

# A Logical Account of PSPACE

Marco Gaboardi

Simona Ronchi Della Rocca

Dipartimento di Informatica, Università degli Studi di  
Torino - Corso Svizzera 185, 10149 Torino, Italy  
gaboardi,ronchi@di.unito.it

Jean-Yves Marion

Nancy-University, ENSMN-INPL, Loria  
B.P. 239, 54506 Vandoeuvre-lès-Nancy, France  
Jean-Yves.Marion@loria.fr

## Abstract

We propose a characterization of PSPACE by means of a type assignment for an extension of lambda calculus with a conditional construction. The type assignment STA<sub>B</sub> is an extension of STA, a type assignment for lambda-calculus inspired by Lafont's Soft Linear Logic.

We extend STA by means of a ground type and terms for booleans. The key point is that the elimination rule for booleans is managed in an additive way. Thus, we are able to program polynomial time Alternating Turing Machines. Conversely, we introduce a call-by-name evaluation machine in order to compute programs in polynomial space. As far as we know, this is the first characterization of PSPACE which is based on lambda calculus and light logics.

**Categories and Subject Descriptors** F.3.3 [*Logics and meanings of programs*]: Studies of program constructs—type structure; F.4.1 [*Mathematical logic and formal languages*]: Mathematical logic—lambda calculus and related systems, proof theory

**General Terms** Languages, Theory, Design

**Keywords** Implicit Computational Complexity, Polynomial Space, Linear Logic, Type Assignment

## 1. Introduction

The argument of this paper fits in the so called Implicit Computational Complexity topic, in particular on the design of programming languages with bounded computational complexity. We want to use a ML-like approach, so having a  $\lambda$ -calculus like language, and a type assignment system for it, where the types guarantee, besides the functional correctness, also complexity properties. So types can be used in a static way in order to check the correct behaviour of the programs, also with respect to the resource usage. If the considered resource is the time, the natural choice is to use as types formulae of the light logics, which characterize some classes of time complexity. Light Linear Logic (LLL) of Girard (Girard 1998), and Soft Linear Logic (SLL) of Lafont (Lafont 2004) characterize polynomial time, while Elementary Linear Logic (EAL) characterizes elementary time. The characterization is based on the fact that cut-elimination in these logics is performed in a number of steps which depends in a polynomial or elementary way from

the initial size of the proof (while the degree of the proof, i.e. the nesting of exponential rules, is fixed). Moreover all these logics are also complete with respect to the related complexity class.

The good properties of such logics have been fruitfully used in order to design type assignment systems for  $\lambda$ -calculus which are correct and complete with respect to the polynomial or elementary complexity bound. Namely every well typed term  $\beta$ -reduces to normal form in a number of steps which depends in a polynomial or elementary way from its size, and moreover all functions with the corresponding complexity are representable by a well typed term. Examples of polynomial type assignment systems are in (Baillot and Terui 2004) and (Gaboardi and Ronchi Della Rocca 2007), based respectively on LAL (an affine variant of LLL designed by Asperti and Roversi (Asperti and Roversi 2002)) and on SLL, and an example of an elementary type assignment system is in (Coppola et al. 2005).

Here we use the same approach for studying space complexity, in particular we build a type system for a  $\lambda$ -calculus like language, in such a way that well typed terms are correct and complete for PSPACE. More precisely, every well typed program reduces in polynomial space and all decision functions computable in polynomial space are computed by well typed programs. There is no previous logical characterization of PSPACE from which we can start. But we will use the fact that polynomial space computations coincide with polynomial time alternating Turing machine computations (APTIME) (Savitch 1970; Chandra et al. 1981). In particular

$$\text{PSPACE} = \text{NPSPACE} = \text{APTIME}$$

So we will start from the type assignment STA for  $\lambda$ -calculus presented in (Gaboardi and Ronchi Della Rocca 2007), which is based on SLL, in the sense that in STA both types are a proper subset of SLL formulae, and type assignment derivations correspond, through the Curry-Howard isomorphism, to a proper subset of SLL derivations. STA is correct and complete (in the sense said before) with respect to polynomial time computations. Then we design a type assignment system (STA<sub>B</sub>), where the types are STA types plus a type  $\mathbf{B}$  for booleans, and the language  $\Lambda_{\mathbf{B}}$  is an extension of  $\lambda$ -calculus with two boolean constants and a conditional constructor. The elimination rule for conditional is the following:

$$\frac{\Gamma \vdash M : \mathbf{B} \quad \Gamma \vdash N_0 : A \quad \Gamma \vdash N_1 : A}{\Gamma \vdash \text{if } M \text{ then } N_0 \text{ else } N_1 : A} (\mathbf{BE})$$

In the if-rule above, contexts are managed in an additive way, that is with free contractions. From a computational point of view, this intuitively means that a computation can repeatedly fork into subcomputations and the result is obtain by a backward computation from all subcomputation results.

While the time complexity result for STA is not related to a particular evaluation strategy, here, for characterizing space

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

POPL'08, January 7–12, 2008, San Francisco, California, USA.  
Copyright © 2008 ACM 978-1-59593-689-9/08/0001...\$5.00

complexity, the evaluation should be done carefully. Indeed, a call-by-value evaluation can use exponential size. So we define a call-by-name evaluation machine, inspired by Krivine's machine (Krivine 2007) for  $\lambda$ -calculus, where substitutions are made only on head variables. This machine is equipped with a memory device thanks to which the space used is easily determined, as the dimension of the maximal machine configuration. Then we prove that, if the machine takes a program (i.e. a closed term well typed with a ground type) as input, then each configuration is bounded in a polynomial way in the size of the input. So every program is evaluated by the machine in polynomial space. Conversely, we encode every polynomial time alternating Turing machine by a term of  $STA_B$ . The simulation relies on a higher order representation of a parameter substitution recurrence schema which was used in (Leivant and Marion 1994).

$STA_B$  is the first characterization of PSPACE through a type assignment system. A proposal for a similar characterization has been made by Terui (Terui 2000), but the work has never been completed.

There are previous implicit characterizations of polynomial space computations. The characterizations in (Leivant and Marion 1994, 1997) and (Oitavem 2001) are based on ramified recursions over binary words. In finite model theory, PSPACE is captured by first order queries with a partial fixed point operator (Vardi 1982; Abiteboul and Vianu 1989). The reader may consult the recent book (Grädel et al. 2007). Finally there are some algebraic characterizations like the one (Goerdt 1992) or (Jones 2001) but which are, in essence, over finite domains.

An example of a characterization of a complexity space class through a light logic is in (Schöpp 2007) where a logical system characterizing logarithmic space computations is defined, the Stratified Bounded Affine Logic (SBAL). Logarithmic space soundness is proved by considering only proofs of certain sequents to represent the functions computable in logarithmic space. Our characterization is strongly based on the additive rule ( $BE$ ). A similar tool has been used by Maurel's Non Deterministic Light Logic (nLLL) (Maurel 2003) in order to characterize non deterministic polynomial time. More precisely nLLL introduces an explicit sum rule to deal with non deterministic computation. A different approach but also based on linear logic is to characterize circuit complexity classes by means of Booleans proof nets (Terui 2004; Mogbil and Rahli 2007) but this does not relate to the task of designing programming language with an intrinsically polynomial computational bound.

**Outline of the paper** In Section 2 the system  $STA_B$  is introduced and the proofs of subject reduction and strong normalization properties are given. In Section 3 the operational semantics of  $STA_B$  program is defined, through an abstract evaluation machine. In Section 4 we show that  $STA_B$  programs can be executed in polynomial space. In Section 5 the completeness for PSPACE is proved. In Section 6 some complementary argument are considered. The Appendix contains the most technical proofs.

## 2. Soft Type Assignment system with Booleans

In this section the type assignment  $STA_B$  is presented, and its properties are proved.  $STA_B$  is an extension of the type system STA for  $\lambda$ -calculus introduced in (Gaboardi and Ronchi Della Rocca 2007), which assigns to terms of the  $\lambda$ -calculus a proper subset of formulae of Lafont's Soft Linear Logic (Lafont 2004). STA has been proved to be correct and complete for polynomial time computations.

$STA_B$  is obtained from STA by extending both the calculus and

the set of types. The calculus is the  $\lambda$ -calculus extended by boolean constants 0, 1 and an `if` constructor, types are the types of STA plus a constant type  $B$  for booleans.

### Definition 1.

1. The set  $\Lambda_B$  of terms is defined by the following grammar:

$$M ::= x \mid 0 \mid 1 \mid \lambda x.M \mid MM \mid \text{if } M \text{ then } M \text{ else } M$$

where  $x$  ranges over a countable set of variables and  $B = \{0, 1\}$  is the set of booleans.

2. The set  $T$  of  $B$  types is defined as follows:

$$\begin{aligned} A &::= B \mid \alpha \mid \sigma \multimap A \mid \forall \alpha.A \quad (\text{Linear Types}) \\ \sigma &::= A \mid !\sigma \end{aligned}$$

where  $\alpha$  ranges over a countable set of type variables and  $B$  is the only ground type.

3. A context is a set of assumptions of the shape  $x : \sigma$ , where all variables are different. We use  $\Gamma, \Delta$  to denote contexts.  $\text{dom}(\Gamma) = \{x \mid \exists x : \sigma \in \Gamma\}$  and  $\Gamma \# \Delta$  means  $\text{dom}(\Gamma) \cap \text{dom}(\Delta) = \emptyset$ .

4.  $STA_B$  proves judgments of the shape  $\Gamma \vdash M : \sigma$  where  $\Gamma$  is a context,  $M$  is a term, and  $\sigma$  is a  $B$  type. The rules are given in Table 1.

5. Derivations are denoted by  $\nabla, \Diamond, \Box$ .  $(\nabla) \Gamma \vdash M : \sigma$  denotes a derivation  $\nabla$  with conclusion  $\Gamma \vdash M : \sigma$ . We let  $\vdash M : \sigma$  abbreviate  $\emptyset \vdash M : \sigma$ .

Note that while all rules in STA have a multiplicative treatment of contexts, the rule ( $BE$ ) of  $STA_B$  is additive and so contraction is free.

**Notation 1.** Terms are ranged over by  $M, N, V, P$ . As usual terms are considered up to  $\alpha$ -equivalence, namely a bound variable can be renamed provided no free variable is captured. Moreover  $M[N/x]$  denotes the capture-free substitution of all free occurrences of  $x$  in  $M$  by  $N$ .  $\text{FV}(M)$  denotes the set of free variables of  $M$ ,  $n_o(x, M)$  the number of free occurrences of the variable  $x$  in  $M$ .

Type variables are ranged over by  $\alpha, \beta$ , linear types by  $A, B, C$ , and types by  $\sigma, \tau, \mu$ .  $\equiv$  denotes the syntactical equality both for types and terms (modulo renaming of bound variables). As usual  $\multimap$  associates to the right and has precedence on  $\forall$ , while  $!$  has precedence on everything else.  $\sigma[A/\alpha]$  denotes the capture free substitution in  $\sigma$  of all occurrences of the type variable  $\alpha$  by the linear type  $A$ .  $\text{FTV}(\Gamma)$  denotes the set of free type variables occurring in the assumptions of the context  $\Gamma$ .

We stress that each type is of the shape  $!^n \forall \vec{\alpha}. A$  where  $\forall \vec{\alpha}. A$  is an abbreviation for  $\forall \alpha_1 \dots \forall \alpha_m. A$ , and  $!^n \sigma$  is an abbreviation for  $! \dots ! \sigma$   $n$ -times, where  $n, m \geq 0$ . In particular  $!^0 \sigma \equiv \sigma$ .

We have the following standard properties for a natural deduction system.

### Lemma 1 (Free variable lemma).

1.  $\Gamma \vdash M : \sigma$  implies  $\text{FV}(M) \subseteq \text{dom}(\Gamma)$ .
2.  $\Gamma \vdash M : \sigma, \Delta \subseteq \Gamma$  and  $\text{FV}(M) \subseteq \text{dom}(\Delta)$  imply  $\Delta \vdash M : \sigma$ .
3.  $\Gamma \vdash M : \sigma, \Gamma \subseteq \Delta$  implies  $\Delta \vdash M : \sigma$ .

The functional behaviour of  $\Lambda_B$  is described in the next definition.

**Definition 2.** The reduction relation  $\rightarrow_{\beta\delta} \subseteq \Lambda_B \times \Lambda_B$  is the contextual closure of the following rules:

$$(\lambda x.M)N \rightarrow_{\beta} M[N/x]$$

$$\text{if } 0 \text{ then } M \text{ else } N \rightarrow_{\delta} M$$

$$\text{if } 1 \text{ then } M \text{ else } N \rightarrow_{\delta} N$$

$\frac{}{x : A \vdash x : A} (Ax)$	$\frac{}{\vdash 0 : \mathbf{B}} (\mathbf{B}_0 I)$	$\frac{}{\vdash 1 : \mathbf{B}} (\mathbf{B}_1 I)$
$\frac{\Gamma \vdash M : \sigma}{\Gamma, x : A \vdash M : \sigma} (w)$	$\frac{\Gamma, x : \sigma \vdash M : A}{\Gamma \vdash \lambda x. M : \sigma \multimap A} (\multimap I)$	
$\frac{\Gamma \vdash M : \sigma \multimap A \quad \Delta \vdash N : \sigma \quad \Gamma \# \Delta}{\Gamma, \Delta \vdash MN : A} (\multimap E)$		
$\frac{\Gamma, x_1 : \sigma, \dots, x_n : \sigma \vdash M : \mu}{\Gamma, x : !\sigma \vdash M[x/x_1, \dots, x/x_n] : \mu} (m)$	$\frac{\Gamma \vdash M : \sigma}{! \Gamma \vdash M : \sigma} (sp)$	
$\frac{\Gamma \vdash M : A \quad \alpha \notin FTV(\Gamma)}{\Gamma \vdash M : \forall \alpha. A} (\forall I)$	$\frac{\Gamma \vdash M : \forall \alpha. B}{\Gamma \vdash M : B[A/\alpha]} (\forall E)$	
$\frac{\Gamma \vdash M : \mathbf{B} \quad \Gamma \vdash N_0 : A \quad \Gamma \vdash N_1 : A}{\Gamma \vdash \text{if } M \text{ then } N_0 \text{ else } N_1 : A} (\mathbf{BE})$		

**Table 1.** The Soft Type Assignment system with Booleans

$\rightarrow_{\beta\delta}^*$  denotes the reflexive and transitive closure of  $\rightarrow_{\beta\delta}$ .

In what follows, we will need to talk about proofs modulo commutations of rules.

**Definition 3.** Let  $\Pi$  and  $\Pi'$  be two derivations in  $\text{STA}_{\mathbf{B}}$ , proving the same conclusion:  $\Pi \rightsquigarrow \Pi'$  denotes the fact that  $\Pi'$  is obtained from  $\Pi$  by commuting or deleting some rules.

The Generation Lemma connects the shape of a term with its possible typings, and will be useful in the sequel.

### Lemma 2 (Generation lemma).

1.  $(\nabla) \Gamma \vdash \lambda x. M : \forall \alpha. A$  implies there is  $\nabla'$  such that  $\nabla \rightsquigarrow \nabla'$  where the last rule of  $\nabla'$  is  $(\forall I)$ .
2.  $(\nabla) \Gamma \vdash \lambda x. M : \sigma \multimap A$  implies there is  $\nabla'$  such that  $\nabla \rightsquigarrow \nabla'$ , whose last rule is  $(\multimap I)$ .
3.  $(\nabla) \Gamma \vdash M : !\sigma$  implies there is  $\nabla'$  such that  $\nabla \rightsquigarrow \nabla'$  where  $\nabla'$  consists of a subderivation, ending with the rule  $(sp)$  proving  $! \Gamma \vdash M : !\sigma$ , followed by a (maybe empty) sequence of rules  $(w)$  and/or  $(m)$ .
4.  $(\nabla) ! \Gamma \vdash M : !\sigma$  implies there is  $\nabla'$  such that  $\nabla \rightsquigarrow \nabla'$ , whose last rule is  $(sp)$ .

The substitution lemma will be the key lemma to show that  $\text{STA}_{\mathbf{B}}$  enjoys the subject reduction property.

**Lemma 3 (Substitution lemma).** Let  $(\nabla) \Gamma, x : \mu \vdash M : \sigma$  and  $(\Diamond) \Delta \vdash N : \mu$  such that  $\Gamma \# \Delta$ . Then there exists  $(\square) \Gamma, \Delta \vdash M[N/x] : \sigma$ .

*Proof.* Since the proof is quite involved, we postpone it to Appendix A.1.  $\square$

We can finally prove the main property of this section.

**Lemma 4 (Subject Reduction).** Let  $\Gamma \vdash M : \sigma$  and  $M \rightarrow_{\beta\delta} N$ . Then  $\Gamma \vdash N : \sigma$ .

*Proof.* The case of a  $\rightarrow_{\delta}$  reduction is easy, the one of  $\rightarrow_{\beta}$  reduction follows by Lemma 3.  $\square$

By strong normalization of STA we have the following.

**Lemma 5 (Strong Normalization).** Let  $\Gamma \vdash M : \sigma$  then  $M$  is strongly normalizing with respect to the reduction relation  $\rightarrow_{\beta\delta}$ .

Nevertheless due to the additive rule  $(\mathbf{BE})$ ,  $\text{STA}_{\mathbf{B}}$  is no more correct for polynomial time. In fact, terms with an exponential number of reductions can be typed by derivations with a priori fixed degree, i.e. the nesting of exponential rules.

**Example 1.** Consider for  $n \in \mathbb{N}$  terms  $M_n$  of the shape:

$$(\lambda f. \lambda z. f^n(z))(\lambda x. \text{if } x \text{ then } x \text{ else } x)0$$

It is easy to verify that for each  $M_n$  there exist reduction sequences of length exponential in  $n$ .

### 3. Structural Operational Semantics

In this section the operational semantics of terms of  $\Lambda_B$  will be given, through an evaluation machine, defined in SOS style, performing the evaluation according to the leftmost outermost strategy. The machine, if restricted to  $\lambda$ -calculus, is quite similar to the Krivine machine (Krivine 2007), since  $\beta$ -reduction is not an elementary step, but the substitution of a term to a variable is performed one occurrence at a time. The evaluation machine is related to the type assignment system  $\text{STA}_{\mathbf{B}}$  in the sense that, when it starts on an empty memory, all the programs (closed terms of ground type) can be evaluated.

**Definition 4.** The set  $\mathcal{P}$  of  $\text{STA}_{\mathbf{B}}$  programs is the set of closed terms typable by the ground type. i.e.  $\mathcal{P} = \{M \mid \vdash M : \mathbf{B}\}$ .

It is easy to check that a  $\text{STA}_{\mathbf{B}}$  term is of the following shape:

$$M \equiv \lambda x_1 \dots x_n. \zeta V_1 \dots V_m$$

where  $\zeta$  is either a boolean  $b$ , a variable  $x$ , a redex  $(\lambda x. N)P$ , or a subterm of the shape  $\text{if } P \text{ then } N_0 \text{ else } N_1$ .

In particular, if a term is a program, then its shape is as before, but with the condition that the number  $n$  of initial abstractions is equal to 0. Moreover if  $\zeta$  is a boolean  $b$  then the number  $m$  of arguments is equal to 0. We will use this characterization of programs to design the evaluation machine  $K_B^C$ .

$K_B^C$  uses two memory devices, the m-context and the  $\mathbf{B}$ -context, that memorize respectively the assignments to variables and the control.

### Definition 5.

1. An m-context  $\mathcal{A}$  is a sequence of variable assignments of the shape  $x_i := M_i$  where all variables  $x_i$  are distinct. The set of m-contexts is denoted by  $\text{Ctx}_m$ .
2. The cardinality of an m-context  $\mathcal{A}$ , denoted by  $\#(\mathcal{A})$ , is the number of variable assignments in  $\mathcal{A}$ .
3. The size of an m-context  $\mathcal{A}$ , denoted by  $|\mathcal{A}|$ , is the sum of the size of each variable assignment in  $\mathcal{A}$ , where a variable assignment  $x := M$  has size  $|M| + 1$ , and  $|M|$  is the number of symbols of  $M$ .
4. Let  $\circ$  be a distinguished symbol. The set  $\text{Ctx}_{\mathbf{B}}$  of  $\mathbf{B}$ -contexts is defined by the following grammar:

$$C[\circ] ::= \circ \mid (\text{if } C[\circ] \text{ then } M \text{ else } N) V_1 \dots V_n$$

5. The size of a  $\mathbf{B}$ -context  $C[\circ]$  denoted  $|C[\circ]|$  is the size of the term obtained by replacing the symbol  $\circ$  by a variable. The cardinality of a  $\mathbf{B}$ -context  $C[\circ]$ , denoted by  $\#(C[\circ])$ , is the number of nested  $\mathbf{B}$ -contexts in it.

**Notation 2.**  $\varepsilon$  denotes the empty m-context and  $\mathcal{A}_1 @ \mathcal{A}_2$  denotes the concatenation of the m-contexts  $\mathcal{A}_1$  and  $\mathcal{A}_2$ .  $[x := M] \in \mathcal{A}$  denotes the fact that  $x := M$  is in the m-context  $\mathcal{A}$ .  $\text{FV}(\mathcal{A}) = \bigcup_{[x := M] \in \mathcal{A}} \text{FV}(M)$ .

As usual  $C[M]$  denotes the term obtained by filling the hole  $[\circ]$  in  $C[\circ]$  by  $M$ . In general we omit the hole  $[\circ]$  and we range over  $\mathbf{B}$ -contexts by  $C$ .  $\text{FV}(C) = \text{FV}(C[M])$  for every closed term  $M$ .

$\frac{}{\mathcal{C}, \mathcal{A} \models b \Downarrow b} (Ax)$
$\frac{\mathcal{C}, \mathcal{A} @ \{x' := N\} \models M[x'/x]V_1 \dots V_m \Downarrow b^*}{\mathcal{C}, \mathcal{A} \models (\lambda x.M)NV_1 \dots V_m \Downarrow b} (\beta)$
$\frac{\{x := N\} \in \mathcal{A} \quad \mathcal{C}, \mathcal{A} \models NV_1 \dots V_m \Downarrow b}{\mathcal{C}, \mathcal{A} \models xV_1 \dots V_m \Downarrow b} (h)$
$\frac{\mathcal{C}[(\text{if } [o] \text{ then } N_0 \text{ else } N_1)V_1 \dots V_m], \mathcal{A} \models M \Downarrow 0 \quad \mathcal{C}, \mathcal{A} \models N_0V_1 \dots V_m \Downarrow b}{\mathcal{C}, \mathcal{A} \models (\text{if } M \text{ then } N_0 \text{ else } N_1)V_1 \dots V_m \Downarrow b} (\text{if 0})$
$\frac{\mathcal{C}[(\text{if } [o] \text{ then } N_0 \text{ else } N_1)V_1 \dots V_m], \mathcal{A} \models M \Downarrow 1 \quad \mathcal{C}, \mathcal{A} \models N_1V_1 \dots V_m \Downarrow b}{\mathcal{C}, \mathcal{A} \models (\text{if } M \text{ then } N_0 \text{ else } N_1)V_1 \dots V_m \Downarrow b} (\text{if 1})$
(*) $x'$ is a fresh variable.

**Table 2.** The Abstract Machine  $K_B^C$

Note that variable assignments in m-contexts are ordered; this fact allows us to define the following closure operation.

**Definition 6.** Let  $\mathcal{A} = [x_1 := N_1, \dots, x_n := N_n]$  be an m-context. Then  $(\ )^A : \Lambda_B \rightarrow \Lambda_B$  is the map associating to each term  $M$  the term  $M[N_n/x_n][N_{n-1}/x_{n-1}] \dots [N_1/x_1]$ .

$K_B^C$  is defined in Table 2. Some comments are in order. The rules will be commented bottom-up, which is the natural direction of the evaluation flow.

Rule  $(Ax)$  is obvious. Rule  $(\beta)$  applies when the head of the subject is a  $\beta$ -redex: then the association between the bound variable and the argument is remembered in the m-context and the body of the term in functional position is evaluated. Note that an  $\alpha$ -rule is always performed. Rule  $(h)$  replaces the head occurrence of the head variable by the term associated to it in the m-context. Rules  $(\text{if 0})$  and  $(\text{if 1})$  perform the  $\delta$  reductions. Here the evaluation naturally erases part of the subject, but the erased information is stored in the B-context. In order to state formally the behaviour of the machine  $K_B^C$  we need a further definition.

#### Definition 7.

1. The evaluation relation  $\Downarrow \subseteq \text{Ctx}_B \times \text{Ctx}_m \times \Lambda_B \times \mathcal{B}$  is the effective relation inductively defined by the rules of  $K_B^C$ . If  $M$  is a program, and if there is a boolean  $b$  such that  $[o], \varepsilon \models M \Downarrow b$  then we say that  $M$  evaluates, and we write  $M \Downarrow \models M \Downarrow b$  is a short for  $[o], \varepsilon \models M \Downarrow b$ .
2. Derivation trees are called computations in the abstract machine and are denoted by  $\Pi, \Sigma$ .  $\Pi :: C, \mathcal{A} \models M \Downarrow b$  denotes a computation with conclusion  $C, \mathcal{A} \models M \Downarrow b$ .
3. Given a computation  $\Pi$  each node of  $\Pi$ , which is of the shape  $C, \mathcal{A} \models M \Downarrow b$  is a configuration.  $C, \mathcal{A} \models M \Downarrow b \in \Pi$  denotes that  $C, \mathcal{A} \models M \Downarrow b$  is a configuration in the computation  $\Pi$ . Configurations are ranged over by  $\phi, \psi$  and  $\phi \triangleright C, \mathcal{A} \models M \Downarrow b$  means that  $\phi$  is the configuration  $C, \mathcal{A} \models M \Downarrow b$ . The conclusion of the derivation tree is called the initial configuration.
4. Given a computation  $\Pi$ , the path to reach a configuration  $\phi$  denoted  $\text{path}_\Pi(\phi)$  is the sequence of configurations between the conclusion of  $\Pi$  and  $\phi$ . In general we will write  $\text{path}(\phi)$  when  $\Pi$  is clear from the context.

We are interested in the behaviour of the machine when applied to programs. By an analysis of the rules of Table 2, and from the previous comments, it is easy to verify the following.

#### Lemma 6.

1. Let  $M \in \mathcal{P}$ ,  $\Pi :: M \Downarrow b$  and  $C, \mathcal{A} \models N \Downarrow b' \in \Pi$ . Then  $(C[N])^A, (N)^A \in \mathcal{P}$ .
2. Let  $M \in \mathcal{P}$  and  $\Pi :: M \Downarrow b$ . For each  $C, \mathcal{A} \models N \Downarrow b' \in \Pi$ 

$$M \xrightarrow[\beta\delta]^* (C[N])^A \xrightarrow[\beta\delta]^* b$$

Note that, in the previous lemma, the m-context and the B-context are essential in proving the desired properties. In fact the B-context recovers the part of the term necessary to complete  $\delta$ -reductions, while the m-context completes  $\beta$ -reductions that have been performed only partially by the machine.

**Example 2.** In Table 5 we present an example of  $K_B^C$  computation on the same term of Example 1.

Note that by Definition 7.1 a term  $M$  evaluates only if it is a program and there exists  $b$  such that  $\models M \Downarrow b$ . We stress here, that the machine  $K_B^C$  is complete with respect to programs, in the sense that all the programs can be evaluated.

#### Theorem 1.

$$M \in \mathcal{P} \text{ implies } M \Downarrow$$

*Proof.* By induction on the reduction to normal form using Lemma 5.  $\square$

#### 3.1 A small step version of $K_B^C$

In Table 3 we depict a small step version of the machine  $K_B^C$ . The rules are similar to the rules in Table 2 but the use of a garbage collector procedure described in Table 4 which is needed in order to maintain the desired complexity property. In fact the small step machine can be easily shown equivalent to the big step one.

The small step machine explicits the evaluation order clarifying that every configuration depends uniquely on the previous one (thanks to the B-context). So the space necessary to evaluate a program turns out to be the maximum space used by one of its configurations.

Nevertheless, the big step machine has the advantage of being more abstract and this make it easy to prove the complexity properties. In fact, the garbage collector procedure make more difficult the proofs of such properties for the small step machine. For this reason in what follows we will work on the big step machine.

$\overline{\langle \mathcal{C}, \mathcal{A} \succ (\lambda x.M)Nv_1 \cdots v_m \rangle \mapsto \langle \mathcal{C}, \mathcal{A} @ [x' := N] \succ M[x'/x]v_1 \cdots v_m \rangle} \quad (\beta)$
$\overline{\langle \mathcal{C}, \mathcal{A}_1 @ [x := N] @ \mathcal{A}_2 \succ xv_1 \cdots v_m \rangle \mapsto \langle \mathcal{C}, \mathcal{A}_1 @ [x := N] @ \mathcal{A}_2 \succ Nv_1 \cdots v_m \rangle} \quad (h_0)$
$\overline{\langle \mathcal{C}, \mathcal{A} \succ (\text{if } M \text{ then } N_0 \text{ else } N_1) v_1 \cdots v_m \rangle \mapsto \langle \mathcal{C}[(\text{if } [o] \text{ then } N_0 \text{ else } N_1) v_1 \cdots v_n], \mathcal{A} \succ M \rangle} \quad (\text{if})$
$\overline{\mathcal{A}' = \text{clear}(\mathcal{C}, \mathcal{A}, N_0 v_1 \cdots v_n)} \quad (r_0)$
$\overline{\langle \mathcal{C}[(\text{if } [o] \text{ then } N_0 \text{ else } N_1) v_1 \cdots v_n], \mathcal{A} \succ 0 \rangle \mapsto \langle \mathcal{C}, \mathcal{A}' \succ N_0 v_1 \cdots v_n \rangle} \quad (r_0)$
$\overline{\mathcal{A}' = \text{clear}(\mathcal{C}, \mathcal{A}, N_1 v_1 \cdots v_n)} \quad (r_1)$
$\overline{\langle \mathcal{C}[(\text{if } [o] \text{ then } N_0 \text{ else } N_1) v_1 \cdots v_n], \mathcal{A} \succ 1 \rangle \mapsto \langle \mathcal{C}, \mathcal{A}' \succ N_1 v_1 \cdots v_n \rangle} \quad (r_1)$

**Table 3.** The small step machine  $k_B^C$

$\overline{\text{clear}(\mathcal{C}, \varepsilon, M) = \varepsilon}$
$\overline{\text{clear}(\mathcal{C}, \mathcal{A}, M) = \mathcal{A}' \quad x \in FV(\mathcal{C}) \cup FV(M) \cup FV(\mathcal{A})}$
$\overline{\text{clear}(\mathcal{C}, [x := N] @ \mathcal{A}, M) = [x := N] @ \mathcal{A}'}$
$\overline{\text{clear}(\mathcal{C}, \mathcal{A}, M) = \mathcal{A}' \quad x \notin FV(\mathcal{C}) \cup FV(M) \cup FV(\mathcal{A})}$
$\overline{\text{clear}(\mathcal{C}, [x := N] @ \mathcal{A}, M) = \mathcal{A}'}$

**Table 4.** The garbage collector procedure.

### 3.2 Space Measures

We can now define the space effectively used to evaluate a term. The remarks in the previous section allows us to consider the following definition.

**Definition 8.** Let  $\phi \triangleright \mathcal{C}, \mathcal{A} \models M \Downarrow b$  be a configuration then its size denoted  $|\phi|$  is the sum  $|\mathcal{C}| + |\mathcal{A}| + |M|$ . Let  $\Pi :: \mathcal{C}, \mathcal{A} \models M \Downarrow b$  be a computation, then its space occupation denoted  $\text{space}(\Pi)$  is the maximal size of a configuration in  $\Pi$ .

In particular since there is a one-to-one correspondence between a program  $M$  and its computation  $\Pi :: [o], \varepsilon \models M \Downarrow b$ , we will usually write  $\text{space}(M)$  in place of  $\text{space}(\Pi)$ . In order to have polynomial space soundness we will show that for each  $M \in \mathcal{P}$  there exists a polynomial  $P(X)$  such that  $\text{space}(M) \leq P(|M|)$ . The result will be proved in next section.

**Example 3.** By returning to the computation of Example 2 it is worth noting that to pass from the configuration  $\phi$  to the configuration  $\psi$  all necessary informations are already present in the configuration  $\phi$  itself. We can view such a step as a  $\rightarrow_\delta$  step  $(\text{if } 0 \text{ then } x_1 \text{ else } x_1)^{\mathcal{A}_3} \rightarrow_\delta (x_1)^{\mathcal{A}_3}$  noting that  $(x_1)^{\mathcal{A}_3} \equiv (x_1)^{\mathcal{A}_2}$ . In fact this can be generalized, so in this sense we don't need neither mechanism for backtracking nor the memorization of parts of the computation tree.

In what follows we will introduce some relations between the size of the contexts and the behaviour of the machine, which will be useful later.

**Definition 9.** Let  $\Pi$  be a computation and  $\phi \in \Pi$  a configuration.

- $\#_\beta(\phi)$  denotes the number of applications of the  $(\beta)$  rule in  $\text{path}(\phi)$ .
- $\#_h(\phi)$  denotes the number of applications of the  $(h)$  rule in  $\text{path}(\phi)$ .
- $\#_{\text{if}}(\phi)$  denotes the number of applications of  $(\text{if } 0)$  and  $(\text{if } 1)$  rules in  $\text{path}(\phi)$ .

The cardinality of the contexts is a measure of the number of some rules performed by the machine.

**Lemma 7.** Let  $\Pi :: \models M \Downarrow b$ . Then for each configuration  $\phi \triangleright \mathcal{C}_i, \mathcal{A}_i \models P_i \Downarrow b' \in \Pi$ :

1.  $\#(\mathcal{A}_i) = \#_\beta(\phi)$
2.  $\#(\mathcal{C}_i) = \#_{\text{if}}(\phi)$

The following is an important property of the machine  $K_B^C$ .

**Property 1.** Let  $M \in \mathcal{P}$  and  $\Pi :: \models M \Downarrow b$  then for each  $\phi \triangleright \mathcal{C}, \mathcal{A} \models P \Downarrow b' \in \Pi$  if  $[x_j := N_j] \in \mathcal{A}_i$  then  $N_j$  is an instance of a subterm of  $M$ .

*Proof.* The property is proven by contradiction. Take the configuration  $\phi$  with minimal path from it to the root of  $\Pi$ , such that in its m-context  $\mathcal{A}_\phi$  there is  $x_j := N_j$ , where  $N_j$  is not an instance of a subterm of  $M$ . Let  $p$  be the length of this path. Since the only rule that makes the m-context grow is a  $(\beta)$  rule we are in a situation like the following:

$$\frac{\mathcal{C}, \mathcal{A}' @ [x_j := N_j] \models P[x_j/x]v_1 \cdots v_n \Downarrow b}{\mathcal{C}, \mathcal{A}' \models (\lambda x.P)N_jv_1 \cdots v_n \Downarrow b}$$

If  $N_j$  is not an instance of a subterm of  $M$  it has been obtained by a substitution. Substitutions can be made only through applications

of rule  $(h)$  replacing the head variable. Hence by the shape of  $(\lambda x.P)N_jV_1 \cdots V_n$ , the only possible situation is that there exists an application of rule  $(h)$  as:

$$\frac{[y := M'] \in A' \quad C, A' \models M'V_1 \cdots V_n \Downarrow b}{C, A' \models yV_1 \cdots V_n \Downarrow b}$$

with  $N_j$  an instance of a subterm of  $M'$ . But this implies  $M'$  is not an instance of a subterm of  $M$  and it has been introduced by a rule of a path of length less than  $p$ , contradicting the hypothesis.  $\square$

The next lemma gives upper bounds to the size of the m-context, of the  $B$ -context and of the subject of a configuration.

**Lemma 8.** *Let  $M \in \mathcal{P}$  and  $\Pi ::= M \Downarrow b$  then for each configuration  $\phi \triangleright C, A \models P \Downarrow b' \in \Pi$ :*

1.  $|A| \leq \#_\beta(\phi)(|M| + 1)$
2.  $|P| \leq (\#_h(\phi) + 1)|M|$
3.  $|C| \leq \#_{if}(\phi)(\max\{|N| \mid \psi \triangleright C', A' \models N \Downarrow b'' \in \Pi\})$

*Proof.* 1. By inspection of the rules of Table 2 it is easy to verify that m-contexts can grow only by applications of the  $(\beta)$  rule. So the conclusion follows by Lemma 7 and Property 1.  
2. By inspection of the rules of Table 2 it is easy to verify that the subject can grow only by substitutions through applications of the  $(h)$  rule. So the conclusion follows by Property 1.  
3. By inspection of the rules of Table 2 it is easy to verify that  $B$ -contexts can grow only by applications of  $(if\ 0)$  and  $(if\ 1)$  rules. So the conclusion follows directly by Lemma 7.  $\square$

## 4. PSPACE Soundness

In this section we will show that  $STA_B$  is correct for polynomial space computation, namely each program typable through a derivation with degree  $d$  can be executed on the machine  $K_B^C$  in space polynomial in its size, where the maximum exponent of the polynomial is  $d$ . The degree of a derivation counts the maximum nesting of applications of the rule  $(sp)$  in it. So considering fixed degrees we get PSPACE soundness. Considering a fixed  $d$  is not a limitation. Indeed until now, in  $STA_B$  programs we do not distinguish between the program code and input data. But it will be shown in Section 5 that data types are typable through derivations with degree 0. Hence the degree can be considered as a real characteristic of the program code.

Moreover every  $STA_B$  program can be typed through derivations with different degrees, nevertheless for each program there is a sort of minimal derivation for it, with respect to the degree. So we can stratify programs with respect to the degree of their derivations, according to the following definition.

### Definition 10.

1. The degree  $d(\nabla)$  of  $\nabla$  is the maximum nesting of applications of rule  $(sp)$  in  $\nabla$ .
2. For each  $d \in \mathbb{N}$  the set  $\mathcal{P}_d$  is the set of  $STA_B$  programs typable through derivation with degree  $d$ .

$$\mathcal{P}_d = \{M \mid (\nabla) \vdash M : B \wedge d(\nabla) = d\}$$

Clearly  $\mathcal{P}$  corresponds to the union for  $n \in \mathbb{N}$  of the different  $\mathcal{P}_n$ . Moreover if  $M \in \mathcal{P}_d$  then  $M \in \mathcal{P}_e$  for every  $e \geq d$ .

This section is divided into two subsections. In the first, we will prove an intermediate result, namely we will give the notion of space weight of a derivation, and we will prove that the subject reduction does not increment it. Moreover this result is extended to the machine  $K_B^C$ . In the second part the soundness with respect to PSPACE will be proved.

### 4.1 Space and $STA_B$

We need to define measures of both terms and proofs, which are an adaptation of those given by Lafont in (Lafont 2004).

#### Definition 11.

1. The rank of a rule  $(m)$ :

$$\frac{\Gamma, x_1 : \sigma, \dots, x_n : \sigma \vdash M : \mu}{\Gamma, x : !\sigma \vdash M[x/x_1, \dots, x/x_n] : \mu} (m)$$

is the number  $k \leq n$  of variables  $x_i$  such that  $x_i$  belongs to the free variables of  $M$ . Let  $r$  be the maximum rank of a rule  $(m)$  in  $\nabla$ . The rank  $rk(\nabla)$  of  $\nabla$  is the maximum between 1 and  $r$ .

2. Let  $r$  be a natural number. The space weight  $\delta(\nabla, r)$  of  $\nabla$  with respect to  $r$  is defined inductively as follows.

- (a) If the last applied rule is  $(Ax), (B_0I), (B_1I)$  then  $\delta(\nabla, r) = 1$ .
- (b) If the last applied rule is  $(-\circ I)$  with premise a derivation  $\Diamond$ , then  $\delta(\nabla, r) = \delta(\Diamond, r) + 1$ .
- (c) If the last applied rule is  $(sp)$  with premise a derivation  $\Diamond$ , then  $\delta(\nabla, r) = r\delta(\Diamond, r)$ .
- (d) If the last applied rule is  $(-\circ E)$  with premises  $\Diamond$  and  $\Box$  then  $\delta(\nabla, r) = \delta(\Diamond, r) + \delta(\Box, r) + 1$ .
- (e) If the last applied rule is:

$$\frac{(\Diamond) \Gamma \vdash M : B \quad (\Box_0) \Gamma \vdash N_0 : A \quad (\Box_1) \Gamma \vdash N_1 : A}{\Gamma \vdash \text{if } M \text{ then } N_0 \text{ else } N_1 : A}$$

$$\text{then } \delta(\nabla, r) = \max\{\delta(\Diamond, r), \delta(\Box_0, r), \delta(\Box_1, r)\} + 1$$

- (f) In every other case  $\delta(\nabla, r) = \delta(\Diamond, r)$  where  $\Diamond$  is the unique premise derivation.

In order to prove that the subject reduction does not increase the space weight of a derivation, we need to rephrase the Substitution Lemma taking into account this measure.

**Lemma 9 (Weighted Substitution Lemma).** *Let  $(\nabla) \Gamma, x : \mu \vdash M : \sigma$  and  $(\Diamond) \Delta \vdash N : \mu$  such that  $\Gamma \# \Delta$  then there exists  $(\Box) \Gamma, \Delta \vdash M[N/x] : \sigma$  such that if  $r \geq rk(\nabla)$ :*

$$\delta(\Box, r) \leq \delta(\nabla, r) + \delta(\Diamond, r)$$

*Proof.* We postpone the proof to Appendix A.2.  $\square$

We are now ready to show that the space weight  $\delta$  gives a bound on the number of both  $\beta$  and  $if$  rules in a computation path of the machine  $K_B^C$ .

**Lemma 10.** *Let  $M \in \mathcal{P}$  and  $\Pi ::= M \Downarrow b$ .*

1. Consider an occurrence in  $\Pi$  of the rule:

$$\frac{C, A @ \{x' := N\} \models M[x'/x]V_1 \cdots V_m \Downarrow b}{C, A \models (\lambda x.M)NV_1 \cdots V_m \Downarrow b} (\beta)$$

Then, for every derivations  $(\Diamond) \vdash ((\lambda x.M)NV_1 \cdots V_m)^A : B$  there exists a derivation  $(\Box) \vdash (M[x'/x]V_1 \cdots V_m)^{A @ \{x' := N\}} : B$  such that for every  $r \geq rk(\Diamond)$ :

$$\delta(\Diamond, r) > \delta(\Box, r)$$

2. Consider an occurrence in  $\Pi$  of an  $if$  rule as:

$$\frac{C', A \models M \Downarrow 0 \quad C, A \models N_0V_1 \cdots V_m \Downarrow b}{C, A \models (\text{if } M \text{ then } N_0 \text{ else } N_1)V_1 \cdots V_m \Downarrow b}$$

where  $C' \equiv C[(\text{if } [o] \text{ then } N_0 \text{ else } N_1)V_1 \cdots V_m]$ . Then, for each derivation  $(\Diamond) \vdash ((\text{if } M \text{ then } N_0 \text{ else } N_1)V_1 \cdots V_m)^A : B$  there are derivations  $(\Box) \vdash (M)^A : B$  and  $(\nabla) \vdash (N_0V_1 \cdots V_m)^A : B$  such that for every  $r \geq rk(\Diamond)$ :

$$\delta(\Diamond, r) > \delta(\Box, r) \text{ and } \delta(\Diamond, r) > \delta(\nabla, r)$$

$\frac{\mathcal{C}_1, \mathcal{A}_3 \models 0 \Downarrow 0}{\mathcal{C}_1, \mathcal{A}_3 \models z_1 \Downarrow 0}$ $\frac{\mathcal{C}_0, \mathcal{A}_3 \models z_1 \Downarrow 0}{\mathcal{C}_1, \mathcal{A}_3 \models x_2 \Downarrow 0}$ $\frac{\mathcal{C}_0, \mathcal{A}_3 \models x_2 \Downarrow 0}{\mathcal{C}_0, \mathcal{A}_3 \models \text{if } x_2 \text{ then } x_2 \text{ else } x_2 \Downarrow 0}$ $\frac{\mathcal{C}_0, \mathcal{A}_3 \models \text{if } x_2 \text{ then } x_2 \text{ else } x_2 \Downarrow 0}{\mathcal{C}_0, \mathcal{A}_2 \models (\lambda x. \text{if } x \text{ then } x \text{ else } x)z_1 \Downarrow 0}$	$\frac{\phi \triangleright \mathcal{C}_0, \mathcal{A}_3 \models 0 \Downarrow 0}{\phi \triangleright \mathcal{C}_0, \mathcal{A}_3 \models z_1 \Downarrow 0}$ $\frac{\mathcal{C}_0, \mathcal{A}_3 \models z_1 \Downarrow 0}{\mathcal{C}_0, \mathcal{A}_3 \models x_2 \Downarrow 0}$ $\frac{\mathcal{C}_0, \mathcal{A}_3 \models x_2 \Downarrow 0}{\mathcal{C}_0, \mathcal{A}_3 \models \text{if } x_2 \text{ then } x_2 \text{ else } x_2 \Downarrow 0}$ $\frac{\mathcal{C}_0, \mathcal{A}_3 \models \text{if } x_2 \text{ then } x_2 \text{ else } x_2 \Downarrow 0}{\mathcal{C}_0, \mathcal{A}_2 \models (\lambda x. \text{if } x \text{ then } x \text{ else } x)z_1 \Downarrow 0}$	$\frac{\mathcal{C}_2, \mathcal{A}_4 \models 0 \Downarrow 0}{\mathcal{C}_2, \mathcal{A}_4 \models z_1 \Downarrow 0}$ $\frac{\mathcal{A}_4 \models z_1 \Downarrow 0}{\mathcal{C}_2, \mathcal{A}_4 \models x_3 \Downarrow 0}$ $\frac{\mathcal{A}_4 \models x_3 \Downarrow 0}{\mathcal{A}_4 \models \text{if } x_3 \text{ then } x_3 \text{ else } x_3 \Downarrow 0}$ $\frac{\mathcal{A}_4 \models \text{if } x_3 \text{ then } x_3 \text{ else } x_3 \Downarrow 0}{\mathcal{A}_2 \models (\lambda x. \text{if } x \text{ then } x \text{ else } x)z_1 \Downarrow 0}$	$\frac{\mathcal{A}_4 \models 0 \Downarrow 0}{\mathcal{A}_4 \models z_1 \Downarrow 0}$ $\frac{\mathcal{A}_4 \models z_1 \Downarrow 0}{\mathcal{A}_4 \models x_3 \Downarrow 0}$ $\frac{\mathcal{A}_4 \models x_3 \Downarrow 0}{\mathcal{A}_4 \models \text{if } x_3 \text{ then } x_3 \text{ else } x_3 \Downarrow 0}$ $\frac{\mathcal{A}_4 \models \text{if } x_3 \text{ then } x_3 \text{ else } x_3 \Downarrow 0}{\mathcal{A}_2 \models (\lambda x. \text{if } x \text{ then } x \text{ else } x)z_1 \Downarrow 0}$
$\frac{\mathcal{C}_0, \mathcal{A}_2 \models f_1 z_1 \Downarrow 0}{\mathcal{C}_0, \mathcal{A}_2 \models x_1 \Downarrow 0}$	$\frac{\mathcal{A}_2 \models f_1 z_1 \Downarrow 0}{\psi \triangleright \mathcal{A}_2 \models x_1 \Downarrow 0}$		
$\frac{\mathcal{A}_2 \models \text{if } x_1 \text{ then } x_1 \text{ else } x_1 \Downarrow 0}{\mathcal{A}_1 \models (\lambda x. \text{if } x \text{ then } x \text{ else } x)(f_1 z_1) \Downarrow 0}$	$\frac{\mathcal{A}_1 \models f_1(f_1 z_1) \Downarrow 0}{\mathcal{A}_0 \models (f_1(f_1 z_1))0 \Downarrow 0}$		
$\begin{aligned} \mathcal{A}_0 &= [f_1 := \lambda x. \text{if } x \text{ then } x \text{ else } x] \\ \mathcal{A}_1 &= \mathcal{A}_0 @ [z_1 := 0] \\ \mathcal{A}_2 &= \mathcal{A}_1 @ [x_1 := f_1 z_1] \\ \mathcal{A}_3 &= \mathcal{A}_2 @ [x_2 := z_1] \\ \mathcal{A}_4 &= \mathcal{A}_2 @ [x_3 := z_1] \end{aligned}$	$\begin{aligned} \mathcal{C}_0 &= \text{if } o \text{ then } x_1 \text{ else } x_1 \\ \mathcal{C}_1 &= \mathcal{C}_0 [\text{if } o \text{ then } x_2 \text{ else } x_2] \\ \mathcal{C}_2 &= \text{if } o \text{ then } x_3 \text{ else } x_3 \end{aligned}$		

**Table 5.** An example of computation in  $K_B^C$ .

*Proof.*

- It suffices to consider the case where  $m = 0$ , and to prove that, if  $(\nabla) \Gamma \vdash (\lambda x.M)N : \sigma$ , then there exists  $(\nabla') \Gamma \vdash M[N/x] : \sigma$  with  $\text{rk}(\nabla) \geq \text{rk}(\nabla')$  such that for  $r \geq \text{rk}(\nabla)$ :

$$\delta(\nabla, r) > \delta(\nabla', r)$$

Since  $(\forall R), (\forall L), (m)$  and  $(w)$  rules don't change the  $\delta$  measure we can without loss of generality assume that  $\nabla$  ends as:

$$\frac{\begin{array}{c} (\Diamond) \Gamma_1, x : \sigma \vdash M : A \\ \Gamma_1 \vdash \lambda x.M : \sigma \multimap A \end{array}}{\Gamma_1, \Gamma_2 \vdash (\lambda x.M)N : A} \quad (\multimap I) \quad \frac{\Box \Gamma_2 \vdash N : \sigma}{\Gamma_1, \Gamma_2 \vdash (\lambda x.M)N : A} \quad (\multimap E)$$

$$\frac{!^n \Gamma_1, !^n \Gamma_2 \vdash (\lambda x.M)N : !^n A}{!^n \Gamma_1, !^n \Gamma_2 \vdash M[N/x] : !^n A} \quad (sp)^n$$

where  $\Gamma_1 \# \Gamma_2$ ,  $\Gamma = !^n \Gamma_1, !^n \Gamma_2$ ,  $\sigma \equiv !^n A$  and  $n \geq 0$ . Clearly we have  $\delta(\nabla, r) = r^n(\delta(\Diamond, r) + 1 + \delta(\Box, r))$ .

By Lemma 9 we have a derivation  $(\Diamond') \Gamma_1, \Gamma_2 \vdash M[N/x] : A$  such that  $\delta(\Diamond', r) \leq \delta(\Diamond, r) + \delta(\Box, r)$ . Hence, we can construct  $\nabla'$  ending as:

$$\frac{(\Diamond') \Gamma_1, \Gamma_2 \vdash M[N/x] : A}{!^n \Gamma_1, !^n \Gamma_2 \vdash M[N/x] : !^n A} \quad (sp)^n$$

Clearly  $\delta(\nabla', r) \leq r^n(\delta(\Diamond, r) + \delta(\Box, r))$ , so the conclusion follows.

- Easy, by definition of  $\delta$ .  $\square$

Since it is easy to verify that  $h$  rules leave the space weight unchanged, a direct consequence of the above lemma is the following.

**Lemma 11.** Let  $(\nabla) \Gamma \vdash M : B$  and  $\Pi :: \vdash M \Downarrow b$ . Then for each  $\phi \triangleright \mathcal{C}, \mathcal{A} \models N \Downarrow b' \in \Pi$  if  $r \geq \text{rk}(\nabla)$ :

$$\#_\beta(\phi) + \#\text{if}(\phi) \leq \delta(\nabla, r)$$

Now we are ready to prove that subject reduction does not increase the space weight.

**Property 2.** Let  $(\nabla) \Gamma \vdash M : \sigma$  and  $M \rightarrow_{\beta\delta}^* N$ . Then there exists  $(\nabla') \Gamma \vdash N : \sigma$  with  $\text{rk}(\nabla) \geq \text{rk}(\nabla')$  such that for each  $r \geq \text{rk}(\nabla)$ :

$$\delta(\nabla, r) \geq \delta(\nabla', r)$$

*Proof.* By Lemma 9 and definition of  $\delta$ , noting that a reduction inside an  $\text{if}$  can leave  $\delta$  unchanged.  $\square$

The previous result can be extended to the machine  $K_B^C$  in the following way.

**Property 3.** Let  $(\nabla) \Gamma \vdash M : B$  and  $\Pi :: \vdash M \Downarrow b$ . For each configuration  $\phi \triangleright \mathcal{C}, \mathcal{A} \models N_i \Downarrow b_i \in \Pi$  such that  $C \not\models o$  there exist derivations  $(\Diamond) \vdash (\mathcal{C}[N_i])^A : B$  and  $(\Box) \vdash (N_i)^A : B$  such that  $\Box$  is a proper subderivation of  $\Diamond$  and for each  $r \geq \text{rk}(\nabla)$ :

$$\delta(\nabla, r) \geq \delta(\Diamond, r) > \delta(\Box, r)$$

## 4.2 Proof of PSPACE Soundness

As we said in the previous section, the space used by the machine  $K_B^C$  is the maximum space used by its configurations. In order to give an account of this space, we need to measure how the size of a term can increase during the evaluation. The key notion for doing it is that of number of the sliced occurrence of a variable, which takes into account that in performing an  $\text{if}$  reduction a subterm of the subject is erased. In particular by giving a bound on the number of sliced occurrence we obtain a bound on the number of applications of the  $h$  rule in a path.

**Definition 12.** The number of sliced occurrences  $n_{so}(x, M)$  of the variable  $x$  occurring free in  $M$  is defined as:

$$n_{so}(x, x) = 1, n_{so}(x, y) = n_{so}(x, 0) = n_{so}(x, 1) = 0,$$

$$n_{so}(x, MN) = n_{so}(x, M) + n_{so}(x, N), n_{so}(x, \lambda y.M) = n_{so}(x, M),$$

$$n_{so}(x, \text{if } M \text{ then } N_0 \text{ else } N_1) = \max\{n_{so}(x, M), n_{so}(x, N_0), n_{so}(x, N_1)\}$$

A type derivation gives us some informations about the number of sliced occurrences of a free variable  $x$  in its subject  $M$ .

**Lemma 12.** Let  $(\nabla) \Gamma, x : !^n A \vdash M : \sigma$  then  $n_{so}(x, M) \leq \text{rk}(\nabla)^n$ .

*Proof.* By induction on  $n$ .

Case  $n = 0$ . The conclusion follows easily by induction on  $(\nabla)$ . Base cases are trivial. In the case  $(\nabla)$  ends by **(BE)** conclusion follows by  $n_{so}(x, M)$  definition and induction hypothesis. The other cases follow directly from the induction hypothesis remembering the side condition  $\Gamma \# \Delta$  in  $(\neg E)$  case.

Case  $n > 0$ . By induction on  $(\nabla)$ . Base cases are trivial. Let the last rule of  $(\nabla)$  be:

$$\frac{(\Diamond) \Gamma \vdash M' : B \quad (\Box_0) \Gamma \vdash N_0 : B \quad (\Box_1) \Gamma \vdash N_1 : B}{\Gamma \vdash \text{if } M' \text{ then } N_0 \text{ else } N_1 : B} \text{ (BE)}$$

where  $x : !^n A \in \Gamma$ . By induction hypothesis  $n_{so}(x, M') \leq \text{rk}(\Diamond)^n$  and  $n_{so}(x, N_i) \leq \text{rk}(\Box_i)^n$  for  $i \in \{0, 1\}$ . By definition  $\text{rk}(\nabla) = \max\{\text{rk}(\Diamond), \text{rk}(\Box_0), \text{rk}(\Box_1)\}$  and since by definition  $n_{so}(x, \text{if } M' \text{ then } N_0 \text{ else } N_1)$  is equal to  $\max\{n_{so}(x, M'), n_{so}(x, N_0), n_{so}(x, N_1)\}$ , then the conclusion follows.

Let the last rule of  $(\nabla)$  be:

$$\frac{(\Diamond) \Gamma, x_1 : !^{n-1} A, \dots, x_m : !^{n-1} A \vdash N : \mu}{\Gamma, x : !^n A \vdash N[x/x_1, \dots, x/x_m] : \mu} (m)$$

where  $N[x/x_1, \dots, x/x_m] \equiv M$ . By induction hypothesis  $n_{so}(x_i, N) \leq \text{rk}(\Diamond)^{n-1}$  for  $1 \leq i \leq m$ . Hence in particular,  $n_{so}(x, N) \leq m \times \text{rk}(\Diamond)^{n-1}$ . Now, since  $m \leq \text{rk}(\nabla)$  and  $\text{rk}(\Diamond) \leq \text{rk}(\nabla)$  it follows  $n_{so}(x, N) \leq \text{rk}(\nabla) \times \text{rk}(\Diamond)^{n-1} \leq \text{rk}(\nabla)^n$  and so the conclusion. In every other case the conclusion follows directly by induction hypothesis.  $\square$

It is worth noting that the above lemma and the subject reduction property gives dynamical informations about the number of sliced occurrences of a variable.

**Lemma 13.** Let  $(\nabla) \Gamma, x : !^n A \vdash M : \sigma$  and  $M \rightarrow_{\beta\delta} N$ . Then  $n_{so}(x, N) \leq \text{rk}(\nabla)^n$ .

The lemma above is essential to prove the following remarkable property.

**Lemma 14.** Let  $M \in \mathcal{P}_d$  and  $\Pi :: \models M \Downarrow b$  then for each  $\phi \triangleright C, \mathcal{A} \models P \Downarrow b' \in \Pi$ :

$$\#_h(\phi) \leq \#(\mathcal{A})|M|^d$$

*Proof.* For each  $[y := N] \in \mathcal{A}$  the variable  $y$  is a fresh copy of a variable  $x$  originally bound in  $M$  hence  $M$  contains a subterm  $(\lambda x.P)Q$  and there exists a derivation  $(\nabla) x : !^n A \vdash P : B$ . Hence by Lemma 13 for every  $P'$  such that  $P \rightarrow_{\beta\delta} P'$  we have  $n_{so}(x, P') \leq \text{rk}(\nabla)^n$ . In particular the number of applications of  $h$  rules on the variable  $y$  is bounded by  $\text{rk}(\nabla)^n$ . Since  $|M| \geq \text{rk}(\nabla)$  and  $d \geq n$  the conclusion follows.  $\square$

The following lemma relates the space weight with both the size of the term and the degree of the derivation.

**Lemma 15.** Let  $(\nabla) \Gamma \vdash M : \sigma$ .

$$1. \delta(\nabla, 1) \leq |M|$$

2.  $\delta(\nabla, r) \leq \delta(\nabla, 1) \times r^{d(\nabla)}$
3.  $\delta(\nabla, \text{rk}(\nabla)) \leq |M|^{d(\nabla)+1}$

*Proof.* 1. By induction on  $(\nabla)$ . Base cases are trivial. Cases  $(sp), (m), (w), (\forall I)$  and  $(\forall E)$  follow directly by induction hypothesis. The other cases follow by definition of  $\delta$ .

2. By induction on  $(\nabla)$ . Base cases are trivial. Cases  $(sp), (m), (w), (\forall I)$  and  $(\forall E)$  follow directly by induction hypothesis. The other cases follow by definition of  $\delta$  and  $d$ .

3. By definition of rank it is easy to verify that  $\text{rk}(\nabla) \leq |M|$ , hence by the previous two points the conclusion follows.  $\square$

The next lemma gives a bound on the dimensions of all the components of a machine configuration, namely the term, the m-context and the B-context.

**Lemma 16.** Let  $M \in \mathcal{P}_d$  and  $\Pi :: \models M \Downarrow b$ . Then for each  $\phi \triangleright C, \mathcal{A} \models N \Downarrow b' \in \Pi$ :

1.  $|\mathcal{A}| \leq 2|M|^{d+2}$
2.  $|N| \leq 2|M|^{2d+2}$
3.  $|C| \leq 2|M|^{3d+3}$

*Proof.*

1. By Lemma 8.1, Lemma 11 and Lemma 15.3.
2. By Lemma 8.2, Lemma 14, Lemma 7.1, Lemma 11 and Lemma 15.3:

$$|N| \leq (\#_h(\phi) + 1)|M| \leq \#(\mathcal{A})|M|^{d+1} + |M| \leq 2|M|^{2d+2}$$

3. By Lemma 8.3, the previous point of this lemma, Lemma 7.2, Lemma 11 and Lemma 15.3:

$$|C| \leq \#(\mathcal{C})2|M|^{2d+2} \leq |M|^{d+1}2|M|^{2d+2} \leq 2|M|^{3d+3}$$

$\square$

The PSPACE soundness follows immediately from the definition of  $\text{space}(\Pi)$ , for a machine evaluation  $\Pi$ , and from the previous lemma.

**Theorem 2 (Polynomial Space Soundness).**  
Let  $M \in \mathcal{P}_d$ . Then:

$$\text{space}(M) \leq 6|M|^{3d+3}$$

## 5. PSPACE completeness

It is well known that the class of problems decidable by a Deterministic Turing Machine (DTM) in space polynomial in the length of the input coincides with the class of problems decidable by an Alternating Turing Machine (ATM) (Chandra et al. 1981) in time polynomial in the length of the input.

In (Gaboardi and Ronchi Della Rocca 2007) it has been shown that polytime DTM are definable by  $\lambda$ -terms typable in STA. Analogously here we will show that polytime ATM are definable by programs of STA<sub>B</sub>. We achieve such a result considering a notion of *function programmable* in STA<sub>B</sub>. We will consider the same representation of data types as in STA, in particular data types typable through derivations with degree 0. (We will recall it briefly but we refer to (Gaboardi and Ronchi Della Rocca 2007) for more details.) Finally we show that for each polytime ATM  $\mathcal{M}$  we can define a recursive evaluation procedure which behaves as  $\mathcal{M}$ .

**Some syntactic sugar** Let  $\circ$  denote composition. In particular  $M \circ N$  stands for  $\lambda z.M(Nz)$  and  $M_1 \circ M_2 \circ \dots \circ M_n$  stands for  $\lambda z.M_1(M_2(\dots(M_n z)))$ .

Tensor product is definable as  $\sigma \otimes \tau \doteq \forall \alpha.(\sigma \multimap \tau \multimap \alpha) \multimap \alpha$ . In particular  $\langle M, N \rangle$  stands for  $\lambda x.xMN$  and let  $z$  be  $x, y$  in  $N$  stands for  $z(\lambda x.\lambda y.N)$ . Note that, since STA<sub>B</sub> is an affine system, tensor product enjoys some properties of the additive conjunction, as to allow the projectors: as usual  $\pi_1(M)$  stands for  $M(\lambda x.\lambda y.x)$  and  $\pi_2(M)$  stands for  $M(\lambda x.\lambda y.y)$ .  $n$ -ary tensor product can be easily defined through the binary one and we use  $\sigma^n$  to denote  $\sigma \otimes \dots \otimes \sigma$   $n$ -times.

**Natural numbers and strings of booleans** Natural numbers are represented by Church numerals, i.e.  $n \doteq \lambda s.\lambda z.s^n(z)$ . Terms defining successor, addition and multiplication are typable by indexed types  $N_i \doteq \forall \alpha.!(\alpha \multimap \alpha) \multimap \alpha \multimap \alpha$ . We write  $N$  to mean  $N_1$ . In particular the following still holds for STA<sub>B</sub>:

**Lemma 17.** *Let  $P$  be a polynomial and  $\deg(P)$  its degree. Then there is a term  $P$  defining  $P$  typable as:*

$$\vdash P : !^{\deg(P)} N \multimap N_{2\deg(P)+1}$$

Strings of booleans are represented by terms of the shape  $\lambda c z.c b_0(\dots(c b_n z)\dots)$  where  $b_i \in \{0, 1\}$ . Such terms are typable by the indexed type  $S_i \doteq \forall \alpha.!(\mathbf{B} \multimap \alpha \multimap \alpha) \multimap \alpha \multimap \alpha$ . Again, we write  $S$  to mean  $S_1$ . Moreover there is a term  $\text{len}$  typable as  $\vdash \text{len} : S_i \multimap N_i$  that given a string of boolean returns its length.

Note that the data types defined above can be typed in STA<sub>B</sub> by derivations with degree 0.

**Programmable functions** The polynomial time completeness in (Gaboardi and Ronchi Della Rocca 2007) relies on the notion of  $\lambda$ -definability, given in (Barendregt 1984), generalized to different kinds of data.

The same can be done here for STA<sub>B</sub>, by using a generalization of  $\lambda$ -definability to the set of terms  $\Lambda_B$ . Nevertheless this is not sufficient, since we want to show that polynomial time ATM can be defined by programs of STA<sub>B</sub>. In fact we have the following definition.

*n-times*

**Definition 13.** *Let  $f : \overbrace{\mathbb{S} \times \dots \times \mathbb{S}}^{n\text{-times}} \rightarrow \mathbb{B}$  and let every string  $s \in \mathbb{S}$  be representable by a term  $s$ . Then,  $f$  is programmable if, there exists a term  $f \in \Lambda_B$ , such that  $fs_1 \dots s_n \in \mathcal{P}$  and:*

$$f(s_1, \dots, s_n) = b \iff \vdash fs_1 \dots s_n \Downarrow b$$

**Boolean connectives** It is worth noting that due to the presence of the (BE) rule it is possible to define the usual boolean connectives. In fact let  $M$  and  $N \doteq \text{if } M \text{ then ( if } N \text{ then } 0 \text{ else } 1 \text{ ) else } 1$  and  $M \text{ or } N \doteq \text{if } M \text{ then } 0 \text{ else ( if } N \text{ then } 0 \text{ else } 1 \text{ )}$ . Then the following rules with an additive management of contexts are derived:

$$\frac{\Gamma \vdash M : \mathbf{B} \quad \Gamma \vdash N : \mathbf{B}}{\Gamma \vdash M \text{ and } N : \mathbf{B}} \quad \frac{\Gamma \vdash M : \mathbf{B} \quad \Gamma \vdash N : \mathbf{B}}{\Gamma \vdash M \text{ or } N : \mathbf{B}}$$

Moreover we have a term  $\text{not}$  defining the expected boolean function.

**ATMs Configurations** The encoding of Deterministic Turing Machine configuration given in (Gaboardi and Ronchi Della Rocca 2007) can be adapted in order to encode Alternating Turing Machine configurations. In fact an ATM configuration can be viewed as a DTM configuration with an extra information about the state. There are four kinds of state: *accepting* (A), *rejecting* (R), *universal* ( $\wedge$ ), *existential* ( $\vee$ ). We can encode such information by tensor pairs of booleans. In particular:

$$\boxed{\langle 1, 0 \rangle \mid A \parallel \langle 1, 1 \rangle \mid R \parallel \langle 0, 1 \rangle \mid \wedge \parallel \langle 0, 0 \rangle \mid \vee}$$

We say that a configuration is accepting, rejecting, universal or existential depending on the kind of its state.

We can encode ATM configurations by terms of the shape:

$$\lambda c. (cb_0^l \circ \dots \circ cb_n^l, cb_0^r \circ \dots \circ cb_m^r, (Q, k))$$

where  $cb_0^l \circ \dots \circ cb_n^l$  and  $cb_0^r \circ \dots \circ cb_m^r$  are respectively the left and right hand-side words on the ATM tape,  $Q$  is a tuple of length  $q$  encoding the state and  $k$  is the tensor pair encoding the kind of state. Such terms can be typed as:

$$\text{ATM}_i \doteq \forall \alpha. !^i (\mathbf{B} \multimap \alpha \multimap \alpha) \multimap ((\alpha \multimap \alpha)^2 \otimes \mathbf{B}^{q+2})$$

It is easy to adapt the term described in (Gaboardi and Ronchi Della Rocca 2007) dealing with TM to the case of ATM. In particular we have:

$$\vdash \text{Init} : S_i \multimap \text{ATM}_i \quad \text{Initial configuration}$$

$$\vdash \text{Tr}_1, \text{Tr}_2 : \text{ATM}_i \multimap \text{ATM}_i \quad \text{Transition functions}$$

Moreover we have a term:

$$\text{Kind} \doteq \lambda x. \text{let } x(\lambda b. \lambda y. y) \text{ be } l, r, s \text{ in (let } s \text{ be } q, k \text{ in } k)$$

typable as  $\vdash \text{Kind} : \text{ATM}_i \multimap \mathbf{B}^2$  which takes a configuration and return its kind. We also have a term

$$\text{Ext} \doteq \lambda x. \text{let } ( \text{Kind } x ) \text{ be } l, r \text{ in } r$$

typable as  $\vdash \text{Ext} : \text{ATM}_i \multimap \mathbf{B}$ . Assuming that a given configuration is either accepting or rejecting Ext returns 0 or 1 respectively.

**Evaluation function** Given an ATM  $\mathcal{M}$  working in polynomial time we define a recursive evaluation procedure  $\text{eval}_{\mathcal{M}}$  which takes a string  $s$  and returns 0 or 1 if the initial configuration (with the tape filled with  $s$ ) leads to an accepting or rejecting configuration respectively.

Without loss of generality we consider ATMs with transition relation of degree two (at each step we consider two transitions). We need to define some auxiliary functions.

$$\alpha(M_0, M_1, M_2) \doteq \text{let } M_0 \text{ be } a_1, a_2 \text{ in ( if } a_1 \text{ then ( if } a_2 \text{ then } \langle a_1, } \pi_2(M_1) \text{ or } \pi_2(M_2) \rangle \text{ else } \langle a_1, } \pi_2(M_1) \text{ and } \pi_2(M_2) \rangle \text{ ) else } \langle a_1, a_2 \rangle$$

which acts as:

$$\begin{array}{ll} \alpha(A, M_1, M_2) = A & \alpha(\wedge, M_1, M_2) = M_1 \wedge M_2 \\ \alpha(R, M_1, M_2) = R & \alpha(\vee, M_1, M_2) = M_1 \vee M_2 \end{array}$$

Note that for  $\alpha$  defined as above we have the following typing rule:

$$\frac{\Gamma \vdash M_0 : \mathbf{B}^2 \quad \Gamma \vdash M_1 : \mathbf{B}^2 \quad \Gamma \vdash M_2 : \mathbf{B}^2}{\Gamma \vdash \alpha(M_0, M_1, M_2) : \mathbf{B}^2}$$

where the management of contexts is additive. We would now define  $\text{eval}_{\mathcal{M}}$  as an iteration of an higher order  $\text{Step}_{\mathcal{M}}$  function over a Base case. Let  $\text{Tr}_{\mathcal{M}}^1$  and  $\text{Tr}_{\mathcal{M}}^2$  be two closed terms defining the two components of the transition relation.

$$\text{Base} \doteq \lambda c. (\text{Kind } c) :$$

$$\text{Step}_{\mathcal{M}} \doteq \lambda h. \lambda c. \alpha((\text{Kind } c), (h(\text{Tr}_{\mathcal{M}}^1 c)), (h(\text{Tr}_{\mathcal{M}}^2 c)))$$

It is easy to verify that such terms are typable as:

$$\begin{aligned} &\vdash \text{Base} : \text{ATM}_i \multimap \mathbf{B}^2 \\ &\vdash \text{Step}_{\mathcal{M}} : (\text{ATM}_i \multimap \mathbf{B}^2) \multimap \text{ATM}_i \multimap \mathbf{B}^2 \end{aligned}$$

Now we can finally define the evaluation function. Let  $P$  be a polynomial definable by a term  $P$  typable as  $\vdash P : !^{\deg(P)} N \multimap N_{2\deg(P)+1}$ . Then the evaluation function of an ATM  $\mathcal{M}$  working in polynomial time  $P$  is definable by the term:

$$\text{eval}_{\mathcal{M}} \doteq \lambda s. \text{Ext}((P(\text{len } s) \text{ Step}_{\mathcal{M}} \text{ Base})(\text{Init } s))$$

which is typable in STA<sub>B</sub> as  $\vdash \text{eval}_{\mathcal{M}} : !^t \mathbf{S} \multimap \mathbf{B}$  where  $t = \max(\deg(P), 1) + 1$ .

Here, the evaluation is performed by a higher order iteration, which represents a recurrence with parameter substitutions. Note that by considering an ATM  $\mathcal{M}$  which decides a language  $\mathcal{L}$  the final configuration is either accepting or rejecting hence the term  $\text{Ext}$  can be applied with the intended meaning.

**Lemma 18.** A decision problem  $\mathcal{D} : \{0, 1\}^* \rightarrow \{0, 1\}$  decidable by an ATM  $\mathcal{M}$  in polynomial time is programmable in STA<sub>B</sub>.

*Proof.*  $\mathcal{D}(s) = b \iff \text{eval}_{\mathcal{MS}} \Downarrow b$   $\square$

From the well known result of (Chandra et al. 1981) we can conclude.

**Theorem 3 (Polynomial Space Completeness).** Every decision problem  $\mathcal{D} \in \text{PSPACE}$  is programmable in STA<sub>B</sub>.

## 6. Related Topic

In this section we will discuss some topic which are related to the work we have presented.

**FPSPACE characterization.** FPSPACE is the class of functions computable in polynomial space. The completeness for FPSPACE can be obtained by replacing booleans by words over booleans. In particular we can add to STA the type **W** and the following rules:

$$\frac{}{\vdash \epsilon : \mathbf{W}} \quad \frac{\Gamma \vdash M : \mathbf{W}}{\Gamma \vdash 0(M) : \mathbf{W}} \quad \frac{\Gamma \vdash M : \mathbf{W}}{\Gamma \vdash 1(M) : \mathbf{W}} \quad \frac{\Gamma \vdash M : \mathbf{W}}{\Gamma \vdash p(M) : \mathbf{W}}$$

and the conditional

$$\frac{\Gamma \vdash M : \mathbf{W} \quad \Gamma \vdash N_\epsilon : \mathbf{W} \quad \Gamma \vdash N_0 : \mathbf{W} \quad \Gamma \vdash N_1 : \mathbf{W}}{\Gamma \vdash D(M, N_\epsilon, N_0, N_1) : \mathbf{W}}$$

The obtained system STA<sub>W</sub> equipped with the obvious reduction relation can be shown to be FPSPACE sound following what we have done for STA<sub>B</sub>. Moreover, analogously to (Leivant and Marion 1993), completeness for FPSPACE can be proved by considering two distinct data types **S** (Church representations of Strings) and **W** (Flat words over Booleans) as input and output data type respectively. The above is one of the reasons that leads us to consider STA<sub>B</sub> instead of the above system.

**STA<sub>B</sub> and Soft Linear Logic.** STA has been introduced as a type assignment counterpart of Soft Linear Logic (Lafont 2004). STA<sub>B</sub> is an extension of STA by booleans constants. We now pose our attention to the question of which is the logical counterpart of such extension.

We can add to SLL (or define by means of second order quantifier) the additive disjunction  $\oplus$  and the rules to deal with it, which in a natural deduction style (Ronchi Della Rocca and Roversi 1997) are:

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \oplus B} \quad \frac{\Gamma \vdash A \oplus B \quad \Delta, A \vdash C \quad \Delta, B \vdash C}{\Gamma, \Delta \vdash C}$$

We can so define **B** = **1**  $\oplus$  **1**, where **1** is the multiplicative unit, and specialize the above rules to booleans:

$$\frac{\Gamma \vdash \mathbf{1} \quad (0)}{\Gamma \vdash \mathbf{1} \oplus \mathbf{1}} \quad \frac{\Gamma \vdash \mathbf{1} \quad (1)}{\Gamma \vdash \mathbf{1} \oplus \mathbf{1}} \\ \frac{\Gamma \vdash \mathbf{1} \oplus \mathbf{1} \quad \Delta, \mathbf{1} \vdash C \quad \Delta, \mathbf{1} \vdash C}{\Gamma, \Delta \vdash C} \quad (\mathbf{E})$$

It is worth noting that such rules do not change the complexity of SLL. In fact it is essential in order to obtain a logical system behaving as STA<sub>B</sub> to modify the above elimination rule allowing free contraction between contexts  $\Gamma$  and  $\Delta$ . Hence we can modify it as:

$$\frac{\Gamma \vdash \mathbf{1} \oplus \mathbf{1} \quad \Gamma, \mathbf{1} \vdash C \quad \Gamma, \mathbf{1} \vdash C}{\Gamma \vdash C} \quad (\mathbf{E})$$

We conjecture that the logical system obtained by adding the above modified rule to SLL behaves like STA<sub>B</sub>. In order to prove the polynomial space soundness for such a system we need to mimic in the cut elimination process the abstract machine mechanism of Section 3. For this reason it could be more interesting introduce proof-nets for such a system and study cut elimination in this framework.

## A. Technical Proofs

### A.1 Proof of Substitution Lemma

The technical notion of height of a variable in a derivation will be useful in the proof of the Substitution Lemma.

**Definition 14.** Let  $(\nabla) \Gamma, x : \tau \vdash M : \sigma$ . The height of  $x$  in  $\nabla$  is inductively defined as follows:

- if the last applied rule of  $\nabla$  is:

$$\frac{}{\Gamma \vdash N : \sigma} \quad \text{or} \quad \frac{}{\Gamma, x : A \vdash N : \sigma}$$

then the height of  $x$  in  $\nabla$  is 0.

- if the last applied rule of  $\nabla$  is:

$$\frac{(\Diamond) \Gamma, x_1 : \tau, \dots, x_k : \tau \vdash N : \sigma}{\Gamma, x : !\tau \vdash N[x/x_1, \dots, x/x_k] : \sigma} \quad (m)$$

then the height of  $x$  in  $\nabla$  is the max between the heights of  $x_i$  in  $\nabla$  for  $1 \leq i \leq k$  plus one.

- Let  $\Gamma' = \Gamma, x : \tau$  and let the last applied rule  $\pi$  of  $\nabla$  be:

$$\frac{(\Diamond) \Gamma' \vdash M : \mathbf{B} \quad (\Box_0) \Gamma' \vdash N_0 : A \quad (\Box_1) \Gamma' \vdash N_1 : A}{\Gamma, x : \tau \vdash \text{if } M \text{ then } N_0 \text{ else } N_1 : A}$$

Then the height of  $x$  in  $\nabla$  is the max between the heights of  $x$  in  $\Diamond, \Box_0$  and  $\Box_1$  respectively plus one.

- In every other case there is an assumption with subject  $x$  both in the conclusion of the rule and in one of its premises  $\Diamond$ . Then the height of  $x$  in  $\nabla$  is equal to the height of  $x$  in  $\Diamond$  plus one.

**Proof of Substitution Lemma.** By induction on the height of  $x$  in  $\nabla$ . Base cases ( $Ax$ ) and ( $w$ ) are trivial. The cases where  $\nabla$  ends by  $(\multimap I), (\forall I), (\forall E)$  and  $(\multimap E)$  follow directly from the induction hypothesis.

Let  $\nabla$  end by (*sp*) rule with premise  $(\nabla') \Gamma, x : \mu' \vdash M : \sigma'$  then by Lemma 2.3  $\Diamond \rightsquigarrow \Diamond''$  which is composed by a subderivation ending with an (*sp*) rule with premise  $(\Diamond') \Delta' \vdash N : \mu'$  followed by a sequence of rules (*w*) and/or (*m*). By the induction hypothesis we have a derivation  $(\Box') \Gamma', \Delta' \vdash M[N/x] : \sigma'$ . By applying the rule (*sp*) and the sequence of (*w*) and/or (*m*) rules we obtain  $(\Box) \Gamma, \Delta \vdash M[N/x] : \sigma$ .

Let  $\nabla$  end by

$$\frac{(\nabla_0) \Gamma \vdash M_0 : \mathbf{B} \quad (\nabla_1) \Gamma \vdash M_1 : A \quad (\nabla_2) \Gamma \vdash M_2 : A}{\Gamma \vdash \text{if } M_0 \text{ then } M_1 \text{ else } M_2 : A} \quad (\mathbf{BE})$$

with  $\Gamma = \Gamma', x : \mu$ . Then by the induction hypothesis there are derivations  $(\Box_0) \Gamma', \Delta \vdash M_0[N/x] : \mathbf{B}$ ,  $(\Box_1) \Gamma', \Delta \vdash M_1[N/x] : A$  and  $(\Box_2) \Gamma', \Delta \vdash M_2[N/x] : A$ . By applying a (**BE**) rule we obtain a derivation  $(\Box)$  with conclusion:

$$\Gamma', \Delta \vdash \text{if } M_0[N/x] \text{ then } M_1[N/x] \text{ else } M_2[N/x] : A$$

Let  $\nabla$  end by

$$\frac{(\nabla') \Gamma, x_1 : \mu', \dots, x_m : \mu' \vdash N : \sigma}{\Gamma, x : !\mu' \vdash N[x/x_1, \dots, x/x_m] : \sigma} \quad (m)$$

By Lemma 2.3  $\Diamond \rightsquigarrow \Diamond''$  ending by an (*sp*) rule with premise  $(\Diamond') \Delta' \vdash N : \mu'$  followed by a sequence of rules (*w*) and/or (*m*).

Consider fresh copies of the derivation  $\Diamond'$  i.e.  $(\Diamond'_j) \Delta'_j \vdash N_j : \mu'$  where  $N_j$  and  $\Delta'_j$  are fresh copies of  $N$  and  $\Delta'$  ( $1 \leq j \leq m$ ). Let  $x_i$  be such that its height is maximal between the heights of all  $x_j$  ( $1 \leq j \leq m$ ). By induction hypothesis there is a derivation  $(\Box_i) \Gamma, x_1 : \mu', \dots, x_{i-1} : \mu', x_{i+1} : \mu', \dots, x_m : \mu', \Delta'_i \vdash M[N_i/x_i] : \sigma'$ . Then we can repeatedly apply induction hypothesis to obtain a derivation  $(\Box') \Gamma, \Delta'_1, \dots, \Delta'_m \vdash M[N_1/x_1, \dots, N_m/x_m] : \sigma$ . Finally by applying repeatedly the rules  $(m)$  and  $(w)$  the conclusion follows.  $\square$

## A.2 Proof of Weighted Substitution Lemma

It suffices to verify how the weights are modified by the proof of Substitution Lemma. We will use exactly the same notation as in the lemma.

**Proof of Weighted Substitution Lemma.** Base cases are trivial and in the cases where  $\nabla$  ends by  $(\neg I), (\forall I), (\forall E)$  and  $(\neg E)$  the conclusion follows directly by induction hypothesis.

If  $\nabla$  ends by  $(sp)$ :  $\delta(\nabla, r) = r\delta(\nabla', r)$  and  $\delta(\Diamond, r) = r\delta(\Diamond', r)$ . By the induction hypothesis  $\delta(\Box', r) \leq \delta(\nabla', r) + \delta(\Diamond', r)$  and applying  $(sp)$ :

$$\delta(\Box, r) \leq r(\delta(\nabla', r) + \delta(\Diamond', r)) = \delta(\nabla, r) + \delta(\Diamond, r)$$

If  $\nabla$  ends by  $(BE)$ :  $\delta(\nabla, r) = \max_{0 \leq i \leq 2}(\delta(\nabla_i, r)) + 1$ . By induction hypothesis we have derivations  $\delta(\Box_i, r) \leq \delta(\nabla_i, r) + \delta(\Diamond, r)$  for  $0 \leq i \leq 2$ . and applying a  $(BE)$  rule:

$$\delta(\Box, r) \leq \max_{0 \leq i \leq 2}(\delta(\nabla_i, r) + \delta(\Diamond, r)) = \max_{0 \leq i \leq 2}(\delta(\nabla_i, r)) + \delta(\Diamond, r)$$

If  $\nabla$  ends by  $(m)$ :  $\delta(\nabla, r) = \delta(\nabla', r)$  and  $\delta(\Diamond, r) = r\delta(\Diamond', r)$ . Clearly  $\delta(\Diamond', r) = \delta(\Diamond'_j, r)$  so  $\delta(\Box, r) \leq \delta(\nabla', r) + m\delta(\Diamond', r)$  and since  $r \geq \text{rk}(\nabla)$  then:

$$\delta(\Box', r) \leq \delta(\nabla', r) + r\delta(\Diamond', r) = \delta(\nabla, r) + \delta(\Diamond, r)$$

Now the rules  $(m)$  and  $(w)$  leave the space weight  $\delta$  unchanged hence the conclusion follows.  $\square$

## Acknowledgments

We are grateful to the anonymous referees for the numerous detailed and fruitful comments and suggestions on the preliminary version of the paper.

## References

- Serge Abiteboul and Victor Vianu. Fixpoint extensions of first-order logic and datalog-like languages. In *Proceedings of the 4th Annual Symposium on Logic in Computer Science - LICS'89*, pages 71–79, Asilomar, California, 1989. IEEE Computer Society Press.
- Andrea Asperti and Luca Roversi. Intuitionistic light affine logic. *ACM Transactions on Computational Logic*, 3(1):137–175, 2002.
- Patrick Baillot and Kazushige Terui. Light types for polynomial time computation in lambda-calculus. In *Proceedings of the 19th Annual Symposium on Logic in Computer Science - LICS'04*, pages 266–275, Turku, Finland, 2004. IEEE Computer Society Press.
- Henk Barendregt. *The Lambda Calculus: Its Syntax and Semantics*. Elsevier/North-Holland, Amsterdam, London, New York, revised edition, 1984.
- Ashok K. Chandra, Dexter C. Kozen, and Larry J. Stockmeyer. Alternation. *Journal of the ACM*, 28(1):114–133, 1981.
- Paolo Coppola, Ugo Dal Lago, and Simona Ronchi Della Rocca. Elementary affine logic and the call by value lambda calculus. In *Proceedings of the Typed Lambda Calculi and Applications, 7th International Conference - TLCA '05*, Nara, Japan, April 21–23, 2005, volume 3461 of *Lecture Notes in Computer Science*, pages 131–145. Springer, 2005.
- Marco Gaboardi and Simona Ronchi Della Rocca. A soft type assignment system for  $\lambda$ -calculus. In *Proceedings of the Computer Science Logic, 21st International Workshop - CSL'07*, Lausanne, Switzerland, September 11–15, 2007, volume 4646 of *Lecture Notes in Computer Science*, pages 253–267. Springer, 2007.
- Jean-Yves Girard. Light linear logic. *Information and Computation*, 143(2):175–204, 1998.
- Andreas Goerdt. Characterizing complexity classes by higher type primitive recursive definitions. *Theoretical Computer Science*, 100(1):45–66, 1992.
- Erich Grädel, Phokion G. Kolaitis, Leonid Libkin, Maarten Marx, Joel Spencer, Moshe Y. Vardi, Yde Venema, and Scott Weinstein. *Finite Model Theory and its applications*. Springer, 2007.
- Neil D. Jones. The expressive power of higher-order types or, life without cons. *Journal of Functional Programming*, 11(1):55–94, 2001.
- Jean-Louis Krivine. A call-by-name lambda calculus machine. *Higher Order and Symbolic Computation*, 2007. To appear.
- Yves Lafont. Soft linear logic and polynomial time. *Theoretical Computer Science*, 318(1–2):163–180, 2004.
- Daniel Leivant and Jean-Yves Marion. Lambda calculus characterizations of poly-time. In *Proceedings of the Typed Lambda Calculi and Applications, 1st International Conference - TLCA '93*, Utrecht, The Netherlands, March 16–18, 1993, volume 664 of *Lecture Notes in Computer Science*, pages 274–288. Springer, 1993.
- Daniel Leivant and Jean-Yves Marion. Ramified recurrence and computational complexity II: Substitution and poly-space. In *Proceedings of the Computer Science Logic, 8th International Workshop - CSL'94*, Kazimierz, Poland September 25 – 30, 1994, volume 933 of *Lecture Notes in Computer Science*, pages 486–500. Springer, 1994.
- Daniel Leivant and Jean-Yves Marion. Predicative functional recurrence and poly-space. In *Proceedings of the Theory and Practice of Software Development, 7th International Joint Conference - TAPSOFT'97*, volume 1214 of *Lecture Notes in Computer Science*, pages 369–380. Springer-Verlag, 1997.
- François Maurel. Nondeterministic light logics and NP-time. In Martin Hofmann, editor, *Proceedings of the Typed Lambda Calculi and Applications, 6th International Conference - TLCA 2003*, Valencia, Spain, June 10–12, 2003, volume 2701 of *Lecture Notes in Computer Science*, pages 241–255. Springer, 2003.
- Virgile Mogbil and Vincent Rahli. Uniform circuits, & boolean proof nets. In Sergei N. Artemov and Anil Nerode, editors, *Proceedings of the Symposium on Logical Foundations of Computer Science - LFCS'07*, volume 4514 of *Lecture Notes in Computer Science*, pages 401–421. Springer, June 2007.
- Isabel Oitavem. Implicit characterizations of pspace. In *Proceedings of the Proof Theory in Computer Science, International Seminar - PTCS 2001*, Dagstuhl Castle, Germany, October 7–12, 2001, volume 2183 of *Lecture Notes in Computer Science*, pages 170–190. Springer, 2001.
- Simona Ronchi Della Rocca and Luca Roversi. Lambda calculus and intuitionistic linear logic. *Studia Logica*, 59(3), 1997.
- Walter J. Savitch. Relationship between nondeterministic and deterministic tape classes. *Journal of Computer and System Sciences*, 4:177–192, 1970.
- Ulrich Schöpp. Stratified bounded affine logic for logarithmic space. In *Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science - LICS '07*, pages 411–420, Wroclaw, Poland, 2007. IEEE Computer Society.
- Kazushige Terui. Linear logical characterization of polysize functions (extended abstract), 2000. URL <http://citeseer.ist.psu.edu/294754.html>. Unpublished.
- Kazushige Terui. Proof nets and boolean circuits. In *Proceedings of the 19th Annual Symposium on Logic in Computer Science - LICS'04*, pages 266–275, Turku, Finland, 2004. IEEE Computer Society Press.
- Moshe Y. Vardi. Complexity and relational query languages. In *Fourteenth Symposium on Theory of Computing*, pages 137–146. ACM, New York, 1982.