Tracing Monoidal Man in the Middle (with hindsight)

Dusko Pavlovic

Royal Holloway

CMCS, Talinn
1 April 2012

Outline

Category of protocols

Trace monad

Future traces

Outline

Category of protocols

- Arities
- Clones
- Programs
- Protocols
- Protocol analysis

Trace monad

Future traces

Category of arities

$$
\begin{aligned}
|\mathbb{A}| &= \left\{n = \{0, 1, \ldots, n-1\} \mid n \in \mathbb{N}\right\} \\
\mathbb{A}(m, n) &= \left\{ (x_0, \ldots, x_{m-1})\langle x_{f(0)}, \ldots, x_{f(n-1)}\rangle \mid f : n \to m\right\} \big/ \alpha
\end{aligned}
$$

Category of arities

Remark

$\mathbb{A}$ is the free strict cartesian category generated by 1.

Algebraic theories

- An algebraic theory is a pair $\mathcal{T} = \langle \Sigma_{\mathcal{T}}, E_{\mathcal{T}} \rangle$ where
  - $\Sigma = \Sigma_{\mathcal{T}}$ is a signature, and
  - $E = E_{\mathcal{T}}$ is a set of equations

Algebraic theories

- An algebraic theory is a pair $\mathcal{T} = \langle \Sigma_{\mathcal{T}}, E_{\mathcal{T}} \rangle$ where
  - $\Sigma = \Sigma_{\mathcal{T}}$ is a signature, and
  - $E = E_{\mathcal{T}}$ is a set of equations
- Algebraic operations $\varphi(x_1, \ldots, x_n)$ are generated from Σ modulo E.
- A $\mathcal{T}$-algebra assigns a map $\varphi \; : \; X^n \to X$ for each n-ary algebraic operation φ.

Lawvere clones (à la Milner)

$$\begin{aligned} |\mathbb{C}_{\mathcal{T}}| &= \mathbb{N} \\ \mathbb{C}_{\mathcal{T}}(m,n) &= \Big\{ (x_0, \ldots, x_{m-1}) \langle \varphi_0, \ldots, \varphi_{n-1} \rangle \Big\} \Big/ \alpha \end{aligned}$$

Programming languges

- A programming language $\mathcal{L}$ generates programs P with inputs $(x_0, \ldots, x_{m-1})$ and outputs $\langle s_0, \ldots, s_{n-1} \rangle$.
- Semantics of $\mathcal{L}$ assigns a map $P : \prod_{i \in m} X_i \to \prod_{j \in n} S_j$ for each program P with m inputs and n outputs.

Category of programs (untyped)

$$\begin{aligned} |\mathbb{P}_{\mathcal{L}}| &= \mathbb{N} \\ \mathbb{P}_{\mathcal{L}}(m,n) &= \Big\{ (x_0, \ldots, x_{m-1}) [P] \langle s_0, \ldots, s_{n-1} \rangle \Big\} \Big/ \alpha \end{aligned}$$

(Functorial semantics)

$$\frac{\text{equational theories}}{\text{algebras}} = \frac{\text{programming languages}}{\text{algebras} \subsetneq \text{coalgebras}}$$

Category of programs

Remark

- typing $\rightsquigarrow$ extended arities

Category of programs

Remark

- typing $\leftrightsquigarrow$ extended arities
- sequential composition $\leftrightsquigarrow$ arrow composition

Category of programs

Remark

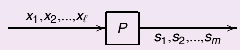
- typing $\leftrightsquigarrow$ extended arities
- sequential composition $\leftrightsquigarrow$ arrow composition
- parallel composition $\leftrightsquigarrow$ monoidal structure

Category of programs

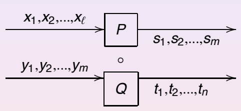
Remark

- typing $\leftrightsquigarrow$ extended arities
- sequential composition $\leftrightsquigarrow$ arrow composition
- parallel composition $\leftrightsquigarrow$ monoidal structure
- program loops $\leftrightsquigarrow$ trace structure

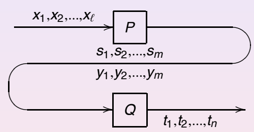
Category of programs: String diagrams



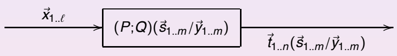
Category of programs: Composition



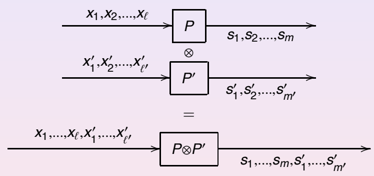
Category of programs: Composition



Category of programs: Composition

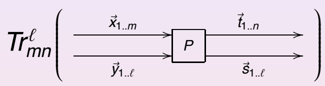


Category of programs: Tensor

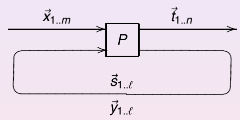


where $\vec{x}_{1..\ell} \cap \vec{x'}_{1..\ell'} = \emptyset$

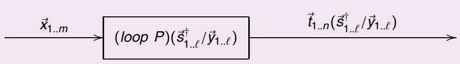
Category of programs: Trace



Category of programs: Trace



Category of programs: Trace



Category of programs: Trace

But verifying the trace structure is a lot of work!

Category of programs: Trace

But verifying the trace structure is a lot of work!

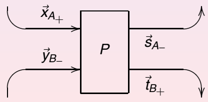
If the traces are OK, we model protocols as follows:

Category of protocols

MonManMid
Dusko Pavlovic
Protocols
Arities
Clones
Programs
Protocols
Protocol analysis
Trace monad
Future traces

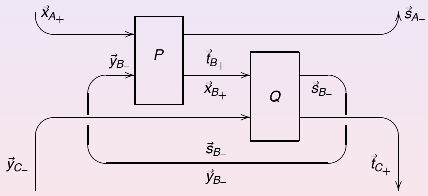
$$
\begin{aligned}
|\mathbb{J}| &= \left\{A = \langle A_+, A_-\rangle \in |\mathbb{P}|^2\right\}\\
\mathbb{J}(A,B) &= \{A_+ \otimes B_- \to A_- \otimes B_+ \text{ in } \mathbb{P}\}
\end{aligned}
$$

$$
\begin{pmatrix} \vec{x}_{A_+} \\ \vec{y}_{B_-} \end{pmatrix} \left[\, P \,\right] \left\langle \begin{matrix} \vec{s}_{A_+} \\ \vec{t}_{B_-} \end{matrix} \right\rangle = \begin{pmatrix} x_1 & x_2 & \dots & x_{A_+} \\ y_1 & y_2 & \dots & y_{B_-} \end{pmatrix} \left[\, P \,\right] \left\langle \begin{matrix} s_1 & s_2 & \dots & s_{A_-} \\ t_1 & t_2 & \dots & t_{B_+} \end{matrix} \right\rangle
$$



Composition of protocols

MonManMid
Dusko Pavlovic
Protocols
Arities
Clones
Programs
Protocols
Protocol analysis
Trace monad
Future traces



Categorical protocol analysis

MonManMid
Dusko Pavlovic
Protocols
Arities
Clones
Programs
Protocols
Protocol analysis
Trace monad
Future traces

A protocol is

- specified by giving
  1. local observations at the interfaces
  2. a (security) requirement on the interactions
- represented as a morphism $A \xrightarrow{p} B$ in $\mathbb{J}$
- analyzed by enumerating

  Man-in-the-Middle: nontrivial decompositions
  $A \to X \to B$

  Chosen Protocol Attack: leaking compositions
  $A \to B \to X$

Outline

MonManMid
Dusko Pavlovic

Category of protocols

Trace monad

Local monoidal categories

Normal traces

Loop categories

Free normal traces

Future traces

Local monoids

MonManMid
Dusko Pavlovic
Protocols
Trace monad
Local moncats
Normal traces
Loop categories
Free traces
Future traces

Definition

Let $\mathbb{M} \times \mathbb{M} \xrightarrow{\cdot} \mathbb{M} \xleftarrow{\iota} 1$ be a commutative monoid.

- $o \in \mathbb{M}$ is *zero* if $ou = o$ for all $u \in \mathbb{M}$
- $s \in \mathbb{M}$ is a *nilpotent* if $s^n = o$ for some $n \in \mathbb{N}$
- $s \in \mathbb{M}$ is *regular* if it is not nilpotent.
- $\mathbb{M}$ is *local* if all regular elements are invertible

Local monoidal categories

Definition

Let $\mathbb{C}\times\mathbb{C}\xrightarrow{\otimes}\mathbb{C}\xleftarrow{I}1$ be a small symmetric monoidal category. Then

- $\mathbb{I}=\mathbb{C}(I,I)$ is a commutative monoid
- $\mathbb{I}\times\mathbb{C}(A,B)\overset{\cdot}{\to}\mathbb{C}(A,B)$ is $\mathbb{I}$-action
- $A\xrightarrow{o_{AB}}B$ is *zero* if $o\cdot o_{AB}=o_{AB}$
- $\mathbb{C}$ is a *local* monoidal category if $\mathbb{I}$ is a local monoid.

Graded monoidal categories

Definition

A small strict symmetric monoidal category

$$\mathbb{C}\times\mathbb{C}\xrightarrow{\otimes}\mathbb{C}\xleftarrow{I}1$$

is *graded* by a monoid homomorphism

$$(\mathbb{C},\otimes,I)\xrightarrow{|-|}(\mathbb{I},\circ,\mathrm{id})$$

where $\mathbb{I}=\mathbb{C}(I,I)$.

Graded monoidal categories

Remark

Every traced monoidal category is graded by

$$|U| \quad = \quad Tr^U(\mathrm{id}_U)$$

Normal traces

Definition

A *normal* trace structure over a monoidal category $\mathbb{C}$ is a family of operators

$$\frac{f\ :\ A\otimes U\to B\otimes U}{Tn^U_{AB}(f)\ :\ A\to B}$$

satisfying the Joyal-Street-Verity axioms and also:

$$Tn^U_{AB}\left(A\otimes U\xrightarrow{g\otimes U}B\otimes U\right) \quad = \quad \begin{cases} A\xrightarrow{g}B & \text{if } U \text{ is regular}\\ A\xrightarrow{o}B & \text{otherwise}\end{cases}$$

Trace decomposition

Proposition 1

Any trace structure over a local monoidal category $\mathbb{C}$ decomposes:

$$Tr^U(f) \quad = \quad |U|\cdot Tn^U(f)$$

Free normal traces

Proposition 2

Normal traces are monadic over local monoidal categories.

Loop categories

Definition

The loop category over a small local monoidal category $\mathbb{C}$ is

$$\begin{aligned} |\mathbb{C}^{\circlearrowleft}| &= |\mathbb{C}| \\ \mathbb{C}^{\circlearrowleft}(A,B) &= \oint_{U\in|\mathbb{C}|} \mathbb{C}(A\otimes U, B\otimes U) \end{aligned}$$

Loop categories

Definition

The loop category over a small local monoidal category $\mathbb{C}$ is

$$\begin{aligned} |\mathbb{C}^{\circlearrowleft}| &= |\mathbb{C}| \\ \mathbb{C}^{\circlearrowleft}(A,B) &= \left(\sum_{U\in|\mathbb{C}|} \mathbb{C}(A\otimes U, B\otimes U) \times \mathbb{I}^*\right)\Big/\sim \end{aligned}$$

Loop categories

...where $\sim$ extends the coend equivalence...

$$\begin{tikzcd} & \mathbb{C}(A\otimes U, B\otimes U) \arrow[dr, dashed] & \\ \mathbb{C}(A\otimes V, B\otimes U) \arrow[ur, "(-)\circ(A\otimes u)"] \arrow[rr, dashed] \arrow[dr, "(B\otimes u)\circ(-)"'] & & \mathbb{C}^{\circlearrowleft}(A,B) \\ & \mathbb{C}(A\otimes V, B\otimes V) \arrow[ur, dashed] & \end{tikzcd}$$

Loop categories

...where $\sim$ extends the coend equivalence...

$$\frac{(B\otimes u)\circ f}{s} \sim \frac{f\circ(A\otimes u)}{s}$$

$$\begin{tikzcd} & A\otimes U \arrow[dl, "f"'] \\ B\otimes V \arrow[dr, "B\otimes u"'] & \\ & B\otimes U \end{tikzcd} \qquad \begin{tikzcd} A\otimes V \arrow[dr, "A\otimes u"] & \\ & A\otimes U \arrow[dl, "f"] \\ B\otimes V & \end{tikzcd}$$

Loop categories

...by

$$\frac{f\otimes c_U}{s} \sim \frac{f\otimes U}{s}$$

$$\begin{tikzcd} A\otimes U\otimes U \arrow[d, "f\otimes c_U"'] \\ B\otimes U\otimes U \end{tikzcd} \qquad \begin{tikzcd} A\otimes U \arrow[d, "f\otimes U"] \\ B\otimes U \end{tikzcd}$$

Loop categories

...and

$$\frac{f}{s} \sim \frac{g}{t}$$

$$\Updownarrow$$

$$\exists uv\in\mathbb{I}^*.\ u\circ f = v\circ g \ \wedge\ u\circ s = v\circ t$$

Composition

Given

- $f \in \mathbb{C}^{\circlearrowleft}(A, B)$ as $A \otimes U \xrightarrow{f_0/f_1} B \otimes U$, and
- $g \in \mathbb{C}^{\circlearrowleft}(B, C)$ as $B \otimes V \xrightarrow{g_0/g_1} C \otimes V$,

the composite

- $f \circ g \in \mathbb{C}^{\circlearrowleft}(A, C)$ can be viewed as

$$\begin{tikzcd}
A \otimes U \otimes V \arrow[r, "\frac{f_0 \otimes V}{f_1 \circ |V|}"'] & B \otimes U \otimes V \arrow[d, "B \otimes c"] & C \otimes U \otimes V \\
& B \otimes V \otimes U \arrow[r, "\frac{g_0 \otimes U}{g_1 \circ |U|}"'] & C \otimes V \otimes U \arrow[u, "C \otimes c"']
\end{tikzcd}$$

Composition

MonManMid
Dusko Pavlovic
Protocols
Trace monad
Local moncats
Normal traces
Loop categories
Free traces
Future traces

Given

- $f \in \mathbb{C}^{\circlearrowleft}(A, B)$ as $A \otimes U \xrightarrow{f_0/f_1} B \otimes U$, and
- $g \in \mathbb{C}^{\circlearrowleft}(B, C)$ as $B \otimes V \xrightarrow{g_0/g_1} C \otimes V$,

the composite

- $f \circ g \in \mathbb{C}^{\circlearrowleft}(A, C)$ can be viewed as

$$\begin{tikzcd}
A \otimes U \otimes V \arrow[r, "\frac{f_0 \otimes V}{f_1 \circ |V|}"'] & B \otimes U \otimes V \arrow[d, "B \otimes c"] & \\
A \otimes V \otimes U \arrow[u, "A \otimes c"'] & B \otimes V \otimes U \arrow[r, "\frac{g_0 \otimes U}{g_1 \circ |U|}"'] & C \otimes V \otimes U
\end{tikzcd}$$

Tensor

MonManMid
Dusko Pavlovic
Protocols
Trace monad
Local moncats
Normal traces
Loop categories
Free traces
Future traces

Given

- $f \in \mathbb{C}^{\circlearrowleft}(A, B)$ as $A \otimes U \xrightarrow{f_0/f_1} B \otimes U$, and
- $h \in \mathbb{C}^{\circlearrowleft}(C, D)$ as $C \otimes V \xrightarrow{h_0/h_1} D \otimes V$,

the tensor product

- $f \otimes h \in \mathbb{C}^{\circlearrowleft}(A \otimes C, B \otimes D)$ can be viewed as

$$\begin{tikzcd}
A \otimes C \otimes U \otimes V \arrow[d, "A \otimes c \otimes V"] & B \otimes D \otimes U \otimes V \\
A \otimes U \otimes C \otimes V \arrow[r, "\frac{f_0 \otimes h_0}{f_1 \circ h_1}"'] & B \otimes U \otimes D \otimes V \arrow[u, "B \otimes c \otimes V"']
\end{tikzcd}$$

Normal trace

MonManMid
Dusko Pavlovic
Protocols
Trace monad
Local moncats
Normal traces
Loop categories
Free traces
Future traces

$$\frac{f \;=\; \dfrac{(A \otimes U) \otimes V \xrightarrow{f_0} (B \otimes U) \otimes V}{f_1} \;\in\; \mathbb{C}^{\circlearrowleft}(A \otimes U, B \otimes U)}{Tn^U_{AB} f \;=\; \dfrac{A \otimes (U \otimes V) \xrightarrow{f_0} B \otimes (U \otimes V)}{f_1} \;\in\; \mathbb{C}^{\circlearrowleft}(A, B)}$$

Free normal traces

MonManMid
Dusko Pavlovic
Protocols
Trace monad
Local moncats
Normal traces
Loop categories
Free traces
Future traces

Proposition 2 (continuation)

The free normal traces are given by the loop monad:

- 2-functor $\circlearrowleft : \mathcal{LM} \to \mathcal{LM}$
- unit functors

$$\begin{aligned} \eta_{\mathbb{C}} \;&:\; \mathbb{C} \to \mathbb{C}^{\circlearrowleft} \\ (A \xrightarrow{f} B) &\longmapsto \left[A \otimes I \xrightarrow{f \otimes I} B \otimes I\right]_{\sim} \end{aligned}$$

Free normal traces

MonManMid
Dusko Pavlovic
Protocols
Trace monad
Local moncats
Normal traces
Loop categories
Free traces
Future traces

Proposition 2 (continuation)

The free normal traces are given by the loop monad:

- 2-functor $\circlearrowleft : \mathcal{LM} \to \mathcal{LM}$
- unit functors

$$\begin{aligned} \eta_{\mathbb{C}} \;&:\; \mathbb{C} \to \mathbb{C}^{\circlearrowleft} \\ (A \xrightarrow{f} B) &\longmapsto \left[A \otimes I \xrightarrow{f \otimes I} B \otimes I\right]_{\sim} \end{aligned}$$

- evaluation functors

$$\mu_{\mathbb{C}} \;:\; \mathbb{C}^{\circlearrowleft\circlearrowleft} \to \mathbb{C}^{\circlearrowleft}$$

$$\left[\frac{\left[\dfrac{(A \otimes U) \otimes V \xrightarrow{f_0} (B \otimes U) \otimes V}{s}\right]_{\sim}}{t}\right]_{\sim} \longmapsto \left[\frac{A \otimes (U \otimes V) \xrightarrow{f_0} B \otimes (U \otimes V)}{s \circ t}\right]_{\sim}$$

Free normal traces

Corollary

$$\begin{aligned} |\mathbb{P}_{\mathcal{L}}| &= \mathbb{N} \\ \mathbb{P}_{\mathcal{L}}(m,n) &= \left\{ (x_0,\ldots,x_{m-1})[P]\langle s_0,\ldots,s_{n-1}\rangle \right\} \big/ \alpha \end{aligned}$$

is a normal traced monoidal category.

Outline

Category of protocols

Trace monad

Future traces

- Weak distributivity
- Weak traces
- Weak interactions

Weakly distributive categories

Definition

A weakly distributive category $\mathbb{C}$ carries two (symmetric!) monoidal structures

$$\mathbb{C}\times\mathbb{C} \xrightarrow{\otimes} \mathbb{C} \xleftarrow{\top} 1$$

$$\mathbb{C}\times\mathbb{C} \xrightarrow{\oplus} \mathbb{C} \xleftarrow{\perp} 1$$

together with

$$A\otimes(B\oplus C) \xrightarrow{d} (A\otimes B)\oplus C \qquad \perp \xrightarrow{m} \top$$

coherently. . .

Weak traces

Definition

The normal trace operator over a weakly distributive category $\mathbb{C}$ is a family of operators

$$\frac{f \;:\; A\otimes U \to B\oplus U}{Tn^U_{AB} f \;:\; A \to B}$$

satisfying the well-typed versions of the familiar laws.[1]

[1] Vanishing can be weakened!

Weak interactions

Definition

Given a weakly distributive traced category $\mathbb{C}$, the induced interaction category $\mathcal{W}\mathbb{J} = \mathrm{Int}(\mathbb{C})$ consists of

$$\begin{aligned} |\mathcal{W}\mathbb{J}| &= \left\{ A = \langle A_+, A_-\rangle \in |\mathcal{C}|^2 \right\} \\ \mathbb{J}(A,B) &= \{ A_+\otimes B_- \to A_-\oplus B_+ \text{ in } \mathcal{C} \} \end{aligned}$$

where

$$\frac{A_+\otimes B_- \xrightarrow{f} A_-\oplus B_+ \qquad B_+\otimes C_- \xrightarrow{g} B_-\oplus C_+}{g\circ f = Tn^{B_-}_{A_+C_-}\left(A_+\otimes B_-\otimes C_- \xrightarrow{f\otimes C_-} A_-\oplus B_+\otimes C_- \xrightarrow{A\oplus g} A_-\oplus B_-\oplus C_+\right)}$$

$$\mathrm{id}_A = \left(A_+\otimes A_- \cong A_+\oplus\perp\otimes A_- \to A_+\oplus\top\otimes A_- \cong A_+\oplus A_-\right)$$

Weak interactions

Conjecture

$\mathbb{C} \to \mathrm{Int}(\mathbb{C})$ is the free $*$-autonomous weakly traced category.

Weak interactions

Conjecture

$\mathbb{C} \to \mathrm{Int}(\mathbb{C})$ is the free $*$-autonomous weakly traced category.

Question

What does this mean logically? Geometrically?