Classical BI
(A logic for reasoning about dualising resources)

James Brotherston*  Cristiano Calcagno

Imperial College London

*Me

POPL, Savannah, Georgia
23 Jan 2009
Boolean BI
(*O’Hearn and Pym ’99*)

- A substructural logic with natural resource interpretation.
- Formula connectives:

  *Additive:*  \( \top, \bot, \neg, \land, \lor, \rightarrow \)
  
  *Multiplicative:*  \( \top^*, \ast, \ast \)

- Additives are interpreted *classically.*
Resource models of BBI

• Models of BBI are relational commutative monoids $\langle R, \circ, e \rangle$ (we assume $\circ$ a partial function), where:

  $R$: a set of resources
  $\circ$: a way of (partially) combining resources
  $e$: the distinguished empty resource

• Separation logic is based on a BBI-model of heaps.

• Multiplicative formulas talk about resources $r \in R$:

  $r \models \top^*$ $\iff$ $r = e$
  $r \models F_1 \ast F_2$ $\iff$ $r = r_1 \circ r_2$ and $r_1 \models F_1$ and $r_2 \models F_2$
  $r \models F_1 \rightarrow^* F_2$ $\iff$ $\forall r'. r \circ r'$ defined and $r' \models F_1$ implies $r \circ r' \models F_2$
Our contribution: classical BI (CBI)

- Why aren’t there multiplicative versions of \(\bot, \neg, \lor\)?
- We obtain CBI by adding them to BBI:

  \[
  \text{Additive:} \quad \top \quad \bot \quad \neg \quad \land \quad \lor \quad \rightarrow \\
  \text{Multiplicative:} \quad \top^* \quad \bot^* \quad \sim \quad * \quad \not\lor \quad \not\rightarrow \\
  \]

  and considering multiplicatives to behave classically.
Problems

- Does a logic like CBI even make any sense?
- How do we interpret the new connectives?
- Is there a nice proof theory?
- What are the potential applications?
A CBI-model is given by a tuple $\langle R, \circ, e, -, \infty \rangle$, where:

- $\langle R, \circ, e \rangle$ is a BBI-model;
- $\infty \in R$ and $- : R \to R$;
- for all $r \in R$, $-r$ is the unique solution to $r \circ -r = \infty$.

Natural interpretation: models of dualising resources.
Every Abelian group is a CBI-model (with $\infty = e$).

We interpret $\bot^*$, $\sim$, $\check{\sim}$ as follows:

$$
\begin{align*}
    r \models \bot^* & \iff r \neq \infty \\
    r \models \sim F & \iff -r \nmid F \\
    r \models F_1 \check{\sim} F_2 & \iff r \models \sim(F_1 \ast F_2)
\end{align*}
$$
Example: Personal finance

- Let $\langle \mathbb{Z}, +, 0, - \rangle$ be the Abelian group of integers (money):
- $m \models F$ means “£$m$ is enough to make $F$ true”.
- Let $C / W$ be the formulas “I’ve enough money to buy cigarettes / whisky”.

\[
m \models C * W \iff \text{“£}m\text{ is enough to buy both cigarettes and whisky”}
\]
\[
m \models \sim C \iff \text{“I owe less than the price of a pack of cigarettes”}
\]
\[
m \models C \triangledown W \iff \text{“so long as I don’t spend more than the price of cigarettes, I can definitely still buy whisky”}
\]
Proof theory

- We give a display calculus proof system, $\text{DL}_{\text{CBI}}$, for CBI.
- Display calculi are essentially generalised sequent calculi, with an enriched meta-level.
- Main technical results about $\text{DL}_{\text{CBI}}$:

  **Theorem (Cut-elimination)**
  Any $\text{DL}_{\text{CBI}}$ proof can be transformed into a cut-free proof.

  **Theorem (Soundness)**
  Any $\text{DL}_{\text{CBI}}$-derivable proof judgement is valid.

  **Theorem (Completeness)**
  Any valid proof judgement is $\text{DL}_{\text{CBI}}$-derivable.
Applications of CBI: what cannot be done

Proposition

CBI is a non-conservative extension of BBI. That is, there are formulas of BBI that are valid wrt. CBI but not BBI.

- Separation logic heap model does not extend to a CBI-model.
- Consequence: we cannot (directly) apply CBI reasoning principles such as $F \mathbin{\star} G \equiv \sim F \mathbin{\uparrow} G$ to the heap model.
- Look for applications where resources are naturally dualising.
A CBI-model of financial portfolios

• Let $ID$ be an infinite set of identifiers.
• Let $P$ be the set of portfolios: functions $p : ID \rightarrow \mathbb{Z}$ s.t. $p(x) \neq 0$ for only finitely many $x \in ID$.
• Define composition $+$, involution $-$ and empty portfolio $e$:

  $$(p_1 + p_2)(x) = p_1(x) + p_2(x)$$
  $$(-p)(x) = -p(x)$$
  $$e(x) = 0$$

• $\langle P, +, e, - \rangle$ is an Abelian group, thus also a CBI-model.
Credit crunch solved!

Let $A(x)$ represent a portfolio consisting of asset $x$. Then $\sim \neg A(x)$ represents a portfolio consisting of liability $x$. 
Summary of CBI

Model theory: based on involutive commutative monoids
- multiplicatives are classical
- a non-conservative extension of BBI

Proof theory: a display calculus gives us:
- cut-elimination
- soundness
- completeness

Applications: reasoning about dualising resources, e.g.:
- money;
- permissions;
- bi-abduction.