Games for the Ambient Logic

Anuj Dawar   Philippa Gardner   Giorgio Ghelli

1 Introduction

Spatial logics have been introduced to provide local reasoning about disjoint data structures: the group centering on O'Hearn and Reynolds developed a new program logic (the separation logic) for low-level programs that manipulate RAM data structures, based on the bunched logic of O'Hearn and Pym; the group centering on Cardelli, Gardner and Ghelli developed techniques for analysing and manipulating tree structures (such as XML), based on the ambient logic of Cardelli and Gordon. These logics extend first-order logic with "spatial" connectives and their corresponding adjuncts. The spatial connectives allow us to reason locally about disjoint substructures. The adjuncts are used to obtain weakest pre-conditions for a Hoare logic for updating heaps, and to specify security properties of ambients.

Without adjuncts, validity is undecidable while model-checking is in PSPACE, as happens with standard first-order logic. However, the adjunct operator $\triangleright$ allows validity of a sentence A to be rephrased as the model-checking problem $\mathbf{0} \models \mathsf{T} \triangleright A$. This seems to indicate that adjuncts add a lot of expressive power to the logic. On the contrary, Etienne Lozes recently proved that adjuncts add no expressive power to the static ambient logic (with revelation and without first-order quantification). This result is frankly astonishing. He also proves that the elimination result for the ambient logic with first-order quantification does not hold, which confuses the picture a bit more.

Lozes' proof is complex. In particular, it is not modular with respect to the operators of the logic. This means that it is difficult to understand, or guess, which variants of the logic enjoy the property. In this paper we take a completely different approach. We define Ehrenfeucht-Fraïssé games for the ambient logic, and use the game to provide an intuitive (but formal) explanation of the results, and proofs which are fully modular. Moreover, we significantly extend Lozes results.

First of all, we prove an equality-elimination result, that states that, for the fragment of ambient logic that better corresponds to first-order logic, for any sentence with equality, a corresponding sentence exists that uses no equality, and has the same rank. This is a surprising result, since equality adds significative expressive power to first-order logic. The ability of implicitly declaring inequality constraints is arguably the central feature of spatial logics, and this result formally tells us that this ability is "complete".

We then present a new, modular proof of adjunct elimination for the static ambient logic which provides an intuitive explanation of the phenomenon. We finally show why this proof fails when first-order quantification is added, and provide an intuition for this phenomenon as well.