APLAS 2016

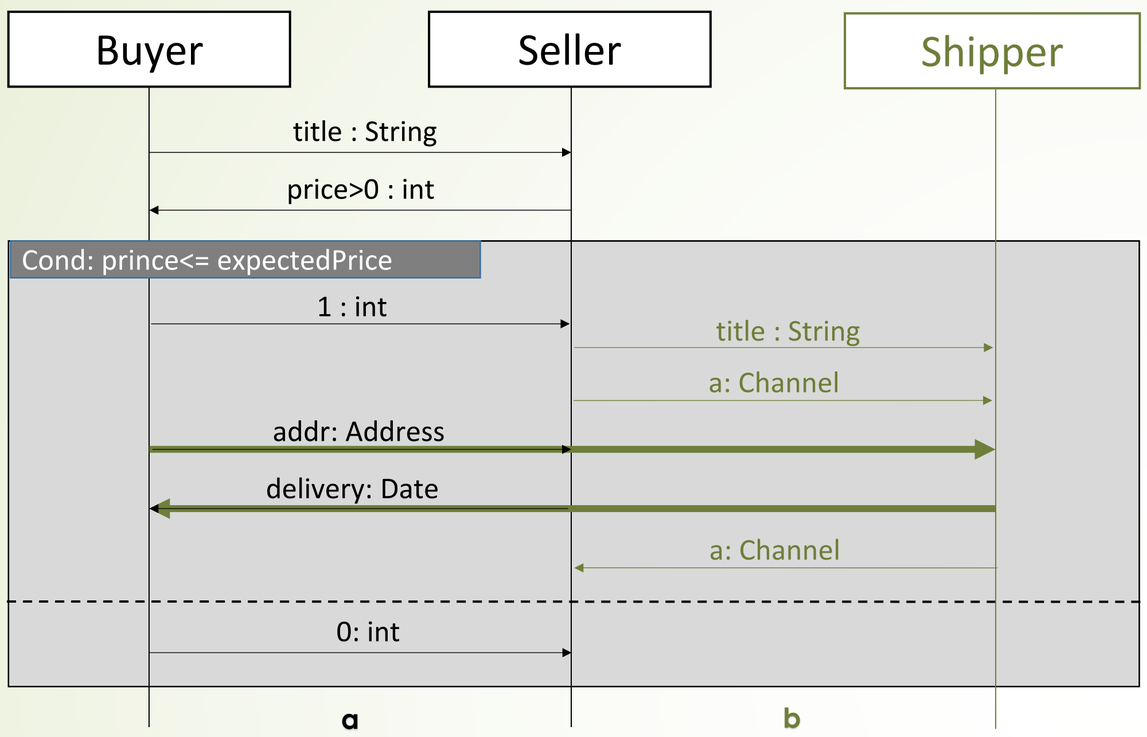
Towards a Session Logic for Multiparty Protocols

by Andreea Costea, Valentina Manea, Wei-Ngan Chin
School of Computing, National University of Singapore

Abstract

We present a multiparty session logic for reasoning about communication-centered applications. Our logic goes beyond the traditional message-type consistency check and deals with more complex properties of the exchanged messages. Similar to the session type approaches, we propose a specification logic which provides the means to formally describe the communication protocols from a global perspective. Unlike the type checking approaches, our specification logic provides the necessary abstractions to describe a wide range of properties about the exchanged message, such as numeric properties or resource handling.

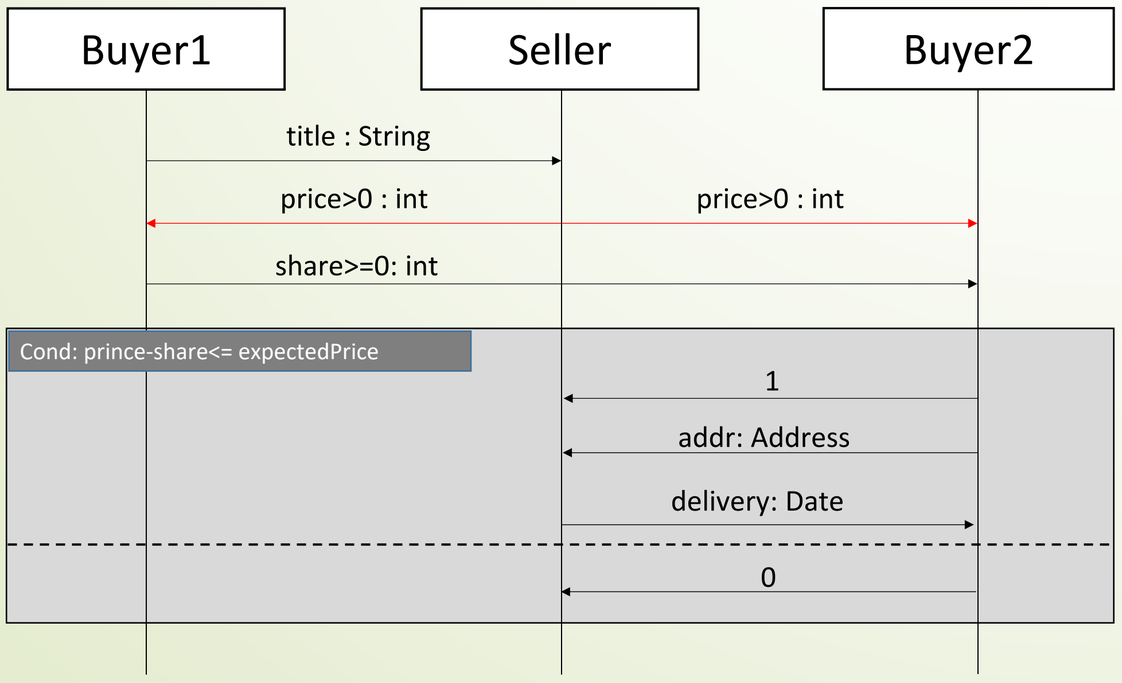
Example 1: binary session



$\mathtt{buyer_a} \triangleq \mathtt{!String; ?int; ((!1; !Address; ?Date) \vee !0)}$
$\mathtt{seller_a} \triangleq \mathtt{?String; !int; ((?1; ?Address; !Date) \vee ?0)}$

$\mathtt{seller_b} \triangleq \mathtt{!String; !v \cdot \mathcal{C}(v, ?Address; !Date); ?v \cdot \mathcal{C}(v, emp)}$
$\mathtt{shipper_b} \triangleq \mathtt{?String; ?v \cdot \mathcal{C}(v, ?Address; !Date); !v \cdot \mathcal{C}(v, emp)}$

Example 2: multiparty session



$$\mathtt{G_{BBS}(B_1, B_2, C)} \triangleq \mathtt{B_1 \to S : String;}$$
$$\mathtt{((S \to B_1 : v \cdot v > 0) \circledast (S \to B_2 : v \cdot v > 0));}$$
$$\mathtt{B_2 \to B_1 : v \cdot v \geq 0;}$$
$$\mathtt{((B_2 \to S : 1; B_2 \to S : Addr; S \to B_2 : Date) \vee (B_2 \to S : 0))}$$

(automatic sync algorithm)

$$\mathtt{G_{BBS}(B_1, B_2, C)} \triangleq \mathtt{B_1 \to S : String; \zeta_1;}$$
$$\mathtt{((S \to B_1 : v \cdot v > 0) \circledast (S \to B_2 : v \cdot v > 0)); \zeta_2;}$$
$$\mathtt{B_2 \to B_1 : v \cdot v \geq 0; \zeta_3;}$$
$$\mathtt{((B_2 \to S : 1; B_2 \to S : Addr; S \to B_2 : Date) \vee (B_2 \to S : 0))}$$

Specification Language

$$G ::= A \to B : \Phi \mid A \xrightarrow{d} B : G \mid p(v^*) \mid \zeta_{id} \mid G \circledast G \mid G \vee G \mid G;G$$
$$P ::= \mathtt{emp} \mid\ !v \cdot \Delta \mid ?v \cdot \Delta \mid p(v^*) \mid \zeta_{id} \mid V \mid P \vee P \mid P;P$$

Projection Rules

$$(A \to B : \Delta)\lfloor_A^B := !v \cdot \Delta \qquad (A \to B : \Delta)\lfloor_B^A := ?v \cdot \Delta$$
$$(A \xrightarrow{d} B : G(A,X))\lfloor_A^B := !v \cdot \mathcal{C}(v, (G(A,X))\lfloor_A^X)$$
$$(A \xrightarrow{d} B : G(A,X))\lfloor_B^A := ?v \cdot \mathcal{C}(v, (G(A,X))\lfloor_A^X)$$
$$(G_1;G_2)\lfloor_R^{R'} := (G_1)\lfloor_R^{R'};(G_2)\lfloor_R^{R'}$$
$$(G_1 \vee G_2)\lfloor_R^{R'} := (G_1)\lfloor_R^{R'} \vee (G_2)\lfloor_R^{R'}$$
$$(G_1 \circledast G_2)\lfloor_R^{R'} := (G_1)\lfloor_R^{R'} \ \mathtt{iff}\ (G_2)\lfloor_R^{R'} = \mathtt{emp}$$
$$:= (G_2)\lfloor_R^{R'} \ \mathtt{iff}\ (G_1)\lfloor_R^{R'} = \mathtt{emp}$$
$$:= \bot \text{ otherwise}$$

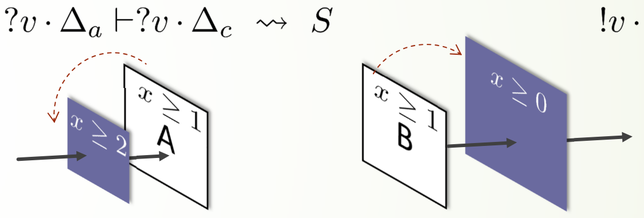
Entailment Rules

$$[\textbf{ENT-SEQ}]\quad \frac{\Box_a \vdash \Box_c \rightsquigarrow S_1 \qquad P_a \vdash P_c \rightsquigarrow S_2 \qquad \text{where } \Box := ?v \cdot \Delta \mid !v \cdot \Delta \mid \bigvee P \mid \mathrm{f}}{\Box_a;P_a \vdash \Box_c;P_c \rightsquigarrow \{\mathtt{emp} \wedge \pi_1 \wedge \pi_2 \mid \pi_1 \in S_1 \wedge \pi_2 \in S_2\}}$$

$$[\textbf{ENT-CHAN}]\quad \frac{P_a \vdash P_c \rightsquigarrow S' \qquad S = \{\pi_i^e \mid \pi_i^e \in S'\}}{\mathcal{C}(v, P_a) \vdash \mathcal{C}(v, P_c) \rightsquigarrow S}$$

$$[\textbf{ENT-RECV}]\quad \frac{\Delta_a \vdash \Delta_c \rightsquigarrow S' \qquad S = \{\pi_i^e \mid \pi_i^e \in S'\}}{?v \cdot \Delta_a \vdash ?v \cdot \Delta_c \rightsquigarrow S}$$

$$[\textbf{ENT-SEND}]\quad \frac{\Delta_c \vdash \Delta_a \rightsquigarrow S' \qquad S = \{\pi_i^e \mid \pi_i^e \in S'\}}{!v \cdot \Delta_a \vdash !v \cdot \Delta_c \rightsquigarrow S}$$



$!x \cdot x \geq 1 \vdash !x \cdot x \geq 2 \qquad ?x \cdot x \geq 1 \vdash ?x \cdot x \geq 0$

Example:

$A \to B : x \geq 1$

Communication Primitives

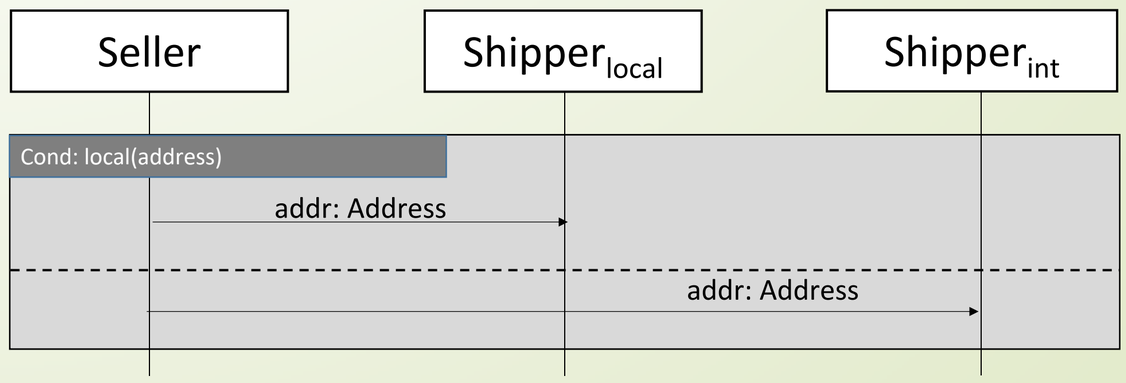
$$[\textbf{FV-OPEN}]$$
$$\vdash \{\mathtt{emp}\}\ \mathtt{open(c)\ with\ P}\ \{\mathcal{C}(\mathtt{c}, \mathtt{S_1}) * \mathcal{C}(\mathtt{c}, \mathtt{S_2})\}$$

$$[\textbf{FV-CLOSE}]$$
$$\vdash\ \{\mathcal{C}(\mathtt{c}, \mathtt{emp}) * \mathcal{C}(\mathtt{c}, \mathtt{emp})\}\ \mathtt{close(c)}\ \{\mathtt{emp}\}$$

$$[\textbf{FV-SEND}]$$
$$\vdash\ \{\mathcal{C}(\mathtt{c}, !v \cdot \mathtt{L(v)}; \mathtt{P}) * \mathtt{L(x)}\}\ \mathtt{send(c, x)}\ \{\mathcal{C}(\mathtt{c}, \mathtt{P})\}$$

$$[\textbf{FV-RECV}]$$
$$\vdash\ \{\mathcal{C}(\mathtt{c}, ?v \cdot \mathtt{L(v)}; \mathtt{P})\}\ \mathtt{x = receive(c)}\ \{\mathtt{L(x)} * \mathcal{C}(\mathtt{c}, \mathtt{P})\}$$

Distributive Conditional



The Take-Away

Type safety → logic with flow awareness (precision)

Communication as resource: concurrency, sequence, nondeterminism

Higher-Order Predicates: expressivity, modularity, maintainability

Contact: andreeac@comp.nus.edu.sg
Website: http://loris-5.d2.comp.nus.edu.sg/msess