Theory Comput Syst (2010) 46: 673–689
DOI 10.1007/s00224-009-9210-x

A Semantic Proof of Polytime Soundness of Light Affine Logic

Ugo Dal Lago · Martin Hofmann

Published online: 7 April 2009

Abstract We define realizability semantics for Light Affine Logic (LAL) which has the property that denotations of functions are polynomial time computable by construction of the model. This gives a new proof of polytime-soundness of LAL which is considerably simpler than the standard proof based on proof nets and is entirely semantical in nature. The model construction uses a new instance of a resource monoid; a general method for interpreting systems based on Linear Logic introduced earlier by the authors.

Keywords Implicit computational complexity · Linear logic · Realizability

1 Introduction

In recent years, a large number of characterizations of complexity classes based on logics and lambda calculi have appeared. At least three different principles have been exploited, namely linear types [4, 14], restricted modalities in the context of Linear Logic [2, 11, 17] and non-size-increasing computation [1, 13]. These systems have been studied with different, often unrelated methodologies. In particular, proofs of soundness (any function which is representable in the system lies in a complexity class) are usually quite complex and cannot be easily generalized. As a consequence, unifying, simple frameworks for the analysis of quantitative properties of computation are desirable. This would help to improve the understanding on existing systems,

U. Dal Lago (✉)
Dipartimento di Scienze dell'Informazione, Università di Bologna, Bologna, Italy
e-mail: dallago@cs.unibo.it

M. Hofmann
Institut für Informatik, LMU München, Munich, Germany
e-mail: hofmann@ifi.lmu.de

since proofs of soundness, especially conceptually simple ones, often shed light on the *reasons why* the system under consideration enjoys certain quantitative properties.

While we take the significance of LAL itself more or less for granted in this paper we may point out that it is the first higher-order system that characterises polynomial time without recourse to explicit resource bounds as found, e.g., in Bounded Arithmetic and in addition allows one to define inductive datatypes as certain formulas by impredicative quantification. Functions acting on those datatypes can thus be naturally represented as proofs via the well-known Curry-Howard correspondence (e.g., logical implication corresponds to functional types). And, noticeably, the class of representable first-order functions *equals* the polynomial time functions. One can thus view LAL as the first resource-free and purely proof-theoretic characterisation of polynomial time.

In a previous paper [8], we have introduced a new semantical framework which consists of an innovative modification of realizability whereby realizers and their runtime are bounded by elements of a certain algebraic structure, a *resource monoid*. The axioms for resource monoids are such that for any resource monoid the category of corresponding realizability sets is symmetric monoidal closed and supports second-order quantification, i.e., impredicative polymorphism. With particular resource monoids one can then realize further constructs and type formers such as modalities or recursors. In [8] we have introduced resource monoids and provided concrete instances for LFPL [13] and Elementary Affine Logic (EAL, see [6]). A fairly complicated resource monoid for LAL with a consequently rather technical and unenlightening proof of correctness has been presented in [8].

In this paper we describe a very simple resource monoid for LAL. Not only do we obtain in this way a new, simpler, and conceptually appealing proof of polytime soundness (all definable functions on binary strings are polynomial time computable) for LAL; we also find that the resource monoid we obtain is quite natural; its members are triples (n, m, f) with $n, m \in \mathbb{N}$ and $f : \mathbb{N} \to \mathbb{N}$ a non-decreasing function bounded by a polynomial; the monoid operation which interprets tensor product is given by

$$(n, m, f) + (l, k, g) = (n + l, \max\{m, k\}, \max\{f, g\}).$$

The order relation between these monoid elements is given by

$$(n, m, f) \leq (l, k, g) \quad \Longleftrightarrow \quad (n \leq l) \wedge (n + m \leq l + k) \wedge (f \leq g).$$

The interpretation of the modalities ! and § of LAL uses the functional $f \mapsto \lambda x.x^2 f(x^2)$ which explains that bounding functions extracted from the interpretation are polynomials whose degree grows exponentially with the nesting depth of the modalities as is expected from the known proof based on proof nets [2] and also the known hardness examples.

The formal similarity of our resource monoid with the one for LFPL from [8] raises hopes for a system that somehow combines LFPL and LAL; we have to admit that these hopes have not, as yet, materialized if one discounts trivial solutions like the disjoint union of the two systems.

Related Work Semantic models for LAL exist [9, 18]; however none of these models yields a proof of polytime soundness. More generally, the method of realizability has been used in connection with resource-bounded computation in several places. The most prominent is Cook and Urquhart's work [5], where terms of a language called PV^ω are used to realize formulas of bounded arithmetic. The contribution of that paper is related to ours in that realizability is used to show "polytime soundness" of a logic. There are important differences though. First, realizers in [5] are typed and very closely related to the logic that is being realized. Second, the language of realizers PV^ω only contains first-order recursion and is therefore too weak for systems like LFPL or LAL that contain or define recursion with higher-order result types. In contrast, we use untyped realizers and interpret types as certain partial equivalence relations on those. This links our work to the untyped realizability model HEO (due to Kreisel [16]). This, in turn, has also been done by Crossley et al. [7]. There, however, one proves externally that untyped realizers (in this case of bounded arithmetic formulas) are polytime, whereas our realizers are polytime bounded by construction.

2 A Computational Model

In this paper, we adopt the lambda calculus [3] as the language of realizers. More precisely, realizers will be closed values of the pure, untyped, weak and call-by-value lambda-calculus. This section summarizes those properties of the calculus which will be relevant in the rest of the paper. For more information, one can consult a recent paper by the first author and Martini [10].

Λ denotes the set of *lambda terms*, defined inductively as follows:

$$M, N ::= x \mid \lambda x.M \mid MM.$$

where x ranges over a denumerable set of *variables*. Given lambda terms M, N and a variable x, $M\{N/x\}$ is the lambda term obtained by substituting N for every free occurrence of x in M (see [3] for more details). The *size* $|M|$ of a term M is defined by induction on M: $|x| = 1$, $|\lambda x.M| = |M| + 1$ and $|MN| = |M| + |N|$. *Values* are abstractions and variables. Capital letters like V, U, W range over values. We consider weak call-by-value reduction on lambda terms, i.e. we take $\rightarrow$ as the closure of

$$(\lambda x.M)V \rightarrow M\{x/V\}$$

under all applicative contexts, i.e. reduction is governed by the following rules:

$$\frac{}{(\lambda x.M)V \rightarrow M\{x/V\}}, \qquad \frac{M \rightarrow N}{ML \rightarrow NL}, \qquad \frac{M \rightarrow N}{LM \rightarrow LN}.$$

A *realizer* is simply a closed value, i.e. an abstraction without free occurrences of variables. Realizers are ranged over by letters like e, f, g. $\mathcal{L}$ is the set of all realizers. The application $\{e\}(f)$ of two realizers is the normal form of ef relative to weak call-by-value reduction (if such a normal form exists). Observe that $\{e\}(f)$, if it exists, is always a realizer.

$\mathcal{B} = \{0, 1\}^*$ is the set of binary strings. Letters like s, t, u range over $\mathcal{B}$. The map $\Phi : \mathcal{B} \to \mathcal{L}$ is defined by induction as follows:

$$\Phi(\varepsilon) = \lambda x.\lambda y.\lambda z.z,$$

$$\Phi(0s) = \lambda x.\lambda y.\lambda z.x\Phi(s),$$

$$\Phi(1s) = \lambda x.\lambda y.\lambda z.y\Phi(s).$$

In other words, $\Phi(s)$ is the lambda-term corresponding to s in a numbering scheme attributed to Scott [21]. Similarly, there is a lambda term $\Phi(n)$ for every natural number $n \in \mathbb{N}$:

$$\Phi(0) = \lambda x.\lambda y.y,$$

$$\Phi(n+1) = \lambda x.\lambda y.x\Phi(n).$$

Pairs can be easily encoded in the lambda calculus: given two realizers e and f, $\langle e, f\rangle$ is simply the realizer $g \equiv \lambda x.xef$. Observe that $|\langle e, f\rangle| = |e| + |f| + cp$, where cp is a constant not depending on e or f.

But what is the cost of computing the normal form of a lambda term (provided it exists)? For this purpose, we define a (ternary) relation $\twoheadrightarrow \subseteq \Lambda \times \mathbb{N} \times \Lambda$. In the following, we will write $M \overset{n}{\twoheadrightarrow} N$ for $(M, n, N) \in \twoheadrightarrow$. The precise definition of $\twoheadrightarrow$ follows:

$$\frac{}{M \overset{0}{\twoheadrightarrow} M}, \qquad \frac{M \to N \quad n = \max\{1, |N| - |M|\}}{M \overset{n}{\twoheadrightarrow} N}, \qquad \frac{M \overset{n}{\twoheadrightarrow} N \quad N \overset{m}{\twoheadrightarrow} L}{M \overset{n+m}{\twoheadrightarrow} L}.$$

It turns out that for every M, N, L such that L is the normal form of MN, there is exactly one integer n such that $MN \overset{n}{\twoheadrightarrow} L$ (a proof of this result can be found in [10]). So, defining $\mathit{Time}(\{M\}(N))$ to be just n is unambiguous. Moreover, the cost model induced by $\mathit{Time}(\{\cdot\}(\cdot))$ is invariant (as shown in [10]), i.e. the lambda calculus and Turing machines can simulate each other with a polynomial overhead.

The properties of this computational model can be turned into an abstract definition. Any concrete computational model satisfying this definition is acceptable, provided the notion of cost induced by the computational model is polynomially invariant in the sense of [20] (otherwise one could prove non-realistic resource bounds in the semantics).

3 Resource Monoids and Length Spaces

In this section, we recall the notion of a resource monoid [8] and the corresponding category of realizability sets, called *length spaces*, as well as its general properties.

A *resource monoid* is a quadruple $M = (|M|, +, \leq_M, \mathcal{D}_M)$ where

(i) $(|M|, +)$ is a commutative monoid;
(ii) $\leq_M$ is a pre-order on $|M|$ which is compatible with $+$;

(iii) $\mathcal{D}_M : \{(\alpha, \beta) \mid \alpha \leq_M \beta\} \to \mathbb{N}$ is a function such that for every α, β, γ

$$\mathcal{D}_M(\alpha, \beta) + \mathcal{D}_M(\beta, \gamma) \leq \mathcal{D}_M(\alpha, \gamma),$$
$$\mathcal{D}_M(\alpha, \beta) \leq \mathcal{D}_M(\alpha + \gamma, \beta + \gamma)$$

and, moreover, for every $n \in \mathbb{N}$ there is α such that $\mathcal{D}_M(0, \alpha) \geq n$.

Given a resource monoid $M = (|M|, +, \leq_M, \mathcal{D}_M)$, the function $\mathcal{F}_M : |M| \to \mathbb{N}$ is defined by putting $\mathcal{F}_M(\alpha) = \mathcal{D}_M(0, \alpha)$.

We shall use elements of a resource monoid to bound data, algorithms, and runtimes in the following way: an element φ bounds an algorithm e if $\mathcal{F}_M(\varphi) \geq |e|$ and, more importantly, whenever α bounds an input x to e then there must be a bound $\beta \leq_M \varphi + \alpha$ for the result $y = \{e\}(x)$ and, most importantly, the runtime of that computation must be bounded by $\mathcal{D}_M(\beta, \varphi + \alpha)$. So, in a sense, we have the option of either producing a large output fast or to take a long time for a small output. The "inverse triangular" law above ensures that the composition of two algorithms bounded by φ_1 and φ_2, respectively, can be bounded by $\varphi_1 + \varphi_2$ or a simple modification thereof. In particular, the contribution of the unknown intermediate result in a composition cancels out using that law. Another useful intuition is that $\mathcal{D}_M(\alpha, \beta)$ behaves like the difference $\beta - \alpha$, indeed, $(\beta - \alpha) + (\gamma - \beta) \leq \gamma - \alpha$.

A *length space* on a resource monoid $M = (|M|, +, \leq_M, \mathcal{D}_M)$ is a pair $A = (|A|, \Vdash_A)$, where $|A|$ is a set and $\Vdash_A \subseteq |M| \times \mathcal{L} \times |A|$ is a(n infix) relation satisfying the following conditions:

(i) if $\alpha, e \Vdash_A a$, then $\mathcal{F}_M(\alpha) \geq |e|$;
(ii) if $\alpha, e \Vdash_A a$ and $\alpha \leq_M \beta$, then $\beta, e \Vdash_A a$;

A *morphism* from length space $A = (|A|, \Vdash_A)$ to length space $B = (|B|, \Vdash_B)$ (on the same resource monoid $M = (|M|, +, \leq_M, \mathcal{D}_M)$) is a function $f : |A| \to |B|$ such that there exist $e \in \mathcal{L}$, $\varphi \in |M|$ with $\mathcal{F}_M(\varphi) \geq |e|$ and whenever $\alpha, d \Vdash_A a$, there must be β, c such that

(i) $\beta, c \Vdash_B f(a)$;
(ii) $\beta \leq_M \varphi + \alpha$;
(iii) $\{e\}(d) = c$;
(iv) $\mathit{Time}(\{e\}(d)) \leq \mathcal{D}_M(\beta, \varphi + \alpha)$.

We call e a *realizer* of f and φ a *majorizer* of f. The set of all morphisms from A to B is denoted as $\mathit{Hom}(A, B)$. If f is a morphism from A to B realized by e and majorized by φ, then we will write $f : A \xrightarrow{e,\varphi} B$ or $\varphi, e \Vdash_{A \multimap B} f$.

Given two length spaces $A = (|A|, \Vdash_A)$ and $B = (|B|, \Vdash_B)$ on the same resource monoid M, we define $A \otimes B = (|A| \times |B|, \Vdash_{A \otimes B})$ (on M) where $\alpha, e \Vdash_{A \otimes B} (a, b)$ iff $\mathcal{F}_M(\alpha) \geq |e|$ and there are f, g, β, γ with

$$\beta, f \Vdash_A a,$$
$$\gamma, g \Vdash_B b,$$
$$e = \langle f, g \rangle,$$
$$\alpha \geq_M \beta + \gamma.$$

Given A and B as above, we can build $A \multimap B = (A \Rightarrow B, \Vdash_{A \multimap B})$ where $A \Rightarrow B$ is the set of functions from A to B and $e, \alpha \Vdash_{A \multimap B} f$ iff f is a morphism from A to B realized by e and majorized by α.

The following result is from [8]:

Lemma 1 *For every resource monoid M, length spaces on M and their morphisms form a symmetric monoidal closed category with tensor and linear implication given as above.*

For every resource monoid M, a length space I_M is defined by $|I_M| = \{0\}$ and $\alpha, \lambda x.x \Vdash_{I_M} 0$ when $\mathcal{F}(\alpha) \geq |\lambda x.x|$. For each length space A there are isomorphisms $A \otimes I \simeq A$ and a unique morphism $A \to I$. The latter serves to justify full weakening.

For every resource monoid M, there is a length space $\mathcal{B}_M = (\{0,1\}^*, \Vdash_{B_M})$ where $\alpha, \Phi(t) \Vdash_{\mathcal{B}_M} t$ whenever $\mathcal{F}(\alpha) \geq |\Phi(t)|$. The function s_0 (respectively, s_1) from $\{0,1\}^*$ to itself which appends 0 (respectively, 1) to the left of its argument can be computed in constant time and, as a consequence, is a morphism from $\mathcal{B}_M$ to itself. Moreover, the function $\varepsilon : \{0\} \to \mathcal{B}$ which returns the empty string is itself a morphism from I_M to $\mathcal{B}_M$.

3.1 Interpreting Multiplicative Affine Logic

Second order multiplicative affine logic (i.e., multiplicative linear logic plus full weakening, MAL) can be interpreted inside the category of length spaces on any monoid M. This result has been originally showed in [8] and we recall it here. Doing this will simplify the analysis of LAL, since the latter can be obtained by enriching multiplicative affine logic with two modalities. Both LAL and MAL will be presented as intuitionistic proof systems.

Formulas of (intuitionistic, second order) multiplicative affine logic are generated by the following productions:

$$A ::= \alpha \mid A \multimap A \mid A \otimes A \mid \forall \alpha.A$$

where α ranges over a countable set of atoms. Rules are reported in Fig. 1. In MAL, the second order existential quantification is defined, as in second order intuitionistic logic [12], i.e., one can define $\exists \alpha.A$ as $\forall \beta.(\forall \alpha.A \multimap \beta) \multimap \beta$. With this definition, the usual rules for existential quantification are both available. Moreover, the presence of full weakening allows to faithfully encode the so-called additive connectives inside MAL:

$$A \& B \equiv \exists \alpha.((\alpha \multimap A) \otimes (\alpha \multimap B) \otimes \alpha),$$
$$A \oplus B \equiv \forall \alpha.((A \multimap \alpha) \multimap (B \multimap \alpha) \multimap \alpha.$$

Actually, the tensor product $\otimes$ could be itself defined in terms of second order quantification and linear implication:

$$A \otimes B \equiv \forall \alpha.((A \multimap B \multimap \alpha) \multimap \alpha).$$

Identity, Cut and Weakening.

$$\frac{}{A \vdash A} I, \qquad \frac{\Gamma \vdash A \quad \Delta, A \vdash B}{\Gamma, \Delta \vdash B} U, \qquad \frac{\Gamma \vdash A}{\Gamma, B \vdash A} W.$$

Multiplicative Logical Rules.

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \otimes B \vdash C} L_{\otimes}, \qquad \frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B} R_{\otimes},$$

$$\frac{\Gamma \vdash A \quad \Delta, B \vdash C}{\Gamma, \Delta, A \multimap B \vdash C} L_{\multimap}, \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \multimap B} R_{\multimap}.$$

Second Order Logical Rules.

$$\frac{\Gamma, \forall\alpha.A \vdash B}{\vdash \Gamma, A[C/\alpha] \vdash B} L^{\forall}, \qquad \frac{\Gamma \vdash \forall\alpha.A}{\Gamma \vdash A \quad \alpha \notin FV(\Gamma)} R^{\forall}.$$

Fig. 1 Intuitionistic Multiplicative Affine Logic

Set-theoretic and realizability interpretations of MAL's formulas and proofs will be now introduced. They are essential tools when proving soundness theorems for LAL. A *set-theoretic environment* is a partial function assigning sets to atoms. Given a formula A and a set-theoretic environment η, we can define a set $[\![A]\!]^{\mathcal{S}}_{\eta}$ by induction on the structure of A as follows:

$$[\![\alpha]\!]^{\mathcal{S}}_{\eta} = \eta(\alpha),$$

$$[\![A \otimes B]\!]^{\mathcal{S}}_{\eta} = [\![A]\!]^{\mathcal{S}}_{\eta} \times [\![B]\!]^{\mathcal{S}}_{\eta},$$

$$[\![A \multimap B]\!]^{\mathcal{S}}_{\eta} = [\![A]\!]^{\mathcal{S}}_{\eta} \Rightarrow [\![B]\!]^{\mathcal{S}}_{\eta},$$

$$[\![\forall\alpha.A]\!]^{\mathcal{S}}_{\eta} = \prod_{C \in \mathcal{U}} [\![A]\!]^{\mathcal{S}}_{\eta[\alpha \to C]}.$$

Here $\mathcal{U}$ stands for the class of all length spaces. If the underlying set-theory is classical, $\mathcal{U}$ cannot exist. However, we follow [15] and assume to work in constructive set theory.

If $n \geq 0$ and $A_1, \ldots, A_n$ are formulas, the expression $[\![A_1 \otimes \ldots \otimes A_n]\!]^{\mathcal{S}}_{\eta}$ stands for I_M if $n = 0$ and $[\![A_1 \otimes \ldots \otimes A_{n-1}]\!]^{\mathcal{S}}_{\eta} \otimes [\![A_n]\!]^{\mathcal{R}}_{\eta}$ if $n \geq 1$. Given a MAL proof π of $A_1, \ldots, A_n \vdash B$ and a set-theoretic environment η, a function

$$[\![\pi]\!]^{\mathcal{S}}_{\eta} : [\![A_1 \otimes \ldots \otimes A_n]\!]^{\mathcal{S}}_{\eta} \to [\![B]\!]^{\mathcal{S}}_{\eta}$$

can be easily defined following the structure of π.

A *realizability environment* for a resource monoid M is a partial function assigning length spaces (on M) to atoms. Given a realizability environment η, $|\eta|$ is the set-theoretic environment returning the carrier of $\eta(\alpha)$ on argument α (provided $\eta(\alpha)$

is defined). Realizability semantics $[\![A]\!]^{\mathcal{R}}_{\eta}$ of a formula A on the realizability environment η is defined by induction on A:

$$[\![\alpha]\!]^{\mathcal{R}}_{\eta} = \eta(\alpha),$$
$$[\![A \otimes B]\!]^{\mathcal{R}}_{\eta} = [\![A]\!]^{\mathcal{R}}_{\eta} \otimes [\![B]\!]^{\mathcal{R}}_{\eta},$$
$$[\![A \multimap B]\!]^{\mathcal{R}}_{\eta} = [\![A]\!]^{\mathcal{R}}_{\eta} \multimap [\![B]\!]^{\mathcal{R}}_{\eta},$$
$$[\![\forall\alpha.A]\!]^{\mathcal{R}}_{\eta} = ([\![\forall\alpha.A]\!]^{\mathcal{S}}_{|\eta|}, \Vdash_{[\![\forall\alpha.A]\!]^{\mathcal{R}}_{\eta}}).$$

where $\otimes$ and $\multimap$ are constructions on length spaces defined in Sect. 3 and $\alpha, e \Vdash_{[\![\forall\alpha.A]\!]^{\mathcal{R}}_{\eta}} a$ iff for every length space C, $\alpha, e \Vdash_{[\![A]\!]^{\mathcal{R}}_{\eta[\alpha\to C]}} a$. Observe that $|[\![A]\!]^{\mathcal{R}}_{\eta}| = [\![A]\!]^{\mathcal{S}}_{|\eta|}$.

Given a MAL proof π of $A_1, \ldots, A_n \vdash B$ and a realizability environment η, we can prove that $[\![\pi]\!]^{\mathcal{S}}_{|\eta|}$ is a morphism from $[\![A_1 \otimes \ldots \otimes A_n]\!]^{\mathcal{R}}_{\eta}$ to $[\![B]\!]^{\mathcal{R}}_{\eta}$. The proof goes by induction on the structure of π. Notice that the result holds independently on the underlying resource monoid, since the main ingredients for the proof (see [8]) hold for every resource monoid M. Formally:

Theorem 1 *For every resource monoid M there is a polynomial $p_M : \mathbb{N} \to \mathbb{N}$ such that the following holds. Let π be a* MAL *proof of a sequent $A_1, \ldots, A_n \vdash B$. Let η be a realizability environment assigning length spaces on M to all atoms appearing free in the sequent. Then the function $[\![\pi]\!]^{\mathcal{S}}_{|\eta|}$ is a morphism (of length spaces on M) from $[\![A_1 \otimes \ldots \otimes A_n]\!]^{\mathcal{R}}_{\eta}$ to $[\![B]\!]^{\mathcal{R}}_{\eta}$ majorized by some $\alpha_\pi \in |M|$, where $\mathcal{F}(\alpha_\pi) \leq p_M(|\pi|)$.*

Please observe that semantics is preserved by reduction: whenever π reduces to ρ then the set-theoretic semantics $[\![\pi]\!]^{\mathcal{S}}_{\eta}$ equals $[\![\rho]\!]^{\mathcal{S}}_{\eta}$. And, clearly, if $[\![\pi]\!]^{\mathcal{S}}_{\eta}$ is realized by e and majorized by α, then $[\![\rho]\!]^{\mathcal{S}}_{\eta}$ will be realized by the same e and majorized by the same α.

4 Light Length Spaces

Light Affine Logic extends MAL by two modalities ! and § which are governed by the rules in Fig. 2. For every LAL proof π, we define the *box depth* $\partial(\pi) \in \mathbb{N}$ of π as the maximum number of instances of $P_{\S}$, $P^1_!$ or $P^2_!$ on any path starting at the root of π and ending at one of its leaves.

Exponential Rules and Contraction.

$$\frac{\Gamma, \Delta \vdash A}{\S\Gamma, !\Delta \vdash \S A} P_{\S}, \qquad \frac{A \vdash B}{!A \vdash !B} P^1_!, \qquad \frac{\vdash A}{\vdash !A} P^2_!, \qquad \frac{\Gamma, !A, !A \vdash B}{\Gamma, !A \vdash B} C.$$

Fig. 2 Intuitionistic Light Affine Logic

In LAL, we can use variations on the usual impredicative encodings of natural numbers, lists, etc. For example, binary lists can be encoded as cut-free proofs for

$$List_{\mathsf{LAL}} \equiv \forall\alpha.!(\alpha \multimap \alpha) \multimap !(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha)$$

while natural numbers correspond to proofs for

$$Int_{\mathsf{LAL}} \equiv \forall\alpha.!(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha).$$

Now, let π be an LAL proof with conclusion $List_{\mathsf{LAL}} \vdash List_{\mathsf{LAL}}$. If we cut π against proofs corresponding to binary lists and we normalize the obtained proof, we get a proof corresponding to a binary list. So any proof like π *represents* a function from binary lists to binary lists. The above definition can be easily generalized to the cases when π has conclusion in the form $\{!, \S\}^j List_{\mathsf{LAL}} \vdash \{!, \S\}^k List_{\mathsf{LAL}}$.

But what is the expressive power of Light Affine Logic? The class of representable functions includes all the polytime functions:

Theorem 2 (Polytime Completeness, [19]) *Every polytime function on binary lists is represented by a* LAL *proof* $\pi : List_{\mathsf{LAL}} \multimap \S^n List_{\mathsf{LAL}}$.

We will now describe a resource monoid with the property that the ensuing category of length spaces provides structure for the interpretation of these modalities while allowing us to extract polytime bounds for functions of basic type. For ease of notation, we denote $\max(m, n)$ by $m \mid n$:

Definition 1 The algebraic structure $\mathcal{L}$ is the quadruple $(|\mathcal{L}|, +, \leq_{\mathcal{L}}, \mathcal{D}_{\mathcal{L}})$ such that:

- Elements of $|\mathcal{L}| \subseteq \mathbb{N} \times \mathbb{N} \times \mathbb{N}^{\mathbb{N}}$ are triples (n, m, f) such that $f : \mathbb{N} \to \mathbb{N}$ is a non-decreasing function bounded (from above) by a polynomial.
- For every $(n, m, f), (l, k, g) \in |\mathcal{L}|$, $(n, m, f) + (l, k, g) = (n + l, m \mid k, f \mid g)$.
- For every $(n, m, f), (l, k, g) \in |\mathcal{L}|$, $(n, m, f) \leq_{\mathcal{L}} (l, k, g)$ iff $n \leq l$, $n + m \leq l + k$ and $f \leq g$.
- For every $(n, m, f), (l, k, g) \in |\mathcal{L}|$ such that $(n, m, f) \leq_{\mathcal{L}} (l, k, g)$,

$$\mathcal{D}_{\mathcal{L}}((n, m, f), (l, k, g)) = (l - n)g(l + k).$$

The triple $(0, 0, 0) \in |\mathcal{L}|$, denoted $0_{\mathcal{L}}$, is an identity for $+$.

The binary relation $\leq_{\mathcal{L}}$ is trivially reflexive. Moreover, it is transitive:

Lemma 2 (Transitivity) *If* α, β, γ *are in* $|\mathcal{L}|$, $\alpha \leq_{\mathcal{L}} \beta$ *and* $\beta \leq_{\mathcal{L}} \gamma$, *then* $\alpha \leq_{\mathcal{L}} \gamma$.

Proof Let $(n, m, f), (l, k, g), (p, q, h) \in |\mathcal{L}|$. Moreover, let $(n, m, f) \leq_{\mathcal{L}} (l, k, g)$ and $(l, k, g) \leq_{\mathcal{L}} (p, q, h)$. Trivially:

$$n \le l \le p;$$
$$n + m \le l + k \le p + q;$$
$$f \le g \le h.$$

In other words $(n, m, f) \le_{\mathcal{L}} (p, q, h)$. □

But $\le_{\mathcal{L}}$ is even compatible with $+$:

Lemma 3 (Compatibility) *$0_{\mathcal{L}} \le_{\mathcal{L}} \alpha$ for every $\alpha \in |\mathcal{L}|$. Moreover, if α, β, γ are in $|\mathcal{L}|$ and $\alpha \le_{\mathcal{L}} \beta$, then $\alpha + \gamma \le_{\mathcal{L}} \beta + \gamma$.*

Proof Let $(n, m, f) \in |\mathcal{L}|$. Clearly, $0 \le n$, $0 + 0 \le n + m$ and $0 \le f$. As a consequence, $0_{\mathcal{L}} \le_{\mathcal{L}} (n, m, f)$. Now, let $(n, m, f), (l, k, g), (p, q, h) \in |\mathcal{L}|$ and let $(n, m, f) \le_{\mathcal{L}} (l, k, g)$. This implies $n \le l$, $n + m \le l + k$ and $f \le g$. Then:

$$n + p \le l + p;$$
$$(n + p) + (m + q) = (n + m) + (p + q) \le (l + k) + (p + q) \le (l + p) + (k + q);$$
$$f \mid h \le g \mid h.$$

This implies $(n, m, f) + (p, q, h) \le_{\mathcal{L}} (l, k, g) + (p, q, h)$. □

It now remains to show that $\mathcal{D}_{\mathcal{L}}$ satisfies the two required axioms in the definition of a resource monoid:

Lemma 4 *If α, β, γ are in $|\mathcal{L}|$ and $\alpha \le_{\mathcal{L}} \beta$, then $\mathcal{D}_{\mathcal{L}}(\alpha, \beta) \le \mathcal{D}_{\mathcal{L}}(\alpha + \gamma, \beta + \gamma)$.*

Proof Let $(n, m, f), (l, k, g), (p, q, h) \in |\mathcal{L}|$ and let $(n, m, f) \le_{\mathcal{L}} (l, k, g)$. Now,

$$\begin{aligned}
&\mathcal{D}_{\mathcal{L}}((n, m, f) + (p, q, h), (l, k, g) + (p, q, h)) \\
&\quad = \mathcal{D}_{\mathcal{L}}((n + p, m \mid q, f \mid h), (l + p, k \mid q, g \mid h)) \\
&\quad = ((l + p) - (n + p))(g \mid h)(l + p + k \mid q)) \\
&\quad \ge (l - n)g(l + k) \\
&\quad = \mathcal{D}_{\mathcal{L}}((n, m, f), (l, k, g)).
\end{aligned}$$

and we are done. □

Lemma 5 *If α, β, γ are in $|\mathcal{L}|$, $\alpha \le_{\mathcal{L}} \beta$ and $\beta \le_{\mathcal{L}} \gamma$, then $\mathcal{D}_{\mathcal{L}}(\alpha, \beta) + \mathcal{D}_{\mathcal{L}}(\beta, \gamma) \le \mathcal{D}_{\mathcal{L}}(\alpha, \gamma)$.*

Proof Let $(n, m, f), (l, k, g), (p, q, h) \in |\mathcal{L}|$ and let $(n, m, f) \le_{\mathcal{L}} (l, k, g)$, $(l, k, g) \le_{\mathcal{L}} (p, q, h)$. Now,

$$\begin{aligned}\mathcal{D}_{\mathcal{L}}((n,m,f),(p,q,h)) &= (p-n)h(p+q)\\ &= ((p-l)+(l-n))h(p+q)\\ &= (p-l)h(p+q)+(l-n)h(p+q)\\ &\geq (p-l)h(p+q)+(l-n)g(p+q)\\ &\geq (p-l)h(p+q)+(l-n)g(l+k)\\ &= +\mathcal{D}_{\mathcal{L}}((l,k,g),(p,q,h))+\mathcal{D}_{\mathcal{L}}((n,m,f),(l,k,g)).\ \square\end{aligned}$$

The following is now immediate.

Lemma 6 *$\mathcal{L}$ is a resource monoid.*

Definition 2 A *light length space* is a length space over the resource monoid $\mathcal{L}$. Given a light length space $A=(|A|,\Vdash_A)$, the light spaces $!A=(|A|,\Vdash_{!A})$ and $\S A=(|A|,\Vdash_{\S A})$ both with underlying set $|A|$, are defined by:

$$\begin{aligned}&(n,m,f),e\Vdash_{!A}a\\ &\quad\iff\quad \exists(l,k,g)\in|\mathcal{L}|.(l,k,g),e\Vdash_A a\wedge(1,l+k,g^+)\leq_{\mathcal{L}}(n,m,f),\\ &(n,m,f),e\Vdash_{\S A}a\\ &\quad\iff\quad \exists(l,k,g)\in|\mathcal{L}|.(lk,k,g),e\Vdash_A a\wedge(l,k,g^+)\leq_{\mathcal{L}}(n,m,f)\end{aligned}$$

where $g^+(x)=x^2g(x^2)$.

The constructions ! and § on light length spaces serve to capture the exponential modalities of light affine logic. Their definition is the crucial contribution of this paper. The relations $\Vdash_{!A},\Vdash_{\S A}$ could equivalently be defined inductively by the following rules:

$$\frac{\alpha,e\Vdash_{!A}a\quad\alpha\leq\beta}{\beta,e\Vdash_{!A}a},\qquad\frac{\alpha,e\Vdash_{\S A}a\quad\alpha\leq\beta}{\beta,e\Vdash_{\S A}a},$$

$$\frac{(l,k,g),e\Vdash_A a}{(1,(l+k),g^+),e\Vdash_{!A}a},\qquad\frac{(lk,k,g),e\Vdash_A a}{(l,k,g^+),e\Vdash_{\S A}a}.$$

Before we embark on the verification that these settings admit an interpretation of all the constructions of LAL let us illustrate the definitions using the particular length space $\mathcal{N}=(\mathbb{N},\Vdash_{\mathcal{N}})$ where $(l,k,g),e\Vdash_{\mathcal{N}}n$ if $e=\Phi(n)$, $l\geq n+1$, $k\geq 0$ and $g(x)\geq w$ for w a constant large enough so that $lw\geq(n+1)w\geq|e|$. Note that the constant w may be chosen independent of n.

Then $(l,k,g),e\Vdash_{\mathcal{N}\otimes\mathcal{N}}(n,m)$ if $l\geq n+m+2$ and $e=\langle d,c\rangle$ where d encodes n, c encodes m and $g(x)\geq w$ and $lg(l+k)\geq|e|$. Note that the latter can be achieved by choosing $g(x)=w+z$ for some fixed constant z.

We see that the diagonal map $n\mapsto(n,n)$ cannot be realized for then we would need a fixed i such that $i+l\geq l+l$ for all l. Similarly, we see that all morphisms f from $\mathcal{N}$ to $\mathcal{N}$ must satisfy $f(x)\leq x+O(1)$. The runtime of such a function

is governed by the rightmost component of its majorizer and is hence an arbitrary polynomial.

On the other hand, the length space $!\mathcal{N}$ has $(l,k,g), e \Vdash_{!\mathcal{N}} n$ if $l \geq 1$ and $k \geq n+1$ and $g(x) \geq wx^2$. Now note that $lg(l+k) \geq w(l+k)^2 \geq wk \geq |e|$. On the other hand, since the first component of the underlying realizer may be chosen 1 we find that the diagonal map $!\mathcal{N} \to !\mathcal{N} \otimes !\mathcal{N}$ is realisable. The identity function from $!\mathcal{N}$ to $\mathcal{N}$ is not realisable because the first component i of its realiser would have to satisfy $i+1 \geq n$ for all n.

Now consider the length space $\S\mathcal{N}$. We have $(l,k,g), e \Vdash_{\S\mathcal{N}} n$ if $lk \geq n+1$ and $g(x) \geq wx^2$. We are now able to realise the identity from $!\mathcal{N}$ to $\S\mathcal{N}$ noticing that, in particular $(1, n+1, x \mapsto wx^2), \Phi(n) \Vdash_{\S\mathcal{N}} n$. We also note that, for instance, the doubling function can be realised as a map from $\mathcal{N}$ to $\S\mathcal{N}$. To do this, we need a majorizer with first component $i = 1$. Given input n realised by $(n+1, 1, x \mapsto w)$ we then realise the result $2n$ by $(n+1, 2, x \mapsto wx^2)$. We can even realise the functions bounded by $1/4n^2 + O(n)$ but not n^2. For this, two instances of § are needed.

Proving light length spaces to be a model for LAL amounts to prove that certain constructions involving the modalities ! and § can be justified in the model. First of all, the diagonal map is a morphism, as can be easily proved:

Lemma 7 *Given light length space A, there is a morphism $contr : !A \to !A \otimes !A$ where $contr(a) = (a,a)$.*

Proof The majorizer for the obvious realiser $e_{contr} = \lambda x.\lambda y.yxx$ is given by a suitably padded version of $(2, 0, x \mapsto 0)$. The central part of the verification is the observation that

$$\begin{aligned} 2.(1, l+k, g^+) = (2, l+k, g^+) &\leq_{\mathcal{L}} (2, 0, x \mapsto 0) + (1, l+k, g^+) \\ &= (3, l+k, g^+). \end{aligned}$$

Moreover, observe that

$$\begin{aligned} \mathcal{D}_{\mathcal{L}}((2, l+k, g^+), (3, l+k, g^+)) &= (3-2)(l+k+3)^2 g((l+k+3)^2) \\ &\geq lg(l+k) \geq \mathcal{F}_{\mathcal{L}}(l,k,g). \end{aligned}$$

This concludes the proof. □

On the other hand, ! is a functor.

Lemma 8 (Functoriality of !) *If $f : A \xrightarrow{e,(n,m,f)} B$, then there is β such that $f : !A \xrightarrow{e,(n+m+1,m,f^+)} !B$.*

Proof Let α be (n,m,f) and suppose $(l,k,g), d \Vdash_{!A} a$. Then $(l,k,g) \geq_{\mathcal{L}} (1, p+q, h^+)$, where $(p,q,h), d \Vdash_A a$. Observe that there must be $(i,j,r), c$ such that $(i,j,r), c \Vdash_B f(a)$, $(i,j,r) \leq_{\mathcal{L}} (n,m,f) + (p,q,h)$ and $Time(\{e\}(d)) \leq$

$\mathcal{D}_{\mathcal{L}}((i,j,r),(n,m,f)+(p,q,h))$. As a consequence, $(1,i+j,r^+),c \Vdash_{!B} f(a)$. But

$$(1,i+j,r^+) \leq_{\mathcal{L}} (n+m+1,m,f^+)+(1,p+q,h^+)$$

because:

- The inequality $1+i+j \leq n+m+2+m \mid (p+q)$ holds, because if $m \leq q$, then

$$1+i+j \leq 1+n+p+m \mid q = 1+n+p+q \leq 2+n+m+m \mid (p+q);$$

  and if $m > q$, then

$$\begin{aligned} 1+i+j &\leq 1+n+p+m \mid q = 1+n+p+m \leq 2+n+m+p+q \\ &\leq 2+n+m+m \mid (p+q). \end{aligned}$$

- For every $x \in \mathbb{N}$,

$$\begin{aligned} r^+(x) &= x^2 r(x^2) \leq x^2(f \mid h)(x^2) \\ &\leq x^2(f(x^2) \mid h(x^2)) = (x^2 f(x^2) \mid x^2 h(x^2)) \\ &= (f^+(x) \mid h^+(x)) = (f \mid h)^+(x). \end{aligned}$$

Moreover:

$$\begin{aligned} &\mathit{Time}(\{e\}(d)) \\ &\leq \mathcal{D}_{\mathcal{L}}((i,j,r),(n,m,f)+(p,q,h)) \\ &\leq (n+p)(f \mid h)(n+p+m \mid q) \\ &\leq (n+m+1)\cdot(n+m+2+m \mid (p+q))^2 \\ &\quad \cdot (f \mid h)((n+m+2+m \mid (p+q))^2) \\ &= (n+m+1)\cdot(f \mid h)^+(n+m+2+m \mid (p+q)) \\ &= (n+m+1)\cdot(f^+ \mid h^+)(n+m+2+m \mid (p+q)) \\ &= \mathcal{D}_{\mathcal{L}}((1,i+j,r^+),(n+m+2,m \mid (p+q),f^+ \mid h^+)) \\ &\leq \mathcal{D}_{\mathcal{L}}((1,i+j,r^+),(n+m+1,m,f^+)+(1,p+q,h^+)) \end{aligned}$$

This means that $f : !A \xrightarrow{e,(n+m+1,m,f^+)} !B$. □

Notice that the distributive law $!A \otimes !B \multimap !(A \otimes B)$ *cannot* be proved in the syntax and is not validated in the model either. Indeed, its introduction would collapse LAL to elementary affine logic, which is elementary time complete. The modality § is a functor itself, and this can be proved with:

Lemma 9 (Functoriality of §) *If* $f : A \xrightarrow{e,(n,m,f)} B$, *then there is* β *such that* $f : \S A \xrightarrow{e,(n+2,m+1,f^+)} \S B$.

Proof Let α be (n, m, f) and suppose $(l, k, g), d \Vdash_{\S A} a$. Then $(l, k, g) \geq_{\mathcal{L}} (p, q, h^+)$, where $(pq, q, h), d \Vdash_A a$. Observe that there must be $(i, j, r), c$ such that $(i, j, r), c \Vdash_B f(a)$, $(i, j, r) \leq_{\mathcal{L}} (n, m, f) + (pq, q, h)$ and $Time(\{e\}(d)) \leq \mathcal{D}_{\mathcal{L}}((i, j, r), (n, m, f) + (pq, q, h))$. As a consequence, we obtain $(n, m, f) + (pq, q, h), c \Vdash_B f(a)$. But notice that

$$\begin{aligned}(n, m, f) + (pq, q, h) &= (n + pq, m \mid q, f \mid h)\\ &\leq_{\mathcal{L}} (((m + 1) \mid q)(n + 1 + p), (m + 1) \mid q, f \mid h).\end{aligned}$$

which implies $(n + 1 + p, (m + 1) \mid q, (f \mid h)^+), c \Vdash_{\S B} f(a)$. Now:

$$\begin{aligned}(n + 1 + p, (m + 1) \mid q, (f \mid h)^+) &= (n + 1, m + 1, f^+) + (p, q, h^+)\\ &\leq_{\mathcal{L}} (n + 2, m + 1, f^+) + (l, k, g).\end{aligned}$$

Moreover:

$$\begin{aligned}&Time(\{e\}(d))\\ &\leq \mathcal{D}_{\mathcal{L}}((i, j, r), (n, m, f) + (pq, q, h))\\ &\leq (n + pq)(f \mid h)(n + pq + m \mid q)\\ &\leq (n + p + 2 + q(m + 1))^2(f \mid h)((n + p + 2 + q \mid (m + 1))^2)\\ &= (f \mid h)^+(n + p + 2 + q \mid (m + 1))\\ &= (f^+ \mid h^+)(n + p + 2 + q \mid (m + 1))\\ &= (p + n + 2 - (p + n + 1))(f^+ \mid h^+)(n + p + 2 + q \mid (m + 1))\\ &= \mathcal{D}_{\mathcal{L}}((n + 1 + p, (m + 1), (f \mid h)^+), (n + 2, m + 1, f^+) + (p, q, h^+))\\ &= \mathcal{D}_{\mathcal{L}}((n + 1 + p, (m + 1), (f \mid h)^+), (n + 2, m + 1, f^+) + (l, k, g)).\end{aligned}$$

This means that $f : \S A \xrightarrow{e,(n+2,m+1,f^+)} \S B$. □

The following lemma establishes the remaining properties required to model LAL: distributivity of § over $\otimes$ and the dereliction axiom relating the two modalities.

Lemma 10 *Given light length spaces A, B, there are morphisms: derelict* $: !A \to \S A$ *and distr* $: \S A \otimes \S B \to \S(A \otimes B)$ *where, for every $a \in |A|$ and $b \in |B|$, derelict$(a) = a$ and distr$(a, b) = (a, b)$.*

Proof Let $e_{distr} = \lambda x.x$. We know $\{e_{distr}\}(d)$ takes constant time, say p. Then, let $\alpha, \beta \in |\mathcal{L}|$ be such that $\mathcal{F}_{\mathcal{L}}(\alpha) \geq p + |e_{distr}|$, and $\beta \geq_{\mathcal{L}} (1, cp, x \mapsto x^2)$. α_{distr} is then defined as $\alpha + \beta$. Now, let $(n, m, f), \langle d, c\rangle \Vdash_{\S A \otimes \S B} (a, b)$. This means that $(n, m, f) \geq_{\mathcal{L}} (l, k, g^+) + (p, q, h^+)$, where $(lk, k, g), d \Vdash_A a$ and $(pq, q, h), c \Vdash_B b$. This in turn means that $(lk + pq + cp, k \mid q, g \mid h \mid (x \mapsto 1)), \langle d, c\rangle \Vdash_{A \otimes B} (a, b)$ which yields

$$((l + p + 1)(k \mid q \mid cp), k \mid q \mid cp, g \mid h \mid (x \mapsto 1)), \langle d, c\rangle \Vdash_{A \otimes B} (a, b),$$

from which

$$(l+p+1,k \mid q \mid cp, g^+ \mid h^+ \mid (x \mapsto x^2)), \langle d,c\rangle \Vdash_{\S(A\otimes B)} (a,b).$$

Moreover:

$$\begin{aligned}
&(l+p+1,k \mid q \mid cp, g^+ \mid h^+ \mid (x \mapsto x^2))\\
&\quad = (l,k,g^+) + (p,q,h^+) + (1, cp, x \mapsto x^2)\\
&\quad \leq_{\mathcal{L}} (l,k,g^+) + (p,q,h^+) + \beta\\
&\quad \leq_{\mathcal{L}} (n,m,f) + \beta\\
&\quad \leq_{\mathcal{L}} (n,m,f) + \alpha_{distr}.
\end{aligned}$$

Finally:

$$\begin{aligned}
&\mathit{Time}(\{e_{distr}\}(\langle d,c\rangle))\\
&\quad \leq p \leq \mathcal{F}_{\mathcal{L}}(\alpha)\\
&\quad \leq \mathcal{D}_{\mathcal{L}}((l+p+1,k \mid q \mid cp, g^+ \mid h^+ \mid x \mapsto x^2), (n,m,f)+\beta) + \mathcal{F}_{\mathcal{L}}(\alpha)\\
&\quad \leq \mathcal{D}_{\mathcal{L}}((l+p+1,k \mid q \mid cp, g^+ \mid h^+ \mid x \mapsto x^2), (n,m,f)+\beta+\alpha)\\
&\quad \leq \mathcal{D}_{\mathcal{L}}((l+p+1,k \mid q \mid cp, g^+ \mid h^+ \mid x \mapsto x^2), (n,m,f)+\alpha_{distr}).
\end{aligned}$$

This proves *distr* to be a morphism. Let $e_{derelict} = \lambda x.x$. We know $\{e_{derelict}\}(d)$ takes constant time, say p. Then, let $\alpha_{derelict} \in |\mathcal{L}|$ be such that $\mathcal{F}_{\mathcal{L}}(\alpha_{derelict}) \geq p + |e_{derelict}|$. Now, let $(n,m,f), d \Vdash_{!A} a$. This means that $(n,m,f) \geq_{\mathcal{L}} (1, l+k, g^+)$, where $(l,k,g), d \Vdash_A a$. This in turn means that $(l+k, l+k, g), d \Vdash_A a$ which hields $(1, l+k, g^+), d \Vdash_{\S A} a$. Clearly,

$$(1,l+k,g^+) \leq_{\mathcal{L}} (1,l+k,g^+) + \alpha_{derelict}.$$

Finally:

$$\begin{aligned}
\mathit{Time}(\{e_{derelict}\}(d)) &\leq p \leq \mathcal{F}_{\mathcal{L}}(\alpha_{derelict})\\
&\leq \mathcal{D}_{\mathcal{L}}((1,l+k,g^+),(1,l+k,g^+)) + \mathcal{F}_{\mathcal{L}}(\alpha_{derelict})\\
&\leq \mathcal{D}_{\mathcal{L}}((1,l+k,g^+),(1,l+k,g^+) + \alpha_{derelict}).
\end{aligned}$$

This proves *derelict* to be a morphism. □

4.1 Interpreting Light Affine Logic

Interpretations of the modalities § and ! are the obvious ones: $[\![!A]\!]^{\mathcal{R}}_{\eta} = ![\![A]\!]^{\mathcal{R}}_{\eta}$ and $[\![\S A]\!]^{\mathcal{R}}_{\eta} = \S[\![A]\!]^{\mathcal{R}}_{\eta}$. Set-theoretic interpretations are not affected by ! nor by §: $[\![!A]\!]^{\mathcal{S}}_{\eta} = [\![A]\!]^{\mathcal{S}}_{\eta}$ and $[\![\S A]\!]^{\mathcal{S}}_{\eta} = [\![A]\!]^{\mathcal{S}}_{\eta}$.

Light length spaces form a model of LAL:

Theorem 3 *For every natural number $m \in \mathbb{N}$ there is a polynomial function $f_m : \mathbb{N} \to \mathbb{N}$ such that, for every* LAL *proof $\pi : A_1, \ldots, A_n \vdash B$ and for every realizability environment η assigning light length spaces to all atoms appearing free in the sequent, we have that*

$$[\![\pi]\!]^{\S}_{|\eta|} : [\![A_1 \otimes \ldots \otimes A_n]\!]^{\mathcal{R}}_{\eta} \xrightarrow{\varphi, e} [\![B]\!]^{\mathcal{R}}_{\eta}.$$

and $\mathcal{F}_{\mathcal{L}}(\varphi) \leq f_{\partial(\pi)}(|\pi|)$.

Proof The Theorem follows from Lemmas 8, 9, 10 and 7, together with Theorem 1. The prescribed bound on $\mathcal{F}_{\mathcal{L}}(\varphi)$ can be proved by observing that the only semantic constructions which induce a significant increase in the "size" of the underlying majorizer are the ones from Lemmas 8 and 9. More formally, the proof goes by induction on π, where the only interesting inductive cases are the ones corresponding to rules $P_{\S}$, $P^1_!$, $P^2_!$ and C, since all the others follows from the symmetric monoidal structure of the underlying category (see [8]). The fact $P_{\S}$ can be justified follows from Lemmas 9 and 10; observe, in particular, that $\partial(\pi)$ increases by one whenever $P_{\S}$ is applied and, on the other hand, the underlying majorizer becomes α^+. Similarly for $P^1_!$ and $P^2_!$. C can be justified since *contr* is a morphism (Lemma 7) and morphisms compose. □

Binary lists can be represented as cut-free proofs with conclusion $\mathit{List}_{\mathsf{LAL}}$ by the usual, impredicative, encoding (see, for example, [12]). In other words, any binary list w can be put in correspondence to a proof π_w, following the so-called Church encoding. Let $\mathit{BtoLAL} : \mathcal{B} \to [\![\mathit{List}_{\mathsf{LAL}}]\!]^{\S}$ be the function mapping each binary list $s \in \mathcal{B}$ to (the denotation of) its encoding. There is a function LALtoB from $[\![\mathit{List}_{\mathsf{LAL}}]\!]^{\S}$ to $\mathcal{B}$ which maps (the denotation of) each cut-free proof representing $w \in \mathcal{B}$ to w: $\mathit{LALtoB}(a)$ simply returns the application of a to ε, s_0, s_1. Actually, LALtoB is a morphism from $[\![\mathit{List}_{\mathsf{LAL}}]\!]^{\mathcal{R}}$ to $\S\mathcal{B}_{\mathcal{L}}$.

Now, let π be a proof with conclusion $\vdash \Theta \mathit{List}_{\mathsf{LAL}} \multimap \Psi \mathit{List}_{\mathsf{LAL}}$ where $\Theta \in \{!, \S\}^j$ and $\Psi \in \{!, \S\}^k$. Any such proofs corresponds to a function f_π from $\mathcal{B}$ to itself, namely to $\mathit{LALtoB} \circ [\![\pi]\!]^{\S} \circ \mathit{BtoLAL}$. But f_π can be computed in polynomial time. Indeed, from the denotation $[\![\pi]\!]^{\S}$ we can build a morphism g from $[\![\Theta \mathit{List}_{\mathsf{LAL}}]\!]^{\mathcal{R}}$ to $\Psi\S\mathcal{B}_{\mathcal{L}}$ by composition with LALtoB. This morphism then induces an algorithm computing f_π: given $w \in \mathcal{B}$, first compute a realizer for the cut-free proof of $\Theta \mathit{List}_{\mathsf{LAL}}$ corresponding to w, then apply the result to a realizer for g. But any cut-free proof ρ of $\Theta \mathit{List}_{\mathsf{LAL}}$ has box depth $\partial(\rho) = j + 1$, which does not depend on the particular binary list w. By Theorem 3, we get:

Corollary 1 (Soundness) *Let π be an* LAL *proof with conclusion $\vdash \Theta \mathit{List}_{\mathsf{LAL}} \multimap \Psi \mathit{List}_{\mathsf{LAL}}$. where $\Theta \in \{!, \S\}^k$ and $\Psi \in \{!, \S\}^j$. Then f_π is computable in polynomial time.*

5 Conclusions

We have introduced a new model for LAL based on realizability. This allows us to give a simplified proof of soundness for the same logic. As any kind of semantics, our model can be used to identify certain axioms are not derivable in LAL (if it's not in the model it can't be in the syntax). Examples of such principles are the identification of the two modalities or commutation of the !-modality with tensor.

References

1. Amadio, R.M.: Max-plus quasi-interpretations. In: Proc. of the 7th International Conference on Typed Lambda Calculi and Applications. LNCS, vol. 2701, pp. 31–45. Springer, Berlin (2003)
2. Asperti, A., Roversi, L.: Intuitionistic light affine logic. ACM Trans. Comput. Log. **3**(1), 137–175 (2002)
3. Barendregt, H.: The Lambda Calculus: Its Syntax and Semantics. Studies in Logic and the Foundations of Mathematics. North Holland, Amsterdam (1984)
4. Bellantoni, S., Niggl, K.H., Schwichtenberg, H.: Higher type recursion, ramification and polynomial time. Ann. Pure Appl. Logic **104**, 17–30 (2000)
5. Cook, S., Urquhart, A.: Functional interpretations of feasible constructive arithmetic. Ann. Pure Appl. Logic **63**(2), 103–200 (1993)
6. Coppola, P., Martini, S.: Typing lambda terms in elementary logic with linear constraints. In: Proc. of the 6th International Conference on Typed Lambda Calculi and Applications. LNCS, vol. 2044, pp. 76–90. Springer, Berlin (2001)
7. Crossley, J., Mathai, G., Seely, R.: A logical calculus for polynomial-time realizability. J. Methods Logic Comput. Sci. **3**, 279–298 (1994)
8. Dal Lago, U., Hofmann, M.: Quantitative models and implicit complexity. In: Proc. Foundations of Software Technology and Theoretical Computer Science. LNCS, vol. 3821, pp. 189–200. Springer, Berlin (2005)
9. Dal Lago, U., Martini, S.: Phase semantics and decidability of elementary affine logic. Theor. Comput. Sci. **318**(3), 409–433 (2004)
10. Dal Lago, U., Martini, S.: The weak lambda calculus as a reasonable machine. Theor. Comput. Sci. **398**(1–3), 32–50 (2008)
11. Girard, J.-Y.: Light linear logic. Inf. Comput. **143**(2), 175–204 (1998)
12. Girard, J.-Y., Lafont, Y., Taylor, P.: Proof and Types. Cambridge University Press, Cambridge (1987)
13. Hofmann, M.: Linear types and non-size-increasing polynomial time computation. In: Proc. of the 14th IEEE Syposium on Logic in Computer Science, pp. 464–473 (1999)
14. Hofmann, M.: Safe recursion with higher types and BCK-algebra. Ann. Pure Appl. Logic **104**, 113–166 (2000)
15. Hofmann, M., Scott, P.: Realizability models for BLL-like languages. Theor. Comput. Sci. **318**(1–2), 121–137 (2004)
16. Kreisel, G.: Interpretation of analysis by means of constructive functions of finite types. In: Heyting, A. (ed.) Constructivity in Mathematics, pp. 101–128. North-Holland, Amsterdam (1959)
17. Lafont, Y.: Soft linear logic and polynomial time. Theor. Comput. Sci. **318**, 163–180 (2004)
18. Murawski, A.S., Ong, C.-H.L.: Discreet games, light affine logic and ptime computation. In: Proc. of 14th International Workshop on Computer Science Logic. LNCS, vol. 1862, pp. 427–441. Springer, Berlin (2000)
19. Roversi, L.: A P-time completeness proof for light logics. In: Proc. of 13th International Workshop on Computer Science Logic. LNCS, vol. 1683, pp. 469–483. Springer, Berlin (1999)
20. van Emde Boas, P.: Machine models and simulation. In: Handbook of Theoretical Computer Science. Algorithms and Complexity, vol. A, pp. 1–66. MIT Press, Cambridge (1990)
21. Wadsworth, C.: Some unusual λ-calculus numeral systems. In: Seldin, J.P., Hindley, J.R. (eds.) To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism. Academic Press, San Diego (1980)