Coalgebraic models for spatial logic based on transition systems with spatial structure

Luís Monteiro

New University of Lisbon

CIC 2006
Braga, 11–14 October, 2006

General motivation

- To study abstract models of spatial logic.
- To study spatial and behavioural features of systems in a unified (coalgebraic) framework.

General motivation

- To study abstract models of spatial logic.
- To study spatial and behavioural features of systems in a unified (coalgebraic) framework.

General motivation

- To study abstract models of spatial logic.
- To study spatial and behavioural features of systems in a unified (coalgebraic) framework.

What is spatial logic ?

In distributed computing verification must handle behavioural and non-behavioural properties:

- Location-dependent access rights to resources.
- Invariants of the communication topology and routing.
- Dynamically created objects and references.
- Security and secrecy features.

Spatial logic addresses both kinds of properties extending temporal logic with constructs for spatial reasoning.

What is spatial logic ?

In distributed computing verification must handle behavioural and non-behavioural properties:

- Location-dependent access rights to resources.
- Invariants of the communication topology and routing.
- Dynamically created objects and references.
- Security and secrecy features.

Spatial logic addresses both kinds of properties extending temporal logic with constructs for spatial reasoning.

What is spatial logic ?

In distributed computing verification must handle behavioural and non-behavioural properties:

- Location-dependent access rights to resources.
- Invariants of the communication topology and routing.
- Dynamically created objects and references.
- Security and secrecy features.

Spatial logic addresses both kinds of properties extending temporal logic with constructs for spatial reasoning.

What is spatial logic ?

In distributed computing verification must handle behavioural and non-behavioural properties:

- Location-dependent access rights to resources.
- Invariants of the communication topology and routing.
- Dynamically created objects and references.
- Security and secrecy features.

Spatial logic addresses both kinds of properties extending temporal logic with constructs for spatial reasoning.

Why abstract models ?

- To provide language independent models of spatial logic.
- To bring the study of models of spatial logic more in line with the models of temporal logic.
- To isolate spatial logic constructions, postulate their properties and analyze the corresponding classes of models.

Why abstract models ?

- To provide language independent models of spatial logic.
- To bring the study of models of spatial logic more in line with the models of temporal logic.
- To isolate spatial logic constructions, postulate their properties and analyze the corresponding classes of models.

Why abstract models ?

- To provide language independent models of spatial logic.
- To bring the study of models of spatial logic more in line with the models of temporal logic.
- To isolate spatial logic constructions, postulate their properties and analyze the corresponding classes of models.

Why abstract models ?

- To provide language independent models of spatial logic.
- To bring the study of models of spatial logic more in line with the models of temporal logic.
- To isolate spatial logic constructions, postulate their properties and analyze the corresponding classes of models.

Why coalgebras ?

- Uniform treatment of time and space.
- Natural refinement of behavioural bisimulation.
- Spatial logics as modal logics for coalgebras.

Why coalgebras ?

- Uniform treatment of time and space.
- Natural refinement of behavioural bisimulation.
- Spatial logics as modal logics for coalgebras.

Why coalgebras ?

- Uniform treatment of time and space.
- Natural refinement of behavioural bisimulation.
- Spatial logics as modal logics for coalgebras.

Why coalgebras ?

- Uniform treatment of time and space.
- Natural refinement of behavioural bisimulation.
- Spatial logics as modal logics for coalgebras.

An example: Topological properties of networks

A simple spatial logic for networks:

$$x, y, z \in Var$$

A, B	$::=$	$l(x, y)$	% a link from x to y
		$x = y$	% equality
		$\top$	% truth
		$\neg A$	% negation
		$A \wedge B$	% conjunction
		$\exists x.A$	% existential quantification
		0	% void
		$A \mid B$	% composition

An example: Topological properties of networks

A simple spatial logic for networks:

$$x, y, z \in Var$$

A, B	$::=$	$l(x, y)$	% a link from x to y
		$x = y$	% equality
		$\top$	% truth
		$\neg A$	% negation
		$A \wedge B$	% conjunction
		$\exists x.A$	% existential quantification
		0	% void
		$A \vert B$	% composition

Example (cont.)
Models

- Set of nodes *Nodes*
- Nets $\mathcal{P}_\omega(Nodes \times Nodes)$
- Spatial function $\boxed{sp : Nets \to \mathcal{P}_\omega(Nets \times Nets)}$

$$sp(N) = \begin{cases} \emptyset & \text{if } N = \emptyset, \\ \{(M,K) : N = M \cup K, M \cap K = \emptyset\} & \text{if } N \neq \emptyset. \end{cases}$$

Example (cont.)

Satisfaction (classical connectives)

$\rho \in Env = Var \to Nodes$

$\models \subseteq Nets \times Env \times L$

- $N, \rho \models I(x, y)$ iff $N = \{(\rho x, \rho y)\}$.
- $N, \rho \models x = y$ iff $\rho x = \rho y$.
- $N, \rho \models \top$ always.
- $N, \rho \models \neg A$ iff $N, \rho \not\models A$.
- $N, \rho \models A \wedge B$ iff $N, \rho \models A$ and $N, \rho \models B$.
- $N, \rho \models \exists x.A$ iff $N, \rho[v/x] \models A$ for some $v \in Nodes$.

- $N, \rho \models 0$ iff $sp(N) = \emptyset$ (iff $N = \emptyset$).
- $N, \rho \models A|B$ iff exists $(M, K) \in sp(N)$ st $M, \rho \models A$ and $K, \rho \models B$.

Example (cont.)
Some properties

- **No link to x:**

$$in_0(x) \triangleq \neg(\exists y.l(y,x)|\top)$$

- **$n+1$ links to x:**

$$in_{n+1}(x) \triangleq \exists y.l(y,x)|in_n(x)$$

- **n links from x:**

$$out_n(x) \quad \text{defined similarly}$$

- **Minimal net satisfying A:**

$$min(A) \triangleq A \wedge \neg(A|\neg 0)$$

- **x is a node in the net:**

$$in\_net(x) \triangleq \exists y.(l(x,y) \vee l(y,x)|\top)$$

- **A net is a path:**

$$is\_path(x,y) \triangleq$$
$$min[x = y \vee (in_0(x) \wedge out_1(x) \wedge in_1(y) \wedge out_0(y) \wedge$$
$$\forall z.z \neq x \wedge z \neq y \wedge in\_net(z) \Rightarrow in_1(z) \wedge out_1(z))]$$

- **Existence of a path:**

$$exists\_path(x,y) \triangleq is\_path(x,y)|\top$$

Transition systems $\langle S, \rightarrow \rangle$ coalgebraically

The transitions from a state are **observed** through an observation function:

$$tr : S \rightarrow \mathcal{P}_\omega(S)$$

$$tr(s) = \{t : s \rightarrow t\}$$

$$s \rightarrow t \quad \text{iff} \quad t \in tr(s)$$

States with internal structure

The internal structure of a state is **observed** through an appropriate function:

$$sp : S \to \mathrm{Structures}(S)$$

$$sp(s) = ?$$

A single coalgebra for space and time

The two observation functions may be combined into a single one:

$$\langle tr, sp \rangle : S \to \mathcal{P}_\omega(S) \times \text{Structures}(S)$$

$$\langle tr, sp \rangle(s) = \langle tr(s), sp(s) \rangle$$

Two classes of spatial models of parallel composition

Using pairs

$$sp : S \to \mathcal{P}_\omega(S \times S)$$

Using (finite) multisets

$$sp : S \to \mathcal{M}(S)$$

A simple spatial logic L

HML-like with spatial operators

$$A, B ::= \top \mid \neg A \mid A \wedge B \mid \Diamond A \mid 0 \mid A|B$$

A simple spatial TS

$$tr : S \rightarrow \mathcal{P}_\omega(S)$$

$$sp : S \rightarrow \mathcal{P}_\omega(S \times S)$$

Satisfaction $\models \subseteq S \times L$

- $s \models \top$ always.
- $s \models \neg A$ iff $s \not\models A$.
- $s \models A \wedge B$ iff $s \models A$ and $s \models B$.
- $s \models \Diamond A$ iff $\exists t \in tr(s)$ such that $t \models A$.
- $s \models 0$ iff $sp(s) = \emptyset$.
- $s \models A|B$ iff $\exists (t, u) \in sp(s)$ st $t \models A$ and $u \models B$.

Spatial bisimulation $R \subseteq S \times S$

sRt implies:

1. $sp(s) = \emptyset$ iff $sp(t) = \emptyset$, and
2. $\forall (s', s'') \in sp(s), \exists (t', t'') \in sp(t)$ such that $s'Rt'$ and $s''Rt''$, and conversely.

Definition

Spatial bisimilarity $\sim_{sp}$ is the greatest bisimulation.

Caracterization of $\sim_{sp}$ by the purely spatial logic L_{sp}

Definition

$s =_{L_{sp}} t$ iff $\{A : s \models A\} = \{B : t \models B\}$.

Theorem

$\sim_{sp}$ coincides with $=_{L_{sp}}$.

The proof technique is similar to the one in the purely temporal case, where the logic is basically HML.

Does a similar result hold for the combined space/time logic and system ?

Yes, combining the proofs for the temporal and spatial cases.

Classes of models described by axioms

- $A|0 \Leftrightarrow A$ (empty states are neutral with respect to parallel composition).
- $A|B \Rightarrow B|A$ (parallel composition is commutative).
- $(A|B)|C \Leftrightarrow A|(B|C)$ (parallel composition is associative).
- $0 \Rightarrow \neg\Diamond T$ (empty states are inactive).
- $(\Diamond A)|B \Rightarrow \Diamond(A|B)$ (local transitions cause global transitions).

Models of $A|B \Rightarrow B|A$

Notation

$s \doteq t|u$ means $(t, u) \in sp(s)$.

Property

The following statements are equivalent:

1. $s \models (A|B) \Rightarrow (B|A)$ for all formulas A and B.
2. $s \doteq t|u$ implies $s \doteq u'|t'$ for some $t' \sim t$ and $u' \sim u$.

Spatial logic as a coalgebraic logic

Predicate lifting (Pattinson)

$$tr : S \to TS, \qquad TS = \mathcal{P}_\omega(S)$$

$$s \models \Diamond A \quad \text{iff} \quad \exists t \in tr(s) \quad \text{such that} \quad t \models A$$

$$\begin{aligned} s \in [\![\Diamond A]\!] &\Leftrightarrow tr(s) \cap [\![A]\!] \neq \emptyset \\ &\Leftrightarrow tr(s) \in \{X : X \cap [\![A]\!] \neq \emptyset\} \end{aligned}$$

$$[\![\Diamond A]\!] = tr^{-1}(\{X : X \cap [\![A]\!] \neq \emptyset\})$$

$$\lambda_S^\Diamond : \mathcal{P}(S) \to \mathcal{P}(TS) \qquad \lambda_S^\Diamond(Y) = \{X : X \cap Y \neq \emptyset\}$$

$$[\![\Diamond A]\!] = tr^{-1}(\lambda_S^\Diamond([\![A]\!]))$$

Spatial logic as a coalgebraic logic

Predicate lifting (Pattinson)

$$tr : S \to TS, \qquad TS = \mathcal{P}_\omega(S)$$

$$s \models \Diamond A \quad \text{iff} \quad \exists t \in tr(s) \quad \text{such that} \quad t \models A$$

$$\begin{aligned} s \in [\![\Diamond A]\!] &\Leftrightarrow tr(s) \cap [\![A]\!] \neq \emptyset \\ &\Leftrightarrow tr(s) \in \{X : X \cap [\![A]\!] \neq \emptyset\} \\ [\![\Diamond A]\!] &= tr^{-1}(\{X : X \cap [\![A]\!] \neq \emptyset\}) \end{aligned}$$

$$\lambda_S^{\Diamond} : \mathcal{P}(S) \to \mathcal{P}(TS) \qquad \lambda_S^{\Diamond}(Y) = \{X : X \cap Y \neq \emptyset\}$$

$$[\![\Diamond A]\!] = tr^{-1}(\lambda_S^{\Diamond}([\![A]\!]))$$

Spatial logic as a coalgebraic logic

Predicate lifting (Pattinson)

$$tr : S \to TS, \qquad TS = \mathcal{P}_\omega(S)$$

$$s \models \Diamond A \quad \text{iff} \quad \exists t \in tr(s) \quad \text{such that} \quad t \models A$$

$$\begin{aligned} s \in [\![\Diamond A]\!] \quad &\Leftrightarrow \quad tr(s) \cap [\![A]\!] \neq \emptyset \\ &\Leftrightarrow \quad tr(s) \in \{X : X \cap [\![A]\!] \neq \emptyset\} \end{aligned}$$

$$[\![\Diamond A]\!] \quad = \quad tr^{-1}(\{X : X \cap [\![A]\!] \neq \emptyset\})$$

$$\lambda_S^{\Diamond} : \mathcal{P}(S) \to \mathcal{P}(TS) \qquad \lambda_S^{\Diamond}(Y) = \{X : X \cap Y \neq \emptyset\}$$

$$[\![\Diamond A]\!] = tr^{-1}(\lambda_S^{\Diamond}([\![A]\!]))$$

Spatial logic as a coalgebraic logic
Predicate lifting (Pattinson)

$$tr : S \to TS, \qquad TS = \mathcal{P}_\omega(S)$$

$$s \models \Diamond A \quad \text{iff} \quad \exists t \in tr(s) \quad \text{such that} \quad t \models A$$

$$\begin{aligned} s \in [\![\Diamond A]\!] \quad &\Leftrightarrow \quad tr(s) \cap [\![A]\!] \neq \emptyset \\ &\Leftrightarrow \quad tr(s) \in \{X : X \cap [\![A]\!] \neq \emptyset\} \end{aligned}$$

$$[\![\Diamond A]\!] \quad = \quad tr^{-1}(\{X : X \cap [\![A]\!] \neq \emptyset\})$$

$$\lambda_S^\Diamond : \mathcal{P}(S) \to \mathcal{P}(TS) \qquad \lambda_S^\Diamond(Y) = \{X : X \cap Y \neq \emptyset\}$$

$$[\![\Diamond A]\!] = tr^{-1}(\lambda_S^\Diamond([\![A]\!]))$$

Spatial logic as a coalgebraic logic

Predicate lifting (Pattinson)

$$tr : S \to TS, \qquad TS = \mathcal{P}_\omega(S)$$

$$s \models \Diamond A \quad \text{iff} \quad \exists t \in tr(s) \quad \text{such that} \quad t \models A$$

$$\begin{aligned} s \in [\![\Diamond A]\!] &\Leftrightarrow tr(s) \cap [\![A]\!] \neq \emptyset \\ &\Leftrightarrow tr(s) \in \{X : X \cap [\![A]\!] \neq \emptyset\} \end{aligned}$$

$$[\![\Diamond A]\!] = tr^{-1}(\{X : X \cap [\![A]\!] \neq \emptyset\})$$

$$\lambda_S^\Diamond : \mathcal{P}(S) \to \mathcal{P}(TS) \qquad \lambda_S^\Diamond(Y) = \{X : X \cap Y \neq \emptyset\}$$

$$[\![\Diamond A]\!] = tr^{-1}(\lambda_S^\Diamond([\![A]\!]))$$

Spatial logic as a coalgebraic logic

Predicate lifting (Pattinson)

$$tr : S \to TS, \qquad TS = \mathcal{P}_\omega(S)$$

$$s \models \Diamond A \quad \text{iff} \quad \exists t \in tr(s) \quad \text{such that} \quad t \models A$$

$$\begin{aligned} s \in [\![\Diamond A]\!] &\Leftrightarrow tr(s) \cap [\![A]\!] \neq \emptyset \\ &\Leftrightarrow tr(s) \in \{X : X \cap [\![A]\!] \neq \emptyset\} \end{aligned}$$

$$[\![\Diamond A]\!] = tr^{-1}(\{X : X \cap [\![A]\!] \neq \emptyset\})$$

$$\lambda_S^\Diamond : \mathcal{P}(S) \to \mathcal{P}(TS) \qquad \lambda_S^\Diamond(Y) = \{X : X \cap Y \neq \emptyset\}$$

$$[\![\Diamond A]\!] = tr^{-1}(\lambda_S^\Diamond([\![A]\!]))$$

$$tr : S \to TS, \qquad TS = \mathcal{P}_\omega(S)$$

$$s \models \Diamond A \quad \text{iff} \quad \exists t \in tr(s) \quad \text{such that} \quad t \models A$$

$$\begin{aligned} s \in [\![\Diamond A]\!] &\Leftrightarrow tr(s) \cap [\![A]\!] \neq \emptyset \\ &\Leftrightarrow tr(s) \in \{X : X \cap [\![A]\!] \neq \emptyset\} \end{aligned}$$

$$[\![\Diamond A]\!] = tr^{-1}(\{X : X \cap [\![A]\!] \neq \emptyset\})$$

$$\lambda_S^\Diamond : \mathcal{P}(S) \to \mathcal{P}(TS) \qquad \lambda_S^\Diamond(Y) = \{X : X \cap Y \neq \emptyset\}$$

$$[\![\Diamond A]\!] = tr^{-1}(\lambda_S^\Diamond([\![A]\!]))$$

Spatial logic as a coalgebraic logic

Predicate lifting (Pattinson)

$$tr : S \to TS, \qquad TS = \mathcal{P}_\omega(S)$$

$$s \models \Diamond A \quad \text{iff} \quad \exists t \in tr(s) \quad \text{such that} \quad t \models A$$

$$\begin{aligned} s \in [\![\Diamond A]\!] &\Leftrightarrow tr(s) \cap [\![A]\!] \neq \emptyset \\ &\Leftrightarrow tr(s) \in \{X : X \cap [\![A]\!] \neq \emptyset\} \\ [\![\Diamond A]\!] &= tr^{-1}(\{X : X \cap [\![A]\!] \neq \emptyset\}) \end{aligned}$$

$$\lambda_S^{\Diamond} : \mathcal{P}(S) \to \mathcal{P}(TS) \qquad \lambda_S^{\Diamond}(Y) = \{X : X \cap Y \neq \emptyset\}$$

$$[\![\Diamond A]\!] = tr^{-1}(\lambda_S^{\Diamond}([\![A]\!]))$$

Predicate lifting defined

The spatial modalities

$$\lambda : \mathcal{P}^*(-)^n \to \mathcal{P}^* \circ T$$

Void $\lambda^0_S : 1 \to \mathcal{P}^*(TS)$ $\quad TS = \mathcal{P}_\omega(S \times S)$

$$\lambda^0_S(*) = \emptyset \qquad [\![0]\!] = sp^{-1}(\lambda^0_S(*))$$

Composition $\lambda^|_S : \mathcal{P}^*(-)^2 \to \mathcal{P}^*(TS)$ $\quad TS = \mathcal{P}_\omega(S \times S)$

$$\lambda^|_S(X, Y) = \{Z : Z \cap (X \times Y) \neq \emptyset\}$$

$$[\![A|B]\!] = sp^{-1}(\lambda^|_S([\![A]\!], [\![B]\!]))$$

Predicate lifting defined

The spatial modalities

$$\lambda : \mathcal{P}^*(-)^n \to \mathcal{P}^* \circ T$$

Void $\lambda^0_S : 1 \to \mathcal{P}^*(TS) \qquad TS = \mathcal{P}_\omega(S \times S)$

$$\lambda^0_S(*) = \emptyset \qquad [\![0]\!] = sp^{-1}(\lambda^0_S(*))$$

Composition $\lambda^|_S : \mathcal{P}^*(-)^2 \to \mathcal{P}^*(TS) \qquad TS = \mathcal{P}_\omega(S \times S)$

$$\lambda^|_S(X, Y) = \{Z : Z \cap (X \times Y) \neq \emptyset\}$$

$$[\![A|B]\!] = sp^{-1}(\lambda^|_S([\![A]\!], [\![B]\!]))$$

Predicate lifting defined

The spatial modalities

$$\lambda : \mathcal{P}^*(-)^n \to \mathcal{P}^* \circ T$$

Void $\lambda^0_S : 1 \to \mathcal{P}^*(TS) \qquad TS = \mathcal{P}_\omega(S \times S)$

$$\lambda^0_S(*) = \emptyset \qquad [\![0]\!] = sp^{-1}(\lambda^0_S(*))$$

Composition $\lambda^|_S : \mathcal{P}^*(-)^2 \to \mathcal{P}^*(TS) \qquad TS = \mathcal{P}_\omega(S \times S)$

$$\lambda^|_S(X, Y) = \{Z : Z \cap (X \times Y) \neq \emptyset\}$$

$$[\![A|B]\!] = sp^{-1}(\lambda^|_S([\![A]\!], [\![B]\!]))$$

Noninterleaving semantics

Another type of system:

$$tr : S \to \mathcal{P}_\omega(S)$$

$$sp : S \to \mathcal{M}(S)$$

Intuition:

$s \in S$ is the parallel composition of the elements in $sp(s)$.

1. For any such system a Petri net can be constructed and vice-versa.
2. The constructions are functorial and form an adjunction.

Main goal: To describe causality and independence relations between events.

Auxiliary definitions

- **State s is local** $sp(s) = [s]$
- **Set of local states** $Loc(S) = \{s \in S : s \text{ is local}\}$
- **Transition $s \to t$ is local**
  If $p \to q$ with $sp(s) = sp(p) \oplus M$ and $sp(t) = sp(q) \oplus M$, then $M = []$.
- **Extension of $\to$ to $\mathcal{M}(Loc(S))$**
  $P \to Q$ iff exists $s \to t$ and M st $P = sp(s) \oplus M$ and $Q = sp(t) \oplus M$

Axioms of spatial TS's

1. $sp(s) \in \mathcal{M}(Loc(S))$.
2. $P \subseteq sp(s)$ implies $P = sp(t)$ for some t.
3. $sp(s) \rightarrow P$ implies $s \rightarrow t$ for some t st $sp(t) = P$.

Morphism $f : S \to S'$ of spatial TS's

1. $sp' \circ f = \mathcal{M}(f) \circ sp$.
2. $tr' \circ f = \mathcal{P}_\omega(f) \circ tr$.
3. $s \to t$ local in S implies $f(s) \to f(t)$ local in S'.
4. $\mathcal{P}_\omega(f) \circ St = St' \circ \mathcal{M}(f)$,

where $St : \mathcal{M}(Loc(S)) \to \mathcal{P}_\omega(S)$ is given by

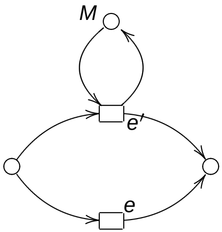
$$St(M) = \{s \in S : sp(s) \subseteq M\}.$$

Petri nets $N = (B, E, pre, post)$

$$pre, post : E \to \mathcal{M}(B)$$

Axiom $pre(e') = pre(e) \oplus M$ and $post(e') = post(e) \oplus M$ imply $M = []$ and $e = e'$.

Kind of situation discarded by the axiom:



Morphism $f : N \to N'$ of Petri nets

Pair of functions

$$f_B : B \to B', \qquad f_E : E \to E'$$

such that

1. $pre' \circ f_E = \mathcal{M}(f_B) \circ pre$.
2. $post' \circ f_E = \mathcal{M}(f_B) \circ post$.
3. $En' \circ \mathcal{M}(f_B) = \mathcal{P}_\omega(f_E) \circ En$.

Here $En : \mathcal{M}(B) \to \mathcal{P}_\omega(E)$ gives the set $En(M)$ of events enabled by $M \in \mathcal{M}(B)$.

From a Petri net N to a spatial TS $ns(N)$

1. $ns(N) = \mathcal{M}(B)$.
2. $sp(M) = [[b] : b \in M]$.
3. $tr(M) = \{M' : M \xrightarrow{e} M'\}$ for some event e.

From a spatial TS S to a Petri net $sn(S)$

1. $B = Loc(S)$.
2. $E = Loc(Tr)$.
3. $pre(s \to t) = sp(s)$.
4. $post(s \to t) = sp(t)$.

Relating the functors

The functor

$$sn : \text{Spatial TS's} \longrightarrow \text{Petri nets}$$

is left adjoint to the functor

$$ns : \text{Petri nets} \longrightarrow \text{Spatial TS's}.$$

A spatial TS for CCS

The transition function is defined as usual.
The spatial function $sp : Proc \to \mathcal{P}_\omega(Proc \times Proc)$ is defined by:

$$sp(P) = \begin{cases} \emptyset & \text{if } P \equiv 0, \\ \{(P_1, P_2) : P \equiv_{sp} P_1 | P_2\} & \text{otherwise.} \end{cases}$$

$\equiv_{sp}$ is defined as $\equiv$ except for the conditions

$$P|0 \equiv 0 \qquad \text{and} \qquad \nu x.0 \equiv 0$$

to guarantee that $sp(P)$ is a finite set.

Future work

- Systematic study of classes of models.
- Spatial operators related to the use of names.
- Predicate liftings for the adjoint modalities.
- Other non-interleaving models of concurrency.