Adjunct Elimination through Games in Static Ambient Logic

Anuj Dawar

University of Cambridge

joint work with Philippa Gardner and Giorgio Ghelli

FSTTCS, 16 December 2004

Spatial Logic

- Separation Logic (O'Hearn, Reynolds, Yang, Calcagno)

  Properties of Heaps

  $A * B$;

- Ambient Logic (Cardelli, Gordon)

  Properties of mobile ambients

  $\Diamond(\nu n)n[A]$

- Spatial (Static) Ambient Logic (Cardelli, Gordon, Gardner, Ghelli)

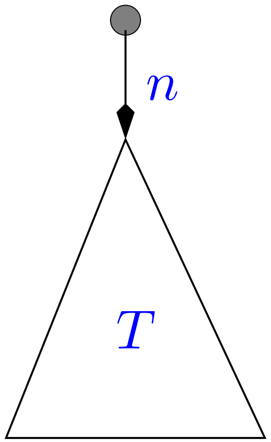
  Properties of trees (and graphs)

  $A|B$;

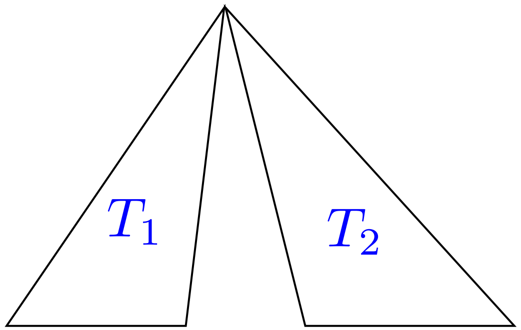
Trees

An algebra for edge-labelled trees where names may be public or private.

$$T ::= 0 \mid n[T] \mid T|T \mid (\nu n)T$$



$n[T]$



$T_1|T_2$

There is a notion of congruence ($T|U \equiv U|T$).

We have *unordered trees*.

Logic

$$A \quad ::= \quad 0 \mid \neg A \mid A \wedge A \mid \mathsf{T} \mid$$
$$\eta[A] \mid A|A \mid \mathsf{H}x.A \mid \copyright\eta$$

$$T \models n[A] \quad \stackrel{\text{def}}{\Leftrightarrow} \quad \exists U.\, T \equiv n[U] \;\wedge\; U \models A$$
$$T \models A|B \quad \stackrel{\text{def}}{\Leftrightarrow} \quad \exists T_1, T_2.\, T \equiv T_1|T_2 \;\wedge\; T_1 \models A \;\wedge\; T_2 \models B$$
$$T \models \mathsf{H}x.A \quad \stackrel{\text{def}}{\Leftrightarrow} \quad \exists n \notin \mathsf{fn}(A), U.\, T \equiv (\nu n)U \wedge U \models\; A\{x \leftarrow n\}$$
$$T \models \copyright n \quad \stackrel{\text{def}}{\Leftrightarrow} \quad n \in \mathsf{fn}(T)$$

Quantification

Contrast the *Hiding quantifier* $\mathsf{H}x.A$ with the existential quantifier $\exists x.A$.

$\exists x \exists y.\ x = y$ is valid.

$\mathsf{H}x\mathsf{H}y.\ x = y$ is always false.

$\exists x\mathsf{H}y.\ x = y$ is always false.

$\mathsf{H}x\exists y.\ x = y$ is true in any tree that contains a private name.

Adjuncts

$A \triangleright B$ an adjunct for $|$

$A@\eta$ an adjunct for $\eta[\cdot]$

$$T \models \quad A \triangleright B \quad \text{if } \forall U.\, U \models A \;\Rightarrow\; T|U \models B.$$

$$T \models \quad A@n \quad \text{if } n[T] \models A.$$

Power of Adjuncts

Without adjuncts

- *validity* is undecidable

  Given A, is it the case that for all T, $T \models A$?

- *model-checking* is in PSPACE

  Given A and T, is it the case that $T \models A$?

With adjuncts, validity reduces to model-checking:

$0 \models \mathsf{T} \triangleright A$ if, and only if, A is valid.

So, model-checking is undecidable.

Adjunct Elimination

Lozes (2003) showed that (a logic essentially equivalent to) static ambient logic admits *adjunct elimination*.

> For every formula with adjuncts, there is a logically equivalent formula without adjuncts.

Since model-checking is undecidable with adjuncts and decidable without, the translation must be uncomputable!

Is it because the logic with adjuncts is more succinct?

> We show it's not!

Alternative Operators

Lozes result was shown for a logic which, in place of H and ⓒ had operators

$$\mathsf{N}x.A \quad \text{and} \quad \eta \circledR A.$$

We show that these are interdefinable with H and ⓒ.

$$\mathsf{H}x.A \quad = \quad \mathsf{N}x.x \circledR A$$

$$\mathsf{N}x.A \quad = \quad \mathsf{H}x.A \wedge \neg ⓒ x$$

Alternative Proof

We provide an alternative proof of Lozes' result based on *Ehrenfeucht-Fraïssé-style games*.

- Gives a more transparent proof of the result.
- Provides a standardised methodology easily adapted to other combinations of operators.
- Refines Lozes' result by showing that there is a *rank-preserving* adjunct elimination.
- Shows that the logic with adjuncts is no more succinct than the one without.

Games

Ehrenfeucht games are played between two players Spoiler and Duplicator on a pair of structures T and U (in our case trees).

Spoiler is attempting to demonstrate that the structures are different.

Duplicator is trying to maintain that the two are the same.

The game is played for a number of rounds fixed in advance.

Game moves correspond to operators in the logic.

First-Order Logic

In the game for first-order logic, the moves correspond to first-order quantification.

At each round i, Spoiler chooses one of the two structures (say U) and selects an element u_i of it. Duplicator must respond with an element t_i of the other structure.

If, at any stage, the partial map $u_i \mapsto t_i$ defined is not a *partial isomorphism*, Spoiler wins.

If Duplicator has a strategy for surviving r rounds, then the two structures are not distinguished by any first-order formula with *quantifier rank* r.

A formula φ that is true in T and false in U describes a strategy for Spoiler to win.

Game Position

For spatial logic, we define a more refined notion of *rank*, that is a tuple of numbers, one for each type of operator.

At any stage, the game position consists of

- two tree T, U;
- f—a partial valuation for the variables; and
- a current rank r.

If, for any operator Op, $r(\text{Op}) > 0$, Spoiler can play an Op-move.

Game Moves

$\_[\cdot]$ *move*:

Spoiler chooses a tree T and an η such that $T \equiv f(\eta)[T']$. If $U \equiv f(\eta)[U']$, the game continues with (T', U'); otherwise, Spoiler wins.

$|$ *move*:

Spoiler chooses, say, T, and two trees T' and T'' such that $T \equiv T'|T''$. Duplicator chooses U' and U'' such that $U \equiv U'|U''$. Spoiler decides whether the game will continue with (T', U'), or with (T'', U'').

Game Moves *(contd.)*

H *move*:

Spoiler chooses, say, T and a name $n \notin \mathsf{fn}(T) \cup \mathsf{fn}(U) \cup \mathit{ran}(f)$, a variable $x \notin \mathit{dom}(f)$, and a tree T' such that $(\nu n)(T') \equiv T$. Duplicator chooses a tree U' such that $(\nu n)(U') \equiv U$. The game continues with $(T', U', (f; x \mapsto n))$.

Adjunct Moves

$\triangleright$ *move*

Spoiler chooses, say, T and a new tree T'; Duplicator chooses a new tree U'. Spoiler decides whether the game will continue with $(T|T', U|U')$ or (T', U').

$@$ *move*

Spoiler chooses a η, and replaces T with $f(\eta)[T]$ and U with $f(\eta)[U]$.

Spoiler Strategy

Why would Spoiler *ever* play an adjunct move?

Spoiler adds a context around the tree T and Duplicator can respond with the identical context around U. This takes Spoiler no closer to winning the game.

If Spoiler has a winning strategy that uses adjunct moves, he also has one without adjunct moves.

There are technical details, but this, in a nutshell, is the game based proof of adjunct elimination.

Quantifiers Revisited

If, instead of the hiding quantifier $\mathsf{H}x.\ A$, we have existential quantification ($\exists x.\ A$) in the language, *adjuncts cannot be eliminated*.

Example (due to Yang) in the paper.

Consider, in general, Spoiler's strategy on the formulas:

$$\exists x.\ (A \triangleright B)$$

$$\mathsf{H}x.\ (A \triangleright B)$$

Composition Lemma

If Duplicator has a winning strategy on the pair (T_1, U_1) and on the pair (T_2, U_2), then she also has a winning strategy on the pair

$$(T_1|T_2, U_1|U_2).$$

This is not true in the presence of $\exists$.

Rank

Our proof actually shows that if Spoiler has a winning strategy *with* adjunct moves, than he has a winning strategy *of the same rank* without adjunct moves.

A formula with adjuncts is equivalent to a formula *of the same rank* without adjuncts.

Though the translation is uncomputable, there isn't an uncomputable blow-up in the size of the formula.

There are only finitely many formulas of a given rank.

Summary

- Adapted Ehrenfeucht-style games to static ambient logic.
- Obtained a transparent proof of Lozes' adjunct elimination result.
- Refined it to a *rank-preserving* adjunct elimination.
- Contrasted H with ∃.
- Studied other combinations of operators for adjunct (or equality elimination.