The hierarchy of analytic semantics of weakly consistent parallelism

Jade Alglave (MSR-Cambridge, UCL, UK)
Patrick Cousot (NYU, Emer. ENS, PSL)

IMDEA seminar
Madrid
Tuesday, May 24th, 2016 — 11:00 AM
Analytic semantics
Weak consistency models (WCM)

- **Sequential consistency:**
  reads $r(p, x)$ are *implicitly coordinated* with writes $w(q, x)$

- **WCM:**
  *No implicit coordination* (depends on architecture, program dependencies, and explicit fences)

\[
\begin{align*}
  &w(q, x) \\
  \hline
  &r(p, x) \\
  &rf(w(q, x), r(p, x))
\end{align*}
\]
Analytic semantic specification

- **Anarchic semantics:** describes computations, no constraints on communications

- **cat specification (Jade Alglave & Luc Maranget):** imposes architecture-dependent communication constraints

- **Hierarchy of anarchic semantics:** many different styles to describe the same computations (e.g. stateless/stateful, interleaved versus true parallelism)
Example: load buffer (LB)

• Program: \{ x = 0; y = 0; \}

- P0 || P1 ;
- r[] r1 x | r[] r2 y ;
- w[] y 1 | w[] x 1 ;
- exists(0:r1=1 \&\& 1:r2=1)

• Example of execution trace \( t \in S^\perp[[P]] \):

\[
\begin{align*}
t &= w(\text{start}, x, 0) \; w(\text{start}, y, 0) \; r(P0, x, 1) \; \text{rf}[w(P1, x, 1), r(P0, x, 1)] \; w(P0, y, 1) \; r(P1, y, 1) \\
&\quad \; w(P1, x, 1) \; \text{rf}[w(P0, y, 1), r(P1, y, 1)] \; r(\text{finish}, x) \; \text{rf}[w(P1, x, 1), r(\text{finish}, x, 1)] \\
&\quad \; r(\text{finish}, y, 1) \; \text{rf}[w(P0, y, 1), r(\text{finish}, y, 1)]
\end{align*}
\]

• Abstraction to cat candidate execution \( \alpha_\Xi(t) \):

- P0
  - a: Rx=1
  - b: Wy=1
- P1
  - c: Ry=1
  - d: Wx=1

J. Alglave & P. Cousot, The hierarchy of analytic semantics of weakly consistent parallelism, IMDEA Seminar, Madrid, 24 May 2016
Example: load buffer (LB), cont’d

- cat specification:

\[ \text{acyclic (po | rf)}^+ \]

The cat semantics rejects this execution \( \alpha_\Xi(t) : \)

\[ \text{\#\#[cat]} \ (\alpha_\Xi(t)) = \text{false} \]

- P₀
  - a: Rx=1
  - po

- P₁
  - b: Wy=1
  - rf
  - c: Ry=1
  - po
  - d: Wx=1

- The herd7 tool: [virginia.cs.ucl.ac.uk/herd/]
The WCM semantics

- Abstraction to a candidate execution:
  \[ \alpha_{\Xi}(t) \triangleq \langle \alpha_e(t), \alpha_{po}(t), \alpha_{rf}(t), \alpha_{iw}(t), \alpha_{fw}(t) \rangle \]
  \[ \alpha_{\Xi}(S) \triangleq \{ \langle t, \alpha_{\Xi}(t) \rangle \mid t \in S \} \]

- The cat semantics:
  \[ \alpha_{\otimes}[\text{cat}](S) \triangleq \{ t \mid \langle t, \Xi \rangle \in S \land \alpha_{\otimes}[\text{cat}](\Xi) \} \]

- The WCM semantics:
  \[ \alpha_{\otimes}[\text{cat}] \circ \alpha_{\Xi}(S[P]) \]

GC:
\[ \langle \circ (\mathcal{C}^{+\infty}), \square \rangle \xrightarrow{\gamma_{\Xi}} \langle \circ (\mathcal{C}^{+\infty} \times \Xi), \square \rangle \xrightarrow{\gamma_{\otimes}[\text{cat}]} \langle \circ (\mathcal{C}^{+\infty}), \square \rangle \]
Definition of the anarchic semantics
Axiomatic parameterized definition of the anarchic semantics

- The semantics $S^\perp[P]$ is a finite/infinite sequence of interleaved events of processes satisfying well-formedness conditions.

Events:

- local computations and tests on registers
- start writing a shared variable $w(q, x)$
- start reading of shared variable $r(p, x)$
- communication event $rf(w(q, x), r(p, x))$
Axiomatic parameterized definition of the anarchic semantics

- Examples of language independent well-formedness conditions of a semantics $S$:

  - uniqueness of events

  $\forall t \in S . \forall t_1, t_2 \in C^*, t_3 \in C^{*\infty} . \forall e, e' \in C . (t = t_1 e t_2 e' t_3) \implies (e \neq e') . \quad (Wf_1(S))$

  - traces start with an initialization of the shared variables

  $t = w(\text{start}, x, 0) w(\text{start}, y, 0) r(\text{P0}, x, 1) r(\text{P1}, y, 1) r(\text{P0}, x, 1) r(\text{P1}, y, 1) w(\text{P0}, x, 1) w(\text{P1}, x, 1) r(\text{P0}, y, 1) r(\text{P1}, y, 1) r(\text{finish}, y, 1) r(\text{finish}, x, 1) r(\text{finish}, x, 1) r(\text{finish}, y, 1) r(\text{finish}, y, 1)$
Axiomatic parameterized definition of the anarchic semantics

- Examples of language independent well-formedness conditions of a semantics \( S \):
  - finite traces are maximal

\[
\forall t \in S \cap \mathcal{E}^+. \not\exists t' \in \mathcal{E}^{+\infty}. t \Join t' \in S. \quad (Wf_3(S))
\]

- the final value of shared variables in finite traces is known thanks to a final read

\[
t = w(\text{start}, x, 0) \Join w(\text{start}, y, 0) \Join r(\text{P0}, x, 1) \Join [w(\text{P1}, x, 1), r(\text{P0}, x, 1)] \Join w(\text{P0}, y, 1) \Join r(\text{P1}, y, 1)
\]

\[
\Join w(\text{P1}, x, 1) \Join [w(\text{P0}, y, 1), r(\text{P1}, y, 1)] \Join r(\text{finish}, x) \Join [w(\text{P1}, x, 1), r(\text{finish}, x, 1)]
\]

\[
\Join r(\text{finish}, y, 1) \Join [w(\text{P0}, y, 1), r(\text{finish}, y, 1)]
\]
Axiomatic parameterized definition of the anarchic semantics

- Examples of language independent well-formedness conditions of a semantics $S$:
  - **read events must be satisfied by a unique communication event**

\[
\forall t \in S . \forall t_1 \in E^*, t_2 \in E^{*\infty} . (t = t_1 \ r(p, x) t_2) \implies \\
(\exists t_3 \in E^*, t_4 \in E^{*\infty} . t = t_3 \ r_f[w(q, x), r(p, x)] t_4) .
\]

\[
\forall t \in S . \forall t_1, t_2 \in E^*, t_3 \in E^{*\infty} . \\
(t \neq t_1 \ r_f[w(q, x), r(p, x)] t_2 \ r_f[w'(q', x), r(p, x)] t_3) .
\]
Axiomatic parameterized definition of the anarchic semantics

- Examples of language independent well-formedness conditions of a semantics $S$:
  - communications cannot be spontaneous (must be originated by a read and a write)

\[
\forall t \in S. \forall t_1 \in \mathcal{C}^*, t_2 \in \mathcal{C}^{*\infty}. \ (t = t_1 \text{rf}[w(q,x), r(p,x)] t_2) \implies \\
(\exists t_3 \in \mathcal{C}^*, t_4 \in \mathcal{C}^{*\infty}. \ t = t_3 w(q,x) t_4 \land \exists t_5 \in \mathcal{C}^*, t_6 \in \mathcal{C}^{*\infty}. \ t = t_5 r(p,x) t_6) .
\]
Axiomatic parameterized definition of the anarchic semantics

- The language:
  - Programs: \( \text{initialisation} \ [P_1 \| \ldots \| P_n] \text{ finalisation} \)

- Actions (labelled \( \ell \in \mathbb{L}(p) \)):
  - \( a ::= m \) imperative actions
  - \( r := e \) assignment
  - \( r := x \) read of shared variable \( x \)
  - \( x := e \) write of shared variable \( x \)
  - \( b | \neg b \) conditional actions

- Next action: \( \text{next}(p, \ell) \) \( \text{nextt}(p, \ell) \) \( \text{nextf}(p, \ell) \) for tests

---

J. Alglave & P. Cousot, The hierarchy of analytic semantics of weakly consistent parallelism, IMDEA Seminar, Madrid, 24 May 2016
Axiomatic parameterized definition of the anarchic semantics

- Example of language-dependent well-formedness condition: computation (markers: skip, fence, begin/end of rmw)

\[ \forall p \in \Pi \ . \ \forall k \in [1, 1 + |\tau|] \ . \ \forall \ell \in \mathbb{L}(p) \ . \ \exists \theta \in \Psi(p) \ . \ \bar{\tau}_k = m(\langle p, \ell, m, \theta \rangle) \]

\[ \implies (\ell \in N^p(\tau, k) \land \text{action}(p, \ell) = m) . \]

(unique) event stamp \( \theta \)

control of process \( p \) is at label \( \ell \)

action of process \( p \) is at label \( \ell \) is the marker action \( m \)
Axiomatic parameterized definition of the anarchic semantics

- Example of language-dependent well-formedness condition: computation (local variable assignment)

\[
\forall p \in \mathcal{P} . \forall k \in [1, 1 + |\tau|] . \forall \ell \in \mathbb{L}(p) . \forall v \in \mathcal{D} . \\
(\exists \theta \in \mathcal{P}(p) . \bar{\tau}_k = a(\langle p, \ell, r := e, \theta \rangle, v)) \\
\implies (\ell \in \mathbb{N}^p(\tau, k) \land \text{action}(p, \ell) = r := e \land v = E_p[e](\tau, k - 1)) .
\]

- Control of process \( p \) is at label \( \ell \)
- Action of process \( p \) is at label \( \ell \) is a register assignment
- Value \( v \) of \( e \) is evaluated by past-travel
Media variables

- With WCM there is no notion of “the current value of shared variable \( x \)”

- At a given time each process may read a different value of the shared variable \( x \) (maybe guessed or unknown since a read may read from a future write)

- We use media variables (to record the values communicated between a write and read, whether the two accesses are on the same process or not)
Axiomatic parameterized definition of the anarchic semantics

**Example:** communication

- a read event is initiated by a read action:
  
  \[
  \forall p \in \Pi . \forall k \in ]1, 1 + |\tau|[ . \forall \ell \in L(p) . \\
  (\exists \theta \in \mathcal{P}(p) . (\overline{\tau}_k = r(\langle p, \ell, \mathbf{r} := x, \theta \rangle, x\theta))) \\
  \implies (\ell \in N^p(\tau, k) \land \text{action}(p, \ell) = \mathbf{r} := x) .
  \]  

- a read must read-from (rf) a write (weak fairness):

  \[
  \forall p \in \Pi . \forall i \in ]1, 1 + |\tau|[ . \forall r \in \mathcal{Rf}(p) . \\
  (\overline{\tau}_i = r) \implies (\exists j \in ]1, 1 + |\tau|[ . \exists w \in \mathcal{W} . \overline{\tau}_j = \text{rf}[w, r]) .
  \]
Axiomatic parameterized definition of the anarchic semantics

- **Predictive evaluation** of media variables:

\[
V^p_{(32)}[x_\theta](\tau, k) \triangleq v \text{ where } \exists i \in [1, 1 + |\tau|] . (\tau_i = r(\langle p, \ell, r := x, \theta \rangle, x_\theta)) \land \\
\exists j \in [1, 1 + |\tau|] . (\tau_j = rf[\nu(\langle p', \ell', x := e', \theta' \rangle, v), \tau_i])
\]

- **Local past-travel evaluation** of an expression:

\[
E^p_{(30)}[r](\tau, k) \triangleq v \quad \text{if } k > 1 \land (\tau_k = a(\langle p, \ell, r := e, \theta \rangle, v)) \lor \\
(\tau_k = r(\langle p, \ell, r := x, \theta \rangle, x_\theta) \land V^p[\cdot]\theta)(\tau, k) = v)
\]

\[
E^p_{(30)}[r](\tau, 1) \triangleq l[0]
\]

\[
E^p_{(30)}[r](\tau, k) \triangleq E^p_{(30)}[r](\tau, k - 1)
\]

i.e. \( \tau_1 = \epsilon_{\text{start}} \) by Wf_{15}(\tau) otherwise.
Abstractions of the anarchic semantics
Abstractions

- **Anarchic semantics:**

\[ S^\perp [P] \triangleq \lambda \langle B, \text{sat, } D, I, \mathcal{G}, V, E, N \rangle \cdot \{ \tau \in \mathcal{T}[P] | \subseteq | Wf_1 (\tau) \wedge \ldots \wedge Wf_{29}(\tau) \} \]

- **Examples of abstractions:**
  - Choose data (e.g. ground values, uninterpreted symbolic expressions, interpreted symbolic expressions i.e. “symbolic guess”)
  - Bind parameters (e.g. how expressions are evaluated)
  - ...

  parameters of the semantics  
  trace well-formedness conditions
Binding a parameter of the semantics

- The abstraction

\[ \alpha_a(f) \overset{\text{def}}{=} f(a) \]

\[ \langle \wp(A, B, \ldots) \rightarrow \wp(R), \subseteq \rangle \overset{\alpha_a}{\leftrightarrow} \langle \wp(B, \ldots) \rightarrow \wp(R), \subseteq \rangle \]

\[ \langle \wp(A, B, \ldots) \rightarrow \wp(R), \subseteq \rangle \overset{\gamma_a}{\leftrightarrow} \langle \wp(B, \ldots) \rightarrow \wp(R), \subseteq \rangle \]
The hierarchy of interleaved semantics

![Diagram of the hierarchy of semantics]

- **WCM**
- **valued**
- **symbolic interpreted**
- **symbolic uninterpreted**
- **data generic**
- **locally sequential**
- **unspecified locality**

The diagram illustrates the relationships between different levels of semantics, with each level representing a specific property or constraint. The hierarchy is organized from the most restrictive at the top (inscrutable) to the most general at the bottom (predictive).
True parallelism with local communications

• Extract from interleaved executions:
  • The subtrace of each process keeping communications in the process that read

⇒ no more global time between processes

⇒ local time between local actions and communications (a read can still tell when it is satisfied by which write)
True parallelism with local communications

- Interleaved execution:  
  \[ t = w(\text{start}, x, 0) \ w(\text{start}, y, 0) \ r(\text{P0}, x, 1) \ r([w(\text{P1}, x, 1), r(\text{P0}, x, 1)]) \ w(\text{P0}, y, 1) \ r(\text{P1}, y, 1) \]

- Parallel executions with interleaved communications:
  \[ t = \text{Initialization:} \quad w(\text{start}, x, 0) \ w(\text{start}, y, 0) \]
  \[ \text{P0:} \quad r(\text{P0}, x, 1) \ r([w(\text{P1}, x, 1), r(\text{P0}, x, 1)]) \ w(\text{P0}, y, 1) \]
  \[ \text{P1:} \quad r(\text{P1}, y, 1) \ w(\text{P1}, x, 1) \ r([w(\text{P0}, y, 1), r(\text{P1}, y, 1)]) \]
  \[ \text{Finalization:} \quad r(\text{finish}, x) \ r([w(\text{P1}, x, 1), r(\text{finish}, x, 1)]) \]
  \[ r(\text{finish}, y, 1) \ r([w(\text{P0}, y, 1), r(\text{finish}, y, 1)]) \]
True parallelism of computations and communications

- Extract from interleaved executions:
  - The subtrace of each process (sequential execution of actions)
  - The rf communication relation (interactions between processes)

$$\Rightarrow$$ no more global time between processes

$$\Rightarrow$$ no more global/local time for communications
True parallelism with separate communications

- Parallel executions with interleaved communications:

  **Initialization:**  
  \[w(\text{start}, x, 0) \quad w(\text{start}, y, 0)\]

  **P0:**  
  \[r(P0, x, 1) \quad w(P0, y, 1)\]

  **P1:**  
  \[r(P1, y, 1) \quad w(P1, x, 1)\]

  **Finalization:**  
  \[r(\text{finish}, x) \quad r(\text{finish}, y, 1)\]

  **Communications:**  
  \[
  \{ \text{tf}[w(P1, x, 1), r(P0, x, 1)], \text{tf}[w(P0, y, 1), r(P1, y, 1)] \}
  \]
True parallelism with separate communications

- This is the semantics used by the herd7 tool:

\[
\begin{align*}
P_0 & \quad P_1 \\
event & \quad a: \ Rx=1 \quad c: \ Ry=1 \\
local\ time & \quad po \quad rf \quad po \\
event & \quad b: \ Wy=1 \quad d: \ Wx=1
\end{align*}
\]

+ interpreted symbolic expressions i.e. “symbolic guess”
The true parallelism hierarchy

separated communication \downarrow \quad \text{true parallelism} \downarrow \quad \text{per process}

WCM

\alpha_{\text{cat}} \circ \alpha_\Xi(S[P])

\tilde{\alpha}_{gp}

interleaved communication

locally sequential

free \uparrow \quad \text{eager} \quad \text{lazy}

J. Alglave & P. Cousot, The hierarchy of analytic semantics of weakly consistent parallelism, IMDEA Seminar, Madrid, 24 May 2016
States

- At each point in a trace, the state abstracts the past computation history up to that point.
- Example: classical environment (assigning values to register at each point $k$ of the trace):

\[
\rho^p(\tau, k) \triangleq \lambda r \in \mathbb{R}(p) \cdot E^p[r](\tau, k)
\]

\[
\nu^p(\tau, k) \triangleq \lambda x_\theta \cdot V_{(32)}^p[x_\theta](\tau, k)
\]
Prefixes, transitions, . . .

• Abstract traces by their prefixes:

\[ \bar{\alpha}(S) \triangleq \bigcup \{ \bar{\alpha}(\tau) \mid \tau \in S \} \]
\[ \bar{\alpha}(\tau) \triangleq \{ \tau[j] \mid j \in [1, 1 + |\tau|] \} \]
\[ \tau[j] \triangleq \langle \overleftarrow{\tau_i} \rightarrow \tau_i \mid i \in [1, 1 + j] \rangle \]

• and transitions: extract transitions from traces

\[ \Rightarrow \text{communication fairness is lost, inexact abstraction,} \]
\[ \Rightarrow \text{add fairness condition} \]
\[ \Rightarrow \text{impossible to implement with a scheduler (≠ process fairness)} \]
Effect of the cat specification on the hierarchy
Exactness and cat preservation
The cat abstraction

- The same cat specification $\alpha \llbracket \text{cat} \rrbracket$ applies equally to any concurrent execution abstraction $\alpha \Xi$ of any interleaved/truly parallel semantics in the hierarchy.

- The appropriate level of abstraction to specify WCM:
  - No states, only marker (e.g. fence), $r$, $w$, $rf(w,r)$ events
  - No values in events
  - No global time (only po order of events per process)
  - Time of communications forgotten (only rf of who communicates with whom)
Conclusion
Conclusion

• **Analytic semantics**: a new style of semantics

• The hierarchy of **anarchic semantics** describes the same computations and potential communications in very different styles

• The **cat semantics** restricts communications to a machine/network architecture in the same way for all semantics in the hierarchy

• This idea of **parameterized semantics at various levels of abstraction** is useful for
  
  • Verification
  • Static analysis
The End