A simple separation logic

Andreas Herzig

University of Toulouse, IRIT-CNRS, France

Workshop ANR DynRes, Toulouse, May 2013

Separation logic

$M \models \varphi_1 * \varphi_2$ iff there are M_1, M_2 such that

1) M can be separated into M_1 and M_2

2) $M_1 \models \varphi_1$ & $M_2 \models \varphi_2$

- idea: separation $\approx$ disjoint union of structures
- originally application: modular verification of programs
- in focus: particular memory structures
  - monoids (words)
  - pointer structures (heaps)
  - ...

Separation logic for knowledge representation

$M \models \varphi_1 * \varphi_2$ iff there are M_1, M_2 such that

1) M can be separated into M_1 and M_2

2) $M_1 \models \varphi_1$ & $M_2 \models \varphi_2$

- application here: knowledge representation
  - memory = models of classical propositional logic, description logics, modal logics, multi-valued logics,. . .
- separability = modularity
  - $\varphi \leftrightarrow (\varphi_1 * \varphi_2)$ = "φ consists in modules φ_1 and φ_2"
  - modular querying (cf. description logic ontologies)
  - modular update and revision
- starting point: propositional logic

Separating classical valuations

$V \models \varphi_1 * \varphi_2$ iff there are V_1, V_2 such that

1) V can be separated into V_1 and V_2
2) $V_1 \models \varphi_1$ & $V_2 \models \varphi_2$

- V = valuation of classical propositional logic
  - set of propositional variables
  - total function from set of propositional variables $\mathbb{P}$ to $\{0, 1\}$
- idea: V separable into V_1 and V_2 if $\{V_1, V_2\}$ partitions V
  - $\text{dom}(V_1) \cap \text{dom}(V_2) = \emptyset$
  - $\text{dom}(V_1) \cup \text{dom}(V_2) = \text{dom}(V)$

$\Rightarrow V_1, V_2$ partial valuations
  - notation: small letters v_1, v_2

Two separation operators

$$V \models \varphi_1 * \varphi_2 \text{ iff there are } v_1, v_2 \text{ such that}$$
$$1)\ \{v_1, v_2\} \text{ partitions } V$$
$$2)\ v_1 \models \varphi_1 \ \&\ v_2 \models \varphi_2$$

- two options to define satisfaction in partial valuations:

$$v \models \varphi \text{ iff } \begin{cases} V \models \varphi \text{ for every total extension } V \text{ of } v \\ V \models \varphi \text{ for some total extension } V \text{ of } v \end{cases}$$

  where the total V is an extension of the partial v if $V(p) = v(p)$ for every $p \in \mathrm{dom}(v)$
- Set Separation Logic SSL

Properties of Set Separation Logic SSL

- decidable
  - $\neq$ most propositional separation logics
    [Larchey-Wendling&Galmiche, LICS 2010],
    [Brotherston&Kanowitch, LICS 2010]
- SAT problem is in PSPACE
  - polynomial translation to Dynamic Logic of Propositional Control DL-PA [Balbiani, Herzig&Troquard, LICS 2013]
- incompatible with standard accounts of update and revision
  - incompatible with AGM postulates for revision
    [Alchourrón, Gärdenfors&Makinson, 1985; Gärdenfors, 1988]
  - incompatible with KM postulates for update
    [Katsuno&Mendelzon, 1990]
- the details are in the rest of the talk...

Outline

Language

$$\varphi \quad ::= \quad p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \dot{\wedge} \varphi \mid \varphi \dot{\parallel} \varphi$$

where p ranges over the set of propositional variables $\mathbb{P}$

$\varphi \dot{\wedge} \psi$ = "φ and ψ are statically separable"
= "update of $\varphi \wedge \psi$ can be done separately"

$\varphi \dot{\parallel} \psi$ = "φ and ψ are dynamically separable"
= "update by $\varphi \wedge \psi$ can be done separately (in parallel)"

Truth conditions

$$
\begin{aligned}
V \models p &\text{ iff } V(p) = 1 \\
V \models \neg\varphi &\text{ iff } V \not\models \varphi \\
V \models \varphi_1 \wedge \varphi_2 &\text{ iff } V \models \varphi_1 \text{ and } V \models \varphi_2 \\
V \models \varphi_1 \dot{\wedge} \varphi_2 &\text{ iff } \text{there is a partition } \{P_1, P_2\} \text{ of } \mathbb{P} \text{ such that} \\
&\phantom{\text{ iff }} V_1 \models \varphi_1 \text{ for every extension } V_1 \text{ of } V|_{P_1} \text{ and} \\
&\phantom{\text{ iff }} V_2 \models \varphi_2 \text{ for every extension } V_2 \text{ of } V|_{P_2} \\
V \models \varphi_1 \dot{\|} \varphi_2 &\text{ iff } \text{there is a partition } \{P_1, P_2\} \text{ of } \mathbb{P} \text{ such that} \\
&\phantom{\text{ iff }} V_1 \models \varphi_1 \text{ for some extension } V_1 \text{ of } V|_{P_1} \text{ and} \\
&\phantom{\text{ iff }} V_2 \models \varphi_2 \text{ for some extension } V_2 \text{ of } V|_{P_2}
\end{aligned}
$$

Truth conditions: examples

- for $p \neq q$,
  for V_{pq} valuation such that $V_{pq}(p) = V_{pq}(q) = 1$:

$$V_{pq} \models p \mathbin{\dot{\wedge}} q \qquad V_{pq} \models p \mathbin{\dot{\|}} q$$

$$V_{pq} \not\models (\neg p) \mathbin{\dot{\wedge}} (\neg q) \qquad V_{pq} \models (\neg p) \mathbin{\dot{\|}} (\neg q)$$

$$V_{pq} \models (p \vee q) \mathbin{\dot{\wedge}} (p \vee q)$$

Validity

- valid formula schemas:

$$\varphi_1 \dot{\wedge} \varphi_2 \leftrightarrow \varphi_2 \dot{\wedge} \varphi_1 \qquad \varphi_1 \dot{\|} \varphi_2 \leftrightarrow \varphi_2 \dot{\|} \varphi_1$$

$$\varphi_1 \dot{\wedge} \varphi_2 \rightarrow \varphi_2 \wedge \varphi_1 \qquad \varphi_1 \wedge \varphi_2 \rightarrow \varphi_2 \dot{\|} \varphi_1$$

$$\top \dot{\wedge} \varphi \leftrightarrow \varphi \qquad \top \dot{\|} \varphi \leftrightarrow \begin{cases} \top & \text{if } \varphi \text{ is satisfiable} \\ \bot & \text{otherwise} \end{cases}$$

$\Rightarrow$ consistency expressible in the language of SSL

- inference rules:

$$\frac{\varphi \rightarrow \psi}{(\varphi \dot{\wedge} \chi) \rightarrow (\psi \dot{\wedge} \chi)} \qquad \frac{\varphi \rightarrow \psi}{(\varphi \dot{\|} \chi) \rightarrow (\psi \dot{\|} \chi)}$$

Validity: examples

- valid equivalences, for $p \neq q$:

$$p \dot{\wedge} p \leftrightarrow \bot \qquad p \dot{\|} p \leftrightarrow p$$

$$p \dot{\wedge} \neg p \leftrightarrow \bot \qquad p \dot{\|} \neg p \leftrightarrow \top$$

$$p \dot{\wedge} q \leftrightarrow p \wedge q \qquad p \dot{\|} q \leftrightarrow \top$$

$$(p \vee q) \dot{\wedge} (p \vee q) \leftrightarrow p \wedge q \qquad (p \vee q) \dot{\|} (p \vee q) \leftrightarrow \top$$

Outline

Complexity: upper bounds

- upper bounds:
  - both $\varphi_1 \dot{\wedge} \varphi_2$ and $\varphi_1 \dot{||} \varphi_2$ can be polynomially expressed in the star-free fragment of dynamic logic of propositional assignments DL-PA
  - star-free DL-PA: satisfiability and model checking both in PSPACE [Balbiani, Herzig&Troquard, Lics13]
- lower bounds: t.b.d.

Outline

Separability for belief change operations

- $\beta \circ \psi$ = result of incorporating the input ψ into the base β
  - $\circ$ be a belief change operator
  - mainly studied from semantical perspective:

$$\beta \circ \psi = \text{set of valuations}$$

- aim: use the SSL operators to formulate new postulates for belief change operations
  - add to the AGM postulates for revision
    [Alchourrón, Gärdenfors&Makinson, 1985; Gärdenfors, 1988]
  - add to the KM postulates for update
    [Katsuno&Mendelzon, 1990]

The basic belief change postulates

- $||\varphi|| = \{V \ : \ V \models \varphi\}$ = set of valuations where φ is true
- common to AGM revision postulates and KM update postulates
  - insensitivity to syntax:
    if $||\beta_1|| = ||\beta_2||$ and $||\psi_1|| = ||\psi_2||$ then $\beta_1 \circ \psi_1 = \beta_2 \circ \psi_2$ (RE)
  - priority of input:
    $\beta \circ \psi \subseteq ||\psi||$ (SUCCESS)
  - weak preservation postulate:
    if $||\beta|| \subseteq ||\psi||$ then $\beta \circ \psi = ||\beta||$ ($PRES_w$)

$\Rightarrow$ “basic postulates for belief change”

Belief change operations and language splitting

- the drastic update operation

$$\beta \circ \psi = \begin{cases} \|\beta\| & \text{if } \|\beta\| \subseteq \|\psi\| \\ \|\psi\| & \text{otherwise} \end{cases}$$

  satisfies the KM postulates
- the drastic revision operation

$$\beta \circ \psi = \begin{cases} \|\beta \wedge \psi\| & \text{if } \|\beta\| \cap \|\psi\| \neq \emptyset \\ \|\psi\| & \text{otherwise} \end{cases}$$

  satisfies the AGM postulates
- further postulate [Parikh 1999; Kourousias&Makinson 2007]:

$$\text{(REL)} \quad (\beta_1 \wedge \beta_2) \circ \psi = (\beta_1 \circ \psi) \cap (\beta_2 \circ \psi) \quad \text{if } \mathbb{P}_{\beta_1} \cap \mathbb{P}_{\beta_2} = \emptyset$$

  $\Rightarrow$ refers to the syntax: splitting of the language of $\beta_1 \wedge \beta_2$
- drastic operations violate REL

Separation-based belief change operations

- idea: strengthen REL using the separation operators
- static version:

$$(\text{REL}_s) \quad (\beta_1 \dot{\wedge} \beta_2) \circ \psi \quad = \quad (\beta_1 \circ \psi) \cap (\beta_2 \circ \psi)$$

  $\Rightarrow$ when β_1 and β_2 are statically separable then they can be updated separately
- dynamic version:

$$(\text{REL}_d) \quad \beta \circ (\psi_1 \dot{\|} \psi_2) \quad = \quad (\beta \circ \psi_1) \circ \psi_2 \quad = \quad (\beta \circ \psi_2) \circ \psi_1$$

  $\Rightarrow$ when ψ_1 and ψ_2 are dynamically separable then the update can be performed in parallel (interleaving)
- violated by any AGM revision operation and and any KM update operation. . .

Static relevance

Proposition

There is no operation $\circ$ satisfying both the basic belief change postulates and REL_s.

Proof.

Suppose $\circ$ satisfies the basic belief change postulates and REL_s.
Consider base $\beta = (p \vee q) \dot{\wedge} (p \vee q)$ and input $\psi = p \vee q$.
As β is equivalent to $p \wedge q$:

$$\begin{aligned}
\beta \circ \psi &= (p \vee q) \dot{\wedge} (p \vee q) \circ p \vee q \\
&= p \wedge q \circ p \vee q && \text{(by RE)} \\
&= \|p \wedge q\| && \text{(by PRES}_w\text{)}
\end{aligned}$$

Incompatible with REL_s:

$$\begin{aligned}
\beta \circ \psi &= (p \vee q) \dot{\wedge} (p \vee q) \circ p \vee q \\
&= p \vee q \circ p \vee q \cap p \vee q \circ p \vee q && \text{(by REL}_s\text{)} \\
&= \|p \vee q\| \cap \|p \vee q\| && \text{(by PRES}_w\text{)} \\
&= \|p \vee q\|
\end{aligned}$$

□

Dynamic relevance

Proposition

There is no operation $\circ$ satisfying both the basic belief change postulates and REL_d.

Proof.

Suppose $\circ$ satisfies the KM postulates and REL_d.
Consider base $\beta = \neg p$ and input $\psi = \neg p \,\dot{\|}\, p$.
As ψ is equivalent to $\top$:

$$\begin{array}{rcll} \beta \circ \psi & = & \neg p \circ \neg p \,\dot{\|}\, p & \\ & = & \neg p \circ \top & \text{(by RE)} \\ & = & \|\neg p\| & \text{(by PRES}_w\text{)} \end{array}$$

Incompatible with REL_d:

$$\begin{array}{rcll} \beta \circ \psi & = & \neg p \circ \neg p \,\dot{\|}\, p & \\ & = & (\neg p \circ \neg p) \diamond p & \text{(by REL}_d\text{)} \\ & = & \neg p \circ p & \text{(by PRES}_w\text{)} \\ & \subseteq & \|p\| & \text{(by SUCCESS)} \end{array}$$

Incompatibility because set of $\neg p$ valuations non empty. □

Conclusion

- SSL = set separation logic
  - resources separable: $\beta_1 \dot{\wedge} \beta_2$
  - updates separable: $\psi_1 \,||\, \psi_2$
- properties:
  - decidable
  - model checking, satisfiability checking in PSPACE
- open:
  - PSPACE upper bound tight?
  - axiomatisation?
  - how integrate implicational connective $-\!\!*$ of separation logic?
- cannot be used to enhance the AGM and KM postulates
- perspective: extension of SSL by DL-PA programs