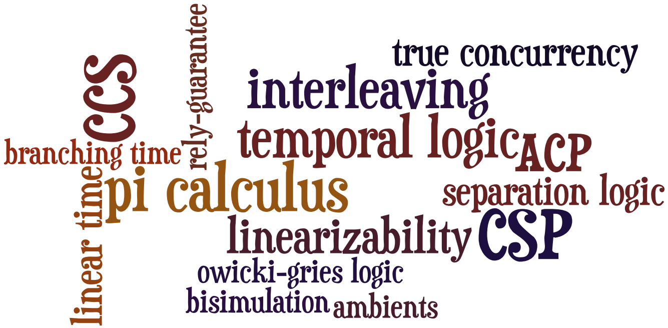
Algebra, Logic, Locality, Concurrency

Peter O'Hearn

ongoing joint work with CAR Hoare, A Hussain, B Möller, RL Petersen, G Struth

Talk Presented at APLAS and CPP
Kenting, Taiwan, 7 December 2011

Diversity in theory of concurrency



Wouldn't it be nice if we had a theory of concurrency that was

- based on a few simple axioms
- satisfied by some diverse models
- and where the axioms implied
  some substantial consequences

Wouldn't it be nice if we had a theory of concurrency that was

- based on a few simple axioms
- satisfied by some diverse models
- and where the axioms implied
  some substantial consequences

- Disclaimer: 'some' because 'all' is unrealistic as of yet: we are not in a position for a 'grand unified theory'... but will try for 'some' and see what we can do.

Wouldn't it be nice if we had a theory of concurrency that was

- based on a few simple axioms
- satisfied by some diverse models
- and where the axioms implied
  some substantial consequences

- Disclaimer: 'some' because 'all' is unrealistic as of yet: we are not in a position for a 'grand unified theory'... but will try for 'some' and see what we can do.
- This talk describes work in progress. Some parts are solid, others we are working on or are potential applications. I will say which as we go along.

Minimalist theory

- A single poset $M, \sqsubseteq$ equipped with two structures:
  - ordered commutative monoid $(\|, \textsf{nothing})$, and
  - an ordered monoid $(;, \textsf{skip})$
- ...

Example
Linearly-ordered model: The Interleaving Model

- We define $M, \sqsubseteq, \mathit{parallel}, \mathit{nothing}, \mathbf{;}, \mathsf{skip}$.
- $M = \mathcal{P}(E^*)$, for a given set E of events. $\sqsubseteq = \subseteq$
- $\mathsf{nothing} = \mathsf{skip} = \{\epsilon\}$
- For $P, Q \subseteq E^*$, define

$$\begin{aligned} P \parallel Q &= \{t \mid \exists t_P \in P, t_Q \in Q \,.\, t \in \mathit{interleave}(t_P, t_Q)\} \\ P \mathbf{;} Q &= \{t \mid \exists t_P \in P, t_Q \in Q.\, t = t_P t_Q\} \end{aligned}$$

Example
Partially-ordered model: the Tracelet Model (aka Tony graphs)

- Start with a partially ordered set $E, \leq$. $M = \mathcal{P}(\mathcal{P}(E))$. Think of $e_1 \leq e_2'$ as 'e_2 depends on e_1'.
- For $X, Y \subseteq E$, define $X \preceq Y$ to mean that nothing in X depends on anything in Y. I.e., $\forall e_X \in X,\ e_Y \in Y.\ e_X \not\leq e_Y$.
- For $p, q \subseteq \mathcal{P}(E)$, define

$$
\begin{aligned}
p \parallel q &= \{X \uplus Y \mid X \in p,\ Y \in q,\ X \cap Y = \emptyset\} \\
p\, ;\, q &= \{X \uplus Y \mid X \in p,\ Y \in q,\ X \cap Y = \emptyset,\ X \preceq Y\}
\end{aligned}
$$

I Wehrman, CAR Hoare, PW O'Hearn: Graphical models of separation logic. Inf. Process. Lett. 109(17): 1001-1004 (2009)

T Hoare, BMöller, G Struth, I Wehrman: Concurrent Kleene Algebra and its Foundations. J. Log. Algebr. Program. 80(6): 266-296 (2011)

Other models

- The pomset model (Pratt, Gischer). Sets of pomsets. $P; Q$ is (lifting of) strong sequential composition (everything in P precedes everything in Q), $\|$ is disjoint concurrency (no dependence).
- The fair interleaving model. Finite and infinite sequences, $\|$ is lifting of fair parallel composition.
- Failures/divergences model of CSP.
- ...

Minimalist theory

- A single poset $M, \sqsubseteq$ equipped with two structures:
  - ordered commutative monoid $(\|, \text{nothing})$, and
  - an ordered monoid $(\mathbf{;}, \text{skip})$
- ...

Minimalist theory

- A single poset $M, \sqsubseteq$ equipped with two structures:
  - ordered commutative monoid $(\|, \mathsf{nothing})$, and
  - an ordered monoid $(;, \mathsf{skip})$
- ...
- Even before completing ..., we start to develop a bit of program logic

The historic triple

- The historic triple $\{p\}\, c\, \{q\}$ is defined by

$$\{p\}\, c\, \{q\} \;\Leftrightarrow\; p; c \sqsubseteq q$$

  for p, c, q all elements of M.

- Consequence and sequencing rules of Hoare logic follow, interpreting entailment as $\sqsubseteq$

$$\frac{p' \sqsubseteq p \qquad p\,;c \sqsubseteq q \qquad q \sqsubseteq q'}{p'\,;c \sqsubseteq q'}$$

$$\frac{p\,;c_1 \sqsubseteq q \qquad q\,;c_2 \sqsubseteq r}{p\,;c_1\,;c_2 \sqsubseteq r}$$

The historic triple

- The historic triple $\{p\}\, c\, \{q\}$ is defined by

$$\{p\}\, c\, \{q\} \;\Leftrightarrow\; p; c \sqsubseteq q$$

  for p, c, q all elements of M.
- Suppose a pre or post represents 'traces up until now'. Then $\{p\}\, c\, \{q\}$ means

  q accounts for (overapproximates) the immediate past p followed by c.

A potential use of the historic triple

- In work with Rinetzky and others we have been looking at highly-concurrent optimistic algorithms.
- In the case of a 'set' algorithm, the remarkable wait free traversal is the hardest operation to prove
- We do it by reasoning about the past, via a 'Hindsight lemma':

  any pointer link encountered in a list traversal was reachable from the head node sometime in the past, since the traversal started.

- No program logic as of PODC'10: We are working on formalization via historic triples.

PW O'Hearn, N Rinetzky, MT Vechev, E Yahav, G Yorsh: Verifying linearizability with hindsight. PODC 2010: 85-94

Slide courtesy of Noam Rinetzky

3. Hindsight

(no need for linearization: existence of past state)

```
bool contains(int k) {

    p,c=LOCATE(k);
    return (c.k==k)

}
```

```
LOCATE(k)
  p = H;
  c = H.n
  while (c.k < k) {
    p = c;
    c = p.n;
  }
```

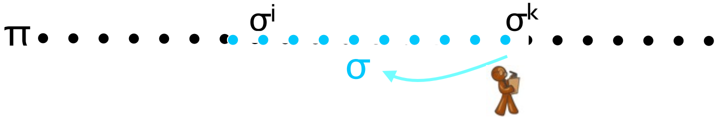
Slide courtesy of Noam Rinetzky

Hindsight Lemma

If $\pi \models \varphi$

$\sigma^i \models \varphi^i$

$\sigma^k \models \varphi^k$



then $\exists\ \sigma \in [\sigma^i \ldots \sigma^k]: \quad \sigma \models \psi$

Futuristic triples

- The futuristic interpretation of triples $\{p\}\,c\,\{q\}$ is defined by

$$\{p\}\,c\,\{q\} \;\Leftrightarrow\; p \sqsupseteq c\,;q$$

Suppose a pre or post represents 'traces into the future'.
Then $\{p\}\,c\,\{q\}$ means

p accounts for (overapproximates) what c might do followed by q.

Futuristic triples

- The futuristic interpretation of triples $\{p\}\, c\, \{q\}$ is defined by

$$\{p\}\, c\, \{q\} \;\Leftrightarrow\; p \sqsupseteq c \,;\, q$$

  Suppose a pre or post represents 'traces into the future'.
  Then $\{p\}\, c\, \{q\}$ means

  > *p accounts for (overapproximates) what c might do followed by q.*

- Example (probable): Singularity OS has a concept of 'contract' in which preconditions and postconditions describe message passing protocols into the future.
- Formalized (Villard) with communicating automata + separation logic

---

M Fähndrich et. al.: Language support for fast and reliable message-based communication in singularity OS. EuroSys 2006: 177-190

J Villard: Heaps and Hops. Thèse de doctorat, ÉNS de Cachan, 2011

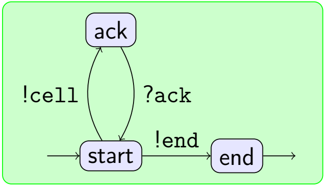
Slide courtesy of Jules Villard

Specs for List Passing

```
message cell [val ↦ –]
message ack [emp]
message endpoint [val ↦ep (L{end}) ∧ val = src]

put(e,x) [e ↦ep (L{start}) ∗ list(x)] {
  local t;
  while(x != 0)
  [e ↦ep (L{start}) ∗ list(x)] {
    t = x->tl;
    send(cell,e,x);
    x = t;
    // e ↦ep (L{ack}) ∗ list(x)
    receive(ack,e);
  }
  send(endpoint,e,e);
} [emp]
```

L



So far...

- Trivial axioms (two ordered monoids), some particular models, and two unusual interpretations of pre/post specs.
- What we have is too little (just monotonicity, associativity...), and there are no axioms linking $\|$ and $;$.
- On our way to program logic, but we need more...

Minimalist theory

- A single poset $M, \sqsubseteq$ equipped with two structures:
  - ordered commutative monoid $(\|, \mathsf{nothing})$, and
  - an ordered monoid $(\mathbf{;}, \mathsf{skip})$

Minimalist theory

- A single poset $M, \sqsubseteq$ equipped with two structures:
  - ordered commutative monoid $(\|, \mathsf{nothing})$, and
  - an ordered monoid $(;, \mathsf{skip})$
- satisfying the exchange law

$$(p\|r);(q\|s) \sqsubseteq (p;q)\|(r;s)$$

- ...

Inequational exchange law emphasized by Hoare (2008-), mentioned before in concurrency by Gischer'88, Bloom-Ésik'95

Exchange law in Interleaving model

- exchange law: $(p \| r);(q \| s) \sqsubseteq (p;q) \| (r;s)$
- Writing a trace t for the singleton $\{t\}$, an instance is

$$(aa \| b);(cc \| d) \sqsubseteq (aa;cc) \| (b;d)$$

Then, for example,

$$aba \in interleave(aa, b) \text{ and } cdc \in interleave(cc, d)$$

Clearly $abacdc \in interleave(aacc, bd)$.

Exchange law in Interleaving model

- exchange law: $(p \| r) ; (q \| s) \sqsubseteq (p ; q) \| (r ; s)$
- Writing a trace t for the singleton $\{t\}$, an instance is

$$(aa \| b) ; (cc \| d) \sqsubseteq (aa ; cc) \| (b ; d)$$

  Then, for example,

$$aba \in \mathit{interleave}(aa, b) \text{ and } cdc \in \mathit{interleave}(cc, d)$$

  Clearly $abacdc \in \mathit{interleave}(aacc, bd)$.

- The reverse inclusion does not hold:

$$aaccbd \in (aa ; cc) \| (b ; d)$$
$$\text{but}$$
$$aaccbd \notin (aa \| b) ; (cc \| d)$$

  so we cannot have the *equational* exchange law.

Exchange in Tracelet model

- Recall: $X \preceq Y$ means that nothing in X depends on anything in Y.
- For $p, q \subseteq \mathcal{P}(E)$, define

$$\begin{aligned} p \parallel q &= \{X \uplus Y \mid X \in p,\ Y \in q,\ X \cap Y = \emptyset\} \\ p\,;q &= \{X \uplus Y \mid X \in p,\ Y \in q,\ X \cap Y = \emptyset,\ X \preceq Y\} \end{aligned}$$

- Special case of exchange law ,

$$(X_1 \parallel Y_1);(X_2 \parallel Y_2) \sqsubseteq (X_1;X_2) \parallel (Y_1;Y_2)$$

boils down to

$$X_1 \uplus Y_1 \preceq X_2 \uplus Y_2 \ \Rightarrow\ \begin{array}{c} X_1 \preceq X_2 \\ \wedge \\ Y_1 \preceq Y_2 \end{array}$$

A negative example: fair $\|$ with subset order

- Consider finite and infinite traces with $\|$ being fair parallel composition.
- Without giving a definition of fairness, let us just assume that any trace of $a^\omega \| t$ for t finite *must* include all of t, and that $tt' = t$ if t is infinite.

A negative example: fair $\|$ with subset order

- Consider finite and infinite traces with $\|$ being fair parallel composition.
- Without giving a definition of fairness, let us just assume that any trace of $a^\omega \| t$ for t finite *must* include all of t, and that $tt' = t$ if t is infinite.
- exchange law: $(p \| r);(q \| s) \sqsubseteq (p;q) \| (r;s)$

A negative example: fair $\|$ with subset order

- Consider finite and infinite traces with $\|$ being fair parallel composition.
- Without giving a definition of fairness, let us just assume that any trace of $a^\omega \| t$ for t finite *must* include all of t, and that $tt' = t$ if t is infinite.
- exchange law: $(p \| r);(q \| s) \sqsubseteq (p;q) \| (r;s)$
- Then

$$(a^\omega \| b);(c \| d) \not\sqsubseteq (a^\omega;c) \| (b;d)$$

because

$$ba^\omega \in (a^\omega \| b);(c \| d)$$

but it doesn't include a d, so

$$ba^\omega \notin (a^\omega;c) \| (b;d)$$

A negative example: fair $\|$ with subset order

- Consider finite and infinite traces with $\|$ being fair parallel composition.
- Without giving a definition of fairness, let us just assume that any trace of $a^\omega \| t$ for t finite *must* include all of t, and that $tt' = t$ if t is infinite.
- exchange law: $(p \| r);(q \| s) \sqsubseteq (p;q) \| (r;s)$
- Then
$$(a^\omega \| b);(c \| d) \not\sqsubseteq (a^\omega;c) \| (b;d)$$
because
$$ba^\omega \in (a^\omega \| b);(c \| d)$$
but it doesn't include a d, so
$$ba^\omega \notin (a^\omega;c) \| (b;d)$$
- I attach no deep significance to this, but am just illustrating that our theory covers 'some' but not 'all' models of interest.

Exchange and logic: Locality on the cheap

- Historic triples $(\{p\}\, c\, \{q\} \;\Leftrightarrow\; p; c \sqsubseteq q)$

$$\dfrac{\dfrac{p_1\,;c_1 \sqsubseteq q_1 \qquad p_2\,;c_2 \sqsubseteq q_2}{(p_1; c_1) \parallel (p_2\,;c_2) \sqsubseteq q_1 \parallel q_2}\ \parallel\ \textit{Monotone}}{(p_1 \parallel p_2)\,;(c_1 \parallel c_2) \sqsubseteq q_1 \parallel q_2}\ \textit{Exchange}$$

Exchange and logic: Locality on the cheap

- Historic triples $(\{p\}\, c\, \{q\} \;\Leftrightarrow\; p; c \sqsubseteq q)$

$$\cfrac{\cfrac{p_1 \,;\, c_1 \sqsubseteq q_1 \qquad p_2 \,;\, c_2 \sqsubseteq q_2}{(p_1 ; c_1) \parallel (p_2 \,;\, c_2) \sqsubseteq q_1 \parallel q_2} \parallel \textit{ Monotone}}{(p_1 \parallel p_2)\,;(c_1 \parallel c_2) \sqsubseteq q_1 \parallel q_2} \textit{ Exchange}$$

- If we squint, this is the concurrency rule of concurrent separation logic

$$\frac{\{P_1\}\, C_1\, \{Q_1\} \quad \{P_2\}\, C_2\, \{Q_2\}}{\{P_1 * P_2\}\, C_1 \| C_2\, \{Q_1 * Q_2\}}$$

- And similar works for futuristic triples.

A CSL example: Parallel Mergesort

$\{array(a, i, j)\}$
$\texttt{procedure ms}(a, i, j)$
$\texttt{newvar } m := (i + j)/2;$
$\texttt{if } \; i < j \texttt{ then}$
$\quad \big(\texttt{ms}(a, i, m) \; \| \; \texttt{ms}(a, m+1, j)\big);$
$\quad \texttt{merge}(a, i, m+1, j);$
$\{sorted(a, i, j)\}$

Main part of proof:

$$\{array(a, i, m) * array(a, m+1, j)\}$$

$$\begin{array}{lcl} \{array(a, i, m)\} & & \{array(a, m+1, j)\} \\ \texttt{ms}(a, i, m) & \| & \texttt{ms}(a, m+1, j) \\ \{sorted(a, i, m)\} & & \{sorted(a, m+1, j)\} \end{array}$$

$$\{sorted(a, i, m) \; * \; sorted(a, m+1, j)\}$$

Concurrency and Frame rules are linked

- Concurrency and Frame rules from SL

$$\frac{\{P_1\}\, C_1\, \{Q_1\} \quad \{P_2\}\, C_2\, \{Q_2\}}{\{P_1 * P_2\}\, C_1 \| C_2\, \{Q_1 * Q_2\}} \qquad \frac{\{P\}\, C\, \{Q\}}{\{P * F\}\, C\, \{Q * F\}}$$

- If $C = C \parallel \mathsf{skip}$ then we can derive Frame from Concurrency

$$\frac{\{P\}\, C\, \{Q\} \qquad \{F\}\, \mathsf{skip}\, \{F\}}{\{P * F\}\, C \parallel \mathsf{skip}\, \{Q * F\}}$$

- In the algebra, we will not *assume* that $C = C \parallel \mathsf{skip}$ for all C, but take this as the *definition* of locality

Minimalist theory
(Locality bimonoid)

- A single poset $M, \sqsubseteq$ equipped with two structures:
  - ordered commutative monoid $(\|, \mathsf{nothing})$, and
  - an ordered monoid $(;, \mathsf{skip})$
- satisfying the exchange law: $(p\|r);(q\|s) \sqsubseteq (p;q)\|(r;s)$

CAR Hoare, A Hussain, B Möller, PW O'Hearn, RL Petersen, G Struth:
On Locality and the Exchange Law for Concurrent Processes. CONCUR 2011

Minimalist theory (Locality bimonoid)

- A single poset $M, \sqsubseteq$ equipped with two structures:
  - ordered commutative monoid $(\|, \mathsf{nothing})$, and
  - an ordered monoid $(;, \mathsf{skip})$
- satisfying the exchange law: $(p \| r);(q \| s) \sqsubseteq (p;q) \| (r;s)$
- skip is an idempotent of $\|$: $\mathsf{skip} \parallel \mathsf{skip} = \mathsf{skip}$. We say that $p \in M$ is *local* if $p = p \parallel \mathsf{skip}$.

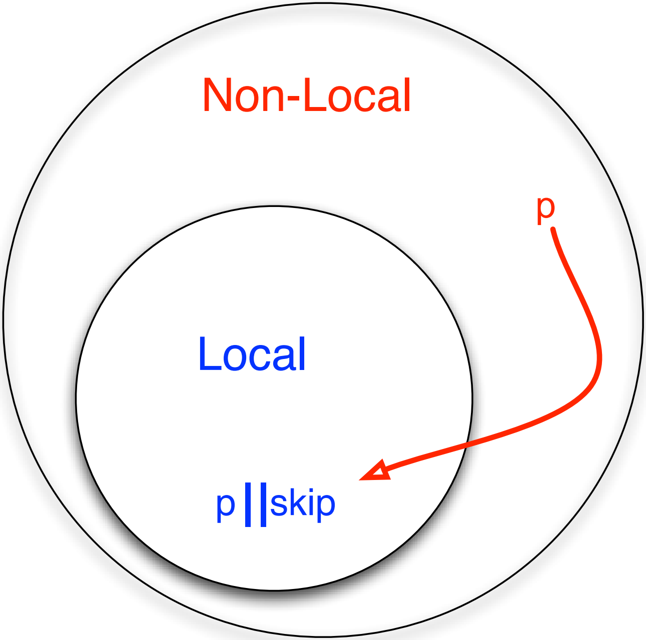
CAR Hoare, A Hussain, B Möller, PW O'Hearn, RL Petersen, G Struth: On Locality and the Exchange Law for Concurrent Processes. CONCUR 2011

Minimalist theory (Locality bimonoid)

- A single poset $M, \sqsubseteq$ equipped with two structures:
  - ordered commutative monoid $(\|, \mathsf{nothing})$, and
  - an ordered monoid $(\mathbf{;}, \mathsf{skip})$
- satisfying the exchange law: $(p \| r)\mathbf{;}(q \| s) \sqsubseteq (p\mathbf{;}q)\|(r\mathbf{;}s)$
- skip is an idempotent of $\|$: $\mathsf{skip} \| \mathsf{skip} = \mathsf{skip}$. We say that $p \in M$ is *local* if $p = p \| \mathsf{skip}$.

- Facts:
  - $\|$ and **;** preserve locality.
  - Let M_{loc} be the local elements. Galois connection with left adjoint $M_{loc} \hookrightarrow M$ and right adjoint $\lambda p.p \| \mathsf{skip}$
  - The SL concurrency rule holds in any locality bimonoid. The frame rule holds of historic triples of the form $\{p\}\, c\, \{q\}$ iff $c = c \| \mathsf{skip}$ (and similarly for futuristic triples)

CAR Hoare, A Hussain, B Möller, PW O'Hearn, RL Petersen, G Struth: On Locality and the Exchange Law for Concurrent Processes. CONCUR 2011


Non-Local
p
Local
p || skip

Perspective

- From our minimalist axioms, we automatically get lots of proof rules (Hoare and concurrent separation logic)
- For a range of models
- Wait a minute: do they mean what we expect? Is this cheating?

Perspective

- From our minimalist axioms, we automatically get lots of proof rules (Hoare and concurrent separation logic)
- For a range of models
- Wait a minute: do they mean what we expect? Is this cheating?

- Turning the tables: Start from Concurrent Separation Logic, see if we can get locality bimonoid. If we succeed we confirm, no cheat in the logic, and we get lots of more example models.

Basic CSL

$$[\texttt{Skip}]\ \frac{}{\{X\}\,\texttt{skip}\,\{X\}} \qquad [\texttt{Frame}]\ \frac{\{X\}\,c\,\{Y\}}{\{X * F\}\,c\,\{Y * F\}}$$

$$[\texttt{Seq}]\ \frac{\{X\}\,c_1\,\{Y\} \quad \{Y\}\,c_2\,\{Z\}}{\{X\}\,c_1; c_2\,\{Z\}} \qquad [\texttt{Par}]\ \frac{\{X_1\}\,c_1\,\{Y_1\} \quad \{X_2\}\,c_2\,\{Y_2\}}{\{X_1 * X_2\}\,c_1 \parallel c_2\,\{Y_1 * Y_2\}}$$

$$[\texttt{Consequence}]\ \frac{X' \vdash X \quad \{X\}\,c\,\{Y\} \quad Y \vdash Y'}{\{X'\}\,c\,\{Y'\}}$$

An *instance* of Basic CSL presumes a preordered commutative monoid $(Props, \vdash, *, \mathtt{emp})$ and a set of axioms $\{X\}\,c_p\,\{Y\}$ for a set of primitive command c_p and $X, Y \in Prop$.

BCSL minus `Frame` can be interpreted in any locality bimonoid. `Frame` holds when primitive commands are local.

Two Instantiations

- The original model. $M = \mathcal{P}(\mathit{Heaps})$, $\vdash = \subseteq$, $* =$ separating conjunction.

Details of session instantiation in A Hussain's upcoming dissertation.

Two Instantiations

- The original model. $M = \mathcal{P}(\mathit{Heaps})$, $\vdash = \subseteq$, $* =$ separating conjunction.
- Session instantiation (inspired by session types, Honda et al)
  - $M =$ (baby) session typing contexts Γ. $\Delta_1 * \Delta_2$ is multiset union.
  - $\Delta_1 \vdash \Delta_2$ if $\Delta_1 = \Delta_2 * \Phi$ where Φ has only end types, or Δ_1 is inconsistent.

Types:	$\alpha, \beta \ ::= \ ![\alpha];\beta \ \mid \ ?[\alpha];\beta \ \mid \ \mathtt{end}$
co-Types:	$\overline{![\alpha];\beta} = ?[\alpha];\overline{\beta} \quad \overline{?[\alpha];\beta} = ![\alpha];\overline{\beta} \quad \overline{\mathtt{end}} = \mathtt{end}$
Contexts:	$\Delta \ ::= \ \{\} \ \mid \ \Delta, k : \alpha$
Consistency:	k appears at most twice in Δ, then by co-type

- **The point to note about the session instantiation is how weak it is logically.** No $\neg$, no $\wedge$, etc. That is why Basic CSL only requires preordered commutative monoid of propositions.

Details of session instantiation in A Hussain's upcoming dissertation.

Embedding

Theorem. From the proof theory of BCSL one can construct a locality bimonoid (model of minimalist theory) together with

- embeddings of propositions and programs into the bimonoid,
- sending $*$ to $\parallel$ and preserving and reflecting order,
- sending programs to elements of the bimonoid, such that

$$\{p\}\, c\, \{q\} \text{ is provable in BCSL} \iff embed(p) \mathbin{;} embed(c) \sqsubseteq embed(q)$$

Ideas in the proof

- Use ideal completion: map a proposition p to everything that entails it $p\Downarrow$. Down-closed subsets have rich structure: complete Heyting algebra, residuated monoid (cf. BI algebra).
- Intuitionistic BI semantics of $*$ on down-closed sets (call it $\circledast$)

$$
\begin{array}{lcl}
P \circledast Q & = & \{X \mid Y \in P \wedge Z \in Q \wedge X \vdash Y * Z\} \\
I & = & \{p \mid p \vdash emp\}
\end{array}
$$

- Monotone function space $[Preds \rightarrow Preds]$ with reverse pointwise order is carrier of our algebra (where *Preds* is the down-closed subsets of $Props, \vdash$)

$$
\begin{array}{lcl}
(F_1 \| F_2)Y & = & \bigcup\{F_1 Y_1 \circledast F_2 Y_2 \mid Y_1 \circledast Y_2 \subseteq Y\} \\
\text{nothing } Y & = & Y \cap I \\
(F_1 ; F_2)Y & = & F_1(F_2(Y)) \\
\text{skip } Y & = & Y
\end{array}
$$

- Inject predicate P into predicate transformers using greatest transformer F satisfying $\mathtt{emp} \subseteq F(P)$. This maps $\circledast$ to $\|$.

Unpacking $\|$ (thanks to H Yang)

The definition

$$(F_1 \| F_2)Y \quad = \quad \bigcup\{F_1 Y_1 \circledast F_2 Y_2 \mid Y_1 \circledast Y_2 \subseteq Y\}$$

comes from instance of the Parallel rule of CSL

$$\frac{\{F_1 Y_1\}\, F_1\, \{Y_1\} \qquad \{F_2 Y_2\}\, F_2\, \{Y_2\}}{\{F_1 Y_1 \circledast F_2 Y_2\}\, F_1 \parallel F_2\, \{Y_1 \circledast Y_2\}}$$

together with the rule of consequence

$$\frac{\{F_1 Y_1 \circledast F_2 Y_2\}\, F_1 \parallel F_2\, \{Y_1 \circledast Y_2\} \qquad Y_1 \circledast Y_2 \subseteq Y}{\{F_1 Y_1 \circledast F_2 Y_2\}\, F_1 \parallel F_2\, \{Y\}}$$

and an infinitary version of the rule of disjunction

$$\frac{\{P_1\}\, C\, \{Q\} \qquad \{P_2\}\, C\, \{Q\}}{\{P_1 \vee P_2\}\, C\, \{Q\}}$$

Comment on transformer model

This predicate transformer model is not a conceptual model that can be used to *justify* the logic.

Rather, it is a technical device that can be used to reveal algebraic structure hidden in the proof rules.

Maybe it has other uses, too. It (and its forwards cousin) corresponds fairly well to how some abstract interpreters work.

Sum up

- Minimalist theory with a few axioms:

  A single poset $M, \sqsubseteq$ *equipped withan ordered commutative monoid* $(\|, \mathsf{nothing})$ *and an ordered monoid* $(;, \mathsf{skip})$*, satisfying the exchange law, where* $\mathsf{skip} \parallel \mathsf{skip} = \mathsf{skip}$*.*

- Connection with program logic: generalized CSL.
- Some diversity in models: interleaving, independence, resource separation...
- Temporal readings of triples which we are exploring

Sum up

- Minimalist theory with a few axioms:

  A single poset $M, \sqsubseteq$ equipped withan ordered commutative monoid $(\|, \mathsf{nothing})$ and an ordered monoid $(;, \mathsf{skip})$, satisfying the exchange law, where $\mathsf{skip} \| \mathsf{skip} = \mathsf{skip}$.

- Connection with program logic: generalized CSL.
- Some diversity in models: interleaving, independence, resource separation...
- Temporal readings of triples which we are exploring
- **Speculation**: programs and assertions are part of the same space. I wonder if we can push this and make a more genuine logic encompassing both, also bringing out the temporal aspect?

Maximalist model (tentative.. speculation)

- The traces model $P(E^*)$ has lots more structure. Ditto for tracelet model.
- $G = (M, \sqsubseteq, *, \text{nothing}, ;, \text{skip})$ is an ordered **residuated** commutative monoid $(*, \text{nothing})$ and a ordered **residuated** monoid $(;, \text{skip})$ on the same **complete boolean algebra** $(M, \sqsubseteq)$, satisfying exchange, where $\text{skip} * \text{skip} = \text{skip}$.
- Residuation means that we have the adjoint cousins

$$p * q \sqsubseteq r \quad \Leftrightarrow \quad p \sqsubseteq q \mathrel{-\!\!*} r$$

$$p; q \sqsubseteq r \quad \Leftrightarrow \quad p \sqsubseteq q \rhd r \quad \Leftrightarrow \quad q \sqsubseteq p \lhd r$$

- We have classical predicate logic (complete bool alg), alongside full-strength substructural logics (like in BI/SL).
- These connectives have a declarative reading given by a Kripke semantics (a la bunched/separation logic), where $;, \lhd, \rhd$ have a temporal flavour

- E.g., in the tracelet model
  (recall that X, Y etc are subsets of a given poset $E, \leq$)

  $Y \preceq X$ means that nothing in X depends on anything in Y.
  Then,

  $$X \models p \lhd q \text{ iff } \forall Y.\, Y \preceq X \text{ and } Y \models p \text{ implies } Y \uplus X \models q$$

- $$\begin{aligned} \text{previous}(p) &= \neg(p \lhd \text{false}) \\ &= \exists Y. \neg(Y \preceq X \textit{ and } Y \models p \textit{ implies } \text{false}) \\ &= \exists Y. Y \preceq X \textit{ and } Y \models p \end{aligned}$$