S^{4n-3}N'_{DLAL}$ for t_{X^n}, and it is possible to check that this is indeed a suitable type in general.

Observe that on these examples the respective times needed for generating the constraints and solving the boolean part (**GEN**) on the one hand, and for simplifying the linear constraints (**SIMPL**) on the other, are comparable. The time needed to solve the linear constraints (**Sol**) is comparatively smaller.

We also generated the system F terms representing the same polynomials but without subterms for cœrcions, and noted with our program that type inference in $DLAL$ for these terms fails: cœrcions are indeed necessary.

$P = X^n$	Size of $\mathbf{t_P}$	# Par	GEN	SIMPL	# CONS	Sol	Type obtained	$4n$
X^2	380	520	0.1	0.1	844	0.0	$N \multimap \S^5 N'$	8
X^3	750	1009	0.3	0.7	1649	0.1	$N \multimap \S^9 N'$	12
X^4	1120	1498	0.9	1.7	2454	0.2	$N \multimap \S^{13} N'$	16
X^5	1490	1987	1.9	3.3	3259	0.4	$N \multimap \S^{17} N'$	20
X^6	1860	2476	3.5	5.5	4064	0.6	$N \multimap \S^{21} N'$	24
X^7	2230	2975	5.9	4.8	4869	0.8	$N \multimap \S^{25} N'$	28
X^8	2600	3454	9.0	6.9	5674	1.1	$N \multimap \S^{29} N'$	32
X^9	2970	3943	13.2	12.4	6479	1.5	$N \multimap \S^{33} N'$	36
X^{10}	3340	4432	18.5	21.0	7284	1.0	$N \multimap \S^{37} N'$	40
X^{16}	5560	7336	86.6	80.5	12114	5.8	$N \multimap \S^{61} N'$	64
X^{32}	11480	15190	810.0	381.3	24994	30.5	$N \multimap \S^{125} N'$	128

In the array N (resp. N') stands for N_{DLAL} (resp. N'_{DLAL}).

Figure 8: Type inference for terms representing polynomials.

Even though the family of terms t_{X^n} is a particular case, these examples illustrate the fact that our algorithm is manageable with lambda-terms of reasonable size, and gives results in a sensible time.

8. Discussion and further work for the case of propositional $DLAL$

It should be stressed that our method can be applied to type untyped lambda-terms in propositional (quantifier-free) $DLAL$. Indeed, propositional $DLAL$ can naturally be seen as a subsystem of $DLAL$. Given an untyped term t, we can thus proceed in the following way (in the lines of previous works for EAL or LAL like [CM01, Bai02]):

(1) search for the principal simple type of t,
(2) using the principal simple type derivation of t, search for a valid $DLAL$ decoration by using our method.

If we find a suitable decoration then it will give a derivation in propositional $DLAL$ (simply because the underlying system F derivation does not use quantification). It can be checked that this method is complete (for instance by a simple adaptation of the argument in [Bai04]): if the term is typable in propositional $DLAL$, then a suitable decoration of the principal simple type decoration will be found.

However, the bound on this procedure given by Theorem 5.5 is polynomial w.r.t. the *size of the principal simple type derivation of t*, and not w.r.t. to the *size $|t|$ of the untyped term t itself*.

Still, we strongly believe that our method can be adapted in order to give an algorithm performing type inference in propositional $DLAL$ for an untyped term t in time polynomial in $|t|$.

The starting point is that it is known that simple type inference can be done in polynomial time by using a shared representation of types. If one designs an algorithm performing together simple type inference and decoration with parameters, one can presumably obtain, instead of a *free decoration* of t, a suitable decoration with a number of parameters polynomial in $|t|$ (by taking advantage of the shared representation of types) and a constraints system also polynomial in $|t|$. Hence in the end type inference would be polynomial w.r.t.

$|t|$. We also believe that in this way we would obtain a notion of principal propositional $DLAL$ type. This would be analogous to the work of [CRdR03] for EAL, but could give a single principal type scheme instead of a finite family of principal type schemes.

However in the present paper we preferred to follow the approach starting with a system F typed term in order to be able to consider second-order $DLAL$ typing, which is more interesting for expressivity reasons (propositional $DLAL$ is not complete for polynomial time computation). The case of polynomial time type inference for propositional $DLAL$ is left for future work.

9. Conclusion

We showed that typing of system F terms in $DLAL$ can be performed in a feasible way, by reducing typability to a constraints solving problem and designing a resolution algorithm. This demonstrates a practical advantage of $DLAL$ over LAL, while keeping the other important properties. We illustrated the manageability of our algorithm by implementing it in CAML and giving some examples of type inference. Note that other typing features could still be automatically inferred, like cœrcions (see [Ata05] for the case of EAL).

This work illustrates how Linear logic proof-net notions like boxes can give rise to techniques effectively usable in type inference, even with the strong boxing discipline of $DLAL$, which extends previous work on EAL. We expect that some of these techniques could be adapted to other variants of Linear logic, existing (like Soft Linear Logic) or to be defined in the future.

References

[Asp98]   A. Asperti. Light Affine Logic. In *Proceedings LICS'98*, pages 300-308, IEEE Computer Press, 1998.

[ABT06]   V. Atassi, P. Baillot, and K. Terui. Verification of Ptime reducibility for system F terms via Dual Light Affine Logic. In *Proceedings of Computer Science Logic (CSL'06)*, volume 4207 of *LNCS*, pages 150–166. Springer, 2006.

[Ama05]   R. Amadio. Synthesis of max-plus quasi-interpretations. *Fundamenta Informaticae*, 65:29–60, 2005.

[AR02]   A. Asperti and L. Roversi. Intuitionistic light affine logic. *ACM Transactions on Computational Logic*, 3(1):1–39, 2002.

[Ata05]   V. Atassi. Inférence de type en logique linéaire élémentaire. Master's thesis, Université Paris 13, 2005.

[Bai02]   P. Baillot. Checking polynomial time complexity with types. In *Proceedings of IFIP TCS'02*, pages 370–382, Montreal, 2002. Kluwer Academic Press.

[Bai04]   P. Baillot. Type inference for light affine logic via constraints on words. *Theoretical Computer Science*, 328(3):289–323, 2004.

[BC92]   S. Bellantoni and S. Cook. New recursion-theoretic characterization of the polytime functions. *Computational Complexity*, 2:97–110, 1992.

[BT04]   P. Baillot and K. Terui. Light types for polynomial time computation in lambda-calculus. In *Proceedings LICS'04*, pages 266–275. IEEE Computer Press, 2004.

[BT05]   P. Baillot and K. Terui. A feasible algorithm for typing in elementary affine logic. In *Proceedings of TLCA'05*, volume 3461 of *LNCS*, pages 55–70. Springer, 2005.

[BMM07]   G. Bonfante, J.-Y. Marion and J.-Y. Moyen. Quasi-interpretations, a way to control resources. To appear in *Theoretical Computer Science*, 2007.

[CDLRdR05]   P. Coppola, U. Dal Lago, and S. Ronchi Della Rocca. Elementary affine logic and the call-by-value lambda calculus. In *Proceedings of TLCA'05*, volume 3461 of *LNCS*, pages 131–145. Springer, 2005.

[CM01]   P. Coppola and S. Martini. Typing lambda-terms in elementary logic with linear constraints. In *Proceedings TLCA'01*, volume 2044 of *LNCS*, pages 76–90, 2001.

[CRdR03]   P. Coppola and S. Ronchi Della Rocca. Principal typing in Elementary Affine Logic. In *Proceedings TLCA'03*, pages 90–104, LNCS, 2003.

[DJ03]   V. Danos and J.-B. Joinet. Linear logic and elementary time. *Information and Computation*, 183(1):123–137, 2003.

[Gir87]   J.-Y. Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.

[Gir98]   J.-Y. Girard. Light linear logic. *Information and Computation*, 143:175–204, 1998.

[HJ03]   M. Hofmann and S. Jost. Static prediction of heap space usage for first-order functional programs. In *Proc. ACM POPL'03*, pages 185–197, 2003.

[Hof03]   M. Hofmann. Linear types and non-size-increasing polynomial time computation. *Information and Computation*, 183(1):57–85, 2003.

[Kac79]   L. G. Kachian. A polynomial algorithm for linear programming. *Soviet Mathematics Doklady*, 20:191–194, 1979.

[Kar84]   N. Karmarkar. A new polynomial-time algorithm for linear programming. *Combinatorica* 4(4): 373–396, 1984.

[LM93]   D. Leivant and J.-Y. Marion. Lambda-calculus characterisations of polytime. *Fundamenta Informaticae*, 19:167–184, 1993.

[MM00]   J.-Y. Marion and J.-Y. Moyen. Efficient first order functional program interpreter with time bound certifications. In *Proceedings of LPAR 2000*, volume 1955 of *LNCS*, pages 25–42. Springer, 2000.

[Ter01]   K. Terui. Light Affine Lambda-calculus and polytime strong normalization. In *Proceedings LICS'01*, pages 209–220. IEEE Computer Society, 2001.

[Ter04a]   K. Terui. Light affine set theory: a naive set theory of polynomial time. *Studia Logica*, 77:9–40, 2004.

[Wel99]   J. B. Wells. Typability and type checking in system F are equivalent and undecidable. *Ann. Pure Appl. Logic*, 98(1–3),pages 111-156, 1999.