Characterizing Polynomial and Exponential Complexity Classes in Elementary Lambda-Calculus

Patrick Baillot, Erika de Benedetti, Simona Ronchi Della Rocca

Characterizing Polynomial and Exponential Complexity Classes in Elementary Lambda-Calculus*

(Long Version)

Patrick Baillot[1], Erika De Benedetti[1,2], and Simona Ronchi Della Rocca[2]

[1] CNRS, ENS de Lyon, INRIA, UCBL, Université de Lyon, LIP - Lyon, France

[2] Università degli Studi di Torino, Dipartimento di Informatica - Torino, Italy

Abstract. In this paper an implicit characterization of the complexity classes `k-EXP` and `k-FEXP`, for $k \geq 0$, is given, by a type assignment system for a stratified λ-calculus, where types for programs are witnesses of the corresponding complexity class. Types are formulae of Elementary Linear Logic (`ELL`), and the hierarchy of complexity classes `k-EXP` is characterized by a hierarchy of types.

Keywords: Implicit computational complexity · Linear logic · Lambda-calculus

1 Introduction

Context. Early work on the study of complexity classes by means of programming languages has been carried out by Neil Jones [9,10], in particular using functional programming. The interest of these investigations is twofold: from the computational complexity point of view, they provide new characterizations of complexity classes, which abstract away from machine models; from the programming language point of view, they are a way to analyze the impact on complexity of various programming features (higher-order types, recursive definitions, read/write operations). This fits more generally in the research line of *implicit computational complexity* (ICC), whose goal is to study complexity classes without relying on explicit bounds on resources but instead by considering restrictions on programming languages and calculi. Seminal research in this direction has been carried out in the fields of recursion theory [3,12], λ-calculus [14] and

* This work was supported by the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

linear logic [8]. These contributions usually exhibit a new specific language or logic for each complexity class, for instance PTIME, PSPACE, LOGSPACE: let us call *monovalent* the characterizations of this kind. We think however that the field would benefit from some more uniform presentations, which would consist in both a general language and a family of static criteria on programs of this language, each of which characterizing a particular complexity class. We call such a setting a *polyvalent* characterization; we believe that this approach is more promising for providing insights on the relationships between complexity classes. Polyvalent characterizations of this nature have been given in [10,13], but their criteria used for reaching point (2) referred to the construction steps of the programs. Here we are interested in defining a polyvalent characterization where (2) is expressed by means of the program's type in a dedicated system.

Stratification and Linear Logic. An ubiquitous notion in implicit complexity is that of *stratification*, by which we informally designate here the fact of organizing computation into distinct strata. This intuition underlies several systems: ramified and safe recursion [12,3], in which data is organized into strata; stratified comprehension [13], where strata are used for quantification; variants of linear logic [8] where programs are divided into strata thanks to a modality. More recently stratification of data has been related fruitfully to type systems for non-interference [17].
The linear logic approach to ICC is based on the proofs-as-programs correspondence. This logic indeed provides a powerful system to analyse the duplication and sharing of arguments in functional computation: this is made possible by a specific logical connective for the duplication of arguments, the ! modality. As in functional computation the reuse of an argument can cause a complexity explosion, the idea is to use weak versions of ! to characterize complexity classes. This intuition is illustrated by elementary linear logic (ELL) [8,7], a simple variant of linear logic which provides a monovalent characterisation of elementary complexity, that is to say computation in time bounded by a tower of exponentials of fixed height. Other variants of linear logic provide characterizations of PTIME, but they use either a more complicated language [8] or a more specific programming discipline [11].

Contribution and Comparison. In [2] a polyvalent characterization in ELL proof-nets of the complexity classes k-EXP $= \cup_{i\in\mathbb{N}}\mathtt{DTIME}(2_k^{n^i})$ for all $k \geq 0$ has been obtained. However this approach has some shortcomings:

1. The complexity soundness proof uses a partly semantic argument ([2] Lemma 3 p. 10) and so it does not provide a syntactic way to evaluate the programs with the given complexity bound.
2. The characterization is given for classes of predicates, and not for classes of functions. Moreover it is not so clear how to extend this result to functions because of the semantic argument mentioned above.
3. The language of proof-nets is not as standard and widespread as say that of λ-calculus.

In the present work, we wish to establish an analogous polyvalent characterization in the setting of λ-calculus, with a stronger complexity soundness result based on a concrete evaluation procedure. We think this could provide a more solid basis to explore other characterizations of this kind. In particular we define the $\lambda^!$-calculus, a variant of λ-calculus with explicit stratifications, which allows both to recover the results of [2] and to characterize also the function complexity classes k-FEXP, by two distinct hierarchies of types. In fact, the characterization obtained through a standard representation of data-types like in [2] does not account for some closure properties of the function classes k-FEXP, in particular composition, so we propose a new, maybe less natural, representation in order to grasp these properties. Our language makes it easier to define such non-standard representation.

Technical Approach. One could expect that the results of [2] might be extended to $\lambda^!$-calculus by considering a translation of terms into proof-nets. However it is not so straightforward: term reduction cannot be directly simulated by the evaluation procedure in [2], because (i) it follows a specific cut-elimination strategy and (ii) ultimately it uses a semantic argument. For this reason we give here a direct proof of the result in $\lambda^!$-calculus, which requires defining new measures on terms and is not a mere adaptation of the proof-net argument.

Related Works. The first results on ELL [8,7] as well as later works [18,5] have been carried out in the setting of proof-nets. Other syntaxes have then been explored. First, specific term calculi corresponding to the related system LLL and to ELL have been proposed [21,16,15]. Alternatively [4] used standard λ-calculus with a type system derived from ELL. The $\lambda^!$-calculus we use here has a syntax similar to e.g. [20,6], and our type system is inspired by [4].

Outline. In the following we first introduce the $\lambda^!$-calculus as an untyped calculus, delineate a notion of well-formed terms and study the complex-

ity of the reduction of these terms (Sect. 2). We then define a type system inspired by ELL and exhibit two families of types corresponding respectively to the hierarchies k-EXP and k-FEXP for $k \geq 0$ (Sect. 3). Finally we introduce a second characterization of this hierarchy, based on a non-standard data-type (Sect. 4). A conclusion follows.

2 The $\lambda^!$-Calculus

2.1 Terms and Reduction

We use a calculus, $\lambda^!$-calculus, which adds to ordinary λ-calculus a ! modality and distinguishes two notions of λ-abstraction:

$$\mathtt{M}, \mathtt{N} ::= \mathtt{x} \mid \lambda\mathtt{x}.\mathtt{M} \mid \lambda^!\mathtt{x}.\mathtt{M} \mid \mathtt{M}\mathtt{N} \mid !\mathtt{M}$$

where $\mathtt{x}$ ranges over a countable set of term variables Var. The usual notions of free variables is extended with $\mathrm{FV}(\lambda^!\mathtt{x}.\mathtt{M}) = \mathrm{FV}(\mathtt{M}) \setminus \{\mathtt{x}\}$, $\mathrm{FV}(!\mathtt{M}) = \mathrm{FV}(\mathtt{M})$. As usual, terms are considered modulo renaming of bound variables, and $=$ denotes the syntactic equality modulo this renaming.

Contexts. We consider the class of (one hole) contexts generated by the following grammar:

$$\mathcal{C} ::= \Box \mid \lambda\mathtt{x}.\mathcal{C} \mid \lambda^!\mathtt{x}.\mathcal{C} \mid \mathcal{C}\mathtt{M} \mid \mathtt{M}\mathcal{C} \mid !\mathcal{C}$$

As usual, capture of variables may occur. The *occurrence* of a term $\mathtt{N}$ in $\mathtt{M}$ is a context $\mathcal{C}$ such that $\mathtt{M} = \mathcal{C}[\mathtt{N}]$; in practice we simply write $\mathtt{N}$ for the occurrence if there is no ambiguity and call it a subterm of $\mathtt{M}$.

Depth. The *depth of the occurrence* $\mathcal{C}$ in $\mathtt{M}$, denoted by $\delta(\mathcal{C}, \mathtt{M})$, is the number of ! modalities surrounding the hole of $\mathcal{C}$ in $\mathtt{M}$.

Moreover, the *depth* $\delta(\mathtt{M})$ of a term $\mathtt{M}$ is the maximal nesting of ! in $\mathtt{M}$.

Example 1. $\mathtt{M} = !((\lambda\mathtt{x}.\mathtt{x})\ !!\mathtt{y}\ !\mathtt{y})$. Then $\delta(!((\lambda\mathtt{x}.\mathtt{x})\ !!\Box\ !\mathtt{y}), \mathtt{M}) = 3$ and $\delta(!((\lambda\mathtt{x}.\mathtt{x})\ !!\mathtt{y}\ !\Box), \mathtt{M}) = 2$; moreover, $\delta(\mathtt{M}) = 3$.

Dynamics. The reduction $\rightarrow$ is the contextual closure of the following rules:

$$(\lambda\mathtt{x}.\mathtt{M})\mathtt{N} \longrightarrow \mathtt{M}[\mathtt{N}/\mathtt{x}] \quad (\beta\text{-rule}) \qquad (\lambda^!\mathtt{x}.\mathtt{M})!\mathtt{N} \longrightarrow \mathtt{M}[\mathtt{N}/\mathtt{x}] \quad (!\text{-rule})$$

where $[\mathtt{N}/\mathtt{x}]$ denotes the capture free substitution of $\mathtt{x}$ by $\mathtt{N}$, whose definition is the obvious extension of the corresponding one for λ-calculus. Observe that a term such as $(\lambda^!\mathtt{x}.\mathtt{M})\mathtt{P}$ is a redex only if $\mathtt{P} = !\mathtt{N}$ for some $\mathtt{N}$; the intuition behind these two kinds of redexes is that the abstraction λ expects an input at depth 0, while $\lambda^!$ expects an input at depth 1.

A *subterm at depth* i in $\mathtt{M}$ is an occurrence $\mathcal{C}$ in $\mathtt{M}$ such that $\delta(\mathcal{C}, \mathtt{M}) = i$; we denote by $\to_i$ the reduction of a redex occurring at depth i. As usual, $\overset{*}{\to}$ ($\overset{*}{\to}_i$) denotes the reflexive and transitive closure of $\to$ ($\to_i$). We say that a term is in *i-normal form* if it does not have any redex at depth less than or equal to i; then $\mathtt{M}$ is in normal form iff it is in $\delta(\mathtt{M})$-normal form. We denote as $\mathbf{nf}_i$ the set of terms in i-normal form.

We have a confluence property, whose proof is adapted from [19], taking into account the notion of depth:

Proposition 1.

(i) *Let* $\mathtt{M} \in \mathbf{nf}_i$ *and* $\mathtt{M} \to_i \mathtt{M}'$*, with* $j \geq i+1$*, then* $\mathtt{M}' \in \mathbf{nf}_i$*.*

(ii) [Confluence at fixed depth] *Let* $\mathtt{M} \to_i \mathtt{P}$ *and* $\mathtt{M} \to_i \mathtt{Q}$*, then there is a term* $\mathtt{N}$ *such that* $\mathtt{P} \overset{*}{\to}_i \mathtt{N}$ *and* $\mathtt{Q} \overset{*}{\to}_i \mathtt{N}$*.*

(iii) [Confluence] *Let* $\mathtt{M} \to \mathtt{P}$ *and* $\mathtt{M} \to \mathtt{Q}$*, then there is a term* $\mathtt{N}$ *such that* $\mathtt{P} \overset{*}{\to} \mathtt{N}$ *and* $\mathtt{Q} \overset{*}{\to} \mathtt{N}$*.*

We consider a specific subclass of terms, inspired by elementary linear logic (ELL) [8,16]:

Definition 1 (Well-formed Term). *A term* $\mathtt{M}$ *is well-formed (w.f.) if and only if, for any subterm* $\mathtt{N}$ *of* $\mathtt{M}$ *which is an abstraction, we have:*

1. *if* $\mathtt{N} = \lambda\mathtt{x}.\mathtt{P}$*, then* $\mathtt{x}$ *occurs at most once and at depth* 0 *in* $\mathtt{P}$*;*
2. *if* $\mathtt{N} = \lambda^!\mathtt{x}.\mathtt{P}$*, then* $\mathtt{x}$ *can only occur at depth* 1 *in* $\mathtt{P}$*.*

Example 2. $\lambda f.\lambda\mathtt{x}.f(f\mathtt{x})$, the standard representation of the Church integer 2, is not w.f.; its w.f. counterpart is $\lambda^! f.!(\lambda\mathtt{x}.f(f\mathtt{x}))$.

The motivation behind such definition is that the depth of subterms in a w.f. term does not change during reduction: if an abstraction expects an input at depth 0 (resp. 1), which is the case of λ (resp. $\lambda^!$), then the substitutions occur at depth 0 (resp. 1), as each occurrence of its bound variable is at depth 0 (resp. 1).

The class of w.f. terms is preserved by reduction and their depth does not increase during reduction:

Lemma 1. *If* $\mathtt{M}$ *is w.f. and* $\mathtt{M} \to \mathtt{M}'$*, then* $\mathtt{M}'$ *is w.f., and* $\delta(\mathtt{M}') \leq \delta(\mathtt{M})$*.*

From now on, we assume that all terms are well formed.

Sizes. In order to study the reduction, it is useful to examine the *size of* $\mathtt{M}$ *at depth* i, denoted by $|\mathtt{M}|_i$, defined as follows:

- If $\mathtt{M} = \mathtt{x}$, then $|\mathtt{x}|_0 = 1$ and $|\mathtt{x}|_i = 0$ for $i \geq 1$;
- If $\mathtt{M} = \lambda\mathtt{x}.\mathtt{N}$ or $\mathtt{M} = \lambda^!\mathtt{x}.\mathtt{N}$, then $|\mathtt{M}|_0 = |\mathtt{N}|_0 + 1$ and $|\mathtt{M}|_i = |\mathtt{N}|_i$ for $i \geq 1$;
- If $\mathtt{M} = \mathtt{NP}$, then $|\mathtt{M}|_0 = |\mathtt{N}|_0 + |\mathtt{P}|_0 + 1$ and $|\mathtt{M}|_i = |\mathtt{N}|_i + |\mathtt{P}|_i$ for $i \geq 1$;
- If $\mathtt{M} = !\mathtt{N}$, then $|\mathtt{M}|_0 = 0$ and $|\mathtt{M}|_{i+1} = |\mathtt{N}|_i$ for $i \geq 0$;

Let $\delta(\mathtt{M}) = d$; then $|\mathtt{M}|_{i+} = \sum_{j=i}^{d} |\mathtt{M}|_j$ and the *size of* $\mathtt{M}$ is $|\mathtt{M}| = \sum_{i=0}^{d} |\mathtt{M}|_i$. The definition is extended to contexts, where $|\Box|_i = 0$ for $i \geq 0$. We consider how the size of a term changes during reduction:

Lemma 2. *If* $\mathtt{M} \to_i \mathtt{M}'$*, then* $|\mathtt{M}'|_i \leq |\mathtt{M}|_i - 1$*, and* $|\mathtt{M}'|_j = |\mathtt{M}|_j$ *for* $j < i$*.*

Strategy. The fact that by Prop. 1.(i) reducing a redex does not create any redex at strictly lower depth suggests considering the following, non-deterministic, *level-by-level* reduction strategy: if the term is not in normal form reduce (non deterministically) a redex at depth i, where $i \geq 0$ is the minimal depth such that $\mathtt{M} \notin \mathbf{nf}_i$. A *level-by-level reduction sequence* is a reduction sequence following the level-by-level strategy. We say that a reduction sequence is *maximal* if either it is infinite, or if it finishes with a normal term.

Proposition 2. *Any reduction of a term by the level-by-level strategy terminates.*

It follows that a maximal level-by-level reduction sequence of a term $\mathtt{M}$ has the shape shown in (1), where $\rightsquigarrow_i$ denotes one reduction step according to the level-by-level strategy, performed at depth i. We call *round* i the subsequence of $\rightsquigarrow_i$ starting from $\mathtt{M}_i^1$. Note that, for all i and $j > i$, $\mathtt{M}_j^1 \in \mathbf{nf}_i$. We simply write $\rightsquigarrow$ when we do not refer to a particular depth.

$$\mathtt{M}_0^1 \rightsquigarrow_0 \ldots \rightsquigarrow_0 \mathtt{M}_0^{n_0} = \mathtt{M}_1^1 \rightsquigarrow_1 \ldots \rightsquigarrow_1 \mathtt{M}_1^{n_1} = \ldots = \mathtt{M}_\delta^1 \rightsquigarrow_\delta \ldots \rightsquigarrow_\delta \mathtt{M}_\delta^{n_\delta} \qquad (1)$$

In a particular case, namely in Lemma 3, we use a deterministic version of the level-by-level strategy, called *leftmost-by-level*, which proceeds at every level from left to right, taking into account the shape of the different redexes in our calculus. That is to say, it chooses at every step the leftmost subterm of the shape $\mathtt{MN}$, where $\mathtt{M}$ is an abstraction, and, in case it is already a redex it reduces it, in case it is of the shape $(\lambda^!\mathtt{x}.\mathtt{P})\mathtt{N}$, where $\mathtt{N} \neq !\mathtt{Q}$, for some $\mathtt{Q}$, then it looks for the next redex in $\mathtt{N}$. This corresponds to using the call-by-name discipline for β-redexes and the call-by-value for !-redexes [19]. A formal definition of this strategy is given in Appendix A.2.

$\mathtt{M} \Longrightarrow \mathtt{N}$ denotes that $\mathtt{N}$ is obtained from $\mathtt{M}$ by performing one reduction step according to the leftmost-by-level strategy. All the notations for $\to$ are extended to $\rightsquigarrow$ and $\Longrightarrow$ in a straightforward way.

2.2 Representation of Functions

In order to represent functions, we first need to encode data. For booleans we can use the familiar encoding $\mathtt{true} = \lambda\mathtt{x}.\lambda\mathtt{y}.\mathtt{x}$ and $\mathtt{false} = \lambda\mathtt{x}.\lambda\mathtt{y}.\mathtt{y}$. For tally integers, the usual encoding of Church integers does not give w.f. terms; instead, we use the following encodings for Church integers and Church binary words:

$$\begin{array}{ll} n \in \mathbb{N}, & \underline{n} = \lambda^! f.!(\lambda\mathtt{x}.f\ (f\ ...(f\ \mathtt{x})...)) \\ w \in \{0,1\}^\star, \quad w = \langle i_1, ..., i_n \rangle, & \underline{w} = \lambda^! f_0.\lambda^! f_1.!(\lambda\mathtt{x}.f_{i_1}\ (f_{i_2}\ ...(f_{i_n}\ \mathtt{x})...)) \end{array}$$

By abuse of notation we also denote by $\underline{1}$ the term $\lambda^! f.!f$. Observe that the terms encoding booleans are of depth 0, while those representing Church integers and Church binary words are of depth 1. We denote the length of a word $w \in \{0,1\}^\star$ by $\mathbf{length}(w)$.

We represent computation on a binary word by considering applications of the form $\mathtt{P}!\underline{w}$, with a ! modality on the argument, because the program should be able to duplicate its input. Concerning the form of the result, since we want to allow computation at arbitrary depth, we require the output to be of the form $!^k\mathtt{D}$, where $k \in \mathbb{N}$ and $\mathtt{D}$ is one of the data representations above.

We thus say that a function $f : \{0,1\}^\star \to \{\mathtt{true}, \mathtt{false}\}$ is represented by a term (*program*) $\mathtt{P}$ if $\mathtt{P}$ is a closed normal term and there exists $k \in \mathbb{N}$ such that, for any $w \in \{0,1\}^\star$ and $\mathtt{D} = f(w) \in \{\mathtt{true}, \mathtt{false}\}$ we have: $\mathtt{P}!\underline{w} \xrightarrow{*} !^k\mathtt{D}$. This definition can be adapted to functions with other domains and codomains.

2.3 Complexity of Reduction

We study the complexity of the reduction of terms of the form $\mathtt{P}!\underline{w}$. Actually it is useful to analyze the complexity of the reduction of such terms to their k-normal form, i.e. by reducing until depth k, for $k \in \mathbb{N}$. We define the notation 2_i^n in the following way: $2_0^x = x$ and $2_{i+1}^x = 2^{2_i^x}$.

Proposition 3. *Given a program* $\mathtt{P}$*, for any* $k \geq 2$*, there exists a polynomial* q *such that, for any* $w \in \{0,1\}^\star$*,* $\mathtt{P}!\underline{w} \overset{*}{\rightsquigarrow} \mathtt{M}_k^1 \in \mathbf{nf}_{k-1}$ *in at most* $2_{k-2}^{q(n)}$ *steps, and* $|\mathtt{M}_k^1| \leq 2_{k-2}^{q(n)}$*, where* $n = \mathbf{length}(w)$*. In particular, in the case where* $k = 2$ *we have a polynomial bound* $q(n)$*.*

In the rest of this section we prove Prop. 3.

Let $\mathtt{M} = \mathtt{P}!\underline{w}$ and consider a level-by-level reduction sequence of $\mathtt{M}$, using the notations of (1). By Lemma 2 we know that the number of steps at depth i is bounded by $|\mathtt{M}_i^1|$ and that there are $(d+1)$ rounds. In order to bound the total number of steps it is thus sufficient to bound $|\mathtt{M}_i^1|$ by means of $|\mathtt{M}|$:

Lemma 3 (Size-Growth). *If* $\mathtt{M} \stackrel{*}{\Longrightarrow}_i \mathtt{M}'$ *by* c *reduction steps, then* $|\mathtt{M}'| \leq |\mathtt{M}| \cdot (|\mathtt{M}|+1)^c$ $(0 \leq i \leq \delta(\mathtt{M}))$.

The proof of Lemma 3 is quite delicate and is given in Appendix A.2.

Proof (Prop. 3). We proceed by induction on $k \geq 2$. We assume that $\mathtt{P}$ is of the form $\lambda^!\mathtt{y}.\mathtt{Q}$ (otherwise $\mathtt{P}!\underline{w}$ is already a normal form).

- Case $k = 2$:
  We consider a level-by-level reduction sequence of $\mathtt{P}!\underline{w}$. We need to examine reduction at depths 0 and 1. At depth 0 we have $(\lambda^!\mathtt{y}.\mathtt{Q})!\underline{w} \to \mathtt{Q}[\underline{w}/\mathtt{y}] = \mathtt{M}_1^1$. Observe that $\mathtt{M}_1^1 \in \mathbf{nf}_0$ because the occurrences of $\mathtt{y}$ in $\mathtt{Q}$ are at depth 1; denote by b the number of occurrences of $\mathtt{y}$ in $\mathtt{Q}$, which does not depend on n.
  Since $|\mathtt{Q}[\underline{w}/\mathtt{y}]|_1 \leq |\mathtt{Q}|_1 + b \cdot |\underline{w}|_0$ and $|\underline{w}|_0 = 2$ (by definition of the encoding), we have that $|\mathtt{M}_1^1|_1 = |\mathtt{Q}[\underline{w}/\mathtt{y}]|_1 \leq |\mathtt{Q}|_1 + 2b$. Let c be $|\mathtt{Q}|_1 + 2b$, which does not depend on n: then, by Lemma 2, the number of steps at depth 1 is bounded by c. This proves the first part of the statement.
  Let $\mathtt{M}_2^1 \in \mathbf{nf}_1$ be the term obtained after reduction at depth 1. By Prop. 1.(ii) we have that $\mathtt{M}_1^1 \stackrel{*}{\Longrightarrow}_1 \mathtt{M}_2^1$ and by Lemma 2 this reduction is done in c' steps, where $c' \leq |\mathtt{M}_1^1|_1 \leq c$, so by Lemma 3 we have that $|\mathtt{M}_2^1| \leq |\mathtt{M}_1^1| \cdot (|\mathtt{M}_1^1|+1)^c$. Moreover $|\mathtt{M}_1^1| \leq |\mathtt{Q}| + b|\underline{w}|$, so it is polynomial in n, and the statement is proved for $k = 2$.
- Assume the property holds for k and let us prove it for $k+1$.
  By assumption $\mathtt{M}$ reduces to $\mathtt{M}_k^1$ in at most $2_{k-2}^{q(n)}$ steps and $|\mathtt{M}_k^1| \leq 2_{k-2}^{q(n)}$. Let $\mathtt{M}_k^1 \stackrel{*}{\rightsquigarrow}_k \mathtt{M}_{k+1}^1 \in \mathbf{nf}_k$. By Lemma 2 this reduction sequence has at most $|\mathtt{M}_k^1|_k$ steps, and $|\mathtt{M}_k^1|_k \leq |\mathtt{M}_k^1| \leq 2_{k-2}^{q(n)}$. So on the whole $\mathtt{M}$ reduces to $\mathtt{M}_{k+1}^1$ in at most $2 \cdot 2_{k-2}^{q(n)} \leq 2_{k-2}^{2q(n)}$ steps. Moreover by Prop. 1.(ii) we have that $\mathtt{M}_k^1 \stackrel{*}{\Longrightarrow} \mathtt{M}_{k+1}^1$ and by Lemma 2 and Lemma 3 we get

  $$|\mathtt{M}_{k+1}^1| \leq |\mathtt{M}_k^1| \cdot (|\mathtt{M}_k^1|+1)^{2_{k-2}^{q(n)}} \leq 2_{k-2}^{q(n)} \cdot (2_{k-2}^{2q(n)})^{2_{k-2}^{q(n)}} \leq 2_{k-2}^{q(n)} \cdot 2^{2_{k-2}^{3q(n)}} \leq 2_{k-1}^{q'(n)}$$

  for some polynomial $q'(n)$.

Approximations. From Prop. 3 we can easily derive a $2^{q(n)}_{k-2}$ bound on the number of *steps* of the reduction of $\mathtt{P}!\underline{w}$ not only to its $(k-1)$-normal form, but also to its k-normal form $\mathtt{M}^1_{k+1}$. Unfortunately this does not yield directly a *time* bound $O(2^{q(n)}_{k-2})$ for the simulation of this reduction on a Turing machine, because during round k the size of the term at depth $k+1$ could grow exponentially. However if we are only interested in the result at depth k, the subterms at depth $k+1$ are actually irrelevant. For this reason we introduce a notion of *approximation*, inspired by the semantics of stratified coherence spaces [1], which allows us to compute up to a certain depth k, while ignoring what happens at depth $k+1$.

We extend the calculus with a constant $*$; its sizes $|*|_i$ are defined as for variables. If $\mathtt{M}$ is a term and $i \in \mathbb{N}$, we define its *i-th approximation* $\overline{\mathtt{M}}^i$ by: $\overline{!\mathtt{M}}^0 = !*$, $\overline{!\mathtt{M}}^{i+1} = !\,\overline{\mathtt{M}}^i$, $\overline{\mathtt{x}}^i = \mathtt{x}$, and for all other constructions $\overline{(\cdot)}^i$ acts as identity, e.g. $\overline{\mathtt{MN}}^i = \overline{\mathtt{M}}^i\overline{\mathtt{N}}^i$. See Appendix A.3 for more details.

So $\overline{\mathtt{M}}^i$ is obtained by replacing in $\mathtt{M}$ all subterms at depth $i+1$ by $*$. For instance we have $\overline{\underline{w}}^0 = \lambda^! f_0.\lambda^! f_1.!*$ and $\overline{\underline{w}}^{i+1} = \underline{w}$ for $i \geq 0$. The proof of the following lemma is given in Appendix A.3:

Lemma 4. *(i) Let $\mathtt{M} \to_i \mathtt{M}'$: if $j \leq i$ then $\overline{\mathtt{M}}^i \to_i \overline{\mathtt{M}'}^i$, otherwise $\overline{\mathtt{M}}^i = \overline{\mathtt{M}'}^i$.*
(ii) Let $\overline{\mathtt{M}}^i \to_i \overline{\mathtt{M}'}^i$: then $|\overline{\mathtt{M}'}^i| < |\overline{\mathtt{M}}^i|$.

Proposition 4. *Given a program $\mathtt{P}$, for any $k \geq 2$, there exists a polynomial q such that for any $w \in \{0,1\}^\star$, the reduction of $\overline{\mathtt{P}!\underline{w}}^k$ to its k-normal form can be computed in time $O(2^{q(n)}_{k-2})$ on a Turing machine, where $n = \mathbf{length}(w)$.*

Proof. Observe that $\overline{\mathtt{P}!\underline{w}}^k = \overline{\mathtt{P}}^k!\underline{w}$. By Prop. 3 and Lemma 4.(i), it reduces to its $(k-1)$-normal form $\overline{\mathtt{M}^1_k}^k$ in $O(2^{q(n)}_{k-2})$ steps and with intermediary terms of size $O(2^{q(n)}_{k-2})$. Now by Lemma 4.(ii) the reduction of $\overline{\mathtt{M}^1_k}^k$ at depth k is done in $O(2^{q(n)}_{k-2})$ steps and with intermediary terms of size $O(2^{q(n)}_{k-2})$. We can then conclude by using the fact that one reduction step in a term $\mathtt{M}$ can be simulated in time $p(|\mathtt{M}|)$ on a Turing machine, for a suitably chosen polynomial p.

3 Type System

We introduce a type assignment system for $\lambda^!$-calculus, based on ELL, such that all typed terms are also w.f. and the previous results are preserved.

Table 1. Derivation rules.

$$\frac{}{\Gamma, \mathtt{x} : \mathtt{A} \mid \Delta \mid \Theta \vdash \mathtt{x} : \mathtt{A}}\ (Ax^L) \qquad \frac{}{\Gamma \mid \Delta \mid \mathtt{x} : \sigma, \Theta \vdash \mathtt{x} : \sigma}\ (Ax^P)$$

$$\frac{\Gamma, \mathtt{x} : \mathtt{A} \mid \Delta \mid \Theta \vdash \mathtt{M} : \tau}{\Gamma \mid \Delta \mid \Theta \vdash \lambda \mathtt{x}.\mathtt{M} : \mathtt{A} \multimap \tau}\ (\multimap I^L) \qquad \frac{\Gamma \mid \Delta, \mathtt{x} : !\sigma \mid \Theta \vdash \mathtt{M} : \tau}{\Gamma \mid \Delta \mid \Theta \vdash \lambda^! \mathtt{x}.\mathtt{M} : !\sigma \multimap \tau}\ (\multimap I^I)$$

$$\frac{\Gamma_1 \mid \Delta \mid \Theta \vdash \mathtt{M} : \sigma \multimap \tau \quad \Gamma_2 \mid \Delta \mid \Theta \vdash \mathtt{N} : \sigma \quad \Gamma_1 \# \Gamma_2}{\Gamma_1, \Gamma_2 \mid \Delta \mid \Theta \vdash \mathtt{MN} : \tau}\ (\multimap E) \qquad \frac{\emptyset \mid \emptyset \mid \Theta' \vdash \mathtt{M} : \sigma}{\Gamma \mid !\Theta', \Delta \mid \Theta \vdash !\mathtt{M} : !\sigma}\ (!)$$

$$\frac{\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \mathtt{S} \quad \mathtt{a} \notin \mathrm{FTV}(\Gamma) \cup \mathrm{FTV}(\Delta) \cup \mathrm{FTV}(\Theta)}{\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \forall \mathtt{a}.\mathtt{S}}\ (\forall I) \qquad \frac{\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \forall \mathtt{a}.\mathtt{S}}{\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \mathtt{S}[\sigma/\mathtt{a}]}\ (\forall E)$$

$$\frac{\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \mathtt{S}[\mu \mathtt{a}.\mathtt{S}/\mathtt{a}]}{\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \mu \mathtt{a}.\mathtt{S}}\ (\mu I) \qquad \frac{\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \mu \mathtt{a}.\mathtt{S}}{\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \mathtt{S}[\mu \mathtt{a}.\mathtt{S}/\mathtt{a}]}\ (\mu E)$$

The set $\mathcal{T}$ of types are generated by the grammar

$$\begin{array}{lll} \mathtt{A} ::= \mathtt{a} \mid \mathtt{S} & & \text{(linear types)} \\ \mathtt{S} ::= \sigma \multimap \sigma \mid \forall \mathtt{a}.\mathtt{S} \mid \mu \mathtt{a}.\mathtt{S} & & \text{(strict linear types)} \\ \sigma ::= \mathtt{A} \mid !\sigma & & \text{(types)} \end{array}$$

where $\mathtt{a}$ ranges over a countable set of type variables. Observe that we consider both polymorphic types ($\forall \mathtt{a}.\mathtt{S}$) and type fixpoints ($\mu \mathtt{a}.\mathtt{S}$); the restriction of both abstractions to act on strict linear types is necessary for the subject reduction property.

A *basis* is a partial function from variables to types, with finite domain; given two bases Γ_1 and Γ_2, let $\Gamma_1 \# \Gamma_2$ iff $\mathrm{dom}(\Gamma_1) \cap \mathrm{dom}(\Gamma_2) = \emptyset$. Following the work of [4], we consider three different bases $\Gamma \mid \Delta \mid \Theta$, called respectively the *linear*, *modal* and *parking* basis, such that $\Gamma \# \Delta$, $\Gamma \# \Theta$ and $\Delta \# \Theta$. The premises in Γ assign to variables linear types, while the premises in Δ assign modal types.

The typing system proves statements of the shape $\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \sigma$, and derivations are denoted by Π, Σ. The rules are given in Table 1. Observe that, in rule $(\multimap E)$, $\mathtt{M}$ and $\mathtt{N}$ share variables in the modal and parking basis, but their linear bases must be disjoint. Note also that there is no axiom rule for variables in the modal basis, so the only way to introduce a variable in this basis is the (!) rule, moving variables from the parking to the modal basis. Finally, observe that there is no abstraction rule for variables in the parking basis: indeed parking variables only have

a "temporary" status, awaiting to be moved to the modal basis.
We say that a term $\mathtt{M}$ is *well-typed* iff there is a derivation $\Pi \triangleright \Gamma \mid \Delta \mid \emptyset \vdash \mathtt{M} : \sigma$ for some Γ, Δ, σ: indeed parking variables are only considered as an intermediary status before becoming modal variables. When all three bases are empty we denote the derivation by $\Pi \triangleright \vdash \mathtt{M} : \sigma$. The main difference w.r.t. the type system of [4] is the (!) rule: here we allow only the parking context to be non-empty, in order to ensure that typable terms are well formed: it is the key to obtain a $2_k^{\mathrm{poly}(n)}$ complexity bound for a specific k depending on the type, instead of just an elementary bound.

Both the type and depth of a term are preserved during reduction:

Theorem 1 (Subject Reduction). *$\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \sigma$ and $\mathtt{M} \to \mathtt{M}'$ imply $\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M}' : \sigma$.*

A sketch of proof of this Lemma is given in Appendix B.1.

Proposition 5. *If a term is well-typed, then it is also well-formed.*

The proof comes easily from the following proposition:

Proposition 6 (Variables Depth). *Let $\Gamma \mid \Delta \mid \Theta \vdash \mathtt{M} : \sigma$. Then:*

- *if $\mathtt{x} \in \mathrm{dom}(\Gamma) \cup \mathrm{dom}(\Theta)$, then $\mathtt{x}$ can only occur at depth 0 in $\mathtt{M}$;*
- *if $\mathtt{x} \in \mathrm{dom}(\Delta)$, then $\mathtt{x}$ can only occur at depth 1 in $\mathtt{M}$.*

3.1 Datatypes

In section 2.2 we introduced w.f. terms encoding data, for which we now define the following types, adapted from system F, representing respectively booleans, Church tally integers and Church binary words:

$$\mathrm{B} = \forall \mathtt{a}.\mathtt{a} \multimap \mathtt{a} \multimap \mathtt{a} \qquad \mathrm{N} = \forall \mathtt{a}.!(\mathtt{a} \multimap \mathtt{a}) \multimap !(\mathtt{a} \multimap \mathtt{a})$$

$$\mathrm{W} = \forall \mathtt{a}.!(\mathtt{a} \multimap \mathtt{a}) \multimap !(\mathtt{a} \multimap \mathtt{a}) \multimap !(\mathtt{a} \multimap \mathtt{a})$$

We also use Scott binary words, defined inductively as

$$\widehat{\epsilon} \stackrel{\mathrm{def}}{=} \lambda f_0.\lambda f_1.\lambda \mathtt{x}.\mathtt{x} \qquad \widehat{0w} \stackrel{\mathrm{def}}{=} \lambda f_0.\lambda f_1.\lambda \mathtt{x}.f_0\widehat{w} \qquad \widehat{1w} \stackrel{\mathrm{def}}{=} \lambda f_0.\lambda f_1.\lambda \mathtt{x}.f_1\widehat{w}$$

having type $\mathrm{W}_S \stackrel{\mathrm{def}}{=} \mu \mathtt{b}.\forall \mathtt{a}.(\mathtt{b} \multimap \mathtt{a}) \multimap (\mathtt{b} \multimap \mathtt{a}) \multimap (\mathtt{a} \multimap \mathtt{a})$.

The following properties ensure that, given a datatype, every derivation having such type reduces to a term having the desired shape:

Proposition 7. *(i) If $\vdash \mathtt{M} :!^k\mathrm{B}$ for $k \geq 0$ and $\mathtt{M} \in \mathbf{nf}_k$, then either $\mathtt{M} =!^k\mathtt{true}$ or $\mathtt{M} =!^k\mathtt{false}$.*
(ii) If $\vdash \mathtt{M} :!^k\mathrm{W}_S$ for $k \geq 0$ and $\mathtt{M} \in \mathbf{nf}_k$, then $\mathtt{M} =!^k\widehat{w}$ for some $\widehat{w}$.

The proof of Proposition 7.i is given in Appendix B.2.

3.2 Complexity Soundness and Completeness

We are interested in giving a precise account of the hierarchy of classes characterized by this typed $\lambda^!$-calculus. Denote by $\mathtt{FDTIME}(F(n))$ and by $\mathtt{DTIME}(F(n))$ respectively the class of functions and the class of predicates on binary words computable on a deterministic Turing machine in time $O(F(n))$; the complexity classes we are interested in, for $k \geq 0$, are:

$$\mathtt{k\text{-}EXP} = \cup_{i\in\mathbb{N}}\mathtt{DTIME}(2_k^{n^i}) \quad \text{and} \quad \mathtt{k\text{-}FEXP} = \cup_{i\in\mathbb{N}}\mathtt{FDTIME}(2_k^{n^i}).$$

In particular, observe that $\mathtt{PTIME} = \cup_{i\in\mathbb{N}}\mathtt{DTIME}(n^i) = \mathtt{0\text{-}EXP}$ and $\mathtt{FPTIME} = \cup_{i\in\mathbb{N}}\mathtt{FDTIME}(n^i) = \mathtt{0\text{-}FEXP}$.

Soundness Let $\mathcal{F}(\sigma)$ denote the set of closed terms representing functions, to which type σ can be assigned: we prove that $\mathcal{F}(!\mathrm{W} \multimap !^{k+2}\mathrm{B}) \subseteq k\text{-}\mathtt{EXP}$ and $\mathcal{F}(!\mathrm{W} \multimap !^{k+2}\mathrm{W}_S) \subseteq k\text{-}\mathtt{FEXP}$.

Theorem 2 (Soundness). *Let* $\vdash \mathtt{P} : !\mathrm{W} \multimap !^{k+2}\mathrm{B}$ *where* $\mathtt{P}$ *is a program, and let* $\vdash \underline{w} : \mathrm{W}$ *where* $\mathbf{length}(w) = n$*; then the reduction* $\mathtt{P}!\underline{w} \xrightarrow{*}_! !^{k+2}\mathtt{D}$ *can be computed in time* $2_k^{p(n)}$*, where* $\mathtt{D}$ *is either* `true` *or* `false` *and* p *is a polynomial.*

Proof. Recall that a program $\mathtt{P}$ is a typed closed term in normal form: we denote by $\mathtt{M}'$ the normal form of $\mathtt{P}!\underline{w}$. By Prop. 4 we know that $\overline{\mathtt{P}!\underline{w}}^{k+2}$ can be reduced to a term $\mathtt{N}$ in $\mathbf{nf}_{k+2}$ in time $O(2_k^{p(n)})$ on a Turing machine, where $n = \mathbf{length}(w)$. Moreover by Lemma 4.(i) and Prop. 1.(iii) we have that $\overline{\mathtt{M}'}^{k+2} = \mathtt{N}$. Now, as $\mathtt{P}!\underline{w}$ has type $!^{k+2}\mathrm{B}$, by Theorem 1 the term $\mathtt{M}'$ is a closed term of type $!^{k+2}\mathrm{B}$ and, by Prop. 7.(i), it is equal to $!^{k+2}\mathtt{true}$ or $!^{k+2}\mathtt{false}$. Then $\mathtt{N} = \overline{\mathtt{M}'}^{k+2} = \mathtt{M}'$, so $\mathtt{P}!\underline{w}$ can be computed in time $O(2_k^{p(n)})$.

Complexity soundness can be proved for functions by a similar proof, in which Prop. 7.(ii) is used in order to read the output as a Scott word:

Theorem 3. *Let* $\vdash \mathtt{P} : !\mathrm{W} \multimap !^{k+2}\mathrm{W}_S$ *where* $\mathtt{P}$ *is a program, and let* $\vdash \underline{w} : \mathrm{W}$ *where* $\mathbf{length}(w) = n$*; then the reduction* $\mathtt{P}!\underline{w} \xrightarrow{*}_! !^{k+2}\widehat{w'}$ *can be computed in time* $2_k^{p(n)}$*, where* p *is a polynomial.*

Completeness We proved that $\mathcal{F}(!\mathrm{W} \multimap !^{k+2}\mathrm{B}) \subseteq k\text{-}\mathtt{EXP}$ and $\mathcal{F}(!\mathrm{W} \multimap !^{k+2}\mathrm{W}_S) \subseteq k\text{-}\mathtt{FEXP}$; now we want to strengthen this result by examining the converse inclusions. To do so we simulate k-$\mathtt{EXP}$ time bounded Turing machines, by an iteration, so as to prove the following results:

Theorem 4 (Extensional Completeness).

- *Let f be a binary predicate in k-*EXP*, for any $k \geq 0$; then there is a term* M *representing f such that* $\vdash \mathtt{M} : !\mathrm{W} \multimap !^{k+2}\mathrm{B}$.
- *Let g be a function on binary words in k-*FEXP*, for $k \geq 0$; then there is a term* M *representing g such that* $\vdash \mathtt{M} : !\mathrm{W} \multimap !^{k+2}\mathrm{W}_S$.

The complete proof is given in Appendix B.3

Note that this characterization, for $k = 0$, does not account for the fact that FPTIME is closed by composition: indeed, programs of type $!\mathrm{W} \multimap !^{k+2}\mathrm{W}_S$ cannot be composed, since we do not have any coercion from W_S to W. For this reason, we explore an alternative characterization.

4 Refining Types for an Alternative Characterization

Our aim is to take a pair $\langle n, w\rangle$ to represent the word w' such that:

$$w' = \begin{cases} w & \text{if } \mathbf{length}(w) \leq n, \\ \text{the prefix of } w \text{ of length } n & \text{otherwise.} \end{cases}$$

For this reason, we introduce a new data-type using the connective $\otimes$ defined by $\sigma \otimes \tau \stackrel{\text{def}}{=} \forall \mathtt{a}.((\sigma \multimap \tau \multimap \mathtt{a}) \multimap \mathtt{a})$ on types and the corresponding constructions on terms:

$$\begin{aligned} \mathtt{M}_1 \otimes \mathtt{M}_2 &\stackrel{\text{def}}{=} \lambda \mathtt{x}.\mathtt{x}\mathtt{M}_1\mathtt{M}_2 \\ \lambda(\mathtt{x}_1 \otimes \mathtt{x}_2).\mathtt{M} &\stackrel{\text{def}}{=} \lambda \mathtt{x}.(\mathtt{x}\lambda \mathtt{y}_1\mathtt{y}_2.\lambda \mathtt{z}.\mathtt{z}\mathtt{y}_1\mathtt{y}_2)\lambda \mathtt{x}_1\mathtt{x}_2.\mathtt{M} \\ \lambda^!(\mathtt{x}_1 \otimes \mathtt{x}_2).\mathtt{M} &\stackrel{\text{def}}{=} \lambda \mathtt{x}.(\mathtt{x}\lambda^! \mathtt{y}_1\mathtt{y}_2.\lambda \mathtt{z}.\mathtt{z}!\mathtt{y}_1!\mathtt{y}_2)\lambda^! \mathtt{x}_1\mathtt{x}_2.\mathtt{M} \end{aligned}$$

Note that we cannot define the abstraction in the usual way, i.e. $\lambda(\mathtt{x}_1 \otimes \mathtt{x}_2).\mathtt{M} \stackrel{\text{def}}{=} \lambda \mathtt{x}.\mathtt{x}(\lambda \mathtt{x}_1.\lambda \mathtt{x}_2.\mathtt{M})$, otherwise we could not type pairs in a uniform way; moreover, when applied to a pair, this term reduces to the usual one.
The associated reduction rules $(\lambda(\mathtt{x}_1 \otimes \mathtt{x}_2).\mathtt{N})(\mathtt{M}_1 \otimes \mathtt{M}_2) \to \mathtt{N}[\mathtt{M}_1/\mathtt{x}_1, \mathtt{M}_2/\mathtt{x}_2]$ and $(\lambda^!(\mathtt{x}_1 \otimes \mathtt{x}_2).\mathtt{N})(!\mathtt{M}_1 \otimes !\mathtt{M}_2) \to \mathtt{N}[\mathtt{M}_1/\mathtt{x}_1, \mathtt{M}_2/\mathtt{x}_2]$ are derivable.

We represent a pair $\langle n, w\rangle$ through a term $!\underline{n} \otimes !^2\widehat{w}$ of type $!\mathrm{N} \otimes !^2\mathrm{W}_S$, i.e. a combined data-type containing a Church integer $!\underline{n}$ and a Scott word $!^2\widehat{w}$: in practice, $\underline{n}$ is meant to represent the length of a list, whose content is described by $\widehat{w}$. In order to mantain this invariant, when computing on elements $!\underline{n} \otimes !^2\widehat{w}$ of this data-type, the property that the length of w is inferior or equal to n is preserved.

As before, we need to be able to extract the result, in this case a pair:

Proposition 8. *If* $\vdash \mathtt{M} : !^k\mathrm{N} \otimes !^{k+1}\mathrm{W}_S$ *for* $k \geq 0$ *and* $\mathtt{M} \in \mathbf{nf}_{k+1}$*, then there exists* $m \in \mathbb{N}$ *and* $w \in \{0,1\}^\star$ *such that* $\mathtt{M} =_{!^k} \underline{m} \otimes !^{k+1}\widehat{w}$*.*

Then we are able to prove both soundness and completeness results:

Theorem 5. *Let* $\vdash \mathtt{P} : (!\mathrm{N} \otimes !^2\mathrm{W}_S) \multimap (!^{k+1}\mathrm{N} \otimes !^{k+2}\mathrm{W}_S)$ *where* $\mathtt{P}$ *is a program, then for any* $\underline{m}$ *and* $\widehat{w}$ *the reduction of* $\mathtt{P}(!\underline{m} \otimes !^2\widehat{w})$ *to its normal form can be computed in time* $2_k^{p(n)}$*, where* p *is a polynomial and* $n = m + \mathbf{length}(w)$*.*

Theorem 6. *Let* f *be a function on binary words in* k-FEXP*, for* $k \geq 0$*; then there is a term* $\mathtt{M}$ *representing* f *such that* $\vdash \mathtt{M} : (!\mathrm{N} \otimes !^2\mathrm{W}_S) \multimap (!^{k+1}\mathrm{N} \otimes !^{k+2}\mathrm{W}_S)$*.*

Proofs of the previous statements are in Appendix C.1-C.3.

Observe that we are able to compose two terms having type $(!\mathrm{N} \otimes !^2\mathrm{W}_S) \multimap (!\mathrm{N} \otimes !^2\mathrm{W}_S)$, so to illustrate the fact that FPTIME is closed by composition; moreover, if $f \in$ FPTIME and $g \in k$-FEXP, then we can compose terms representing them, which shows that $g \circ f \in k$-FEXP.

While the previous characterization of k-FEXP in Section 3.2 offers the advantage of simplicity, because it uses classical data-types (Church and Scott binary words), this second characterization offers a better account of the closure properties of these complexity classes, at the price of a slightly more involved representation of words.

5 Conclusions

We have shown how the concept of !-stratification coming from linear logic can be fruitfully employed in λ-calculus and characterize the hierarchies k-EXP and k-FEXP, including the classes PTIME and FPTIME. A nice aspect of our system with respect to former polyvalent characterizations [10,13] is that the complexity bound can be deduced by looking only at the interface of the program (its type) without refering to the constructions steps. In our proofs we have carefully distinguished the respective roles played by syntactic ingredients (well-formedness) and typing ingredients. This has allowed us to illustrate how types can provide two different characterizations of the class k-FEXP, based on the use of different data-types. We believe that the separation between syntactic and typing arguments can facilitate the possible future usage of our calculus with other type

systems. As future work it would be challenging to investigate if similar characterizations could be obtained for other hierarchies, like possibly space hierarchies.

References

1. Baillot, P.: Stratified coherence spaces: a denotational semantics for light linear logic. Theor. Comput. Sci. 318(1-2), 29–55 (2004)
2. Baillot, P.: Elementary linear logic revisited for polynomial time and an exponential time hierarchy. In: Yang, H. (ed.) APLAS. Lecture Notes in Computer Science, vol. 7078, pp. 337–352. Springer (2011)
3. Bellantoni, S., Cook, S.A.: A new recursion-theoretic characterization of the polytime functions. Computational Complexity 2, 97–110 (1992)
4. Coppola, P., Dal Lago, U., Ronchi Della Rocca, S.: Light logics and the call-by-value lambda-calculus. Logical Methods in Computer Science 4(4) (2008)
5. Dal Lago, U.: Context semantics, linear logic, and computational complexity. ACM Trans. Comput. Log. 10(4) (2009)
6. Dal Lago, U., Masini, A., Zorzi, M.: Quantum implicit computational complexity. Theor. Comput. Sci. 411(2), 377–409 (2010)
7. Danos, V., Joinet, J.B.: Linear logic and elementary time. Inf. Comput. 183(1), 123–137 (2003)
8. Girard, J.Y.: Light linear logic. Inf. Comput. 143(2), 175–204 (1998)
9. Jones, N.D.: Computability and complexity - from a programming perspective. Foundations of computing series, MIT Press (1997)
10. Jones, N.D.: The expressive power of higher-order types or, life without cons. J. Funct. Program. 11(1), 5–94 (2001)
11. Lafont, Y.: Soft linear logic and polynomial time. Theor. Comput. Sci. 318(1-2), 163–180 (2004)
12. Leivant, D.: Predicative recurrence and computational complexity I: word recurrence and poly-time. In: Feasible Mathematics II, pp. 320–343. Birkhauser (1994)
13. Leivant, D.: Calibrating computational feasibility by abstraction rank. In: LICS. pp. 345–. IEEE Computer Society (2002)
14. Leivant, D., Marion, J.Y.: Lambda-calculus characterizations of poly-time. Fundam. Inform. 19(1/2), 167–184 (1993)
15. Madet, A.: Implicit Complexity in Concurrent Lambda-Calculi. Ph.D. thesis, Université Paris 7 (December 2012), http://tel.archives-ouvertes.fr/tel-00794977
16. Madet, A., Amadio, R.M.: An elementary affine lambda-calculus with multithreading and side effects. In: Ong, C.H.L. (ed.) TLCA. Lecture Notes in Computer Science, vol. 6690, pp. 138–152. Springer (2011)
17. Marion, J.Y.: A type system for complexity flow analysis. In: LICS. pp. 123–132. IEEE Computer Society (2011)
18. Mazza, D.: Linear logic and polynomial time. Mathematical Structures in Computer Science 16(6), 947–988 (2006)
19. Ronchi Della Rocca, S., Paolini, L.: The Parametric Lambda-Calculus: a Metamodel for Computation. Texts in Theoretical Computer Science, Springer, Berlin (2004), `http://www.springer.com/sgw/cda/frontpage/0,,5-40356-72-14202886-0,00.html`
20. Ronchi Della Rocca, S., Roversi, L.: Lambda-calculus and intuitionistic linear logic. Studia Logica 59(3), 417–448 (1997)

21. Terui, K.: Light affine lambda-calculus and polynomial time strong normalization. Arch. Math. Log. 46(3-4), 253–280 (2007)

APPENDIX

A The $\lambda^!$-calculus

A.1 Proof of of Proposition 2

Let $\delta = \delta(\mathtt{M})$. First by Prop. 1 we know that to reduce $\mathtt{M}$ it is sufficient to reduce it to a δ-normal form. We will prove for any $i \leq \delta$ the following statement by induction on i:

$\mathcal{H}(i)$: any maximal level-by-level reduction sequence s of $\mathtt{M}$ contains an i-normal form.

For proving $\mathcal{H}(0)$, just observe that by Lemma 2 the number of reduction steps at depth 0 is bounded by $|\mathtt{M}|_0$.

Now assume $\mathcal{H}(i)$ for $i < \delta$, and consider a maximal level-by-level reduction sequence s. Let $\mathtt{M}_i$ be the first i-normal form reached by s. Then by Prop. 1.(i) all reduction steps in s after $\mathtt{M}_i$ occur at depth strictly superior to i. Moreover by Lemma 2 there are at most $|\mathtt{M}_i|_{i+1}$ reduction steps at depth $i+1$, therefore s does reach an $(i+1)$-normal form and thus $\mathcal{H}(i+1)$ is proved. The statement then follows from $\mathcal{H}(\delta)$.

A.2 Proof of Lemma 3

In order to prove this Lemma, we need a formal definition of the leftmost-by-level strategy. To this aim, we need some additional definitions for contexts. We consider a more general notion of context than that introduced in Sect. 2.1, with possibly several holes:

$$\mathcal{C} ::= \Box \mid \mathtt{x} \mid \lambda\mathtt{x}.\mathcal{C} \mid \lambda^!\mathtt{x}.\mathcal{C} \mid \mathcal{C}\mathcal{C} \mid !\mathcal{C}$$

We call *simple contexts* the contexts defined in Sect. 2.1, with only one hole.

We denote by $\mathcal{C}[\underbrace{\_, ..., \_}_{n}]_i$ with $i \in \mathbb{N}$ a context that has exactly n subterms at depth i, which are all holes. Note that this definition implies that, given a term $\mathtt{M}$ and an integer i, there is a unique way of representing it as $\mathcal{C}[\mathtt{N}_1, ..., \mathtt{N}_n]_i$. For example, let $\mathtt{M} = (\lambda^!\mathtt{x}.\mathtt{y}!\mathtt{x}!(\lambda^!\mathtt{z}.!\mathtt{z}))!I$, where $I = \lambda\mathtt{x}.\mathtt{x}$. Then $M = \mathcal{C}[\mathtt{x}, \lambda^!\mathtt{z}.!\mathtt{z}, I]_1$, where $\mathcal{C} = (\lambda^!\mathtt{x}.\mathtt{y}!\Box!\Box)!\Box$.

Now we define a notion of evaluation context which will be useful to describe the leftmost-by-level strategy.

Definition 2 (Stratified evaluation context). *The stratified evaluation context of* $\mathtt{M}$ *at depth* i $(i \leq \delta(\mathtt{M}))$*, denoted by* $\mathcal{E}_i^{\mathtt{M}}$*, is a simple context defined by induction on* i*:*

– $\mathcal{E}_0^{\mathtt{M}}$ *is defined inductively as*

$$\begin{array}{ll}
\boxdot & \text{if } \mathtt{M} = (\lambda \mathtt{x}.\mathtt{P})\mathtt{Q} \text{ or } \mathtt{M} = (\lambda^! \mathtt{x}.\mathtt{P})!\mathtt{Q} \\
(\lambda^! \mathtt{x}.\mathtt{P})\mathcal{E}_0^{\mathtt{Q}} & \text{if } \mathtt{M} = (\lambda^! \mathtt{x}.\mathtt{P})\mathtt{Q} \text{ and } \mathtt{Q} \neq !\mathtt{Q}' \\
(\lambda^! \mathtt{x}.\mathcal{E}_0^{\mathtt{P}})\mathtt{Q} & \text{if } \mathtt{M} = (\lambda^! \mathtt{x}.\mathtt{P})\mathtt{Q}, \mathtt{Q} \in \mathbf{nf}_0 \text{ and } \mathtt{Q} \neq !\mathtt{Q}' \\
\lambda \mathtt{x}.\mathcal{E}_0^{\mathtt{N}} & \text{if } \mathtt{M} = \lambda \mathtt{x}.\mathtt{N} \\
\lambda^! \mathtt{x}.\mathcal{E}_0^{\mathtt{N}} & \text{if } \mathtt{M} = \lambda^! \mathtt{x}.\mathtt{N} \\
\mathtt{N}\mathcal{E}_0^{\mathtt{Q}} & \text{if } \mathtt{M} = \mathtt{NQ}, \mathtt{N} \text{ is not an abstraction and } \mathtt{N} \in \mathbf{nf}_0 \\
\mathcal{E}_0^{\mathtt{N}}\mathtt{Q} & \text{if } \mathtt{M} = \mathtt{NQ} \text{ and } \mathtt{N} \text{ is not an abstraction} \\
\textit{undefined} & \textit{in any other case}
\end{array}$$

– *Let* $\mathtt{M} = \mathcal{C}[\mathtt{N}_1, ..., \mathtt{N}_n]_i$*, and let* $\mathtt{N}_k$ *(*$1 \leq k \leq n$*) be the leftmost subterm of* M *such that* $\mathtt{N}_k \notin \mathbf{nf}_i$*: then* $\mathcal{E}_i^{\mathtt{M}} = \mathcal{E}_0^{\mathtt{N}_k}$

The evaluation context of a term is defined accordingly as follows.

Definition 3 (Evaluation context). *The evaluation context* $\mathcal{E}$ *of a term* M*, denoted by* $\mathcal{E}^{\mathtt{M}}$*, is defined by the following procedure:*

```
i := 0;
while i ≤ δ(M)
```

{ if $\mathcal{E}_i^{\mathtt{M}}$ is defined then $\mathcal{E}^{\mathtt{M}} = \mathcal{E}_i^{\mathtt{M}}$ else $i := i + 1$ }

Now the leftmost-by-level strategy $\Longrightarrow$ is described by:

$\mathtt{M} \Longrightarrow \mathtt{M}'$ if there are an evaluation context $\mathcal{E}^{\mathtt{M}}$, a redex N and a term $\mathtt{N}'$ such that $\mathtt{M} = \mathcal{E}^{\mathtt{M}}[\mathtt{N}]$, $\mathtt{M}' = \mathcal{E}^{\mathtt{M}}[\mathtt{N}']$ and $\mathtt{N} \to \mathtt{N}'$.

In order to find a sharp bound for the increase of size at depth i or greater, we want to find a measure at depth i which decreases with every reduction at depth $i-1$, for any $i > 0$. Clearly the size at depth i does not have such a property, as any !-redex can make the size at depth i grow quadratically.

Let us consider $\mathtt{M} \Longrightarrow_i \mathtt{M}'$ [3]: the measure we will use is the maximum number of potential duplications of a subterm at depth i during the reduction of M, called *active points*, denoted by $\lceil \mathtt{M} \rceil_i$. Such measure is dynamic, since it counts the number of occurrences of variables bound by $\lambda^!$ which could be replaced during the reduction, so it depends strictly on the evaluation strategy.

Definition 4. *1. The maximum number of* $\lambda^!$*-bounded occurrences at depth* i *in* M*, denoted by* $\mathtt{o}_i(\mathtt{M})$*, for* $i > 0$*, is defined inductively as follows:*

[3] By the α-rule, we assume that all bound variables in M are different.

- *If* $i = 1$, *then*
  - $\mathtt{M} = \mathtt{x}$ *implies* $\mathtt{o}_1(\mathtt{M}) = 0$;
  - $\mathtt{M} = \lambda\mathtt{x}.\mathtt{P}$ *implies* $\mathtt{o}_1(\mathtt{M}) = \mathtt{o}_1(\mathtt{P})$;
  - $\mathtt{M} = \lambda^!\mathtt{x}.\mathtt{P}$ *implies* $\mathtt{o}_1(\mathtt{M}) = \max\{\mathrm{occ}(\mathtt{x},\mathtt{P}), \mathtt{o}_1(\mathtt{P})\}$;
  - $\mathtt{M} = \mathtt{NP}$ *implies* $\mathtt{o}_1(\mathtt{M}) = \max\{\mathtt{o}_1(\mathtt{N}), \mathtt{o}_1(\mathtt{P})\}$;
  - $\mathtt{M} = !\mathtt{N}$ *implies* $\mathtt{o}_1(\mathtt{M}) = 0$
- *If* $i > 1$, *then* $\mathtt{M} = \mathcal{C}[\mathtt{N}_1, ..., \mathtt{N}_m]_{i-1}$ *implies* $\mathtt{o}_1(\mathtt{M}) = \max_{1\leq j\leq m} \mathtt{o}_1(\mathtt{N}_j)$.

2. *The number of active points of* $\mathtt{M}$ *at depth* i, *denoted by* $\lceil\mathtt{M}\rceil_i$, *is defined by induction on* $\mathcal{E}^{\mathtt{M}}$ *as follows:*
   - *If* $\mathcal{E}^{\mathtt{M}} = \mathcal{E}^{\mathtt{M}}_0$, *then*
     - $\mathcal{E}^{\mathtt{M}}_0 = \boxdot$ *implies* $\lceil\mathtt{M}\rceil_1 = \mathtt{o}_1(\mathtt{M})$;
     - $\mathcal{E}^{\mathtt{M}}_0 = \lambda\mathtt{x}.\mathcal{E}^{\mathtt{N}}_0$ *implies* $\lceil\mathtt{M}\rceil_1 = \lceil\mathtt{N}\rceil_1$;
     - $\mathcal{E}^{\mathtt{M}}_0 = \lambda^!\mathtt{x}.\mathcal{E}^{\mathtt{N}}_0$ *implies* $\lceil\mathtt{M}\rceil_1 = \lceil\mathtt{N}\rceil_1$;
     - $\mathcal{E}^{\mathtt{M}}_0 = \mathtt{P}\mathcal{E}^{\mathtt{N}}_0$ *implies* $\lceil\mathtt{M}\rceil_1 = \lceil\mathtt{N}\rceil_1$;
     - $\mathcal{E}^{\mathtt{M}}_0 = \mathcal{E}^{\mathtt{P}}_0\mathtt{N}$ *implies* $\lceil\mathtt{M}\rceil_1 = \max\{\lceil\mathtt{P}\rceil_1, \mathtt{o}_1(\mathtt{N})\}$;
     - $\mathcal{E}^{\mathtt{M}}_0 = (\lambda^!\mathtt{x}.\mathtt{P})\mathcal{E}^{\mathtt{N}}_0$ *implies* $\lceil\mathtt{M}\rceil_1 = \max\{\mathtt{o}_1(\lambda^!\mathtt{x}.\mathtt{P}), \lceil\mathtt{N}\rceil_1\}$;
     - $\mathcal{E}^{\mathtt{M}}_0 = (\lambda^!\mathtt{x}.\mathcal{E}^{\mathtt{P}}_0)\mathtt{N}$ *implies* $\lceil\mathtt{M}\rceil_1 = \lceil\mathtt{P}\rceil_1$.
   - *If* $\mathcal{E}^{\mathtt{M}} = \mathcal{E}^{\mathtt{M}}_i$ *for some* $i > 0$, *then by definition* $\mathtt{M} = \mathcal{C}[\mathtt{N}_1, ..., \mathtt{N}_m]_i$, *and* $\lceil\mathtt{M}\rceil_{i+1} = \max_{1\leq j\leq m}\lceil\mathtt{N}_j\rceil_1$.
   - *If* $\mathcal{E}^{\mathtt{M}}_i$ *is undefined for all* $i \geq 0$, *then* $\lceil\mathtt{M}\rceil_{i+1} = 0$.

Observe that the number of active points is defined starting from depth 1: indeed there are no active points at depth 0, because all variables bound by $\lambda^!$ occur at depth greater than 1. Moreover, it is easy to see that $\lceil\mathtt{M}\rceil_1 \leq |\mathtt{M}|_1$ for any $\mathtt{M}$.

Now our goal is to show that the number of active points does not increase during a reduction; to do so, we first prove that the number of active points of a term $\mathtt{M}$ at depth i is bounded by $\mathtt{o}_i(\mathtt{M})$, and that reducing a redex $\mathtt{M}$ to $\mathtt{M}'$ implies $\mathtt{o}_1(\mathtt{M}') \leq \mathtt{o}_1(\mathtt{M})$.

Lemma 5. *1. If* $\mathtt{x}$ *occurs at level* 0 *in* $\mathtt{P}$, *then* $\mathtt{o}_i(\mathtt{P}[\mathtt{Q}/\mathtt{x}]) \leq \max\{\mathtt{o}_i(\mathtt{P}), \mathtt{o}_i(\mathtt{Q})\}$, *otherwise* $\mathtt{o}_i(\mathtt{P}[\mathtt{Q}/\mathtt{x}]) \leq \mathtt{o}_i(\mathtt{P})$.

2. $\lceil\mathtt{M}\rceil_{i+1} \leq \mathtt{o}_{i+1}(\mathtt{M})$ *for every* $\mathtt{M}$, $i \geq 0$.

3. Let $\mathtt{M} = (\lambda\mathtt{x}.\mathtt{P})\mathtt{Q}$ *or* $\mathtt{M} = (\lambda^!\mathtt{x}.\mathtt{P})!\mathtt{Q}$: *then* $\mathtt{M}' = \mathtt{P}[\mathtt{Q}/\mathtt{x}]$ *implies* $\mathtt{o}_1(\mathtt{M}') \leq \lceil\mathtt{M}\rceil_1$.

Proof. All proofs are easy.

Lemma 6. $\mathtt{M} \Longrightarrow \mathtt{M}'$ *implies* $\lceil\mathtt{M}'\rceil_{i+1} \leq \lceil\mathtt{M}\rceil_{i+1}$, *for every* $i \geq 0$.

Proof. We proceed by induction on i.

If $i = 0$, then we proceed by induction on $\mathcal{E}_0^{\mathtt{M}}$. Observe that if $\mathtt{M}' \in \mathbf{nf}_0$ then the proof is trivial, since $\lceil \mathtt{M}' \rceil_1 = 0 \leq \lceil \mathtt{M} \rceil_1$; therefore we consider all possible cases where $\mathcal{E}_0^{\mathtt{M}'}$ is defined. As an example, let $\mathcal{E}_0^{\mathtt{M}} = (\lambda^!\mathtt{x}.\mathtt{P})\mathcal{E}_0^{\mathtt{N}}$, so $\mathtt{M} = (\lambda^!\mathtt{x}.\mathtt{P})\mathtt{N}$ and $\mathtt{M}' = (\lambda^!\mathtt{x}.\mathtt{P})\mathtt{N}'$ where $\mathtt{N} \Longrightarrow_0 \mathtt{N}'$. By inductive hypothesis, $\lceil \mathtt{N}' \rceil_1 \leq \lceil \mathtt{N} \rceil_1$. We consider three cases:

- if $\mathcal{E}_0^{\mathtt{M}'} = (\lambda^!\mathtt{x}.\mathtt{P})\mathcal{E}_0^{\mathtt{N}'}$, then the proof follows by induction;
- if $\mathcal{E}_0^{\mathtt{M}'} = (\lambda^!\mathtt{x}.\mathcal{E}_0^{\mathtt{P}})\mathtt{N}'$, then by definition $\lceil \mathtt{M}' \rceil_1 = \lceil \mathtt{P} \rceil_1$ and by Lemma 5.(2) $\lceil \mathtt{P} \rceil_1 \leq \max\{\mathtt{o}_1(\lambda^!\mathtt{x}.\mathtt{P}), \lceil \mathtt{N} \rceil_1\} = \lceil \mathtt{M} \rceil_1$;
- if $\mathcal{E}_0^{\mathtt{M}'} = \boxdot$, then $\mathtt{N}' = !\mathtt{N}''$ for some term $\mathtt{N}''$, and $\mathtt{M}' = (\lambda^!\mathtt{x}.\mathtt{P})!\mathtt{N}''$, so by definition $\lceil \mathtt{M}' \rceil_1 = \mathtt{o}_1(\lambda^!\mathtt{x}.\mathtt{P}) \leq \max\{\mathtt{o}_1(\lambda^!\mathtt{x}.\mathtt{P}), \lceil \mathtt{N} \rceil_1\} = \lceil \mathtt{M} \rceil_1$;

Finally the property can be easily proved for $i > 0$ by using the definition of context.

We now need to study how performing a $\Longrightarrow_n$ step at depth n changes the size of the whole term at higher depths.

Lemma 7. $\mathtt{M} \Longrightarrow_n \mathtt{N}$ *implies* $|\mathtt{N}|_i \leq \lceil \mathtt{M} \rceil_{n+1} \cdot |\mathtt{M}|_i + |\mathtt{M}|_i$ *for every* $i > n$.

Proof. We proceed by induction on n, and then by induction on $\mathcal{E}_n^{\mathtt{M}}$, again by considering all possible cases.

In this way we can obtain easily a sort of stratified version of Lemma 3.

Lemma 8. *Let* $\mathtt{M}$ *be a well-formed term:* $\mathtt{M} \stackrel{*}{\Longrightarrow}_n \mathtt{M}'$ *in* k *reduction steps implies* $|\mathtt{M}|'_i \leq |\mathtt{M}|_i \cdot (\lceil \mathtt{M} \rceil_{n+1} + 1)^k$ *for every* $i > n$.

Proof. Let $\mathtt{M} = \mathtt{M}_0 \Longrightarrow_n \mathtt{M}_1 \Longrightarrow_n ... \Longrightarrow_n \mathtt{M}_k = \mathtt{M}'$: we proceed by induction on k.

If $k = 1$, then $\mathtt{M} \Longrightarrow \mathtt{M}'$ and $\lceil \mathtt{M} \rceil_{n+1} = |\mathtt{M}|_{n+1}$, so by Lemma 7 $|\mathtt{M}|'_i \leq |\mathtt{M}|_i \cdot (\lceil \mathtt{M} \rceil_{n+1} + 1)$.

Now let $\mathtt{M} \Longrightarrow_n \mathtt{M}^{h-1}$ in h reduction steps, for some $h > n$, so by inductive hypothesis $|\mathtt{M}^{h-1}|_i \leq |\mathtt{M}|_i \cdot (\lceil \mathtt{M} \rceil_{n+1} + 1)^{h-1}$ for every $i > n$.

If $\mathtt{M}^{h-1} \Longrightarrow_n \mathtt{M}^h$, then

$$
\begin{aligned}
|\mathtt{M}^h|_i &\leq |\mathtt{M}^{h-1}|_i \cdot (\lceil \mathtt{M}^{h-1} \rceil_{n+1} + 1) && \text{by Lemma 7} \\
&\leq |\mathtt{M}^{h-1}|_i \cdot (\lceil \mathtt{M} \rceil_{n+1} + 1) && \text{by Lemma 5} \\
&\stackrel{\text{Hp}}{\leq} |\mathtt{M}|_i \cdot (\lceil \mathtt{M} \rceil_{n+1} + 1) \cdot (\lceil \mathtt{M} \rceil_{n+1} + 1)^{h-1} \\
&= |\mathtt{M}|_i \cdot (\lceil \mathtt{M} \rceil_{n+1} + 1)^h
\end{aligned}
$$

The proof of Lemma 3 now follows trivially from Lemma 8.

A.3 Proof of Lemma 4

Approximations $\overline{\mathtt{M}}^i$ and $\overline{\mathcal{C}}^i$ of a term and a context are defined inductively by:

$$\overline{!\mathtt{M}}^0 = !*, \quad \overline{!\mathtt{M}}^{i+1} = !\,\overline{\mathtt{M}}^i, \quad \overline{\mathtt{x}}^i = \mathtt{x}, \quad \overline{\Box}^i = \Box,$$
$$\overline{\mathtt{MN}}^i = \overline{\mathtt{M}}^i\overline{\mathtt{N}}^i, \quad \overline{\lambda\mathtt{x}.\mathtt{M}}^i = \lambda\mathtt{x}.\overline{\mathtt{M}}^i, \quad \overline{\lambda^!\mathtt{x}.\mathtt{M}}^i = \lambda^!\mathtt{x}.\overline{\mathtt{M}}^i.$$

We need first to examine the effect of approximation on substitutions and on contexts.

Lemma 9.
- *If all occurrences of* $\mathtt{x}$ *in* $\mathtt{M}$ *are at depth 0, then* $\overline{\mathtt{M}[\mathtt{N}/\mathtt{x}]}^i = \overline{\mathtt{M}}^i[\overline{\mathtt{N}}^i/\mathtt{x}]$.
- *If all occurrences of* $\mathtt{x}$ *in* $\mathtt{M}$ *are at depth 1, then* $\overline{\mathtt{M}[\mathtt{N}/\mathtt{x}]}^0 = \overline{\mathtt{M}}^0$, $\overline{\mathtt{M}[\mathtt{N}/\mathtt{x}]}^{i+1} = \overline{\mathtt{M}}^{i+1}[\overline{\mathtt{N}}^i/\mathtt{x}]$, *for* $i \geq 0$.

In the rest of this Section denote by $\mathcal{C}[\_]_i$ a context with a single hole, which is at depth i; note that here the context might contain other subterms at depth i than this hole. Note that it follows from the definition that $\overline{\mathcal{C}[\mathtt{M}]_j}^i = \overline{\mathcal{C}}^i$, if $i < j$, and $\overline{\mathcal{C}[\mathtt{M}]_j}^i = \overline{\mathcal{C}}^i[\overline{\mathtt{M}}^{i-j}]_j$, if $i \geq j$.

Lemma 10. *We have for* $i \geq 0$*:*

$$\overline{(\lambda\mathtt{x}.\mathtt{M})\mathtt{N}}^i \to \overline{\mathtt{M}[\mathtt{N}/\mathtt{x}]}^i$$
$$\overline{(\lambda^!\mathtt{x}.\mathtt{M})!\mathtt{N}}^i \to \overline{\mathtt{M}[\mathtt{N}/\mathtt{x}]}^i$$

and these reduction steps take place at depth 0.

Proof. It is sufficient to examine each case and to use Lemma 9.

Proof (of Lemma 4).

(i) As $\mathtt{M} \to \mathtt{M}'$ by one step at depth j, we have that $\mathtt{M} = \mathcal{C}[\mathtt{P}]_j$ and $\mathtt{M}' = \mathcal{C}[\mathtt{P}']_j$where $\mathtt{P}$ is a redex and $\mathtt{P}'$ is its contractum. Therefore by Lemma 9:
- If $i + 1 \leq j$, then $\overline{\mathtt{M}}^i = \overline{\mathtt{M}'}^i$,
- If $i \geq j$, then $\overline{\mathtt{M}}^i = \overline{\mathcal{C}}^i[\overline{\mathtt{P}}^{i-j}]_j \to \overline{\mathcal{C}}^i[\overline{\mathtt{P}'}^{i-j}]_j = \overline{\mathtt{M}'}^i$, by using Lemma 10, and the reduction takes place at depth j.

(ii) Assume that $\overline{\mathtt{M}}^i \to \overline{\mathtt{M}'}^i$ by one step at depth i. We already know that

$$|\overline{\mathtt{M}'}^i|_j \leq |\overline{\mathtt{M}}^i|_j, \quad \text{for } j < i,$$
$$|\overline{\mathtt{M}'}^i|_i < |\overline{\mathtt{M}}^i|_i.$$

We now need to examine what happens to $|\overline{\mathtt{M}}^i|_{i+1}$.
We have that $\overline{\mathtt{M}}^i = \mathcal{C}[\mathtt{P}]_i$ and $\overline{\mathtt{M}'}^i = \mathcal{C}[\mathtt{P}']_i$ where $\mathtt{P}$ is a redex and $\mathtt{P}'$ is its contractum.

– If $\mathtt{P}$ is a β redex then we have $|\overline{\mathtt{M}'}^i|_{i+1} < |\overline{\mathtt{M}}^i|_{i+1}$.
– If $\mathtt{P}$ is a ! redex then as $\overline{\mathtt{M}}^i = \mathcal{C}[\mathtt{P}]_i$ we have that $\mathtt{P} = (\lambda^!\mathtt{x}.\mathtt{N})!*$. Moreover as the term is well-formed, if there is an occurrence of $\mathtt{x}$ in $\mathtt{N}$ then it should be at depth 1 in $\mathtt{N}$, so at depth $i+1$ in $\overline{\mathtt{M}}^i$. But any subterm of $\overline{\mathtt{M}}^i$ at depth $i+1$ is of the form $*$. So $\mathtt{x}$ has no occurrence in $\mathtt{N}$, and thus $\mathtt{P}' = \mathtt{N}$ and $|\overline{\mathtt{M}'}^i|_{i+1} < |\overline{\mathtt{M}}^i|_{i+1}$.

Moreover for $j \geq 2$ we have that $|\overline{\mathtt{M}'}^i|_j = 0 = |\overline{\mathtt{M}}^i|_j$. So the statement follows.

B Type system

B.1 Proof of Theorem 1

Remark 1. $\Pi \triangleright \Gamma \mid \Delta \mid \Theta \vdash !\mathtt{M} : !\sigma$ implies Π ends with an application of rule (!).

Lemma 11 (Weakening). *If $\Pi \triangleright \Gamma_1 \mid \Delta_1 \mid \Theta_1 \vdash \mathtt{M} : \sigma$, then there is a derivation $\Sigma \triangleright \Gamma_1, \Gamma_2 \mid \Delta_1, \Delta_2 \mid \Theta_1, \Theta_2 \vdash \mathtt{M} : \sigma$, for every $\Gamma_2, \Delta_2, \Theta_2$ disjoint from each other and from $\Gamma_1, \Delta_1, \Theta_1$.*

Lemma 12 (Substitution). *Let $\Gamma_1 \# \Gamma_2$. Then:*

(i) If $\Pi \triangleright \Gamma_1, \mathtt{x} : \mathtt{A} \mid \Delta \mid \Theta \vdash \mathtt{M} : \tau$ and $\Sigma \triangleright \Gamma_2 \mid \Delta \mid \Theta \vdash \mathtt{N} : \mathtt{A}$, then there is a derivation $S(\Sigma, \Pi) \triangleright \Gamma_1, \Gamma_2 \mid \Delta \mid \Theta \vdash \mathtt{M}[\mathtt{N}/\mathtt{x}] : \tau$.
(ii) If $\Pi \triangleright \Gamma_1 \mid \Delta \mid \Theta, \mathtt{x} : \sigma \vdash \mathtt{M} : \tau$ and $\Sigma \triangleright \emptyset \mid \Delta \mid \Theta \vdash \mathtt{N} : \sigma$, then there is a derivation $S(\Sigma, \Pi) \triangleright \Gamma_1 \mid \Delta \mid \Theta \vdash \mathtt{M}[\mathtt{N}/\mathtt{x}] : \tau$.
(iii) If $\Pi \triangleright \Gamma_1 \mid \Delta, \mathtt{x} : !\sigma \mid \Theta \vdash \mathtt{M} : \tau$ and $\Sigma \triangleright \Gamma_2 \mid \Delta \mid \Theta \vdash !\mathtt{N} : !\sigma$, then there is a derivation $S(\Sigma, \Pi) \triangleright \Gamma_1, \Gamma_2 \mid \Delta \mid \Theta \vdash \mathtt{M}[\mathtt{N}/\mathtt{x}] : \tau$.

Proof. All three points follow easily by induction on Π. In particular it is worth noticing the case where, in point *iii*), the last applied rule is (!); then either $\mathtt{x} \notin \mathrm{FV}(\mathtt{P})$ and Π is

$$\frac{\Pi' \triangleright \emptyset \mid \emptyset \mid \Theta' \vdash \mathtt{P} : \rho}{\Gamma_1 \mid \Delta, \mathtt{x} : !\sigma \mid \Theta \vdash !\mathtt{P} : !\rho} \ (!)$$

where $\mathtt{M} = !\mathtt{P}$, $\tau = !\rho$ and $\Delta = !\Theta', \Delta'$, so $S(\Sigma, \Pi)$ is

$$\frac{\Pi' \triangleright \emptyset \mid \emptyset \mid \Theta' \vdash \mathtt{P} : \rho}{\Gamma_1, \Gamma_2 \mid \Delta \mid \Theta \vdash !\mathtt{P} : !\rho} \ (!)$$

or $\mathtt{x} \in \mathrm{FV}(\mathtt{P})$ and Π is

$$\frac{\Pi' \triangleright \emptyset \mid \emptyset \mid \Theta', \mathtt{x} : \sigma \vdash \mathtt{P} : \rho}{\Gamma_1 \mid \Delta, \mathtt{x} : !\sigma \mid \Theta \vdash !\mathtt{P} : !\rho} \ (!)$$

where $\mathtt{M} = !\mathtt{P}$, $\tau = !\rho$ and $\Delta = !\Theta', \Delta'$. By Remark 1, Σ is

$$\frac{\Sigma' \triangleright \emptyset \mid \emptyset \mid \Theta'' \vdash \mathtt{N} : \sigma}{\Gamma \mid \Delta \mid \Theta \vdash !\mathtt{N} : !\sigma} \ (!)$$

where $\Delta = !\Theta'', \Delta''$. By Lemma 11 we can obtain $\Pi'' \triangleright \emptyset \mid \emptyset \mid \Theta''', \mathtt{x} : \sigma \vdash \mathtt{P} : \rho$ and $\Sigma'' \triangleright \emptyset \mid \emptyset \mid \Theta''' \vdash \mathtt{N} : \sigma$ such that $\Theta''' = \Theta', \Theta''$ and $\Delta = !\Theta''', \Delta'''$ for some context Δ'''. Then by applying point (ii) of the current Lemma to Π'', followed by one application of rule (!), $S(\Sigma, \Pi)$ is

$$\frac{S(\Sigma'', \Pi'') \triangleright \emptyset \mid \emptyset \mid \Theta''' \vdash \mathtt{P}[\mathtt{N}/\mathtt{x}] : \rho}{\Gamma_1, \Gamma_2 \mid \Delta \mid \Theta \vdash !(\mathtt{P}[\mathtt{N}/\mathtt{x}]) : !\rho} \ (!)$$

Proof (of Theorem 1). The subject reduction theorem follows easily from Lemma 12.

B.2 Proof of Proposition 7.(i)

We call rules $(\mu I), (\mu E), (\forall I), (\forall E)$ of Table 1 *non structural*-rules, since they do not contribute to the construction of a term.

We first need to show two properties on terms: the first one is about terms having a modal type, while the second one is about conditions for showing that a term is not an application.

Proposition 9. *Let $\Pi \triangleright \Gamma \mid \Delta \mid \emptyset \vdash \mathtt{M} : !\sigma$, where $\mathtt{M} \in \mathbf{nf}_0$. Then:*

1. *$\Gamma = \emptyset$ implies $\mathtt{M} = !\mathtt{N}$ for some $\mathtt{N}$.*
2. *if there exists a variable $\mathtt{x}$ occurring free in $\mathtt{M}$ and such that $\Gamma(\mathtt{x})$ is defined, then we have $\mathtt{M} = \mathtt{NQ}$, for some $\mathtt{N}$,$\mathtt{Q}$.*

Proof. Let $\Pi \triangleright \Gamma \mid \Delta \mid \emptyset \vdash \mathtt{M} : !\sigma$, for some σ: both points follow by induction on Π and by observing that the only rules that can assign a non-linear type are (!) and $(\multimap E)$.

Lemma 13. *Assume $\Pi \triangleright \Gamma \mid \emptyset \mid \emptyset \vdash \mathtt{M} : \sigma$ and:*

(i) $\mathtt{M} \in \mathbf{nf}_0$;
(ii) for every $\mathtt{x} \in \mathrm{FV}(\mathtt{M})$, $\Gamma(\mathtt{x})$ is a type variable $\mathtt{a}$ or a linear type $\mathtt{A} \multimap \mathtt{a}$;

then $\mathtt{M}$ is not an application.

Proof. By induction on Π. The only non obvious case is when Π is an application of the rule $(\multimap E)$, followed by a (possibly empty) sequence δ of non-structural rules; then the proof follows by contradiction by applying Prop. 9.

Proof (of Prop. 7.(i)). We proceed by induction on k.

– First consider the case where $k = 0$. By Lemma 13, $\mathtt{M}$ is not an application and it cannot be a variable, since it is closed. So $\mathtt{M} = \lambda\mathtt{x}.\mathtt{N}$ or $\lambda^!\mathtt{x}.\mathtt{N}$ and the derivation is

$$\dfrac{\dfrac{\Gamma \mid \Delta \mid \emptyset \vdash \mathtt{N} : \tau}{\emptyset \mid \emptyset \mid \emptyset \vdash \mathtt{M} : \sigma \multimap \tau}\ (\multimap I^*)}{\emptyset \mid \emptyset \mid \emptyset \vdash \mathtt{M} : \forall \mathtt{a}.\mathtt{a} \multimap \mathtt{a} \multimap \mathtt{a}}\ \delta$$

where either the rule is $(\multimap I^L)$ and $\Gamma = \mathtt{x} : \sigma$, $\Delta = \emptyset$, or the rule is $(\multimap I^I)$, $\Gamma = \emptyset$ and $\Delta = \mathtt{x} : \sigma$, and δ is a sequence of non-structural rules: then δ is a $(\forall I)$ rule, and so $\sigma \multimap \tau = \mathtt{a} \multimap \mathtt{a} \multimap \mathtt{a}$. So the only possibility is $\mathtt{x} : \mathtt{a} \mid \emptyset \mid \emptyset \vdash \mathtt{N} : \mathtt{a} \multimap \mathtt{a}$. Again by Lemma 13, $\mathtt{N}$ cannot be an application. It cannot be a variable either, because of the context, so either $\mathtt{N} = \lambda\mathtt{y}.\mathtt{P}$ or $\mathtt{N} = \lambda^!\mathtt{y}.\mathtt{P}$. By repeating the same reasoning, we have $\mathtt{N} = \lambda\mathtt{y}.\mathtt{P}$, and $\mathtt{x} : \mathtt{a}, \mathtt{y} : \mathtt{a} \mid \emptyset \mid \emptyset \vdash \mathtt{P} : \mathtt{a}$. By Lemma 13, $\mathtt{P}$ cannot be an application, and it cannot be an abstraction, since in this case $\mathtt{x} : \mathtt{a}, \mathtt{y} : \mathtt{a} \mid \emptyset \mid \emptyset \vdash \mathtt{P} : \mathtt{a}$ would be obtained by a rule $(\multimap I^*)$ (where $* \in \{L, I\}$), followed by a sequence of non-structural rules. But a rule $(\multimap I^*)$ derives a type of the shape $\sigma \multimap \tau$ and $\mathtt{a}$ cannot be obtained from $\sigma \multimap \tau$ by a sequence of non-structural rules. So $\mathtt{P}$ is either $\mathtt{x}$ or $\mathtt{y}$, and the proof is given.

– Now consider the case $k + 1$. By repeatedly applying Prop. 9.1, $\mathtt{M} = !^{k+1}\mathtt{N}$, and $\emptyset \mid \emptyset \mid \emptyset \vdash \mathtt{N} : \forall\mathtt{a}.\mathtt{a} \multimap \mathtt{a} \multimap \mathtt{a}$.
Then the proof of the previous point applies.

B.3 Proof of Theorem 4

We prove the functoriality of the ! modality:

Proposition 10. *Let* $\vdash \mathtt{M} : \sigma_1 \multimap ... \multimap \sigma_n \multimap \tau$ *for some* $n > 0$*: then there is a term* $\mathtt{M}_k$ *such that* $\vdash \mathtt{M}_k : !^k\sigma_1 \multimap ... \multimap !^k\sigma_n \multimap !^k\tau$*, and* $\mathtt{M}_k!^k\mathtt{P}_1...!^k\mathtt{P}_n$ *and* $!^k(\mathtt{M}\mathtt{P}_1...\mathtt{P}_n)$ *have the same normal form, for any closed term* $\mathtt{P}_i$ *(*$1 \leq i \leq n$*), for any* $k \geq 1$*.*

Proof. By induction on k. Let us consider the base case $k = 1$: by first applying n times rule $(\multimap E)$ to $\vdash \mathtt{M} : \sigma_1 \multimap ... \multimap \sigma_n \multimap \tau$ and to the (parking) axioms $\emptyset \mid \emptyset \mid \mathtt{x}_i : \sigma_i \vdash \mathtt{x}_i : \sigma_i$ $(1 \leq i \leq n)$, we obtain the proof $\emptyset \mid \emptyset \mid \mathtt{x}_1 : \sigma_1, ..., \mathtt{x}_n : \sigma_n \vdash \mathtt{M}\mathtt{x}_1...\mathtt{x}_n : \tau$; then we apply a rule (!), followed by n applications of rule $(\multimap I^I)$, so obtaining $\vdash \lambda^!\mathtt{x}_1...\mathtt{x}_n.!(\mathtt{M}\mathtt{x}_1...\mathtt{x}_n) : !\sigma_1 \multimap ...!\sigma_n \multimap !\tau$. Observe that $(\lambda^!\mathtt{x}_1...\mathtt{x}_n.!(\mathtt{M}\mathtt{x}_1...\mathtt{x}_n))!\mathtt{P}_1...!\mathtt{P}_n$ and $!(\mathtt{M}\mathtt{P}_1...\mathtt{P}_n)$ have the same normal form.

The inductive case follows easily.

In order to prove completeness, we need to represent some functions over tally integers:

Lemma 14. *If p is a polynomial over one variable with coefficients in $\mathbb{N}$, then*

(i) there is $\mathtt{M}$ *representing* $p(n)$ *such that* $\vdash \mathtt{M} : !\mathrm{N} \multimap !\mathrm{N}$*;*

(ii) there is $\mathtt{M}$ *representing* $2_k^{p(n)}$ *such that* $\vdash \mathtt{M} : !\mathrm{N} \multimap !^{k+1}\mathrm{N}$*, for any* $k \geq 1$*.*

Proof. We give a sketch of the proof, showing that, by composing addition and multiplication with the term representing the exponential function, it is possible to represent all the functions of the form $2_k^{q(n)}$ on tally integers, for some polynomial $q(n)$ and $k \geq 0$.

The sum and multiplication of two tally integers are given respectively by $\vdash \mathtt{add} : \mathrm{N} \multimap \mathrm{N} \multimap \mathrm{N}$ and $\vdash \mathtt{mult} : \mathrm{N} \multimap \mathrm{N} \multimap \mathrm{N}$, where $\mathtt{add} \stackrel{\text{def}}{=} \lambda n.\lambda m.\lambda^! \mathtt{s}.(\lambda^! \mathtt{x}.\lambda^! \mathtt{y}.!(\lambda \mathtt{z}.\mathtt{x}(\mathtt{yz})))(n!\mathtt{s})(m!\mathtt{s})$ and $\mathtt{mult} \stackrel{\text{def}}{=} \lambda n.\lambda m.\lambda^! \mathtt{s}.n(m!\mathtt{s})$.

(i) By composing $\mathtt{add}$ and $\mathtt{mult}$ in a suitable way, we can build a term $\mathtt{M}$ representing the polynomial $q(n)$, such that $\mathtt{M} : !\mathrm{N} \multimap !\mathrm{N}$.

(ii) The function $f(n) = 2n$ is represented by $\Pi_{\mathtt{double}} \triangleright \vdash \mathtt{double} \stackrel{\text{def}}{=} \mathtt{mult}\ \underline{2} : \mathrm{N} \multimap \mathrm{N}$; then the function 2^n can be represented by iterating $\mathtt{double}$, so the resulting derivation is $\Pi_{\mathtt{exp}} \vdash \mathtt{exp} : \mathrm{N} \multimap !\mathrm{N}$, where $\mathtt{exp} \stackrel{\text{def}}{=} \lambda \mathtt{x}.(\lambda^! \mathtt{y}.!(\mathtt{y}\ \underline{1}))(\mathtt{x}\ !\mathtt{double})$.
Now, by applying Prop. 10 to $\Pi_{\mathtt{exp}}$ and composing k times $\mathtt{exp}$, we can represent the function 2_k^n by $\Pi_{\mathtt{exp}_k} \triangleright \vdash \mathtt{exp}_k : \mathrm{N} \multimap !^k\mathrm{N}$ and, by applying Prop. 10 to it, we compose the resulting derivation with $\vdash \mathtt{M} : !\mathrm{N} \multimap !\mathrm{N}$ such that $\mathtt{M}$ represents the polynomial $q(n)$, obtaining the term of type $!\mathrm{N} \multimap !^{k+1}\mathrm{N}$ representing $2_k^{q(n)}$.

In the main proof we will use the construction $\otimes$ on terms and types, which is defined in Sect. 4 of the paper.

Scott words allow for an easy definition of the basic operations on binary words and of a $\mathtt{case}$ function:

$$\mathtt{cons}_0 \stackrel{\text{def}}{=} \lambda w.\lambda \mathtt{s}_0.\lambda \mathtt{s}_1.\lambda \mathtt{x}.\mathtt{s}_0 w : \mathrm{W}_S \multimap \mathrm{W}_S \qquad \mathtt{nil} \stackrel{\text{def}}{=} \lambda \mathtt{s}_0.\lambda \mathtt{s}_1.\lambda \mathtt{x}.\mathtt{x} : \mathrm{W}_S$$

$$\mathtt{cons}_1 \stackrel{\text{def}}{=} \lambda w.\lambda \mathtt{s}_0.\lambda \mathtt{s}_1.\lambda \mathtt{x}.\mathtt{s}_1 w : \mathrm{W}_S \multimap \mathrm{W}_S \qquad \mathtt{tail} \stackrel{\text{def}}{=} \lambda w.w\ I\ I\ \mathtt{nil} : \mathrm{W}_S \multimap \mathrm{W}_S$$

$$\mathtt{case} \stackrel{\text{def}}{=} \lambda \mathtt{s}_0.\lambda \mathtt{s}_1.\lambda \mathtt{x}.\lambda \mathtt{w}.\mathtt{ws}_0\mathtt{s}_1\mathtt{x} : \forall \mathtt{a}.(\mathrm{W}_S \multimap \mathtt{a}) \multimap (\mathrm{W}_S \multimap \mathtt{a}) \multimap \mathtt{a} \multimap (\mathrm{W}_S \multimap \mathtt{a})$$

It is possible to define a term $\mathtt{length} \stackrel{\text{def}}{=} \lambda w.\lambda^! \mathtt{s}.(\lambda^! \mathtt{x}.!(\lambda \mathtt{z}.\mathtt{xz}))(w\mathtt{ss}) : \mathrm{W} \multimap \mathrm{N}$, returning the length of a word as a tally integer, and also a

term $\mathtt{conv} \stackrel{\text{def}}{=} \lambda w.(\lambda^! \mathtt{x}.!(\mathtt{x}\ \mathtt{nil}))(w\ !\mathtt{cons}_0\ !\mathtt{cons}_1) : \mathrm{W} \multimap !\mathrm{W}_S$, converting a Church binary word into the corresponding Scott binary word. Note: in the following, for any given $\mathtt{term} : \sigma_1 \multimap ... \multimap \sigma_n \multimap \tau$, we will denote by $\mathtt{term}_k :!^k\sigma_1 \multimap ... \multimap !^k\sigma_n \multimap !^k\tau$ the term such that $!^k(\mathtt{term}\ \mathtt{P}_1...\mathtt{P}_n)$ and $\mathtt{term}_k!^k\mathtt{P}_1...!^k\mathtt{P}_n$ reduce to the same normal form, by implicitly applying Prop. 10.

Starting from a few basic operations on Church binary words

$$\mathtt{S}_0 \stackrel{\text{def}}{=} \lambda w.\lambda^! \mathtt{s}_0.\lambda^! \mathtt{s}_1.(\lambda^! \mathtt{y}.!(\lambda \mathtt{x}.\mathtt{y}(\mathtt{s}_0\mathtt{x})))(w!\mathtt{s}_0!\mathtt{s}_1) : \mathrm{W} \multimap \mathrm{W}$$

$$\mathtt{S}_1 \stackrel{\text{def}}{=} \lambda w.\lambda^! \mathtt{s}_0.\lambda^! \mathtt{s}_1.(\lambda^! \mathtt{y}.!(\lambda \mathtt{x}.\mathtt{y}(\mathtt{s}_1\mathtt{x})))(w!\mathtt{s}_0!\mathtt{s}_1) : \mathrm{W} \multimap \mathrm{W} \qquad \mathtt{Z} \stackrel{\text{def}}{=} \lambda^! \mathtt{s}_0.\lambda^! \mathtt{s}_1.!(\lambda \mathtt{x}.\mathtt{x}) : \mathrm{W}$$

it is possible to define a program $\mathtt{coer} \stackrel{\text{def}}{=} \lambda \mathtt{w}.(\lambda^! \mathtt{y}.!(\mathtt{y}\mathtt{Z}))(w!\mathtt{S}_0!\mathtt{S}_1) : \mathrm{W} \multimap !\mathrm{W}$, such that $\mathtt{coer}\ \underline{w} =!\underline{w}$; moreover, we can build the term $\mathtt{coer}^k \stackrel{\text{def}}{=} \lambda^! w.\mathtt{coer}_k(\mathtt{coer}_{k-1}(...(\mathtt{coer}_1\ !w)...)) :!\mathrm{W} \multimap !^{k+1}\mathrm{W}$, for $k \geq 1$, such that $\mathtt{coer}^k!\underline{w} \stackrel{*}{\to} !^{k+1}\underline{w}$ for any Church word $\underline{w}$.

Finally, we define $\vdash \mathtt{iter} :!\mathtt{A} \multimap !(\mathtt{A} \multimap \mathtt{A}) \multimap \mathrm{N} \multimap !\mathtt{A}$ as the term which, when applied to a base, a step function and a value n, iterates the step function n times starting from the base.

Let $\mathcal{M}$ be a Turing machine with alphabet $\Sigma = \{0, 1\}$ and a set of n states $Q_n = \{q_1, ..., q_n\}$. We can represent the configurations of a one-tape Turing machine $\mathcal{M}$ over a binary alphabet with n states, through a term $\mathtt{N}_L \otimes \mathtt{P} \otimes \mathtt{N}_R \otimes \mathtt{P}$ having type $\mathtt{Conf}_S \stackrel{\text{def}}{=} \mathrm{W}_S \otimes \mathrm{B} \otimes \mathrm{W}_S \otimes \mathrm{B}^n$ where: the first component represents the portion of the tape on the left-hand side of the scanned symbol, in reverse order; the second component represents the scanned symbol; the third component represents the portion of the tape on the right-hand side of the scanned symbol; the fourth component represents the current state of the machine.

Before proving the completeness lemma, we need do define three more terms, which will allow us to simulate the operations of a Turing machine through $\lambda^!$-calculus.

Lemma 15. *Let $\mathcal{M}$ be a one-tape deterministic Turing machine over a binary alphabet; then the following terms can be defined:*

(i) $\mathtt{init} : \mathrm{W}_S \multimap \mathtt{Conf}_S$
(ii) $\mathtt{step} : \mathtt{Conf}_S \multimap \mathtt{Conf}_S$
(iii) $\mathtt{accept} : \mathtt{Conf}_S \multimap \mathrm{B}$

such that init *maps a Scott word into the corresponing initial configuration of $\mathcal{M}$,* step *computes the next configuration of $\mathcal{M}$ based on a given configuration, and* accept *returns* true *(respectively* false*) if the state of the given configuration is accepting (respectively rejecting).*

Proof. For simplicity, we extend the notation for the tensor product to the n-ary case, so $\mathtt{M}_1 \otimes ... \otimes \mathtt{M}_n \stackrel{\text{def}}{=} \lambda \mathtt{x}.\mathtt{x}\mathtt{M}_1...\mathtt{M}_n$, and $\mathtt{let\ z\ be\ x}_1 \otimes ... \otimes \mathtt{x}_n \mathtt{in\ N} \stackrel{\text{def}}{=} \mathtt{z}(\lambda \mathtt{x}_1.\ ...\lambda \mathtt{x}_n.\mathtt{N})$.

(i) We define $\mathtt{init}$ to be $\mathtt{init} \stackrel{\text{def}}{=} \mathtt{case}\ \mathtt{M}_1\mathtt{M}_2\mathtt{M}_3 : \mathrm{W}_S \multimap \mathtt{Conf}_S$ where
$\mathtt{M}_1 = \lambda w.\mathtt{nil} \otimes \mathtt{true} \otimes w \otimes \tilde{1} \quad \mathtt{M}_2 = \lambda w.\mathtt{nil} \otimes \mathtt{false} \otimes w \otimes \tilde{1} \quad \mathtt{M}_3 = \mathtt{nil} \otimes \mathtt{false} \otimes \mathtt{nil} \otimes \tilde{1}$
and $\tilde{1} : \mathrm{B}^n$ represents (by convention) the initial state.

(ii) The term $\mathtt{step}$ can be defined based on the transition function of $\mathcal{M}$ by doing a case distinction through the $\mathtt{case}$ term.

(iii) Finally, we define $\mathtt{accept} \stackrel{\text{def}}{=} \lambda \mathtt{z}.\mathtt{let\ z\ be\ y}_L \otimes \mathtt{x} \otimes \mathtt{y}_R \otimes \mathtt{s\ in\ sQ}_1...\mathtt{Q}_n : \mathtt{Conf}_S \multimap \mathrm{B}$ where, for $1 \leq i \leq n$, $\mathtt{Q}_i = \mathtt{true}$ (respectively $\mathtt{Q}_i = \mathtt{false}$) if the state encoded by the i-th element of type B^n is accepting (respectively rejecting) for $\mathcal{M}$.

Finally we can prove the main completeness result:

Proof (of Theorem 4).

Let $\mathcal{M}$ be a deterministic Turing machine of time $2_k^{q(n)}$ computing a binary function f on binary words. By Lemma 14, there is a derivation $\vdash \mathtt{Q} :!\mathrm{N} \multimap !^{k+1}\mathrm{N}$ representing $2_k^{q(n)}$. By applying $\emptyset \mid w :!\mathrm{W} \mid \emptyset \vdash \mathtt{iter}_{k+1} :!^{k+2}\mathtt{Conf}_S \multimap !^{k+2}(\mathtt{Conf}_S \multimap \mathtt{Conf}_S) \multimap !^{k+1}\mathrm{N} \multimap !^{k+2}\mathtt{Conf}_S$ to the arguments

$$\Pi \triangleright \emptyset \mid w :!\mathrm{W} \mid \emptyset \vdash \mathtt{init}_{k+2}(\mathtt{conv}_{k+1}(\mathtt{coer}^k\ !w)) :!^{k+2}\mathtt{Conf}_S$$

$$\Sigma \triangleright \emptyset \mid w :!\mathrm{W} \mid \emptyset \vdash !^{k+2}\mathtt{step} :!^{k+2}(\mathtt{Conf}_S \multimap \mathtt{Conf}_S) \quad \Phi \triangleright \emptyset \mid w :!\mathrm{W} \mid \emptyset \vdash \mathtt{Q}(\mathtt{length}_1\ !w) :!^{k+1}\mathrm{N}$$

the resulting derivation Ψ is

$$\emptyset \mid w :!\mathrm{W} \mid \emptyset \vdash \mathtt{iter}_{k+1}(\mathtt{init}_{k+2}(\mathtt{conv}_{k+1}(\mathtt{coer}^k\ !w)))(!^{k+2}\mathtt{step})(\mathtt{Q}(\mathtt{length}_1\ !w)) :!^{k+2}\mathtt{Conf}_S$$

Then we can apply rule $(\multimap E)$ to $\emptyset \mid w :!\mathrm{W} \mid \emptyset \vdash \mathtt{accept}_{k+2} :!^{k+2}\mathtt{Conf}_S \multimap !^{k+2}\mathrm{B}$ and to Ψ, followed by one application of rule $(\multimap I^I)$ to abstract over w, and we get the desired derivation.

C Refining types for an alternative characterization

It is easy to check that the following typing rules are derivable:

$$\frac{\Gamma, \mathtt{x}_1 : \mathtt{A}_1, \mathtt{x}_2 : \mathtt{A}_2 \mid \Delta \mid \Theta \vdash \mathtt{M} : \tau}{\Gamma \mid \Delta \mid \Theta \vdash \lambda(\mathtt{x}_1 \otimes \mathtt{x}_2).\mathtt{M} : \mathtt{A}_1 \otimes \mathtt{A}_2 \multimap \tau}\ (\multimap I^L_\otimes)$$

$$\frac{\Gamma \mid \Delta, \mathtt{x}_1 :!\sigma_1, \mathtt{x}_2 :!\sigma_2 \mid \Theta \vdash \mathtt{M} : \tau}{\Gamma \mid \Delta \mid \Theta \vdash \lambda^!(\mathtt{x}_1 \otimes \mathtt{x}_2).\mathtt{M} :!\sigma_1 \otimes !\sigma_2 \multimap \tau}\ (\multimap I^I_\otimes)$$

$$\frac{\Gamma_1 \mid \Delta \mid \Theta \vdash \mathtt{M}_1 : \sigma_1 \quad \Gamma_2 \mid \Delta \mid \Theta \vdash \mathtt{M}_2 : \sigma_2 \quad \Gamma_1 \# \Gamma_2}{\Gamma_1, \Gamma_2 \mid \Delta \mid \Theta \vdash \mathtt{M}_1 \otimes \mathtt{M}_2 : \sigma_1 \otimes \sigma_2}\ (\otimes I)$$

C.1 Proof of Prop. 8

In order to prove Prop. 8, we will need a few intermediary lemmas. A derivation is *clean* if it does not contain any $\forall$ nor μ detours, in the sense of natural deduction.

Lemma 16. *Let* $\Pi \triangleright \Pi \mid \emptyset \mid \Theta \vdash \mathtt{M} : !\tau$ *and* $\mathtt{M} \in \mathbf{nf}_0$*, such that* $\Gamma, \Theta \subseteq \mathtt{x} : \sigma_1 \multimap ... \multimap \sigma_n \multimap \mathtt{a}, \mathtt{y}_1 : \mathtt{a}_1, ..., \mathtt{y}_k : \mathtt{a}_k$ *($n \geq 1, k \geq 0$): then* $\mathtt{M} = !\mathtt{N}$ *for some* $\mathtt{N}$*.*

Proof. By induction on Π. By inspecting the rules of the system, the last rule of Π is either (!) or ($\multimap E$). If the last rule is (!) then the result follows trivially. Otherwise, let Π be

$$\frac{\Pi_1 \triangleright \Gamma_1 \mid \emptyset \mid \Theta \vdash \mathtt{P} : \rho \multimap !\tau \quad \Pi_2 \triangleright \Gamma_2 \mid \emptyset \mid \Theta \vdash \mathtt{Q} : \rho}{\Gamma_1, \Gamma_2 \mid \emptyset \mid \Theta \vdash \mathtt{PQ} : !\tau} \ (\multimap E)$$

where $\mathtt{M} = \mathtt{PQ}$ and $\Gamma = \Gamma_1, \Gamma_2$. We check all three possible cases:

- $\mathtt{M} = (\lambda \mathtt{z}.\mathtt{R})^{\mathtt{A} \multimap !\tau} \mathtt{Q}^{\mathtt{A}}$: this case is not possible, because then $\mathtt{M}$ would be a β-redex, contradicting the inital hypothesis that $\mathtt{M} \in \mathbf{nf}_0$.
- $\mathtt{M} = (\lambda^{!} \mathtt{z}.\mathtt{R})^{!\sigma \multimap !\tau} \mathtt{Q}^{!\sigma}$: but by induction hypothesis on Π_2 we know that $\mathtt{Q} = !\mathtt{Q}'$ for some $\mathtt{Q}'$, so $\mathtt{M}$ would be a !-redex, contradicting the initial hypothesis that $\mathtt{M} \in \mathbf{nf}_0$, so this case is not possible.
- $\mathtt{M} = \mathtt{z}^{\rho_1 \multimap ... \multimap \rho_m \multimap !\tau} \mathtt{P}_1^{\rho_1} ... \mathtt{P}_m^{\rho_m}$: because the only variable with an arrow type (if any) is $\mathtt{x}$, we have that $\mathtt{z} = \mathtt{x}$, so $\Pi_1 \triangleright \Gamma_1 \mid \emptyset \mid \Theta \vdash \mathtt{xP}_1 ... \mathtt{P}_{m-1} : \sigma \multimap !\tau$ and $\Pi_2 \triangleright \Gamma_2 \mid \emptyset \mid \Theta \vdash \mathtt{P}_m : \sigma$; but any application of $\mathtt{x}$ to $m \leq n$ subterms will produce a term having either an arrow type or a type variable, so this case is not possible either.

Lemma 17. *Let* $\Pi \triangleright \Gamma \mid \emptyset \mid \Theta \vdash \mathtt{M} : \mathtt{a}$*, such that* $\mathtt{M} \in \mathbf{nf}_0$ *and* $\Gamma, \Theta = \mathtt{x} : \sigma_1 \multimap ... \multimap \sigma_n \multimap \mathtt{a}, \mathtt{y}_1 : \mathtt{a}_1, ..., \mathtt{y}_k : \mathtt{a}_k$ *($n \geq 1, k \geq 0$): then either* $\mathtt{M} = \mathtt{y}_i$*, if* $\mathtt{a} = \mathtt{a}_i$*, or* $\mathtt{M} = \mathtt{xP}_1 ... \mathtt{P}_n$ *for some* $\mathtt{P}_1, ..., \mathtt{P}_n$*.*

Proof. Consider the shape of Π. The last rule cannot be ($\multimap I^L$) or ($\multimap I^I$), since $\mathtt{a}$ is not an arrow type. Similarly, we know that the last rule can not be a $\forall$ or a μ rule, since the assumption of Π being clean. Moreover, since the type is linear we know that the last rule is not (!).

If the last rule is (Ax^L) (resp. (Ax^P)), then there is $\mathtt{y}_i \in \mathrm{dom}(\Gamma)$ (resp. $\mathtt{y}_i \in \mathrm{dom}(\Theta)$) such that $\mathtt{x} = \mathtt{y}_i$ and $\mathtt{a} = \mathtt{a}_i$; so the first point is proved.

Otherwise the last rule is ($\multimap E$), so Π is

$$\frac{\Pi_1 \triangleright \Gamma_1 \mid \emptyset \mid \Theta \vdash \mathtt{P} : \rho \multimap \mathtt{a} \quad \Pi_2 \triangleright \Gamma_2 \mid \emptyset \mid \Theta \vdash \mathtt{Q} : \rho}{\Gamma_1, \Gamma_2 \mid \emptyset \mid \Theta \vdash \mathtt{PQ} : \mathtt{a}} \ (\multimap E)$$

where $\mathtt{M} = \mathtt{PQ}$ and $\Gamma = \Gamma_1, \Gamma_2$. Since $\mathtt{M} \in \mathbf{nf}_0$, there are only two possibilities:

- $\mathtt{M} = (\lambda^!\mathtt{y}.\mathtt{P})^{!\tau \multimap \mathtt{a}}\mathtt{Q}^{!\tau}$ where $\mathtt{Q} \neq !\mathtt{Q}'$, i.e. $\mathtt{M}$ is a block: but by Lemma 16 applied to $\Pi_2 \triangleright \Gamma_2 \mid \emptyset \mid \Theta \vdash \mathtt{Q} : !\tau$ we know that $\mathtt{Q} = !\mathtt{Q}'$, which contradicts the hypothesis that $\mathtt{M} \in \mathbf{nf}_0$. So $\mathtt{M}$ is not a block.
- $\mathtt{M} = \mathtt{z}^{\rho_1 \multimap \ldots \multimap \rho_m \multimap \mathtt{a}}\mathtt{P}_1^{\rho_1}\ldots\mathtt{P}_m^{\rho_m}$: since $\mathtt{x}$ is the only variable having an arrow type ending with $\mathtt{a}$, $m = n$ and $\Pi \triangleright \Gamma \mid \emptyset \mid \Theta \vdash \mathtt{xP}_1\ldots\mathtt{P}_n : \mathtt{a}$, where $\mathtt{x}$ is introduced either through rule (Ax^L), if $\mathtt{x} \in \mathrm{dom}(\Gamma)$, or through rule (Ax^P), if $\mathtt{x} \in \mathrm{dom}(\Theta)$. So the second point is proved.

Lemma 18. *If* $\vdash \mathtt{M} : (\sigma_1 \otimes \sigma_2)$ *and* $\mathtt{M} \in \mathbf{nf}_0$*, then there are* $\vdash \mathtt{M}_1 : \sigma_1$ *and* $\vdash \mathtt{M}_2 : \sigma_2$ *such that* $\mathtt{M} = \mathtt{M}_1 \otimes \mathtt{M}_2$.

Proof. We consider a clean derivation Π proving $\vdash \mathtt{M} : \forall\mathtt{a}.((\sigma_1 \multimap \sigma_2 \multimap \mathtt{a}) \multimap \mathtt{a})$. Since Π is clean, the last rule is $(\forall I)$ applied to the premise $\Pi' \triangleright \vdash \mathtt{M} : (\sigma_1 \multimap \sigma_2 \multimap \mathtt{a}) \multimap \mathtt{a}$. Now consider Π': by Lemma 13 we know that $\mathtt{M}$ is not an application, and moreover $\mathtt{M}$ is not a variable, since the empty bases; therefore, $\mathtt{M}$ is an abstraction, in particular a linear one since the type is of the shape $\mathtt{A} \multimap \mathtt{a}$; then $\mathtt{M} = \lambda\mathtt{x}.\mathtt{N}$ and the last rule of Π' is $(\multimap I^L)$ applied to the premise $\Pi'' \vdash \mathtt{x} : \sigma_1 \multimap \sigma_2 \multimap \mathtt{a} \mid \emptyset \mid \emptyset \vdash \mathtt{N} : \mathtt{a}$. Finally, by applying Lemma 17 to Π'', it follows that $\mathtt{N} = \mathtt{xM}_1\mathtt{M}_2$ for some terms $\mathtt{M}_1, \mathtt{M}_2$: so Π'' is

$$\dfrac{\dfrac{\overline{\Gamma \mid \emptyset \mid \emptyset \vdash \mathtt{x} : \sigma_1 \multimap \sigma_2 \multimap \mathtt{a}}\ (Ax^L) \qquad \Sigma_1 \triangleright \vdash \mathtt{M}_1 : \sigma_1}{\Gamma \mid \emptyset \mid \emptyset \vdash \mathtt{xM}_1 : \sigma_2 \multimap \mathtt{a}}\ (\multimap E) \qquad \Sigma_2 \triangleright \vdash \mathtt{M}_2 : \sigma_2}{\Gamma \mid \emptyset \mid \emptyset \vdash \mathtt{xM}_1\mathtt{M}_2 : \mathtt{a}}\ (\multimap E)$$

where $\Gamma = \mathtt{x} : \sigma_1 \multimap \sigma_2 \multimap \mathtt{a}$; so $\mathtt{M} = \lambda\mathtt{x}.\mathtt{xM}_1\mathtt{M}_2 = \mathtt{M}_1 \otimes \mathtt{M}_2$ and the desired derivations for $\mathtt{M}_1$ and $\mathtt{M}_2$ are respectively Σ_1 and Σ_2.

Lemma 19. *If* $\vdash \mathtt{M} :!^k\mathrm{N}$ *for* $k \geq 0$ *and* $\mathtt{M} \in \mathbf{nf}_{k+1}$*, then there exists* $n \in \mathbb{N}$ *such that* $\mathtt{M} =!^k\underline{n}$.

Proof. Recall that $\underline{n} = \lambda^! f.!(\lambda\mathtt{x}.f^n\mathtt{x})$ for any $n \in \mathbb{N}$. Let Π be a clean derivation for $\vdash \mathtt{M} :!^k\mathrm{N}$; we proceed by induction on k.

Let $k = 0$, so $\Pi \triangleright \vdash \mathtt{M} : \mathrm{N}$ and $\mathtt{M} \in \mathbf{nf}_1$, and let us consider the shape of Π. Since Π is clean, the derivation ends with an application of rule $(\forall I)$ to the premise $\Pi' \triangleright \vdash \mathtt{M} :!(\mathtt{a} \multimap \mathtt{a}) \multimap !(\mathtt{a} \multimap \mathtt{a})$. By Lemma 13, $\mathtt{M}$ is not an application; moreover, $\mathtt{M}$ is not a variable since the term is closed; so $\mathtt{M}$ is an abstraction, and in particular $\mathtt{M} = \lambda^! f.\mathtt{N}$ since the type has the shape $!\sigma \multimap \tau$: then Π' ends with an application of rule $(\multimap I^I)$ to the premise $\emptyset \mid f :!(\mathtt{a} \multimap \mathtt{a}) \mid \emptyset \vdash \mathtt{N} :!(\mathtt{a} \multimap \mathtt{a})$. By Prop. 9, we know that $\mathtt{N} =!\mathtt{P}$ for some $\mathtt{P}$: then $\mathtt{M} = \lambda^! f.!\mathtt{P}$ and Π'' ends with an application of rule $(!)$ to the

premise $\Sigma \triangleright \emptyset \mid \emptyset \mid f : \mathtt{a} \multimap \mathtt{a} \vdash \mathtt{P} : \mathtt{a} \multimap \mathtt{a}$. Again by Lemma 13, $\mathtt{P}$ is not an application. If $\mathtt{P} = f$, then $\mathtt{M} = \lambda^! f.!f$ and Σ is a parking axiom, so the proof is done. Otherwise $\mathtt{P}$ is an abstraction, and in particular $\mathtt{P} = \lambda \mathtt{x}.\mathtt{Q}$ since the type has the shape $\mathtt{A} \multimap \tau$: then Σ ends with an application of rule $(\multimap I^L)$ to the premise $\Sigma' \triangleright \mathtt{x} : \mathtt{a} \mid \emptyset \mid f : \mathtt{a} \multimap \mathtt{a} \vdash \mathtt{Q} : \mathtt{a}$: then by Lemma 17 we know that either $\mathtt{Q} = \mathtt{x}$, so $\mathtt{M} = \underline{0}$, or $\mathtt{Q} = f\mathtt{Q}'$: in the second case, Σ' ends with an application of rule $(\multimap E)$ to parking axiom $\emptyset \mid \emptyset \mid f : \mathtt{a} \multimap \mathtt{a} \vdash f : \mathtt{a} \multimap \mathtt{a}$ and to $\Sigma'' \vdash \mathtt{x} : \mathtt{a} \mid \emptyset \mid f : \mathtt{a} \multimap \mathtt{a} \vdash \mathtt{Q}' : \mathtt{a}$; finally, by repeating the same reasoning n times on the right premise of rule $(\multimap E)$ we get $\mathtt{M} = \lambda^! f.!(\lambda \mathtt{x}.f^n \mathtt{x})$ for some $n \in \mathbb{N}$: so $\mathtt{M} = \underline{n}$ and the proof is complete.

Now consider the case $k+1$. By repeatly applying Prop. 9, $\mathtt{M} =!^{k+1}\mathtt{N}$, and $\Pi' \triangleright \vdash \mathtt{N} : \mathrm{N}$: then the proof of the previous point applies.

Proof (of Prop. 8). By Lemma 18, we know that $\vdash \mathtt{M} :!^k \mathrm{N} \otimes !^{k+1} \mathrm{W}_S$ and $\mathtt{M} \in \mathbf{nf}_0$ imply there are derivations $\vdash \mathtt{M}_1 :!^k \mathrm{N}$ and $\vdash \mathtt{M}_2 :!^{k+1} \mathrm{W}_S$ such that $\mathtt{M} = \mathtt{M}_1 \otimes \mathtt{M}_2$: then the result follows easily by Prop. 7.(ii) in the paper and Lemma 19.

C.2 Proof of Theorem 5

Proposition 11. *Given a program $\mathtt{P}$, for any $k \geq 2$, there exists a polynomial q such that, for any $m \in \mathbb{N}$, $w \in \{0,1\}^\star$, $\mathtt{P}(!\underline{m} \otimes !^2 \widehat{w}) \overset{*}{\rightsquigarrow} \mathtt{M}^1_k \in \mathbf{nf}_{k-1}$ in at most $2^{q(n)}_{k-2}$ steps, and $|\mathtt{M}^1_k| \leq 2^{q(n)}_{k-2}$, where $n = m + \mathbf{length}(w)$. In particular, in the case where $k = 2$ we have a polynomial bound $q(n)$.*

Proof (Sketch). This statement can be proved in a way similar to Prop. 3. The only difference is in the case $k = 2$ for bounding the number of reduction steps at depths 0 and 1, but it can be checked that here also the number of steps at depths 0 and 1 are bounded by a constant, essentially because the structure of the term $\mathtt{P}!\underline{m} \otimes !^2 \widehat{w}$ at depth lower or equal to 1 does not depend on m or w.

Proposition 12. *Given a program $\mathtt{P}$, for any $k \geq 2$, there exists a polynomial q such that for any $m \in \mathbb{N}$, $w \in \{0,1\}^\star$, the reduction of $\mathtt{P}(!\underline{m} \otimes !^2 \widehat{w})$ to its k-normal form can be computed in time $O(2^{q(n)}_{k-2})$ on a Turing machine, where $n = m + \mathbf{length}(w)$.*

Proof (of Theorem 5). By combining the results of Prop. 12, the subject-reduction property and Prop. 8.

C.3 Proof of Theorem 6

The following lemma states that from any pair $!\underline{n} \otimes !^2 \widehat{w}$ we can obtain the prefix of $\widehat{w}$ of length n, possibly at higher depth:

Lemma 20. *For any $k \geq 0$, there exists a term $\vdash \mathtt{M} : (!\mathrm{N} \otimes !^2 \mathrm{W}_S) \multimap !^{k+2}\mathrm{W}_S$ such that for any $\underline{n}$, $\widehat{w}$, the term $\mathtt{M}(!\underline{n} \otimes !^2\widehat{w})$ reduces to $!^{k+2}\widehat{w'}$, where $w' = w$ if w is of length inferior or equal to n, and otherwise w' is the prefix of w of length n.*

The completeness proof is very similar to the one of Theorem 4, showing how to simulate a Turing machine for a function of k-`FEXP` by a term of type $!\mathrm{W} \multimap !^{k+2}\mathrm{W}_S$:

Proof (Sketch, of Theorem 6). Consider a Turing machine $\mathcal{M}$ of time $2_k^{q(n)}$ computing f: then the size of the word output is bounded by $2_k^{q(n)}$. By Lemma 14, let $\vdash \mathtt{Q} : !\mathrm{N} \multimap !^{k+1}\mathrm{N}$ be a term representing $2_k^{q(n)}$; moreover, denote by $!\underline{m} \otimes !^2\widehat{w}$ the input of `M`, where we assume that $\mathbf{length}(w) \leq m$. By Lemma 20, there is a term `P` which can be applied to $!\underline{m} \otimes !^2\widehat{w}$ and outputs $!^{k+2}\widehat{w}$. By applying the term $\vdash \mathtt{Q} : !\mathrm{N} \multimap !^{k+1}\mathrm{N}$ to $!\underline{m}$, we obtain $!^{k+1}\underline{2_k^{q(m)}}$: this term is used as the first component of the output pair. Now we proceed as in the proof of Theorem 4: first we apply $\vdash \mathtt{init}'_S : !^{k+2}\mathrm{W}_S \multimap !^{k+2}\mathtt{Conf}_S$ to $!^{k+2}\widehat{w}$ and we obtain the initial configuration $!^{k+2}c_0$; then we use $!^{k+1}\underline{2_k^{q(m)}}$ to iterate the term `step` executing one step of the machine, starting from base $!^{k+2}c_0$; we then obtain the final configuration $!^{k+2}c$, from which we can extract the expected word $!^{k+2}\widehat{w'}$. Finally we output the pair $!^{k+1}\underline{2_k^{q(m)}} \otimes !^{k+2}\widehat{w'}$, of type $(!^{k+1}\mathrm{N} \otimes !^{k+2}\mathrm{W}_S)$.