Classical BI
(A logic for reasoning about dualising resources)

James Brotherston* Cristiano Calcagno

Imperial College London

*Me

Logic seminar
Imperial College London, 13 Nov 2008
BI: the logic of bunched implications
(O’Hearn and Pym ’99)

• A substructural logic with natural resource interpretation.
• BI formula connectives:

  Additive: \( \top \quad \bot \quad \neg \quad \land \quad \lor \quad \to \)

  Multiplicative: \( \top^* \quad * \quad * \quad \times \)

• Two flavours:
  • BI (intuitionistic additives)
  • Boolean BI (classical additives)

• Our main reference point: Boolean BI (BBI).
• Killer application of BBI: separation logic.
Our contribution: classical BI (CBI)

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

  \[
  \text{Additive:} \quad \top \quad \bot \quad \neg \quad \land \quad \lor \quad \rightarrow
  \]

  \[
  \text{Multiplicative:} \quad \top^* \quad \bot^* \quad \sim \quad \ast \quad \triangledown \quad \leftarrow
  \]

  and considering both families to behave classically.

• Are there non-trivial models of CBI?
• How do we interpret the new connectives?
• Is there a nice proof theory?
Part I

Model theory
Algebraic semantics of BBI

• Models of BBI are partial commutative monoids $\langle R, \circ, e \rangle$.
• $\langle R, \circ, e \rangle$ is understood as an abstract model of resource:
  - $R$: a set of resources
  - $\circ$: a way of (partially) combining resources
  - $e$: the distinguished empty resource

• E.g., separation logic model $\langle H, \#, \text{emp} \rangle$, where:
  - $H$: the set of heaps $=_{\text{def}} Var \rightarrow_{\text{fin}} Val$
  - $\#$: domain-disjoint union of heaps
  - $\text{emp}$: the empty heap s.t. $\text{emp}(x)$ undefined all $x \in Var$
Interpreting the BBI connectives

- An environment for $M = \langle R, \circ, e \rangle$ is a map $\rho: \mathcal{V} \rightarrow R$.
- We have the satisfaction relation $r \models F$:

\[
\begin{align*}
    r \models P & \iff r \in \rho(P) \\
    & \vdots \\
    r \models F_1 \land F_2 & \iff r \models F_1 \text{ and } r \models F_2 \\
    & \vdots \\
    r \models \top^* & \iff r = e \\
    r \models F_1 \ast F_2 & \iff r = r_1 \circ r_2 \text{ and } r_1 \models F_1 \text{ and } r_2 \models F_2 \\
    r \models F_1 \Rightarrow F_2 & \iff \forall r'. r \circ r' \text{ defined and } r' \models F_1 \text{ implies } r \circ r' \models F_2
\end{align*}
\]

- A formula $F$ is BBI-valid iff, in every BBI-model $M$, we have $r \models F$ for all $r \in R$ and all environments for $M$. 
A CBI-model is given by a tuple $\langle R, \circ, e, -, \infty \rangle$, where:

- $\langle R, \circ, e \rangle$ is a partial commutative monoid;
- $\infty \in R$ 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.

- Clearly CBI-models are (special) BBI-models.
- Every Abelian group is a CBI-model (with $\infty = e$).
Interpreting the CBI connectives

- **Main problem:** we want $\neg\neg F \equiv F$ but also $F \not\rightarrow \bot * \equiv \neg F$.
- Temporarily define atomic formula $\bowtie$ by:

  $$r \models \bowtie \iff r = \infty$$

- **Key observation:**

  $$\neg r \models F \iff r \models \neg (F \not\rightarrow \neg \bowtie)$$

- Thus we interpret $\bot^*$, $\sim$, $\checkmark$ as follows:

  $$r \models \bot^* \iff r \neq \infty$$

  $$r \models \sim F \iff \neg r \not\models F$$

  $$r \models F_1 \checkmark F_2 \iff \forall r_1, r_2. \neg r \in r_1 \circ r_2 \text{ implies } \neg r_1 \models F_1 \text{ or } \neg r_2 \models F_2$$

- **CBI-validity** is as for BBI.
Some semantic equivalences of CBI

\[ \neg \top \equiv \bot \]
\[ \neg \bot^* \equiv \bot^* \]
\[ \neg \neg F \equiv F \]
\[ F \neg* \bot^* \equiv \neg F \]
\[ \neg \neg F \equiv \neg \neg F \]
\[ F \backwardsvee G \equiv \neg (\neg F \neg* \neg G) \]
\[ F \neg* G \equiv \neg F \backwardsvee G \]
\[ F \neg* G \equiv \neg G \neg* \neg F \]
\[ F \backwardsvee \bot^* \equiv F \]
Example: Personal finance

- Let \( \langle \mathbb{Z}, +, 0, - \rangle \) be the Abelian group of integers.
- View \( m \in \mathbb{Z} \) as money (£):
  - \( m > 0 \): credit
  - \( m < 0 \): debt
- \( m \models F \) means “£\( m \) is enough to make \( F \) true”.
- Let \( C \) be the formula “I’ve enough money to buy cigarettes (£5)” and \( W \) be “I’ve enough to buy whisky (£20)”. So:
  \[
  m \models C \iff m \geq 5 \\
  m \models W \iff m \geq 20
  \]
Example contd.: Personal finance

- \( m \models C \land W \iff m \models C \text{ and } m \models W \iff m \geq 20 \)
  \text{ ”I have enough to buy cigarettes and also to buy whisky”}

- \( m \models C \ast W \iff m = m_1 + m_2 \text{ and } m_1 \models C \text{ and } m_2 \models W \iff m \geq 25 \)
  \text{ ”I have enough to buy both cigarettes and whisky”}

- \( m \models C \rightarrow W \iff \forall m'. m' \models C \text{ implies } m + m' \models W \iff m \geq 15 \)
  \text{ ”if I acquire enough money to buy cigarettes then, in total, I have enough to buy whisky”}
Example contd.: Personal finance

• $m \models \bot^* \iff m \neq 0$
  “I am either in credit or in debt”

• $m \models \neg C \iff -m \not\models C \iff m > -5$
  “I owe less than the price of a pack of cigarettes”

• $m \models C \uparrow W \iff \forall m_1, m_2. -m = m_1 + m_2$
  implies $-m_1 \models C$ or $-m_2 \models W$
  $\iff m \geq 24$

Note that $C \uparrow W \iff \neg C \dashv W \iff \neg W \dashv C$, i.e.:
“if I spend less than the price of a pack of cigarettes,
then I will still have enough money to buy whisky
(and vice versa!)”
Part II

Proof theory
Bunches

- Bunches $\Gamma$ are given by:

$$\Gamma ::= F \mid \emptyset \mid \emptyset \mid \Gamma; \Gamma \mid \Gamma, \Gamma$$

- Bunches represent formulas at the meta-level:

<table>
<thead>
<tr>
<th></th>
<th>Antecedent meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\emptyset$</td>
<td>$\top$</td>
</tr>
<tr>
<td>$\emptyset$</td>
<td>$\bot^*$</td>
</tr>
<tr>
<td>;</td>
<td>$\land$</td>
</tr>
<tr>
<td>,</td>
<td>$*$</td>
</tr>
</tbody>
</table>

- ‘;’ and ‘,’ associative and commutative with units $\emptyset$ resp. $\emptyset$.
- Weakening and contraction hold for ‘;’ but not ‘,’.
- $\Gamma(\Delta)$ is notation for: $\Delta$ is a sub-bunch occurring in $\Gamma$. 


Sequent calculus rules for (B)BI

\[
\frac{\Gamma(F_1; F_2) \vdash F}{\Gamma(F_1 \land F_2) \vdash F} \quad (\land L)
\]

\[
\frac{\Gamma \vdash F \quad \Gamma \vdash G}{\Gamma \vdash F \land G} \quad (\land R)
\]

\[
\frac{\Gamma(F_1, F_2) \vdash F}{\Gamma(F_1 * F_2) \vdash F} \quad (*L)
\]

\[
\frac{\Gamma \vdash F_1 \quad \Delta \vdash F_2}{\Gamma, \Delta \vdash F_1 * F_2} \quad (*R)
\]

\[
\frac{\Delta \vdash F_1 \quad \Gamma(\Delta; F_2) \vdash F}{\Gamma(\Delta; F_1 \rightarrow F_2) \vdash F} \quad (\rightarrow L)
\]

\[
\frac{\Gamma \vdash F_1 \quad \Gamma \vdash F_2}{\Gamma \vdash F_1 \rightarrow F_2} \quad (\rightarrow R)
\]

- **Cut-elimination** holds for BI sequent calculus (Pym 2002).
- For BBI, need to add a rule like:

\[
\frac{\Gamma \vdash \neg\neg F}{\Gamma \vdash F} \quad \text{(RAA)}
\]
**Sequent calculus for CBI**

- **Obvious approach for CBI:** write two-sided sequents $\Gamma \vdash \Delta$ where $\Gamma, \Delta$ are bunches.
- **Natural rules** for the negations:

  \[
  \frac{\Gamma \vdash F; \Delta}{\Gamma; \neg F \vdash \Delta} (\neg L) \quad \frac{\Gamma; F \vdash \Delta}{\Gamma \vdash \neg F; \Delta} (\neg R) \\
  \frac{\Gamma \vdash F, \Delta}{\Gamma, \neg F \vdash \Delta} (\sim L) \quad \frac{\Gamma, F \vdash \Delta}{\Gamma \vdash \neg F, \Delta} (\sim R)
  \]

- **But there are no cut-free proofs** of e.g.

  \[A, (B; \neg B) \vdash C\]

  \[\neg \neg F \vdash \neg \neg F\]

- **Alternative formulation** of rules for negation?
**DL_{CBI}: a display calculus proof system for CBI**

- We give a display calculus à la Belnap for CBI.
- Write consecutions $X \vdash Y$, where $X, Y$ are structures:

  $$X ::= F \mid \emptyset \mid \emptyset \mid \#X \mid \flat X \mid X; X \mid X, X$$

- Here the negations are represented at the meta-level:

<table>
<thead>
<tr>
<th></th>
<th>Antecedent meaning</th>
<th>Consequent meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\emptyset$</td>
<td>$\top$</td>
<td>$\bot$</td>
</tr>
<tr>
<td>$\emptyset$</td>
<td>$\top^*$</td>
<td>$\bot^*$</td>
</tr>
<tr>
<td>$#X$</td>
<td>$\neg$</td>
<td>$\neg$</td>
</tr>
<tr>
<td>$\flat X$</td>
<td>$\sim$</td>
<td>$\sim$</td>
</tr>
<tr>
<td>$X; X$</td>
<td>$\wedge$</td>
<td>$\vee$</td>
</tr>
<tr>
<td>$X, X$</td>
<td>$\ast$</td>
<td>$\ast$</td>
</tr>
</tbody>
</table>
Proof rules for $DL_{CBI}$

Three types of proof rules:

1. **display postulates** allowing structures to be shuffled:

   \[
   X; Y \vdash Z \quad \vdash Y \Rightarrow X \quad Y \vdash \#X
   \]

2. **left- and right-introduction** rules for each logical connective:

   \[
   X \vdash F \quad G \vdash Y \quad (\rightarrow L) \\
   F \rightarrow G \vdash bX, Y \quad X, F \vdash G \quad (\rightarrow R)
   \]

3. **structural rules** governing the structural connectives:

   \[
   W; (X; Y) \vdash Z \quad (AAL) \\
   (W; X); Y \vdash Z \quad X \vdash Z \quad (WkR) \\
   X \vdash Y, \emptyset \quad X \vdash Y \quad (MIR)
   \]
Results about $DL_{CBI}$

Easy consequence of the fact that $DL_{CBI}$ is a display calculus:

*Theorem (Cut-elimination)*

Any $DL_{CBI}$ proof of $X \vdash Y$ can be transformed into a cut-free proof of $X \vdash Y$.

Main technical results:
(NB. Validity for formulas extends easily to consecutions.)

*Theorem (Soundness)*

Any $DL_{CBI}$-derivable consecution is valid.

*Theorem (Completeness)*

Any valid consecution is $DL_{CBI}$-derivable.
Part III

Applications
Proposition

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

Basic reason: in CBI-models \( \langle R, \circ, e, -, \infty \rangle \) we have:

\[
 r \models \neg \top^* \neg^* \bot \Rightarrow r = \infty
\]

whereas in BBI-models there can be more than one such \( r \).

Consequence: we cannot (directly) apply CBI reasoning principles such as \( F \neg^* G \equiv \neg F \nabla G \) to BBI models (e.g. separation logic heap model).
A CBI-model of financial portfolios

- Let $ID$ be an infinite set of identifiers.
- Let $P$ be the set of portfolios: functions $p : ID \to \mathbb{Z}$ 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.
Elementary assets and liabilities

• Let \( \text{dom}(p) = \{ x \in ID \mid p(x) \neq 0 \} \).

• Define atomic formula \( A(x) \) by:

\[
p \models A(x) \iff \text{dom}(p) = \{ x \} \text{ and } p(x) > 0
\]

i.e. \( A(x) \) holds of portfolios containing only an asset \( x \).

• Then we have:

\[
p \models \sim \neg A(x) \iff \neg p \models A(x)
\]

\[
\iff \text{dom}(p) = \{ x \} \text{ and } p(x) < 0
\]

i.e. \( \sim \neg A(x) \) holds of portfolios having only a liability \( x \).
Representing financial derivatives

- **Put option**: the right to sell asset \( x \) for price \( y \):
  \[
  A(x) \rightarrow* A(y)
  \]

- **Call option**: the right to buy asset \( x \) for price \( y \).
  \[
  A(y) \rightarrow* A(x)
  \]

- **Credit default swap**: premium \( y \) for a payout of \( x \) in the event of a default \( D \)
  \[
  \sim \neg A(y) \ast (D \rightarrow A(x))
  \]
Consider writing Hoare triples $\{P_1\}T\{P_2\}$ where $P_1$, $P_2$ are “symbolic portfolios” and $T$ is a structured trade.

**Verification problem:** given $P_1$, $T$, $P_2$, check that $\{P_1\}T\{P_2\}$.

**Planning problem:** given $P_1$, $P_2$, find $T$ s.t. $\{P_1\}T\{P_2\}$.

**Weakest precondition problem:** given $T$, $P_2$, find the weakest $P_1$ s.t. $\{P_1\}T\{P_2\}$.

**Strongest postcondition problem:** given $P_1$, $T$, find the strongest $P_2$ s.t. $\{P_1\}T\{P_2\}$. 
Summary of CBI

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

Proof theory: display logic gives us:
- cut-elimination
- soundness
- completeness

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