Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

On subexponentials, focusing and modalities in concurrent systems

Vivek Nigam [a,d,*], Carlos Olarte [b,*], Elaine Pimentel [c,*]

[a] Universidade Federal da Paraíba, João Pessoa, Brazil
[b] ECT, Universidade Federal do Rio Grande do Norte, Natal, Brazil
[c] DMAT, Universidade Federal do Rio Grande do Norte, Natal, Brazil
[d] fortiss, Munich, Germany

ARTICLE INFO

Article history:
Received 13 February 2014
Received in revised form 12 June 2017
Accepted 13 June 2017
Available online xxxx
Communicated by D. Sannella

Keywords:
Linear logic
Concurrent constraint programming
Proof systems

ABSTRACT

In this work we present the focused proof system SELLF$^{\textcircled{n}}$, which extends intuitionistic linear logic with subexponentials with the ability of quantifying over them, hence allowing for the use of an arbitrary number of modalities. We show that the view of subexponentials as specific modalities is general enough to give a modular encoding of different flavors of Concurrent Constraint Programming (CCP), a simple and powerful model of concurrency. More precisely, we encode CCP calculi capturing time, spatial and epistemic behaviors into SELLF$^{\textcircled{n}}$, thus providing a proof theoretic foundation for those calculi and, at the same time, setting SELLF$^{\textcircled{n}}$ as a general framework for specifying such systems.

1. Introduction

In order to specify the behavior of distributed agents or the policies governing a distributed system, it is often necessary to reason by using different types of modalities, such as time, space, or even the epistemic state of agents. For instance, the access-control policies of a building might allow Bob to have access only in some pre-defined time, such as its opening hours. Another policy might also allow Bob to ask Alice who has higher credentials to grant him access to the building, or even specify that Bob has only access to some specific rooms of the building. Following this need, many formalisms have been proposed to specify, program and reason about such policies, *e.g.*, Ambient Calculus [1], Concurrent Constraint Programming [2,3], Authorization Logics [4], just to name a few.

Logic and proof theory have often inspired the design of many of these formalisms. For example, Saraswat et al. proposed Concurrent Constraint Programming (CCP) [3,5], a model for concurrency that combines the traditional operational view of process calculi with a declarative view based on logic (see [6] for a survey). Agents in CCP *interact* with each other by *telling* and *asking* information represented as *constraints* to a global store. Later, Fages et al. in [7] proposed Linear Concurrent Constraint (`lcc`), inspired by linear logic [8], to allow the use of linear constraints, that is, tokens of information that, once used by an agent, are removed from the global store.

In order to capture the behavior of distributed systems which take into account spatial, temporal and/or epistemic properties, new formalisms have been proposed. For instance, Saraswat et al. proposed `tcc` [9], which extends CCP with time modalities. Later, Knight et al. [10] proposed a CCP-based language with spatial and epistemic modalities. Some of these developments have also been followed by a similar development in proof theory. For instance, Nigam proposed a

* Corresponding authors.
E-mail addresses: vivek.nigam@gmail.com (V. Nigam), carlos.olarte@gmail.com (C. Olarte), elaine.pimentel@gmail.com (E. Pimentel).

http://dx.doi.org/10.1016/j.tcs.2017.06.009
0304-3975/

framework for linear authorization logics [11], which allows the specification of access control policies that may mention the affirmations, possessions and knowledge of principals. It is also shown in [11] that a wide range of linear authorization policies can be specified in linear logic with subexponentials (SELL) [12,13].

This paper shows that time, spatial, and epistemic modalities can be *uniformly* specified in a single logical framework called SELLF$^{\Uparrow}$. Our first contribution is the introduction of the proof system SELL$^{\Uparrow}$, which extends intuitionistic SELL with universal ($\Uparrow$) and existential ($\Downarrow$) quantifiers over subexponentials. The new quantifiers have a pleasant similarity with the corresponding first-order quantifiers. However, subexponentials in SELL, unlike first-order variables, are organized in a pre-order $\preceq$, which specifies the provability relation among them. This implies that one should be careful on proposing a generalization of such a pre-order, in order to handle subexponential eingenvariables (introduced by the quantifiers) together with constants.

The key step in a standard proof of cut-elimination for first-order logic is showing that a proof Ξ for the sequent $\Gamma \longrightarrow P[e/x]$ can be translated into a proof $\Xi[t/e]$ for the sequent $\Gamma \longrightarrow P[t/e]$, where e is an eingenvariable and t is a term. For the subexponential case, the natural question to be answered is: *what should be the relation between x, e and t so that the substitution can be done?* One trivial answer could be: they should be not related. This collapses the quantification over subexponentials to the discrete case, which can be easily handled by mimicking the approach for first order logics. A more general answer implies proposing a smooth and consistent extension of the usual concept of first order quantification. For that, we decided to use types. Our answer is: you may proceed with the substitutions only in the case that the variables/terms have the same type. More specifically, we considered the quantification over *ideals* of existing subexponentials: we attached to each eingenvariable l_e a type "$l_e : a$" specifying that l_e can be instantiated with any subexponential in the ideal of a. This is sufficient for proving cut-elimination, which guarantees consistency. Surprisingly enough, this also guarantees the smoothness of the extension, since ideals are used in the promotion rule (even if in a hidden way): asking $a \preceq a_i, 1 \leq i \leq n$ is the same as stating that a is in the intersection of the ideals generated by a_i for each i.

With this typing requirement, we can also show that SELL$^{\Uparrow}$ admits a complete focusing discipline [14], giving rise to the focused system SELLF$^{\Uparrow}$.

For our second contribution, we show that subexponentials can be interpreted as spatial, epistemic and temporal modalities, thus providing a framework for specifying concurrent systems with these modalities. This is accomplished by encoding in SELLF$^{\Uparrow}$ different CCP languages, for which the proposed quantifiers play an important role. For instance, they enable the use of an *arbitrary number of subexponentials*, required to model the unbounded nesting of modalities, which is a common feature in epistemic and spatial systems. This does not seem possible in existing logical frameworks such as [15] which do not contain subexponentials nor its quantifiers. Finally, the focusing discipline enforces that the obtained encodings are *faithful* w.r.t. CCP's operational semantics in a strong sense: one operational step matches exactly one logical phase. This is the strongest level of adequacy called adequacy on the level of derivations [16]. Such level of adequacy is not possible for similar encodings of linear CCP systems, such as [7].

Another important feature of our encodings is that by coupling subexponential with a suitable pre-order, it is possible to specify *declaratively* the rules in which agents can manipulate information. For example, an agent cannot see the information contained in a space that she does not have access to. The boundaries are naturally implied by the pre-order of subexponentials.

This work opens a number of possibilities for specifying the behavior of distributed systems. For instance, unlike [10], it seems possible in our framework to handle an infinite number of agents. Moreover, we discuss how linearity of constraints can be straightforwardly included to these systems to represent, *e.g.*, agents that can *update*/*change* the content of the distributed spaces. Also, by changing the underlying subexponential structure, different modalities can be put in the hands of the modelers and programmers. Finally, all the linear logic meta-theory becomes available for reasoning about distributed systems featuring modalities.

Organization. In Section 2 we review the basic proof theory of intuitionistic linear logic and subexponentials (SELL). The system SELL$^{\Uparrow}$, extending SELL with quantification of subexponentials ($\Uparrow$ and $\Downarrow$), is defined in Section 3. We prove that SELL$^{\Uparrow}$ admits cut-elimination. Section 4 discusses SELLF$^{\Uparrow}$, a focused proof system for SELL$^{\Uparrow}$. Section 5 reviews some background on CCP, for which we provide a sound and faithful encoding in SELLF$^{\Uparrow}$. As we shall show, our encoding is modular enough to extend it so to specify new constructs involving modalities, namely, constructs for epistemic (Section 7), spatial (Section 8) and temporal modalities (Section 9). Section 10 concludes the paper.

A preliminary short version of this paper without proofs was published in [17]. In this paper we give many more details and explanations. We also refine several technical details. Moreover, in Section 4, we present at length the focused proof system SELLF$^{\Uparrow}$ that is used in Sections 7, 8 and 9 for proving the adequacy results.

2. Intuitionistic linear logic and subexponentials

Although we assume that the reader is familiar with linear logic, we review some of its basic proof theory (see [18] for more details). Intuitionistic linear logic is a substructural logic proposed by Girard [8], where not all formulas are allowed to be contracted or weakened.

The grammar for formulas in intuitionistic linear logic (without exponentials) is shown below, and the proof rules for the first-order fragment of intuitionistic linear logic without exponentials are depicted in Fig. 1.

Please cite this article in press as: V. Nigam et al., On subexponentials, focusing and modalities in concurrent systems, Theoret. Comput. Sci. (2017), http://dx.doi.org/10.1016/j.tcs.2017.06.009