Separation

Murdoch J Gabbay

Joint work with Joe Wells

Heriot-Watt University, Scotland, 6/3/2006

Work with Joe

My work with Joe has exposed me to a new idea!

(Well, several new ideas, but this one in particular I want to talk about.)

Additive implication

$$\frac{P,\ \Gamma \vdash \Delta,\ Q}{\Gamma \vdash \Delta,\ P \supset Q} \qquad \frac{\Gamma \vdash \Delta,\ P \quad Q,\ \Gamma \vdash \Delta}{P \supset Q,\ \Gamma \vdash \Delta}$$

$\supset$ ‘shares resources’. We always use the same Γ and Δ.

Compare this with. . .

. . . multiplicative implication

$$\frac{P,\ \Gamma \vdash \Delta,\ Q}{\Gamma \vdash \Delta,\ P \multimap Q} \qquad \frac{\Gamma \vdash \Delta,\ P \qquad Q,\ \Gamma' \vdash \Delta'}{P \multimap Q,\ \Gamma, \Gamma' \vdash \Delta, \Delta'}$$

$\multimap$ ‘separates resources’. Look! No sharing!

Interesting because

There seems to be something ‘in the air’ right now about separation.

A standard technique to handle a complex (programming/systems design) problem is:

- break the problem into pieces,
- solve the pieces,
- put the solutions back together.

Much agony results from unforseen interactions in the final step.

Logics with separation

Thus logics such as Bunched Implications, Separation Logic, and Ambient Logic, adopt two implications (and two conjunctions).

One is additive, so we can reason ‘normally’ about ‘truth’.

One is multiplicative, so we can reason in ways which guarantee, in whatever appropriate formal sense, absence of agony.

So we should ask the obvious question:

The obvious question is:

The obvious question!

Is there one implication behind $\supset$ and $\multimap$?

If there is, $\supset$ and $\multimap$ are probably obtained from it by modalities.

(A modality is a connective which transforms predicates to predicates, e.g. $\Box P$ from modal logic, $!P$ from linear logic.)

Semantics

Semantically, additive implication seems to correspond to statements about the entire domain:

$U \vdash P \supset Q$ when if $U \vdash P$ then $U \vdash Q$.

Semantics

Multiplicative implication seems to correspond to splitting the domain:

$$U \vdash P \multimap Q \quad \text{when}$$

$$\text{for all } U' \quad \text{if} \quad U' \vdash P \quad \text{then} \quad U|U' \vdash Q.$$

Here $U|U'$ is some notion of disjoint union for underlying domains, for example:

- Heaps and heap union (separation logic; U is a heap).
- Process $P|P'$ (ambient logic; U is syntax of a process).
- Context union Γ, Γ' (contexts are multisets).
- Abstract semantics (categories).
- Many others.

Another semantics!

Fix $c \in \mathcal{C}$ some countably infinite set of colours.

Write $d \in \mathcal{D}$ for the set of finite sets of colours. Call d data.

Another semantics!

A universe U a rooted tree (possibly infinitely branching and infinitely deep, with unordered daughters) with edges labelled by data.

Write $c \in U$ when c occurs in some label in U.

U has finite support there is some d such that if $c \in U$ then $c \in d$.

Write $\mathcal{U}$ for universes with finite support.

Separation

U has a concrete notion of splitting $U \vert U'$ given by taking subtrees at the root, write this $U \uplus U'$.

Given U_1 and U_2, write $U_1 \uplus U_2$ for the tree obtained by joining U_1 and U_2 at the root.

Operations on sets of universes

Predicates are on universes, so define operations on sets of universes corresponding to the syntax of a logic we give later.

Let $\mathcal{P}, \mathcal{Q}$ vary over sets of universes.

Write $\bot$ for $\{\}$.

As we know, a set of universes is equivalent to a predicate on universes. Then $\bot$ is ‘always false’.

Operations on sets of universes

Write V_{-c} for a copy of V with c added to every label; we may write this V (a ‘green copy of V’; c is understood).

Write V_{+c} for a copy of V with c removed from every label; we may write this V (a ‘red copy of V’).

Write RG_c for the set of universes of the form $V \uplus V$.

Write $RG^{\neg}{}_{c}(\mathcal{P})$ for $\mathcal{P} \cup (\mathcal{U} \setminus RG_c)$.

Operations on sets of universes

Write G_c for the set of universes of the form V_{-c} (that is, V).

Write $G_c(\mathcal{P})$ for $\mathcal{P} \cap G_c$.

Operations on sets of universes

Let $U \in \mathcal{P} \Rightarrow_c \mathcal{Q}$ when:

For every U', if $U' \in \mathcal{P}$ then $U' \uplus U \in \mathcal{Q}$.

Syntax

Predicates are:

$$P, Q ::= P \Rightarrow_c P \;\mid\; \text{И}c.\,P \;\mid\; G_c(P) \;\mid\; R\,G^{\neg}{}_c(P) \;\mid\; \bot \;\mid\; p, q, r.$$

Write $\equiv$ for syntactic equivalence; identify up to binding by И.

p, q, r are atomic propositions.

Interpretation of syntax

Interpret p by $[\![p]\!] = \{U^p\}$, for some $U^p = U^p_{-c}$.

Interpret $\bot$ by $\bot$.

Interpret $P \Rightarrow_c Q$ by $[\![P]\!] \Rightarrow_c [\![Q]\!]$, also $RG^{\neg}{}_c(P)$ by $RG^{\neg}{}_c[\![P]\!]$ and $G_c P$ by $G_c[\![P]\!]$.

$U \in [\![\text{И}c.\ P]\!]$ when $U \in [\![P]\!]$ for some/any $c \notin U$ (‘fresh c’).

RG and $RG^\neg$

Write $RG^\neg{}_c$ for $RG^\neg{}_c(\bot)$.

Lemma 1. $U \in [\![RG^\neg{}_c(P)]\!]$ *holds when* U *is not of the form* $V_{-c} \uplus V_{+c}$ *for any* V.

(That is, $U \neq V \uplus V$.)

Proof. Direct from definition of $\bot$ and $RG^\neg{}_c$. □

Negation

Lemma 2. *If* $U \in [\![P]\!]$ *then* $U \notin [\![\text{И}c.\,(P \Rightarrow_c R\,G^{\neg}{}_c)]\!]$.

Proof. Suppose $U \in [\![P]\!]$. Take any $U' = U'_{-c}$.

If $U' \neq U$ then $U' \uplus U \in [\![R\,G^{\neg}{}_c]\!]$ holds.

If $U' = U$ then $U \in [\![P]\!]$. □

Lemma 3. *If* $U \notin [\![P]\!]$ *then* $U \in [\![\text{И}c.\,(P \Rightarrow_c R\,G^{\neg}{}_c)]\!]$.

Proof. If $U \in [\![P]\!]$ there is nothing to prove unless $U' = U$.

In that case $U \notin [\![P]\!]$. □

Additive implication

Write $\neg P$ for $\text{И}c.\ (P \Rightarrow_c RG^{\neg}{}_c)$.

Write $P \supset Q$ for $\text{И}c.\ (P \Rightarrow_c RG^{\neg}{}_c(Q))$.

By similar calculations we can verify this recovers usual additive implication.

So we can write:

- $P \vee Q$ for $(\neg P) \supset Q$,
- $P \wedge Q$ for $\neg(P \supset \neg Q)$,
- $\top$ for $\bot \supset \bot$, and so on.

Wow!

Multiplicative implication

Write $P \multimap Q$ for $\text{И}c.\,(P \Rightarrow_c G_c(Q))$.

This recovers the usual separating implication.

(Jamie does calculations on the board.)

Conclusions

I have presented a semantics for a simple logic which appears, judging by the semantics, to be able to implement additive and multiplicative implication by means of:

- a И quantifier (the Gabbay-Pitts NEW quantifier),
- two modalities, and
- an implication ‘specialised’ to a particular ‘colour’.

Conclusions

Though this is suggestive, it would be good to formally translate BI into this logic and verify that the derivation rules for BI [”The logic of bunched implications”] are sound (I think they are).

It would be interesting to develop the proof-theory of the logic given here, preferably complete with cut-elimination.

Can we also translate linear logic into this system, and if not, what should we add to it?

Conclusions

This work has independent interest but came out of an attempt to give an abstract account of Wells’s polystar system using (because I’m doing it) Kripke-style semantics.

The trees are obviously Kripke universes, and we now have a novel account of the additive/multiplicative part of polystar.

There’s lots more to polystar, and our semantics given here is designed with this in mind.