1 MODEL

1.1 Preliminaries

The syntax is built from

- a set of *values* $\mathcal{V}$, ranged over by v, w, ℓ, k,
- a set of *registers* $\mathcal{R}$, ranged over by r, s,
- a set of *expressions* $\mathcal{M}$, ranged over by M, N, L,
- a set of *thread ids* $\mathcal{T}$, ranged over by α, γ.

Memory references are tagged values, written $[\ell]$. Let $\mathcal{X}$ be the set of memory references, ranged over by x, y, z.

We require that

- values and registers are disjoint,
- values include at least the constants 0 and 1,
- expressions include at least registers and values,
- expressions do *not* include references: $M[N/x] = M$,
- there are registers $\mathcal{S}_{\mathcal{E}} = \{s_e \mid e \in \mathcal{E}\}$,
- registers $\mathcal{S}_{\mathcal{E}}$ do not appear in programs: $S[N/s_e] = S$.

Alternative to the last assumption, we sometimes assume each register is assigned at most once.[1]

We model the following language.

$$\mu ::= \mathsf{wk} \mid \mathsf{rlx} \mid \mathsf{ra} \mid \mathsf{sc} \qquad \nu ::= \mathsf{acq} \mid \mathsf{rel} \mid \mathsf{ar} \qquad \sigma, \rho ::= \mathsf{grp} \mid \mathsf{proc} \mid \mathsf{sys}$$

$$S ::= \mathtt{skip} \mid r := M \mid r := [L]^{\mu}_{\sigma} \mid [L]^{\mu}_{\sigma} := M \mid \mathtt{F}^{\nu}_{\sigma} \mid \mathtt{if}(M)\{S_1\}\mathtt{else}\{S_2\} \mid S_1; S_2$$
$$\mid S_1 \parallel_{\gamma} S_2 \mid r := \mathtt{CAS}^{\mu_1,\mu_2}_{\sigma}([L], M, N) \mid r := \mathtt{FADD}^{\mu_1,\mu_2}_{\sigma}([L], M) \mid r := \mathtt{EXCHG}^{\mu_1,\mu_2}_{\sigma}([L], M)$$

Access modes, μ, are weak (wk), are relaxed (rlx), release-acquire (ra), and sequentially consistent (sc). ra/sc accesses are collectively known as *synchronized accesses*.

Fence modes, ν, are acquire (acq), release (rel), and acquire-release (ar).

Scopes, σ, are thread group (grp), processor (proc) and system (sys).

Commands, aka *statements*, S, include memory accesses at a given mode, as well as the usual structural constructs. Following [Ferreira et al. 1996], $\parallel$ denotes parallel composition. If $(S_1 \parallel_{\gamma} S_2)$ is executed with thread ID α, then S_2 runs with ID γ and S_1 continues under ID α. Top level programs run with thread ID 0. In examples, we usually drop thread IDs. We use the symmetric $\|$ operator when there is no continuation after the parallel composition.

The semantics is built from the following.

- a set of *events* $\mathcal{E}$, ranged over by e, d, c, b,
- a set of *actions* $\mathcal{A}$, ranged over by a,
- a set of *logical formulae* Φ, ranged over by ϕ, ψ, θ.

Subsets of $\mathcal{E}$ are ranged over by E, D, C, B.

We require that:

- formulae include equalities $(M{=}N)$ and $(x{=}M)$,
- formulae are closed under negation, conjunction, disjunction, and substitutions $[M/r]$, $[M/x]$,
- there is a relation $\vDash$ between formulae, capturing entailment,
- $\vDash$ has the expected semantics for $=$, $\neg$, $\wedge$, $\vee$, $\Rightarrow$ and substitution.

Logical formulae include equations over registers, such as $(r{=}s{+}1)$. For LIR, we also include equations over memory references, such as $(x{=}1)$. Formulae are subject to substitutions; actions

[1] We make this assumption when discussing any semantics of load $(r := [L]^{\mu}_{\sigma})$ that does not include the substitution $[s_e/r]$.

are not. We use expressions as formulae, coercing M to $M{\neq}0$. Equations have precedence over logical operators; thus $r{=}v \Rightarrow s{>}w$ is read $(r{=}v) \Rightarrow (s{>}w)$. As usual, implication associates to the right; thus $\phi \Rightarrow \psi \Rightarrow \theta$ is read $\phi \Rightarrow (\psi \Rightarrow \theta)$.

We say ϕ is a *tautology* if $\mathsf{tt} \vDash \phi$. We say ϕ is *unsatisfiable* if $\phi \vDash \mathsf{ff}$.

We require several binary relations between actions, detailed in the next subsection: *overlaps*, *matches*, *strongly-matches*, *blocks*, *strongly-blocks*, *synchronization-delays* and *coherence-delays*. We also require that there is a subsets of actions, distinguishing *read* and *release* actions, and an operator $\mathsf{merge} : \mathcal{A} \times \mathcal{A} \to 2^{\mathcal{A}}$.

1.2 Actions

We combine access and fence modes into a single order:

$$\mathsf{wk} \longrightarrow \mathsf{rlx} \longrightarrow \mathsf{ra} \longrightarrow \mathsf{sc} \qquad\qquad \begin{matrix}\mathsf{acq} \\ \mathsf{rel}\end{matrix} \rightrightarrows \mathsf{ar}$$

We write $\mu \sqsubseteq \nu$ for this order. Let $\mu \sqcup \nu$ denote the least upper bound of μ and ν.

Let actions be reads, writes and fences:

$$a, b \ ::= \ \alpha\mathsf{W}^{\mu}_{\sigma} x v \ \mid \ \alpha\mathsf{R}^{\mu}_{\sigma} x v \ \mid \ \alpha\mathsf{F}^{\nu}_{\sigma}$$

In definitions, we drop elements of actions that are existentially quantified. In examples, we drop elements of actions, using defaults. We write $(\alpha\mathsf{A}^{\mu}_{\sigma})$ to stand for $(\alpha\mathsf{W}^{\mu}_{\sigma})$, $(\alpha\mathsf{R}^{\mu}_{\sigma})$, or $(\alpha\mathsf{F}^{\mu}_{\sigma})$. We write $(\mathsf{W}^{\sqsupseteq\mathsf{ra}})$ to stand for either $(\mathsf{W}^{\mathsf{ra}})$ or $(\mathsf{W}^{\mathsf{sc}})$, and similarly for other actions and modes.

We say *a matches b* if $a = (\mathsf{W} x v)$ and $b = (\mathsf{R} x v)$.

We say *a blocks b* if $a = (\mathsf{W} x)$ and $b = (\mathsf{R} x)$, regardless of value.

We say *a overlaps b* if they access the same location.

We say *a coherence-delays b* if $(a, b) \in \{(\mathsf{W}x, \mathsf{W}x),\ (\mathsf{R}x, \mathsf{W}x),\ (\mathsf{W}x, \mathsf{R}x),\ (\mathsf{A}^{\mathsf{sc}}, \mathsf{A}^{\mathsf{sc}})\}$.

We say *a synchronization-delays b* if $(a, b) \in \{(a, \mathsf{W}^{\sqsupseteq\mathsf{ra}}),\ (a, \mathsf{F}^{\sqsupseteq\mathsf{rel}}),\ (\mathsf{R}, \mathsf{F}^{\sqsupseteq\mathsf{acq}}),\ (\mathsf{R}x, \mathsf{R}^{\sqsupseteq\mathsf{ra}}x),\ (\mathsf{R}^{\sqsupseteq\mathsf{ra}}, b),\ (\mathsf{F}^{\sqsupseteq\mathsf{acq}}, b),\ (\mathsf{F}^{\sqsupseteq\mathsf{rel}}, \mathsf{W}),\ (\mathsf{W}^{\sqsupseteq\mathsf{ra}}x, \mathsf{W}x)\}$.

Let $(\mathsf{W}^{\sqsupseteq\mathsf{ra}})$ and $(\mathsf{F}^{\sqsupseteq\mathsf{rel}})$ be *release* actions. Actions (R) are *read* actions.

Let $\mathsf{merge} : \mathcal{A} \times \mathcal{A} \to 2^{\mathcal{A}}$ be defined as follows. Let $\mathsf{merge}(\mathsf{R}^{\mu} x v,\ \mathsf{R}^{\nu} x v) = \{\mathsf{R}^{\mu\sqcup\nu} x v\}$, $\mathsf{merge}(\mathsf{W}^{\mu} x v,\ \mathsf{W}^{\nu} x w) = \{\mathsf{W}^{\mu\sqcup\nu} x w\}$, $\mathsf{merge}(\mathsf{W}^{\nu} x v,\ \mathsf{R}^{\mathsf{rlx}} x v) = \{\mathsf{W}^{\nu} x v\}$, $\mathsf{merge}(\mathsf{F}^{\mu},\ \mathsf{F}^{\nu}) = \{\mathsf{F}^{\mu\sqcup\nu}\}$, and $\mathsf{merge}(a,\ b) = \emptyset$, otherwise. If $a_0 \in \mathsf{merge}(a_1,\ a_2)$, then a_1 and a_2 can coalesce, resulting in a_0. This allows optimizations such as $(x := 1;\ x := 2)$ to $(x := 2)$ and $(x := 1;\ r := x)$ to $(x := 1;\ r := 1)$.

Definition 1.1. When modeling IMM, we ban access mode wk; the default access mode is rlx. We also ban scopes grp and proc; the only allowed scope is sys. We assume there is only one thread ID ($|\mathcal{T}| = 1$), which we elide. Let *strongly-blocks* be $\mathcal{A}{\times}\mathcal{A}$. We say *a strongly-matches b* if *a* overlaps *b* and neither has mode rlx.

Definition 1.2. When modeling PTX, the default access mode is wk. The default scope is grp. We assume two equivalences: $(=_{\mathsf{proc}}) \subseteq (\mathcal{T} \times \mathcal{T})$ partitions threads by *processor*, and $(=_{\mathsf{grp}}) \subseteq (=_{\mathsf{proc}})$ refines the processor partitioning into *thread groups*. Strong matching and strong blocking coincide. We say $(\alpha\mathsf{A}^{\mu}_{\sigma})$ *strongly-matches/blocks* $(\gamma\mathsf{A}^{\nu}_{\rho})$ when either (1) $\alpha = \gamma$ or (2) all of the following hold:

(2a) $\mu, \nu \neq \mathsf{wk}$,
(2b) if $\sigma = \mathsf{grp}$ or $\rho = \mathsf{grp}$ then $\alpha =_{\mathsf{grp}} \gamma$,
(2c) if $\sigma = \mathsf{proc}$ or $\rho = \mathsf{proc}$ then $\alpha =_{\mathsf{proc}} \gamma$,
(2d) if either action is an access then they overlap.

1.3 Pomsets with Predicate Transformers

Definition 1.3. A *predicate transformer* is a function $\tau : \Phi \to \Phi$ such that

(1) $\tau(\mathsf{ff})$ is ff,
(2) $\tau(\psi_1 \wedge \psi_2)$ is $\tau(\psi_1) \wedge \tau(\psi_2)$,
(3) $\tau(\psi_1 \vee \psi_2)$ is $\tau(\psi_1) \vee \tau(\psi_2)$,
(4) if $\phi \vDash \psi$, then $\tau(\phi) \vDash \tau(\psi)$.

Definition 1.4. A *family of predicate transformers* for E consists of a predicate transformer τ^D for each $D \subseteq \mathcal{E}$, such that if $C \cap E \subseteq D$ then $\tau^C(\psi) \vDash \tau^D(\psi)$.

Definition 1.5. A *pomset with predicate transformers* is a tuple $(E, \lambda, \kappa, \tau, \checkmark, \trianglelefteq, \leq, \sqsubseteq, \mathsf{rmw})$ where
(M1) $E \subset \mathcal{E}$ is a set of *events*,
(M2) $\lambda : E \to \mathcal{A}$ defines a *label* for each event,
(M3) $\kappa : E \to \Phi$ defines a *precondition* for each event,
(M4) $\tau : 2^{\mathcal{E}} \to \Phi \to \Phi$ is a *family of predicate transformers* over E,
(M5) $\checkmark : \Phi$ defines a *termination condition*,
(M6) $\trianglelefteq : (E \times E)$ is a partial order capturing *dependency*,
(M7) $\leq : (E \times E)$ is a partial order capturing *synchronization*,
(M8) $\sqsubseteq : (E \times E)$ is a partial order capturing *per-location order*, such that
(M8a) if $\lambda(d)$ overlaps $\lambda(e)$ then $d \leq e$ implies $d \sqsubseteq e$,
(M9) $\mathsf{rmw} : E \to E$ is a partial function capturing read-modify-write *atomicity*, such that
(M9a) if $d \xrightarrow{\mathsf{rmw}} e$ then $\lambda(e)$ blocks $\lambda(d)$,
(M9b) if $d \xrightarrow{\mathsf{rmw}} e$ then $d \leq e$ and $d \sqsubseteq e$,
(M9c) if $\lambda(c)$ overlaps $\lambda(d)$ then
(i) if $d \xrightarrow{\mathsf{rmw}} e$ then $c \trianglelefteq e$ implies $c \trianglelefteq d$, $c \leq e$ implies $c \leq d$, $c \sqsubseteq e$ implies $c \sqsubseteq d$,
(ii) if $d \xrightarrow{\mathsf{rmw}} e$ then $d \trianglelefteq c$ implies $e \trianglelefteq c$, $d \leq c$ implies $e \leq c$, $d \sqsubseteq c$ implies $e \sqsubseteq c$.

A pomset is a *candidate* if there exists a relation $\mathsf{rf} : E \times E$, capturing *reads-from*, such that
(C1) if $d \xrightarrow{\mathsf{rf}} e$ and $c \xrightarrow{\mathsf{rf}} e$ then $d = c$ (ie, rf is injective),
(C2) if $d \xrightarrow{\mathsf{rf}} e$ then $\lambda(d)$ matches $\lambda(e)$,
(C3) if $d \xrightarrow{\mathsf{rf}} e$ and $\lambda(c)$ blocks $\lambda(e)$ then either $c \tilde{\sqsubseteq} d$ or $e \tilde{\sqsubseteq} c$,
where $d' \tilde{\sqsubseteq} e'$ when $e' \not\sqsubseteq d'$, and if $\lambda(d')$ strongly-blocks $\lambda(e')$ then $d' \sqsubseteq e'$,
(C4) if $d \xrightarrow{\mathsf{rf}} e$ then $d \trianglelefteq e$ and $d \sqsubseteq e$,
(C5) if $d \xrightarrow{\mathsf{rf}} e$ and $\lambda(d)$ strongly-matches $\lambda(e)$ then $d \leq e$.

A candidate pomset is *top-level* if for every $e \in E$:
(T1) $\kappa(e)$ is a tautology,
(T2) if $\lambda(e)$ is a read then there is some $d \xrightarrow{\mathsf{rf}} e$.

Note that for the IMM model, C3 is equivalent to:

$$\text{if } d \xrightarrow{\mathsf{rf}} e \text{ and } \lambda(c) \text{ blocks } \lambda(e) \text{ then either } c \sqsubseteq d \text{ or } e \sqsubseteq c.$$

Let P range over pomsets, and $\mathcal{P}$ over sets of pomsets.

We lift terminology from actions to events. For example, we say that e writes x if $\lambda(e)$ writes x. We also drop quantifiers when clear from context, such as $(\forall e \in E)(\forall x \in \mathcal{X})$. We write $d < e$ when $d \leq e$ and $d \neq e$, and similarly for $\lhd$ and $\sqsubset$.

Definition 1.6. $\mathcal{P}_1$ *refines* $\mathcal{P}_2$ if $\mathcal{P}_1 \subseteq \mathcal{P}_2$.

1.4 Semantics

Definition 1.7. If $P \in \mathit{SKIP}$ then $E = \emptyset$ and $\tau^D(\psi) \vDash \psi$.
If $P \in \mathcal{P}_1 \parallel \mathcal{P}_2$ then $(\exists P_1 \in \mathcal{P}_1)\ (\exists P_2 \in \mathcal{P}_2)$
(P1) $E = (E_1 \cup E_2)$, $\trianglelefteq \supseteq (\trianglelefteq_1 \cup \trianglelefteq_2)$, $\leq \supseteq (\leq_1 \cup \leq_2)$, $\sqsubseteq \supseteq (\sqsubseteq_1 \cup \sqsubseteq_2)$, $\mathsf{rmw} = (\mathsf{rmw}_1 \cup \mathsf{rmw}_2)$,
(P2) $\lambda = (\lambda_1 \cup \lambda_2)$,

(P3a) if $e \in E_1$ then $\kappa(e) \vDash \kappa_1(e)$,
(P3b) if $e \in E_2$ then $\kappa(e) \vDash \kappa_2(e)$,
(P4) $\tau^D(\psi) \vDash \tau_1^D(\psi)$,
(P5) $\checkmark \vDash \checkmark_1 \wedge \checkmark_2$,
(P6) E_1 and E_2 are disjoint.

If $P \in \mathcal{P}_1 ; \mathcal{P}_2$ then $(\exists P_1 \in \mathcal{P}_1)$ $(\exists P_2 \in \mathcal{P}_2)$
(S1) as in P1,
(S2a) if $e \in E_1 \setminus E_2$ then $\lambda(e) = \lambda_1(e)$,
(S2b) if $e \in E_2 \setminus E_1$ then $\lambda(e) = \lambda_2(e)$,
(S2c) if $e \in E_1 \cap E_2$ then $\lambda(e) \in \mathsf{merge}(\lambda_1(e),\ \lambda_2(e))$,
(S3a) if $e \in E_1 \setminus E_2$ then $\kappa(e) \vDash \kappa_1(e)$,
(S3b) if $e \in E_2 \setminus E_1$ then $\kappa(e) \vDash \kappa_2'(e)$,
(S3c) if $e \in E_1 \cap E_2$ then $\kappa(e) \vDash \kappa_1(e) \vee \kappa_2'(e)$, where $\kappa_2'(e) = \tau_1^{\downarrow e}(\kappa_2(e))$,
where $\downarrow e = \{c \mid c \lhd e\}$ if $\lambda(e)$ is a write, and $\downarrow e = E_1$, otherwise,
(S3d) if $\lambda_2(e)$ is a release then $\kappa(e) \vDash \checkmark_1$,
(S4) $\tau^D(\psi) \vDash \tau_1^D(\tau_2^D(\psi))$,
(S5) $\checkmark \vDash \checkmark_1 \wedge \tau_1^{E_1}(\checkmark_2)$,
(S6a) if $\lambda_1(d)$ synchronization-delays $\lambda_2(e)$ then $d \leq e$,
(S6b) if $\lambda_1(d)$ coherence-delays $\lambda_2(e)$ then $d \sqsubseteq e$.

If $P \in \mathit{IF}(\phi, \mathcal{P}_1, \mathcal{P}_2)$ then $(\exists P_1 \in \mathcal{P}_1)$ $(\exists P_2 \in \mathcal{P}_2)$
(I1) as in P1,
(I2) $\lambda = (\lambda_1 \cup \lambda_2)$,
(I3a) if $e \in E_1 \setminus E_2$ then $\kappa(e) \vDash \phi \wedge \kappa_1(e)$,
(I3b) if $e \in E_2 \setminus E_1$ then $\kappa(e) \vDash \neg\phi \wedge \kappa_2(e)$,
(I3c) if $e \in E_1 \cap E_2$ then $\kappa(e) \vDash (\phi \Rightarrow \kappa_1(e)) \wedge (\neg\phi \Rightarrow \kappa_2(e))$,
(I4) $\tau^D(\psi) \vDash (\phi \Rightarrow \tau_1^D(\psi)) \wedge (\neg\phi \Rightarrow \tau_2^D(\psi))$,
(I5) $\checkmark \vDash (\phi \Rightarrow \checkmark_1) \wedge (\neg\phi \Rightarrow \checkmark_2)$.

If $P \in \mathit{LET}(r, M)$ then $E = \emptyset$ and $\tau^D(\psi) \vDash \psi[M/r]$.
If $P \in \mathit{FENCE}(\mu, \sigma)_\alpha$ then
(F1) if $d, e \in E$ then $d = e$,
(F2) $\lambda(e) = \alpha \mathsf{F}_\sigma^\mu$,
(F4) $\tau^D(\psi) \vDash \psi$,
(F5) if $E = \emptyset$ then $\checkmark \vDash \mathsf{ff}$.

If $P \in \mathit{READ}(r, x, \mu, \sigma)_\alpha$ then $(\exists v \in \mathcal{V})$
(R1) if $d, e \in E$ then $d = e$,
(R2) $\lambda(e) = \alpha \mathsf{R}_\sigma^\mu x v$,
(R4a) $\tau^D(\psi) \vDash v{=}r \Rightarrow \psi$, if $(E \cap D) \neq \emptyset$,
(R4b) $\tau^D(\psi) \vDash \psi$, if $(E \cap D) = \emptyset$.

If $P \in \mathit{WRITE}(x, M, \mu, \sigma)_\alpha$ then $(\exists v \in \mathcal{V})$
(W1) if $d, e \in E$ then $d = e$,
(W2) $\lambda(e) = \alpha \mathsf{W}_\sigma^\mu x v$,
(W3) $\kappa(e) \vDash M{=}v$,
(W4) $\tau^D(\psi) \vDash \psi$,
(W5a) if $E = \emptyset$ then $\checkmark \vDash \mathsf{ff}$,
(W5b) if $E \neq \emptyset$ then $\checkmark \vDash M{=}v$.

$$[\![r := M]\!]_\alpha = LET(r,\ M) \qquad [\![\texttt{skip}]\!]_\alpha = SKIP$$
$$[\![r := x^\mu]\!]_\alpha = READ(r,\ x,\ \mu,\ \sigma)_\alpha \qquad [\![S_1 \parallel_\gamma S_2]\!]_\alpha = [\![S_1]\!]_\gamma \parallel [\![S_2]\!]_\alpha$$
$$[\![x^\mu := M]\!]_\alpha = WRITE(x,\ M,\ \mu,\ \sigma)_\alpha \qquad [\![S_1;\ S_2]\!]_\alpha = [\![S_1]\!]_\alpha;\ [\![S_2]\!]_\alpha$$
$$[\![\mathsf{F}^\nu_\sigma]\!]_\alpha = FENCE(\nu,\ \sigma)_\alpha \qquad [\![\texttt{if}(M)\{S_1\}\texttt{else}\{S_2\}]\!]_\alpha = IF(M{\neq}0,\ [\![S_1]\!]_\alpha,\ [\![S_2]\!]_\alpha)$$

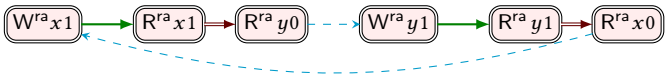
P3 Full versions (everything but address calculation):

If $P \in WRITE(x,\ M,\ \mu,\ \sigma)_\alpha$ then $(\exists v : E \to \mathcal{V})\ (\exists \theta : E \to \Phi)$
(W1) if $\theta_d \wedge \theta_e$ is satisfiable then $d = e$,
(W2) $\lambda(e) = \alpha \mathsf{W}^\mu_\sigma x v_e$,
(W3) $\kappa(e) \vDash \theta_e \wedge M{=}v_e$,
(W4) $\tau^D(\psi) \vDash \theta_e \Rightarrow \psi[M/x]$,
(W5) $\checkmark \vDash \bigvee_{e\in E} \theta_e$.

If $P \in READ(r,\ x,\ \mu,\ \sigma)_\alpha$ then $(\exists v : E \to \mathcal{V})\ (\exists \theta : E \to \Phi)$
(R1) if $\theta_d \wedge \theta_e$ is satisfiable then $d = e$,
(R2) $\lambda(e) = \alpha \mathsf{R}^\mu_\sigma x v_e$
(R3) $\kappa(e) \vDash \theta_e$,
(R4a) $(\forall e \in E \cap D)\ \tau^D(\psi) \vDash \theta_e \Rightarrow v_e{=}s_e \Rightarrow \psi[s_e/r]$,
(R4b) $(\forall e \in E \setminus D)\ \tau^D(\psi) \vDash \theta_e \Rightarrow (v_e{=}s_e \vee x{=}s_e) \Rightarrow \psi[s_e/r]$,
(R5) $(\forall s)\ \tau^D(\psi) \vDash (\bigwedge_{e\in E} \neg\theta_e) \Rightarrow \psi[s/r]$.

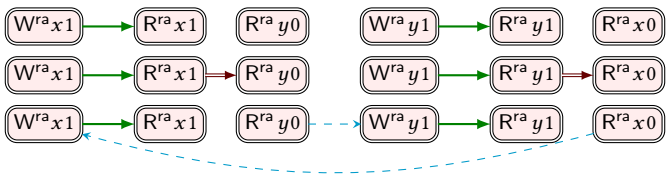
Example 1.8. Consider IRIW with all ra access:

$$x^{\mathsf{ra}} := 1 \parallel r := x^{\mathsf{ra}};\ s := y^{\mathsf{ra}} \parallel y^{\mathsf{ra}} := 1 \parallel r := y^{\mathsf{ra}};\ s := x^{\mathsf{ra}} \qquad \text{(IRIW-ACQ-ACQ)}$$



(✓POWER,C11)

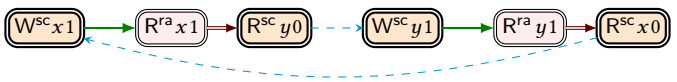
We allow this execution:



(⊴) (≤) (⊑)

IRIW-ACQ-SC, is allowed by trailing-sync compilation to power [Lahav et al. 2017, §1].

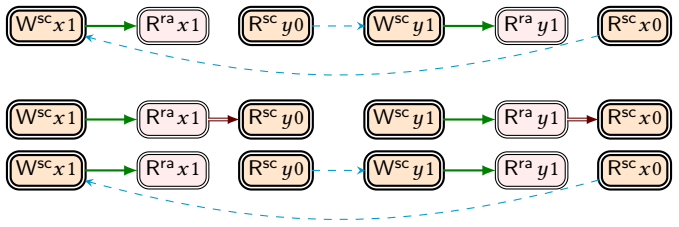
$$x^{\mathsf{sc}} := 1 \parallel r := x^{\mathsf{ra}};\ s := y^{\mathsf{sc}} \parallel y^{\mathsf{sc}} := 1 \parallel r := y^{\mathsf{ra}};\ s := x^{\mathsf{sc}} \qquad \text{(IRIW-ACQ-SC)}$$



(✓POWER,✗C11)

To model this it is convenient that synchronization is not included in dependency order:

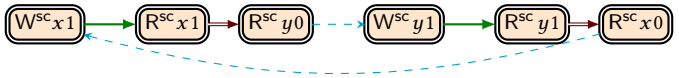
- add sc bullet to def of $\sqsubseteq$ in C3,
- add SC access to *synchronization-delays*.



(⪯) (≤) (⊑)

This correctly forbids the all sc version:

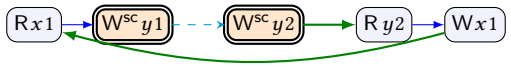
$$x^{sc} := 1 \parallel r := x^{sc};\ s := y^{sc} \parallel y^{sc} := 1 \parallel r := y^{sc};\ s := x^{sc} \qquad \text{(IRIW-sc-sc)}$$



(⪯)

Example 1.9. Thin air with an SC antidependency:

$$y^{sc} := x \parallel y^{sc} := 2 \parallel x := y - 1$$



(⪯)

1.5 Fulfillment

[This is old.]

Definition 1.10. Define $\sqsubseteq_\approx$ as follows.

$$d \sqsubseteq_\approx e \text{ when } \begin{cases} d \sqsubseteq e & \text{if } d \text{ is morally strong with } e \\ e \not\sqsubset d & \text{otherwise} \end{cases}$$

A read event e is *strongly fulfilled* if there is a $d \xrightarrow{\text{rf}} e$ and

for any c that can block e, either $c \sqsubseteq d$ or $e \sqsubseteq c$.

A read event e is *weakly fulfilled* if there is a $d \xrightarrow{\text{rf}} e$ and

for any c that can block e, either $c \sqsubseteq_\approx d$ or $e \sqsubseteq_\approx c$.

If all accesses are morally strong with each other, weak fulfillment degenerates to

$$\forall \lambda(c) = (\mathsf{W}x) \text{ either } c \sqsubseteq d \text{ or } e \sqsubseteq c$$

If no accesses are morally strong with each other, weak fulfillment degenerates to

$$\nexists \lambda(c) = (\mathsf{W}x) \text{ both } d \sqsubset c \text{ and } c \sqsubset e$$

Note that the difference between strong and weak fulfillment is limited to $\sqsubseteq$. We sometimes write 𝔰 for strong fulfillment and 𝔴 for weak fulfillment.

In diagrams, we use different shapes and colors for arrows and events. These are included only to help the reader understand why order is included. We adopt the following conventions:

- $e \to d$ arises from *reads-from* (rf),
- $e \dashrightarrow d$ arises from *fulfillment*,
- $e \to d$ arises from control/data/address *dependency*,
- $e \Rightarrow d$ arises from *synchronized access*.

2 NOTES

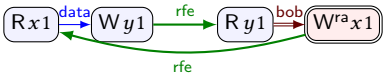
GPU stuff:

- Vulcan/Alloy
- OpenCL
- AMD PTX
- Matthew Sinclair/Sarita Adve stuff "Chasing Away RAts- Semantics and Evaluation for Relaxed Atomics on Heterogeneous Systems" and his thesis

3 ANTON'S RECENT EXAMPLES RELATING IMM AND PTX

It looks like we cannot prove compilation correctness from IMM to PTX. (In this email I assume that all threads are in the same CTA, so any relation is a morally strong one if it is applicable.) The problem is in the LB-data-rel example:

$$r := x \,;\, y := r \parallel s := y \,;\, x^{\mathsf{ra}} := 1$$



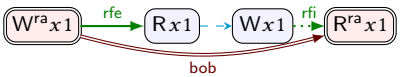
IMM forbids it, but PTX allows it. The point is that IMM mixes dependencies and release/acquire-induced po-order in its NoOOTA axiom, whereas PTX doesn't — release/acquire are only used to have coherence.

The problem is related to the one we have already discussed in the context of the C++ model – if you don't have acquire reads in the program, then you can erase release annotations from writes. In this regard, PTX is closer to PL memory models than to hardware ones.

AFAIU for the same reason we won't be able to show compilation correctness from the Pomset model to PTX even directly, if the Pomset model mixes release/acquire induced order with dependencies in the same causality relation.

Another oddity: PTX includes the bob edge below; IMM does not.

$$x^{\mathsf{ra}} := 1 \parallel r := x \,;\, x := 1 \,;\, 1 := x^{\mathsf{ra}}$$



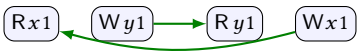
4 THIN AIR

Need $\trianglelefteq$ to prevent thin air on rlx:

$$y := x \parallel x := y$$

($\trianglelefteq$)

($\leq$)



($\leq_{\mathsf{s}}$)

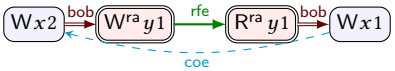
5 IMM EXAMPLES

Interpreting this definition for the IMM:

- No wk, default is rlx
- All threads in same grp (only one scope)
- Actions are morally strong when both are ra/sc, mimicking happens-before
- Strong fulfillment may do the right thing

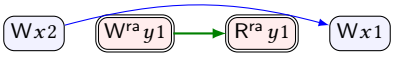
Disallowed by IMM:

$x := 2\,;\, y^{\mathsf{ra}} := 1 \parallel r := y^{\mathsf{ra}}\,;\, x := 1$ (PUB-REL-ACQ-COE)



(✗IMM)

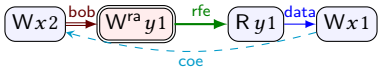
($\trianglelefteq = \leq$)



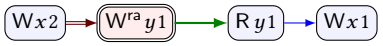
(s)

Allowed by IMM, but not by Power/ARMv7/ARMv8/TSO:

$x := 2\,;\, y^{\mathsf{ra}} := 1 \parallel r := y\,;\, x := 1$ (PUB-REL-RLX-COE)

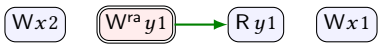


(✓IMM)



($\trianglelefteq$)

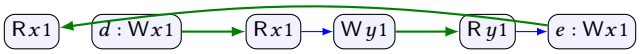
($\leq$)



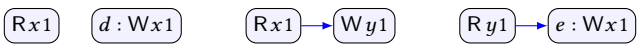
(s)

Example from talk:

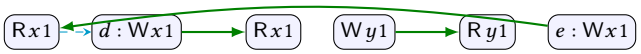
$r := x\,;\, x := 1 \parallel y := x \parallel x := y$ (ARM7-WEAK)



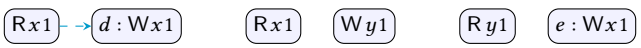
($\trianglelefteq$)



($\leq$)



(s)



(w)

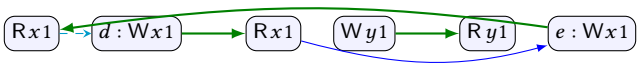
6 TWO ORDER IDEA

The two order idea from OOPSLA talk is:

- Require: $d \sqsubseteq e$ when $d \trianglelefteq e$ and they conflict

This does not work for the IMM or ARMv7, but it may work for Power, TSO, ARMv8. That would be nice. Let's write w for this notion, with strong fulfillment.

With this there is a cycle in ARM7-WEAK (weak/strong fulfillment not relevant here):



(w)

Anton says: ARM7-WEAK is forbidden by Power, TSO, ARMv8, but allowed by ARMv7. Maybe it isn't that important to support it anymore.

There is also a cycle in PUB-REL-RLX-COE. Anton says: I checked Power/ARMv7 models in this regard. They disallow the behavior (as well as ARMv8 and TSO), so we can in principle strengthen IMM to forbid it as well. For that, we may add axiom to IMM forbidding cycles in $\mathsf{co} \cup ([\mathsf{W}]; \mathsf{rfe}^?; ([\mathsf{R}^{\mathsf{acq}}] \cup \mathsf{po}; [\mathsf{FW}^{\mathsf{rel}}]); \mathsf{ar}^*; [\mathsf{W}])$. This works if we have acquire/release accesses on the path since they are compiled with fences to Power.

7 PTX EXAMPLES

Based on [Lustig et al. 2019; NVIDIA 2020].

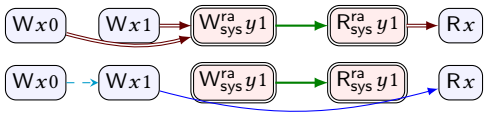
PTX requires weak fulfillment.

Default scope is grp. In examples, all threads in different grps.

Default mode is wk.

$(\mathsf{R}x0)$ must be forbidden. Before fulfilling the read:

$$x := 0;\ x := 1;\ y^{\mathsf{ra}}_{\mathsf{sys}} := 1 \parallel r := y^{\mathsf{ra}}_{\mathsf{sys}};\ s := x \qquad (\text{PUB1}_{\text{SYS}})$$



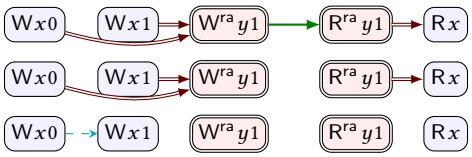
$(\trianglelefteq = \leq)$

$(\sqsubseteq)$

$(\mathsf{W}x1) \sqsubseteq_{\sim} (\mathsf{R}x)$ is required by M7, enforcing publication.

$(\mathsf{R}x0)$ must be allowed:

$$x := 0;\ x := 1;\ y^{\mathsf{ra}} := 1 \parallel r := y^{\mathsf{ra}};\ s := x \qquad (\text{PUB1}_{\text{CTA}})$$



$(\trianglelefteq)$

$(\leq)$

$(\sqsubseteq)$

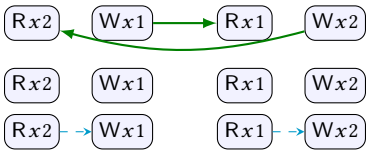
We do not have $(\mathsf{W}^{\mathsf{ra}}y1) \leq (\mathsf{R}^{\mathsf{ra}}y1)$ since F3 only requires order for things that are morally strong.

Another example that may be of interest (nothing morally strong). Can this $(\mathsf{R}x0)$?

$$x := 0;\ x := 1 \parallel y := x \parallel \texttt{if}(y)\{r := x\}$$

PTX allows TC16 for events that are not mutually strong (TC16_{WK}), but disallows it when events are mutually strong (TC16_{SYS}). Note that $\leq$ imposes no requirements here. Fulfillment imposes no order. This example shows that F3C cannot be strengthened to require that $d \sqsubseteq e$.

$$r := x;\ x := 1 \parallel s := x;\ x := 2 \qquad (\text{TC16}_{\text{WK}})$$

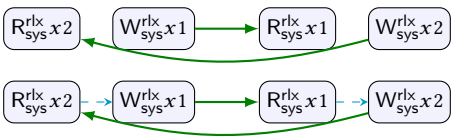


$(\trianglelefteq)$

$(\leq)$

$(\sqsubseteq)$

$$r := x^{\mathsf{rlx}}_{\mathsf{sys}};\ x^{\mathsf{rlx}}_{\mathsf{sys}} := 1 \parallel s := x^{\mathsf{rlx}}_{\mathsf{sys}};\ x^{\mathsf{rlx}}_{\mathsf{sys}} := 2 \qquad (\text{TC16}_{\text{SYS}})$$

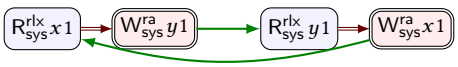


$(\trianglelefteq = \leq)$

$(\sqsubseteq)$

About Release-Acquire semantics. Anton confirms that the following example is allowed in C11, but disallowed in the IMM. It is apparently allowed in C11 with the intention to allow releasing writes to be downgraded to relaxed in the case that only fulfill relaxed reads.

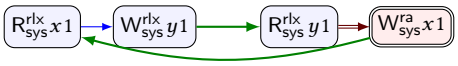
$$r := x^{\mathsf{rlx}}_{\mathsf{sys}};\ y^{\mathsf{ra}}_{\mathsf{sys}} := 1 \parallel s := y^{\mathsf{rlx}}_{\mathsf{sys}};\ x^{\mathsf{ra}}_{\mathsf{sys}} := 1 \qquad (\text{LB-REL})$$



$(\trianglelefteq = \leq)$

Another example from Anton. This is allowed in PTX because it does not include synchronization in the no-tar axiom, only in coherence and causality.

$$r := x^{\mathsf{rlx}}_{\mathsf{sys}}\,;\; y^{\mathsf{rlx}}_{\mathsf{sys}} := r \;\|\; s := y^{\mathsf{rlx}}_{\mathsf{sys}}\,;\; x^{\mathsf{ra}}_{\mathsf{sys}} := 1 \qquad \text{(LB-DATA-REL)}$$

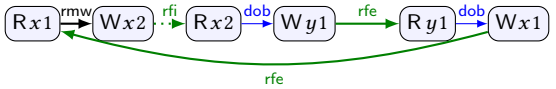


$(\trianglelefteq = \leq)$

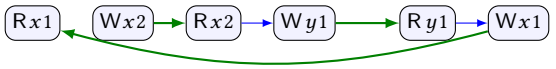
8 RFI EXAMPLES

Bad example:

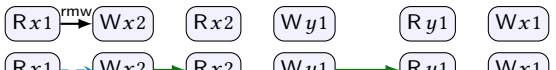
$$r := \mathsf{EXCHG}(x, 2)\,;\; s := x\,;\; y := s-1 \;\|\; r := y\,;\; x := r$$



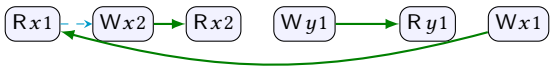
(✓Arm8)



$(\trianglelefteq)$

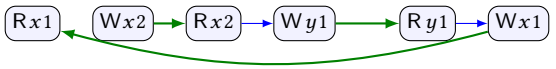


$(\leq)$

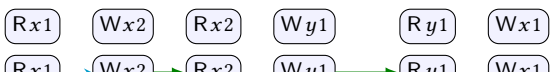


$(\sqsubseteq)$

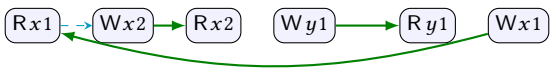
$$r := x\,;\; x := 2\,;\; s := x\,;\; y := s-1 \;\|\; r := y\,;\; x := r$$



$(\trianglelefteq)$



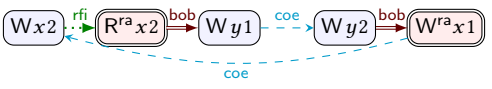
$(\leq)$



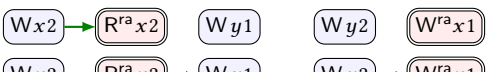
$(\sqsubseteq)$

Anton example 1 (Allowed by ARM) `[rfi-coe-coe]`

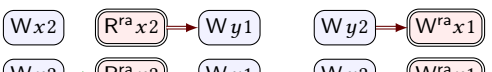
$$x := 2\,;\; r := x^{\mathsf{ra}}\,;\; y := 1 \;\|\; y := 2\,;\; x^{\mathsf{ra}} := 1 \qquad \text{(RFI-COE-COE)}$$



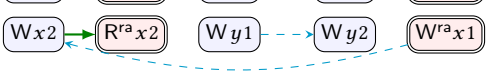
(✓Arm8)



$(\trianglelefteq)$



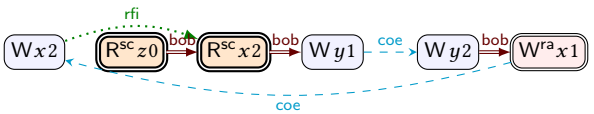
$(\leq)$



$(\sqsubseteq)$

Internal reads survive acquires `[rfi-acq-coe-coe]` (where SC read = LDAR)

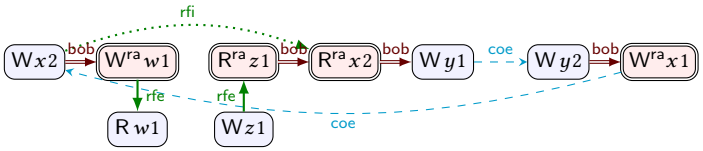
$$x := 2\,;\; s := z^{\mathsf{sc}}\,;\; r := x^{\mathsf{sc}}\,;\; y := 1 \;\|\; y := 2\,;\; x^{\mathsf{ra}} := 1 \qquad \text{(RFI-ACQ-COE-COE)}$$



(✓Arm8)

And release-acquire pairs `[rfi-ra-coe-coe]` (where acquiring read = LDAPR)

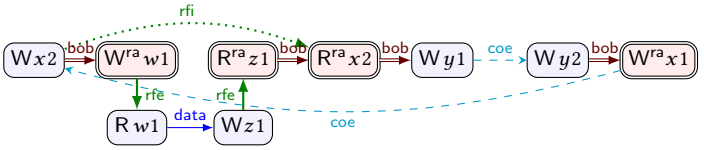
$$x := 2;\ w^{\mathsf{ra}} := 1;\ s := z^{\mathsf{ra}};\ r := x^{\mathsf{ra}};\ y := 1 \ \|\ y := 2;\ x^{\mathsf{ra}} := 1 \ \|\ r := w;\ z := 1; \qquad \text{(RFI-RA-COE-COE2)}$$



(✓Arm8)

But not if either acquire is strengthened to SC (where SC read = LDAR). The execution is also disallowed if an external thread places order between the ra accesses:

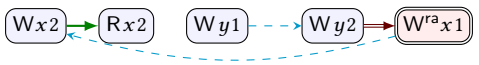
$$x := 2;\ w^{\mathsf{ra}} := 1;\ s := z^{\mathsf{ra}};\ r := x^{\mathsf{ra}};\ y := 1 \ \|\ y := 2;\ x^{\mathsf{ra}} := 1 \ \|\ r := w;\ z := r; \qquad \text{(RFI-RA-DATA-COE-COE)}$$



(✗Arm8)

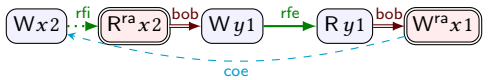
To allow this, weaken ra to rlx when read fulfilled by relaxed write of same thread (don't need to allow this when the write is part of an RMW).

$$x := 2;\ r := x^{\mathsf{ra}};\ y := 1 \ \|\ y := 2;\ x^{\mathsf{ra}} := 1$$



RF variant `[rfi-rfe-coe]`:

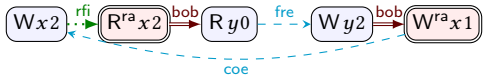
$$x := 2;\ r := x^{\mathsf{ra}};\ y := 1 \ \|\ s := y;\ x^{\mathsf{ra}} := 1 \qquad \text{(RFI-RFE-COE)}$$



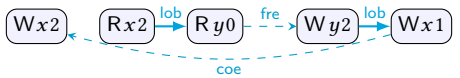
(✓Arm8)

TSO variant `[rfi-fre-coe]`:

$$x := 2;\ r := x^{\mathsf{ra}};\ s := y \ \|\ y := 2;\ x^{\mathsf{ra}} := 1 \qquad \text{(RFI-COE-COE)}$$



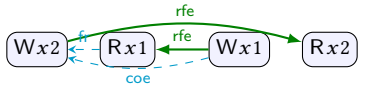
(✓Arm8)



(✓TSO)

Note that TSO does not order W to R in local order, even in poloc. Nonetheless, TSO disallows the following because of local visibility in first thread.

$$x := 2;\ r := x \ \|\ x := 1;\ s := x$$



(✗TSO)

[Higham and Kawash 2000] describe TSO as a linearization of partial order including:

- poloc

- lws = po; [W]
- $d \overset{po}{\cdots\blacktriangleright} e$ when $c \overset{rfe}{\longrightarrow} d \overset{po}{\cdots\blacktriangleright} e$

[Alglave et al. 2020] describe TSO as linearization of partial order satisfying internal visibility and including

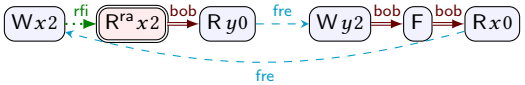
- [W]; po; [W]
- $d \overset{po}{\cdots\blacktriangleright} e$ when $c \overset{rfe}{\longrightarrow} d \overset{po}{\cdots\blacktriangleright} e$, from `(range(rfe) * _)`
- [R]; po; [W], from `(rfi^-1; lob)`

Ignoring fences and RMWs:

```
let rec lob = po \ ([W]; po; [R])
let IM0 = loc & ((IW * (M\IW)) | ((W\FW) * FW))
let gc-req = (W * _) | ((R * _) & ((range(rfe) * _) | (rfi^-1; lob))
let preorder-gcb = IM0 | lob & gc-req
```

Double FRE variant `[rfi-fre-fre]`:

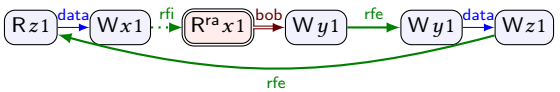
$$x := 2; r := x^{ra}; s := y \parallel y := 2; \mathsf{F}; r := x \qquad \text{(RFI-FRE-FRE)}$$



(✓Arm8)

It does not seem possible to do this only with rfe. ARM disallows this `[data-rfi-rfe-rfe]`:

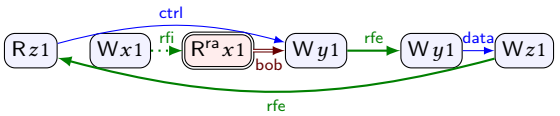
$$x := z; r := x^{ra}; y := 1 \parallel z := y \qquad \text{(DATA-RFI-RFE-RFE)}$$



(✗Arm8)

It also disallows `[ctrl-rfi-rfe-rfe]`:

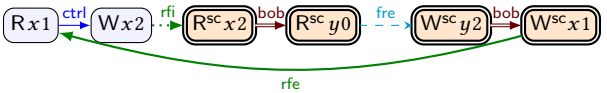
$$\texttt{if}(z)\{\}; x := 1; r := x^{ra}; y := 1 \parallel z := y \qquad \text{(CTRL-RFI-RFE-RFE)}$$



(✗Arm8)

ARM allows some counterintuitive results for SC access `[ctrl-rfi-fre-rfe]`:

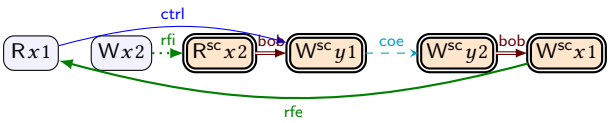
$$\texttt{if}(x)\{\}; x := 2; r := x^{sc}; s := y^{sc} \parallel y^{sc} := 2; x^{sc} := 1 \qquad \text{(CTRL-RFI-FRE-RFE)}$$



(✓Arm8)

Not possible with coe `[ctrl-rfi-coe-rfe]`:

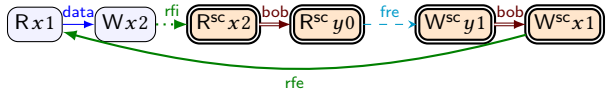
$$\texttt{if}(x)\{\}; x := 2; r := x^{sc}; y^{sc} := 1 \parallel y^{sc} := 2; x^{sc} := 1 \qquad \text{(CTRL-RFI-COE-RFE)}$$



(✗Arm8)

This is not allowed with a data dependency instead of a control dependency [data-rfi-fre-rfe]:

$x := x+1;\ r := x^{sc};\ s := y^{sc} \parallel y^{sc} := 1;\ x^{sc} := 1$ (DATA-RFI-FRE-RFE)

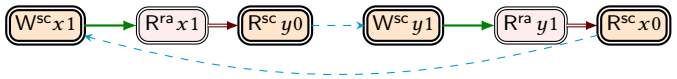


(✗Arm8)

9 SC EXAMPLES

IRIW-ACQ-SC is allowed by trailing-sync compilation to power [Lahav et al. 2017, §1].

$x^{sc} := 1 \parallel r := x^{ra};\ s := y^{sc} \parallel y^{sc} := 1 \parallel r := y^{ra};\ s := x^{sc}$ (IRIW-ACQ-SC)

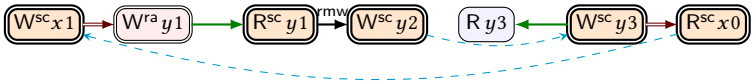


(✓POWER,RC11)

This example is hard to get right for power because it must be allowed with ra reads, but disallowed with sc reads. This seems unsolvable: To allow the version with ra, we would need to weaken the order between the reads in each thread for the ra case, and that would break publication.

Leading sync is also unsound in C11 with RMW [Lahav et al. 2017, §2.1].

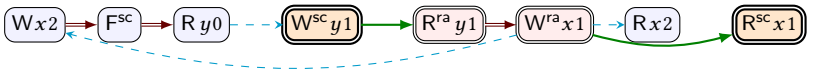
$x^{sc} := 1;\ y^{ra} := 1 \parallel \mathsf{FADD}^{sc,sc}(y, 1);\ s := y \parallel y^{sc} := 3;\ s := x^{sc}$ (Z6.U)



(✓POWER,RC11)

Leading sync is also unsound in C11 with SC fences [Lahav et al. 2017, §A.1].

$x := 2;\ \mathsf{F}^{sc};\ r := y \parallel y^{sc} := 1 \parallel r := y^{ra};\ x^{ra} := 1;\ s := x \parallel r := x^{sc}$ (RSYNC+RSC)

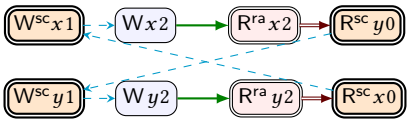


(✓RC11)

Fulfillment of $(\mathsf{R}x2)$ requires that either $(\mathsf{W}^{ra}x1) \dashrightarrow (\mathsf{W}x2)$ or $(\mathsf{R}x2) \dashrightarrow (\mathsf{W}^{ra}x1)$. It's interesting that in the pomset, $(\mathsf{R}^{sc}x1)$ is not needed to get a cycle.

There is a long discussion of this in [Bender and Palsberg 2019, §5.2, Fig. 17], where they also discuss this example:

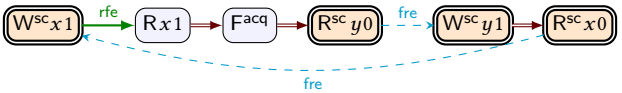
$x^{sc} := 1;\ x := 2 \parallel y^{sc} := 1;\ y := 2 \parallel r := x^{ra};\ s := y^{sc} \parallel r := y^{ra};\ s := x^{sc}$ (IRIW-SC-RLX-ACQ)



(✓RC11)

[Lahav et al. 2017, §A.2] claims that Arm8 allows this [RWC+acq+sc], but herd7 rejects it. Reason: they are citing the flowing/pop model [Flur et al. 2016] rather than [Pulte et al. 2018].

$x^{sc} := 1 \parallel r := x;\ \mathsf{F}^{acq};\ s := y^{sc} \parallel y^{sc} := 1;\ r := x^{sc}$ (RWC+ACQ+SC)

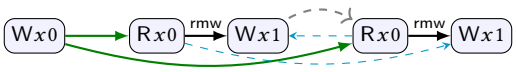


(✗Arm8)

10 ADDITIONAL RMW EXAMPLES

It is not possible for two RMWs to see the same write.

$$x := 0;\ \left(\mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(x,1)\ \|\ \mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(x,1)\right)$$

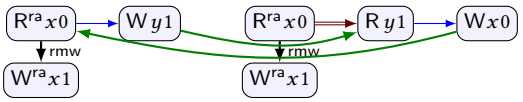


(RMW0)

The gray arrow is required the RMW atomicity axioms.

Lee et al. [2020] introduce PS2.0 to refine the treatment of RMWs in the promising semantics (PS). Their examples have the expected results here, with far less work. First they recall that PS requires quantification over multiple futures in order to disallow executions such as CDRF:

$$r := \mathsf{FADD}^{\mathsf{ra},\mathsf{ra}}(x,1);\ \mathtt{if}(r{=}0)\{y := 1\}\ \|\ r := \mathsf{FADD}^{\mathsf{ra},\mathsf{ra}}(x,1);\ \mathtt{if}(r{=}0)\{\mathtt{if}(y)\{x := 0\}\}$$

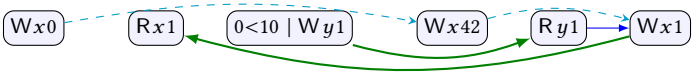


(CDRF)

This execution is clearly impossible, due to the cycle above. In this diagram, we have not drawn order adjacent to the writes of the RMWs, since this is not necessary to produce the cycle. If CDRF is allowed then DRF-RA fails.

PS does not support global value range analysis, as modeled by GA+E below. Our semantics permits GA+E:

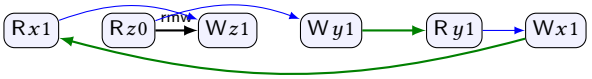
$$x := 0;\ \left(r := \mathsf{CAS}^{\mathsf{rlx},\mathsf{rlx}}(x,0,1);\ \mathtt{if}(r{<}10)\{y := 1\}\ \|\ x := 42;\ x := y\right)$$



(GA+E)

PS also does not support register promotion, as modeled by RP below. Our semantics permits RP:

$$r := x;\ s := \mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(z,r);\ y := s{+}1\ \|\ x := y$$

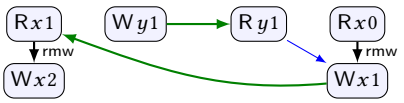


(RP)

These following examples are from "Modular Data-Race-Freedom Guarantees in the Promising Semantics" to appear in PLDI21.

CDRF shows that our semantics is not too permissive for ra-RMWs. But what about rlx-RMWs. The following execution is allowed by Arm8, and PS2.0, but disallowed by PS2.1.

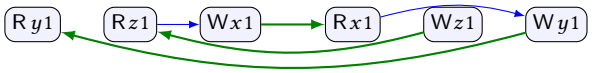
$$r := \mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(x,1);\ y := 1\ \|\ r := y;\ s := \mathsf{FADD}^{\mathsf{rlx},\mathsf{rlx}}(x,r)$$



(RMW-W)

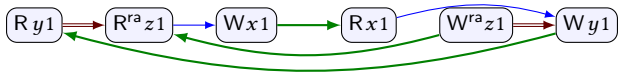
If this $\{z\}$-DRF-RA?

$$\mathtt{if}(y)\{x := z\}\,\mathtt{else}\,\{x := 1\}\ \|\ r := x;\ z := 1;\ y := r$$



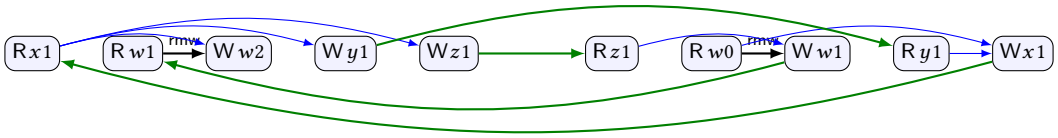
(NAIVE-LDRF-RA-FAIL)

Interpreting $\{z\}$ as ra:



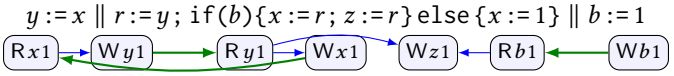
Our semantics already disallows LDRF-FAIL-PS, which is similar to OOTA4.

$$\texttt{if}(x)\{\texttt{FADD}(w,1);\, y:=1;\, z:=1\} \parallel \texttt{if}(!z)\{x:=1\}\,\texttt{else}\,\{\texttt{if}(!\texttt{FADD}(w,1))\{x:=y\}\}$$



(LDRF-FAIL-PS)

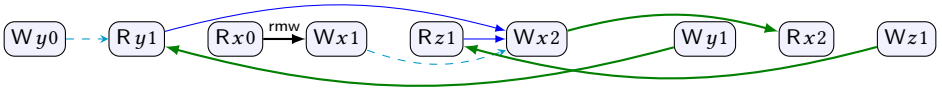
$$y:=x \parallel r:=y;\, \texttt{if}(b)\{x:=r;\, z:=r\}\,\texttt{else}\,\{x:=1\} \parallel b:=1$$



(OOTA4)

If RMWs simply use the same semantics as read and write, then we allow LDRF-PF-FAIL, which is used to show failure of LDRF-SC.

$$y:=0;\, \texttt{if}(y)\{\texttt{if}(!\texttt{CAS}(x,0,1))\{\texttt{if}(z)\{x:=2\}\}\} \parallel y:=1;\, \texttt{if}(1{\neq}\texttt{CAS}(x,0,3))\{z:=1\}$$



(LDRF-PF-FAIL)

To disallow this, we need to retain the dependency $(\mathsf{R}x2) \longrightarrow (\mathsf{W}z1)$. For this, we need to avoid the substitution for x. This is clearer in the LICS semantics. You just use L6 rather than L5 for the independent case on RMWs.

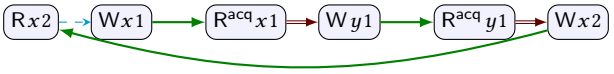
11 EXAMPLE FROM JAM PAPER

From [Bender and Palsberg 2019, §3.3]. With partial coherence/weak fulfillment you need to be careful that RMWs are totally ordered (if that's a property you want). May not come for free.

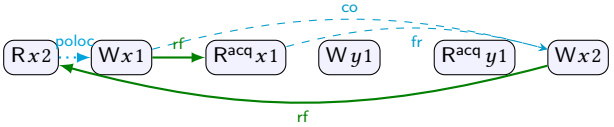
From [Bender and Palsberg 2019, §B]: "Here we demonstrate that it is possible to construct a program that is only forbidden due to the total coherence order"

$$r:=x;\, x:=1 \parallel r:=x^{\mathsf{ra}};\, x:=1 \parallel r:=y^{\mathsf{ra}};\, x:=2$$

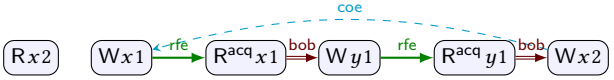
(TOTAL-CO)



(✗Arm8)



(✗Arm8)



(✗Arm8)

12 OLD MODEL

μ	::= wk	(Weak)	σ	::= grp	(Thread group)
	| rlx	(Relaxed)		| proc	(Processor)
	| ra	(Release/Acquire)		| sys	(System)
	| sc	(Sequentially Consistent)			

Orders/Relations in model

- $\trianglelefteq$ is the old $\leq$ (without coherence stuff from F4 and P5B).
  This provides the NO-TAR axiom.
- $\leq$ is a the *happens-before* suborder, which only includes rf when they are morally strong.
  This serves as a cross-location transitive kernel for the per-location order.
- $\sqsubseteq$ is a per-location order that relates morally strong and poloc accesses
  This includes $\leq$ for morally strong accesses.
  This provides the SC-PER-LOC axiom.

Write $d \vartriangle e$ if they conflict (ie, read/write or write/write, same location).
Write $d \blacktriangle e$ if they conflict and are morally strong

Definition 12.1. A *pomset with preconditions* is a tuple $(E, \lambda, \leq, \trianglelefteq, \sqsubseteq)$ where

(M1) E is a set of *events*
(M2) $\lambda : E \to (\Phi \times \mathcal{A})$ is a *labeling* from which we derive functions
- $\kappa : E \to \Phi$ *(formulae)*
- $\lambda : E \to \mathcal{A}$ *(actions)*

(M3) $\leq \subseteq (E \times E)$, $\trianglelefteq \subseteq (E \times E)$, and $\sqsubseteq \subseteq (E \times E)$ are partial orders
(M4) $\bigwedge_e \kappa(e)$ is satisfiable *(consistency)*
(M5) if $d \trianglelefteq e$ then $\kappa(e)$ implies $\kappa(d)$ *(causal strengthening)*
(M6) if $d \leq e$ then $d \trianglelefteq e$
(M7) if $d \leq e$ and d conflicts with e then $d \sqsubseteq e$

Definition 12.2 (Strong fulfillment). We say $\lambda(d) = (\mathsf{W}xv)$ *fulfills* $\lambda(e) = (\mathsf{R}xv)$ if

(F3A) $d \vartriangleleft e$
(F3B) $d < e$ if d is morally strong with e
(F3C) $d \sqsubseteq e$ (if d is not morally strong with e)
(F4) $\forall \lambda(c) = (\mathsf{W}x..)$ either $c \sqsubseteq d$ or $e \sqsubseteq c$,

Definition 12.3 (Weak fulfillment). We say $\lambda(d) = (\mathsf{W}xv)$ *fulfills* $\lambda(e) = (\mathsf{R}xv)$ if

(F3A) $d \vartriangleleft e$
(F3B) $d < e$ if d is morally strong with e
(F3C) $e \not\sqsubseteq d$ (if d is not morally strong with e)
(F4) $\forall \lambda(c) = (\mathsf{W}x..)$ either $c \sqsubseteq\!\!\!\sim d$ or $e \sqsubseteq\!\!\!\sim c$, where

$$d \sqsubseteq\!\!\!\sim e \text{ when } \begin{cases} d \sqsubseteq e & \text{if } d \text{ is morally strong with } e \\ e \not\sqsubseteq d & \text{otherwise} \end{cases}$$

If all accesses are morally strong with each other, weak fulfillment degenerates to

(F3) $d < e$
(F4) $\forall \lambda(c) = (\mathsf{W}x..)$ either $c \sqsubseteq d$ or $e \sqsubseteq c$

If no accesses are morally strong with each other, weak fulfillment degenerates to

(F3) $e \not\sqsubseteq d$
(F4) $\nexists \lambda(c) = (\mathsf{W}x..)$ both $d \sqsubset c$ and $c \sqsubset e$

Note that the difference between strong and weak fulfillment is limited to $\sqsubseteq$. We sometimes write $\mathbb{E}$ for strong fulfillment and $\mathbb{W}$ for weak fulfillment.

Prefixing is as in OOPSLA, using $\leq$ for order everywhere except P5B, which has $\sqsubseteq$.

Definition 12.4. Let $P' \in (\phi \mid a) \Rightarrow \mathcal{P}$ when $(\exists P \in \mathcal{P})$ $(\forall e \in E)$

(P1) $E' = E \cup \{d\}$
(P2) $\leq' \supseteq \leq$, $\trianglelefteq' \supseteq \trianglelefteq$, and $\sqsubseteq' \supseteq \sqsubseteq$
(P3A) $\lambda'(e) = \lambda(e)$
(P3B) $\lambda'(d) = a$
(P4A) $\kappa'(d)$ implies $\phi \wedge (d \notin E \vee \kappa(d))$
(P4B) if $d \neq (\mathsf{R}..)$ then $e = d$ or $\kappa'(e)$ implies $\kappa(e)$
(P4C) if $d = (\mathsf{R}vx)$ then $e = d$ or $\kappa'(e)$ implies $\kappa(e)[v/x]$
(P5A) if $d = (\mathsf{R}..)$, $e = (\mathsf{W}..)$ then $e = d$ or $\kappa'(e)$ implies $\kappa(e)$ or $d \leq' e$
(P5B) if d conflicts with e then $d \sqsubseteq' e$
(P5C) if d is an acquire or e is a release then $d \leq' e$
(P5D) if d is an SC write and e is an SC read then $d \leq' e$
(P5E) if d reads, and e is an acquiring fence, then $d \leq' e$
(P5F) if d is a releasing fence, and e writes, then $d \leq' e$

REFERENCES

Jade Alglave, Will Deacon, Richard Grisenthwaite, Antoine Hacquard, and Luc Maranget. 2020. Armed cats: Formal Concurrency Modelling at Arm. Draft. , 49 pages.

John Bender and Jens Palsberg. 2019. A formalization of Java's concurrent access modes. *Proc. ACM Program. Lang.* 3, OOPSLA (2019), 142:1–142:28. https://doi.org/10.1145/3360568

William Ferreira, Matthew Hennessy, and Alan Jeffrey. 1996. A Theory of Weak Bisimulation for Core CML. In *Proceedings of the 1996 ACM SIGPLAN International Conference on Functional Programming, ICFP 1996, Philadelphia, Pennsylvania, USA, May 24-26, 1996*, Robert Harper and Richard L. Wexelblat (Eds.). ACM, 201–212. https://doi.org/10.1145/232627.232649

Shaked Flur, Kathryn E. Gray, Christopher Pulte, Susmit Sarkar, Ali Sezgin, Luc Maranget, Will Deacon, and Peter Sewell. 2016. Modelling the ARMv8 architecture, operationally: concurrency and ISA. In *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2016, St. Petersburg, FL, USA, January 20 - 22, 2016*, Rastislav Bodík and Rupak Majumdar (Eds.). ACM, 608–621. https://doi.org/10.1145/2837614.2837615

Lisa Higham and Jalal Kawash. 2000. Memory Consistency and Process Coordination for SPARC Multiprocessors. In *High Performance Computing - HiPC 2000, 7th International Conference, Bangalore, India, December 17-20, 2000, Proceedings (Lecture Notes in Computer Science, Vol. 1970)*, Mateo Valero, Viktor K. Prasanna, and Sriram Vajapeyam (Eds.). Springer, 355–366. https://doi.org/10.1007/3-540-44467-X_32

Ori Lahav, Viktor Vafeiadis, Jeehoon Kang, Chung-Kil Hur, and Derek Dreyer. 2017. Repairing sequential consistency in C/C++11. In *Proceedings of the 38th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI 2017, Barcelona, Spain, June 18-23, 2017*, Albert Cohen and Martin T. Vechev (Eds.). ACM, 618–632. https://doi.org/10.1145/3062341.3062352

Sung-Hwan Lee, Minki Cho, Anton Podkopaev, Soham Chakraborty, Chung-Kil Hur, Ori Lahav, and Viktor Vafeiadis. 2020. Promising 2.0: global optimizations in relaxed memory concurrency. In *Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI 2020, London, UK, June 15-20, 2020*, Alastair F. Donaldson and Emina Torlak (Eds.). ACM, 362–376. https://doi.org/10.1145/3385412.3386010

Daniel Lustig, Sameer Sahasrabuddhe, and Olivier Giroux. 2019. A Formal Analysis of the NVIDIA PTX Memory Consistency Model. In *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS 2019, Providence, RI, USA, April 13-17, 2019*, Iris Bahar, Maurice Herlihy, Emmett Witchel, and Alvin R. Lebeck (Eds.). ACM, 257–270. https://doi.org/10.1145/3297858.3304043

NVIDIA. 2020. Parallel Thread Execution ISA Version 7.1. https://docs.nvidia.com/cuda/parallel-thread-execution/index.html#memory-consistency-model.

Christopher Pulte, Shaked Flur, Will Deacon, Jon French, Susmit Sarkar, and Peter Sewell. 2018. Simplifying ARM concurrency: multicopy-atomic axiomatic and operational models for ARMv8. *PACMPL* 2, POPL (2018), 19:1–19:29. https://doi.org/10.1145/3158107