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:	$\top$	$\bot$	$\neg$	$\wedge$	$\vee$	$\rightarrow$
Multiplicative:	$\top^*$			$*$		$-\!\!*$

- 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 $\bot, \neg, \vee$?
- We obtain CBI by adding them to BBI:

Additive:	$\top$	$\bot$	$\neg$	$\wedge$	$\vee$	$\rightarrow$
Multiplicative:	$\top^*$	$\bot^*$	$\sim$	$*$	$\overset{*}{\vee}$	$-\!\!*$

  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 $\langle H, \sharp, \mathrm{emp} \rangle$, where:

  H: the set of heaps $=_{\mathrm{def}} Var \rightharpoonup_{\mathrm{fin}} Val$

  $\sharp$: domain-disjoint union of heaps

  emp: the empty heap s.t. $\mathrm{emp}(x)$ undefined all $x \in Var$

Interpreting the BBI *connectives*

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

$$
\begin{array}{rcl}
r \models P & \Leftrightarrow & r \in \rho(P) \\
 & \vdots & \\
r \models F_1 \wedge F_2 & \Leftrightarrow & r \models F_1 \text{ and } r \models F_2 \\
 & \vdots & \\
r \models \top^* & \Leftrightarrow & r = e \\
r \models F_1 * F_2 & \Leftrightarrow & r = r_1 \circ r_2 \text{ and } r_1 \models F_1 \text{ and } r_2 \models F_2 \\
r \models F_1 \mathrel{-\!\!*} F_2 & \Leftrightarrow & \forall r'.\ r \circ r' \text{ defined and } r' \models F_1 \text{ implies } r \circ r' \models F_2
\end{array}
$$

- 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.

Dualising resource models of CBI

- 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 $\sim\sim F \equiv F$ but also $F \mathrel{-\!\!*} \bot^* \equiv \sim F$.
- Temporarily define atomic formula $\bowtie$ by:

$$r \models \bowtie \;\Leftrightarrow\; r = \infty$$

- Key observation:

$$-r \models F \;\Leftrightarrow\; r \models \neg(F \mathrel{-\!\!*} \neg\bowtie)$$

- Thus we interpret $\bot^*, \sim, \mathbin{\overset{*}{\vee}}$ as follows:

$$\begin{array}{rcl} r \models \bot^* & \Leftrightarrow & r \neq \infty \\ r \models \sim F & \Leftrightarrow & -r \not\models F \\ r \models F_1 \mathbin{\overset{*}{\vee}} F_2 & \Leftrightarrow & \forall r_1, r_2.\ -r \in r_1 \circ r_2 \text{ implies } -r_1 \models F_1 \text{ or } -r_2 \models F_2 \end{array}$$

- CBI-validity is as for BBI.

Some semantic equivalences of CBI

$$
\begin{aligned}
{\sim}\top &\equiv \bot \\
{\sim}\top^* &\equiv \bot^* \\
{\sim}{\sim}F &\equiv F \\
F \mathrel{-\!\!*} \bot^* &\equiv {\sim}F \\
\neg{\sim}F &\equiv {\sim}\neg F \\
F \overset{*}{\vee} G &\equiv {\sim}({\sim}F * {\sim}G) \\
F \mathrel{-\!\!*} G &\equiv {\sim}F \overset{*}{\vee} G \\
F \mathrel{-\!\!*} G &\equiv {\sim}G \mathrel{-\!\!*} {\sim}F \\
F \overset{*}{\vee} \bot^* &\equiv F
\end{aligned}
$$

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:

$$\begin{aligned} m \models C \quad &\Leftrightarrow \quad m \geq 5 \\ m \models W \quad &\Leftrightarrow \quad m \geq 20 \end{aligned}$$

Example contd.: Personal finance

- $m \models C \wedge W \iff m \models C \text{ and } m \models W$
  $\iff m \geq 20$
  "I have enough to buy cigarettes and also to buy whisky"

- $m \models C * W \iff m = m_1 + m_2 \text{ and } m_1 \models C \text{ and } m_2 \models W$
  $\iff m \geq 25$
  "I have enough to buy both cigarettes and whisky"

- $m \models C \mathrel{-\!\!*} W \iff \forall m'.\, m' \models C \text{ implies } m + m' \models W$
  $\iff m \geq 15$
  "if I acquire enough money to buy cigarettes then, in total, I have enough to buy whisky"

Example contd.: Personal finance

- $$m \models \bot^* \quad \Leftrightarrow \quad m \neq 0$$
  "I am either in credit or in debt"

- $$m \models {\sim}C \quad \Leftrightarrow \quad -m \not\models C \;\Leftrightarrow\; m > -5$$
  "I owe less than the price of a pack of cigarettes"

- $$m \models C \mathbin{\overset{*}{\vee}} W \quad \Leftrightarrow \quad \forall m_1, m_2.\ -m = m_1 + m_2 \text{ implies } -m_1 \models C \text{ or } -m_2 \models W \quad \Leftrightarrow \quad m \geq 24$$

Note that $C \mathbin{\overset{*}{\vee}} W \Leftrightarrow {\sim}C \mathrel{-\!\!*} W \Leftrightarrow {\sim}W \mathrel{-\!\!*} C$, 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 Γ are given by:

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

- Bunches represent formulas at the meta-level:

	Antecedent meaning
$\emptyset$	$\top$
$\varnothing$	$\top^*$
;	$\wedge$
,	$*$

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

Sequent calculus rules for (B)BI

$$\frac{\Gamma(F_1; F_2) \vdash F}{\Gamma(F_1 \wedge F_2) \vdash F}\ (\wedge\mathrm{L}) \qquad \frac{\Gamma \vdash F \quad \Gamma \vdash G}{\Gamma \vdash F \wedge G}\ (\wedge\mathrm{R})$$

$$\frac{\Gamma(F_1, F_2) \vdash F}{\Gamma(F_1 * F_2) \vdash F}\ ({*}\mathrm{L}) \qquad \frac{\Gamma \vdash F_1 \quad \Delta \vdash F_2}{\Gamma, \Delta \vdash F_1 * F_2}\ ({*}\mathrm{R})$$

$$\frac{\Delta \vdash F_1 \quad \Gamma(\Delta; F_2) \vdash F}{\Gamma(\Delta; F_1 \to F_2) \vdash F}\ (\to\mathrm{L}) \qquad \frac{\Gamma; F_1 \vdash F_2}{\Gamma \vdash F_1 \to F_2}\ (\to\mathrm{R})$$

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

$$\frac{\Gamma \vdash \neg\neg F}{\Gamma \vdash F}\ (\mathrm{RAA})$$

Sequent calculus for CBI

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

$$\frac{\Gamma \vdash F; \Delta}{\Gamma; \neg F \vdash \Delta}\,(\neg\mathrm{L}) \qquad \frac{\Gamma; F \vdash \Delta}{\Gamma \vdash \neg F; \Delta}\,(\neg\mathrm{R})$$

$$\frac{\Gamma \vdash F, \Delta}{\Gamma, {\sim}F \vdash \Delta}\,({\sim}\,\mathrm{L}) \qquad \frac{\Gamma, F \vdash \Delta}{\Gamma \vdash {\sim}F, \Delta}\,({\sim}\,\mathrm{R})$$

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

$$A, (B; \neg B) \vdash C$$

$${\sim}\neg F \vdash \neg{\sim}F$$

- Alternative formulation of rules for negation?

$\mathrm{DL_{CBI}}$: *a display calculus proof system for* CBI

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

$$X ::= F \mid \emptyset \mid \varnothing \mid \sharp X \mid \flat X \mid X ; X \mid X , X$$

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

	Antecedent meaning	Consequent meaning
$\emptyset$	$\top$	$\bot$
$\varnothing$	$\top^*$	$\bot^*$
$\sharp$	$\neg$	$\neg$
$\flat$	$\sim$	$\sim$
;	$\wedge$	$\vee$
,	$*$	$\overset{*}{\vee}$

Proof rules for $\mathrm{DL}_{\mathrm{CBI}}$

Three types of proof rules:

1. display postulates allowing structures to be shuffled:

$$\frac{X ; Y \vdash Z}{X \vdash \sharp Y ; Z} \qquad \frac{X \vdash Y}{\sharp Y \vdash \sharp X}$$

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

$$\frac{X \vdash F \quad G \vdash Y}{F \mathrel{-\!\!*} G \vdash \flat X , Y}\ (\mathrel{-\!\!*}\mathrm{L}) \qquad \frac{X , F \vdash G}{X \vdash F \mathrel{-\!\!*} G}\ (\mathrel{-\!\!*}\mathrm{R})$$

3. structural rules governing the structural connectives:

$$\frac{W ; (X ; Y) \vdash Z}{(W ; X) ; Y \vdash Z}\ (\mathrm{AAL}) \qquad \frac{X \vdash Z}{X \vdash Y ; Z}\ (\mathrm{WkR}) \qquad \frac{X \vdash Y , \varnothing}{X \vdash Y}\ (\mathrm{MIR})$$

Results about $\mathrm{DL}_{\mathrm{CBI}}$

Easy consequence of the fact that $\mathrm{DL}_{\mathrm{CBI}}$ is a display calculus:

Theorem (Cut-elimination)

Any $\mathrm{DL}_{\mathrm{CBI}}$ *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 $\mathrm{DL}_{\mathrm{CBI}}$*-derivable consecution is valid.*

Theorem (Completeness)

Any valid consecution is $\mathrm{DL}_{\mathrm{CBI}}$*-derivable.*

Part III

Applications

What can be done in theory?

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:

$$r \models \neg\top^* \mathrel{-\!\!*} \bot \;\; \Rightarrow \;\; r = \infty$$

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

Consequence: we cannot (directly) apply CBI reasoning principles such as $F \mathrel{-\!\!*} G \equiv {\sim}F \mathbin{\overset{*}{\vee}} G$ to BBI models (e.g. separation logic heap model).

A CBI-*model of financial portfolios*

- Let ID be an infinite set of identifers.
- 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:

$$\begin{aligned}(p_1 + p_2)(x) &= p_1(x) + p_2(x) \\ (-p)(x) &= -p(x) \\ e(x) &= 0\end{aligned}$$

- $\langle P, +, e, - \rangle$ is an Abelian group, thus also a CBI-model.

Elementary assets and liabilities

- Let $dom(p) = \{x \in ID \mid p(x) \neq 0\}$.
- Define atomic formula $A(x)$ by:

$$p \models A(x) \;\; \Leftrightarrow \;\; dom(p) = \{x\} \text{ and } p(x) > 0$$

  i.e. $A(x)$ holds of portfolios containing only an asset x.
- Then we have:

$$\begin{aligned} p \models {\sim}\neg A(x) \;\; &\Leftrightarrow \;\; -p \models A(x) \\ &\Leftrightarrow \;\; dom(p) = \{x\} \text{ and } p(x) < 0 \end{aligned}$$

  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:

$$A(x) \multimap A(y)$$

- Call option: the right to buy asset x for price y.

$$A(y) \multimap A(x)$$

- Credit default swap: premium y for a payout of x in the event of a default D

$$\sim\neg A(y) * (D \to A(x))$$

Hoare logic for finance?

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.