Università degli Studi di Pisa
Corso di Laurea Magistrale in Informatica

Anno Accademico 2021-2022

Insegnamento di

Foundation of Computing

Pagina del corso: `http:/pages.di.unipi.it/montanari/FOC.html`

Note di

History Dependent Automata

a cura di
Ugo Montanari
Dipartimento di Informatica
Università degli Studi di Pisa
ugo@di.unipi.it

Dagstuhl Seminar 13422
13-16/10/2013 - Nominal Computation Theory

Named Graphs and HD Automata for Network-Conscious π-Calculus

Ugo Montanari
Dipartimento di Informatica
Università di Pisa

Joint work with Matteo Sammartino (and many others)

Information Society Technologies

Roadmap

- History Dependent automata
  - No symmetries
  - Spans of open maps
  - With symmetries
  - For verification
- Named sets vs. presheaves
- Network Conscious π-calculus
- Named graphs
- Conclusion

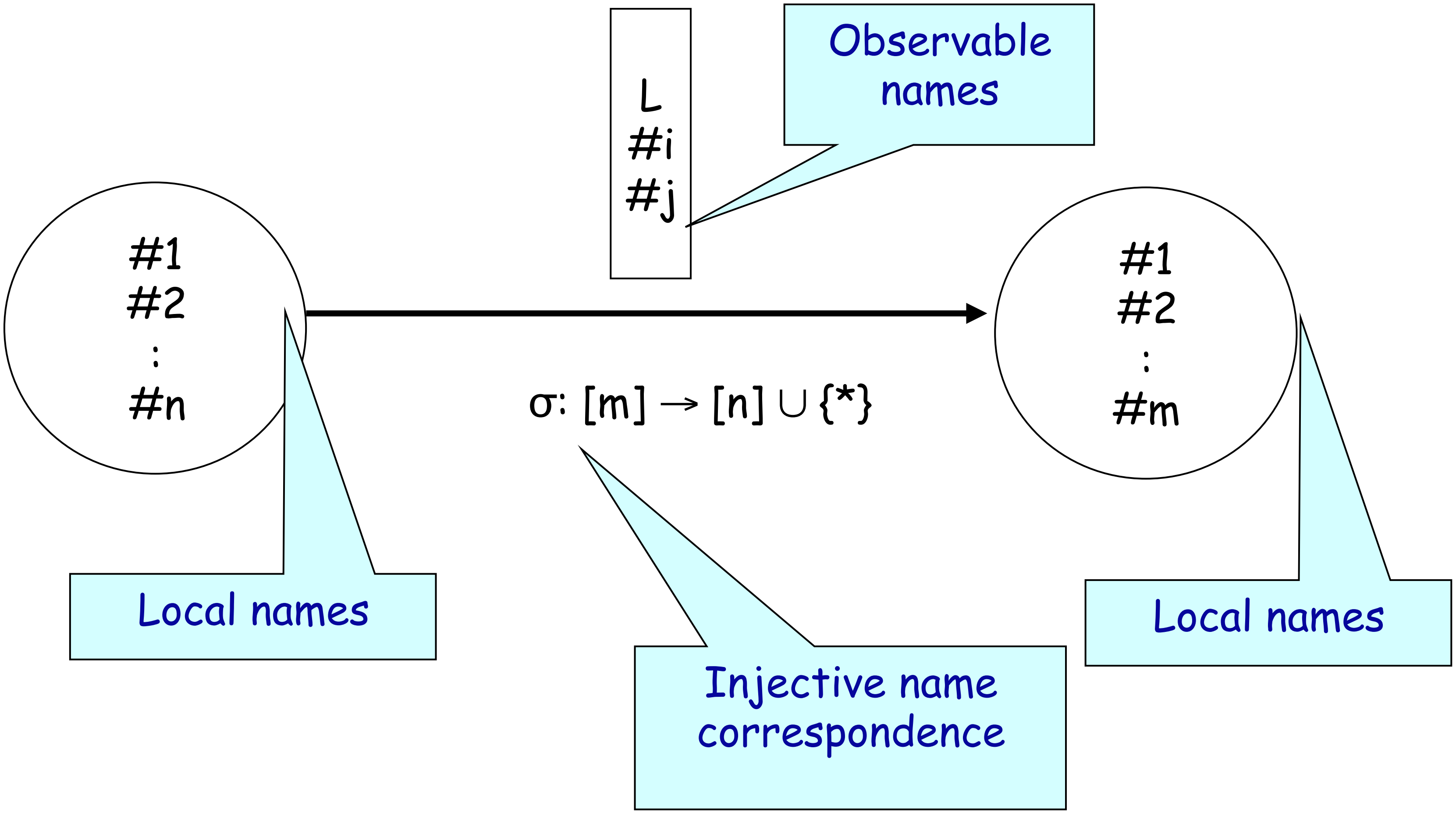
Operational Models with Resource Generation

- Generation of fresh resources is a basic operation in most distributed systems
  - Sessions, objects, keys, storage, links…
- We need models whose states are enriched with names
- We should be able to allocate, and possibly deallocate names
- Often more general kinds of resources

Roadmap

- History Dependent automata
  - No symmetries
  - Spans of open maps
  - With symmetries
  - For verification
- Named sets vs. presheaves
- Network Conscious π-calculus
- Named graphs
- Conclusion

HD-Automata: Structure of Transitions



First Version: Location Automata

Definition 7 (location automaton). A *location automaton* is a tuple $A = \langle Q, w, \mapsto, q_0 \rangle$ where:

- Q is a set of *states*;
- $w : Q \to 2^{Loc}_{f}$ associates to each state a finite set of locations;
- $\mapsto$ is a set of *transitions*; each transition has the form $\boxed{q \overset{a}{\underset{l}{\longmapsto}}_{\sigma} q'}$ (*visible transition*) or the form $q \overset{\tau}{\longmapsto}_{\sigma} q'$ (*invisible transition*), where:
  - $q, q' \in Q$ are the *source* and *target* states;
  - $l \in w(q)$ is the location of the transition;
  - $\boxed{\sigma : w(q') \hookrightarrow w(q) \cup \{\star\}}$ ($\sigma : w(q') \hookrightarrow w(q)$ for an invisible transition) is the injective (inverse) *renaming* corresponding to the transition; the newly created location is denoted with the special mark $\star \notin Loc$;
- $q_0 \in Q$ is the *initial state*; we require that $w(q_0) = \{l\}$ for some $l \in Loc$.

- Ugo Montanari, Marco Pistore, Daniel Yankelevich: Efficient Minimization up to Location Equivalence. ESOP 1996.

Location Automata Bisimulation

Definition 8 (la-bisimulation). Two location automata A and B are *location-automaton bisimilar*, written $A \approx_{la} B$, if there is some set $\mathcal{R}$ of triples, called *la-bisimulation*, such that:

- if $\boxed{\langle p, \delta, q \rangle \in \mathcal{R}}$ then $p \in Q_A$, $q \in Q_B$ and $\boxed{\delta : w_A(p) \multimap w_B(q)}$ is a partial bijection;
- $\langle q_{0A}, \delta_0, q_{0B} \rangle \in \mathcal{R}$, where δ_0 maps the location associated to q_{0A} to the location associated to q_{0B};
- for each $\boxed{p \overset{a}{\underset{l}{\Longmapsto}}_{\sigma} p'}$ in A there exist some δ' and some $\boxed{q \overset{a}{\underset{\delta(l)}{\Longmapsto}}_{\rho} q'}$ in B such that $\boxed{\langle p', \delta', q' \rangle \in \mathcal{R} \text{ and } \delta'(m) = n}$ implies $\boxed{\sigma(m) = \star = \rho(n) \text{ or } \delta(\sigma(m)) = \rho(n);}$

- Ugo Montanari, Marco Pistore, Daniel Yankelevich: Efficient Minimization up to Location Equivalence. ESOP 1996.

The Zoo of History Dependent Automata (no Symmetries)

No minimal automaton

π-calculus

- Ugo Montanari and Marco Pistore, Checking Bisimilarity for Finitary pi-calculus, CONCUR'95.

Causality

- Ugo Montanari and Marco Pistore, M., History Dependent Verification for Partial Order Systems, in: DIMACS Series 1996.

Causality for Petri nets. The name HD comes from sets ofevents as shorthands for the process of HPB containing the causes of future actions

- Ugo Montanari, Marco Pistore, Minimal Transition Systems for History-Preserving Bisimulation. STACS 1997.

Asynchronous π-calculus

- Ugo Montanari, Marco Pistore, Finite State Verification for the Asynchronous pi-Calculus. TACAS 1999

Causality for contextual Petri nets.

- Paolo Baldan, Andrea Corradini, Ugo Montanari, History Preserving Bisimulation for Contextual Nets. WADT 1999

Causality for graph grammars

- Baldan, P., Corradini, A. and Montanari, U., Bisimulation Equivalences for Graph Grammars, Festschrift in Honor of Grzegorz Rozenberg, Springer LNCS 2002.

Roadmap

- History Dependent automata
  - No symmetries
  - Spans of open maps
  - With symmetries
  - For verification
- Named sets vs. presheaves
- Network Conscious π-calculus
- Named graphs
- Conclusion

Bisimilarity Via Spans of Open Maps, I

$$\begin{tikzcd} X \arrow[r, "x"] \arrow[d, "f"'] & M \arrow[d, "m"] \\ Y \arrow[r, "y"] & N \end{tikzcd}$$

(a)

$$\begin{tikzcd} X \arrow[r, "x"] \arrow[d, "f"'] & M \arrow[d, "m"] \\ Y \arrow[r, "y"] \arrow[ur, "y'"] & N \end{tikzcd}$$

(b)

$$\begin{tikzcd} & M \arrow[dl, "m_1"'] \arrow[dr, "m_2"] & \\ M_1 & & M_2 \end{tikzcd}$$

(c)

- An *agent category* with agents M, N as objects and arrows m, x, y
- An *observation subcategory* with observations X, Y as objects and arrows f
- An arrow m is an open map if for every commuting square (a) there is a commuting diagonal y' (b).
- Agents M_1 and M_2 are bisimilar if there is a span (c) of open maps.

Bisimilarity Via Spans of Open Maps, II

Definition 3.1 (named sets) A *named set* E is a set denoted by E, and a family of name sets indexed by E, namely $\{\mathsf{E}[e] \in \mathit{Set}\}_{e \in E}$ (i.e., $\mathsf{E}[\_]$ is a map from E to Set).

Given two named sets E and E', a *named function* $\mathsf{m} : \mathsf{E} \to \mathsf{E}'$ is a function on the sets $m : E \to E'$ and a family of name embeddings (i.e., of injective functions) indexed by m, namely $\{\mathsf{m}[e, e'] : \mathsf{E}'[e'] \hookrightarrow \mathsf{E}[e]\}_{\langle e, e' \rangle \in m}$.

$$\begin{tikzcd}
\mathsf{E} \arrow[d, "\mathsf{m}"] & \ni & e \arrow[d, mapsto, "m"] & \mathsf{E}[e] \\
\mathsf{E}' & \ni & e' & \mathsf{E}'[e'] \arrow[u, hook, "{\mathsf{m}[e,e']}"']
\end{tikzcd}$$

Ugo Montanari and Marco Pistore, An Introduction to History Dependent Automata, HOOTS II, ENTCS, 1998.

Bisimilarity Via Spans of Open Maps, I

$$
\begin{tikzcd}
L & T \arrow[l, "o"'] \arrow[r, bend left, "s"] \arrow[r, bend right, "d"'] & Q & I \arrow[l, "i"']
\end{tikzcd}
\qquad
\begin{tikzcd}
 & T_1 \arrow[dl, "o_1"'] \arrow[r, bend left, "s_1"] \arrow[r, bend right, "d_1"'] \arrow[dd, "m_T"'] & Q_1 \arrow[dd, "m_Q"] & \\
L & & & I \arrow[ul, "i_1"'] \arrow[dl, "i_2"] \\
 & T_2 \arrow[ul, "o_2"] \arrow[r, bend left, "s_2"] \arrow[r, bend right, "d_2"'] & Q_2 &
\end{tikzcd}
$$

- The agent category is a category of algebras of labelled multigraphs on the category of named sets.
- Agents are span of open maps bisimilar iff they are HD bisimilar
- Ugo Montanari and Marco Pistore, An Introduction to History Dependent Automata, HOOTS II, ENTCS, 1998.
- Marco Pistore PhD Thesis, University of Pisa, 1999.

Roadmap

- History Dependent automata
  - No symmetries
  - Spans of open maps
  - With symmetries
  - For verification
- Named sets vs. presheaves
- Network Conscious π-calculus
- Named graphs
- Conclusion

Information Society Technologies

HD Automata with Symmetries, I

Definition 33 (*HD-automata*). A HD-automaton with symmetries (or simply *HD-automaton*) $\mathcal{A}$ is a tuple $\langle \mathcal{S}, \mathrm{sym}, \mathcal{L}, \mapsto \rangle$, where:

- $\mathcal{S}$ is the set of *states*;
- $\boxed{\mathrm{sym} : \mathcal{S} \to \mathcal{S}ym \text{ associates to each state a finite-support } \textit{symmetry};}$
- $\mathcal{L}$ is the set of *labels*;
- $\mapsto \subseteq \{\langle Q, l, \zeta, Q' \rangle | Q, Q' \in \mathcal{S}, l \in \mathcal{L}, \zeta$ is a finite-kernel permutation$\}$ is the *transition relation*, where:
  - Q and Q' are, respectively, the source and the target states;
  - l is the label of the transition, and
  - ζ is a permutation that describes how the names of the target state Q' correspond, along this transition, to the names of the source state Q.

Moreover, we assume that $\mathcal{L} = \mathcal{L}_0 \cup \mathcal{L}_1$, with $\mathcal{L}_0 \cap \mathcal{L}_1 = \emptyset$, and that $l \in \mathcal{L}_i$ iff $\rho(l) \in \mathcal{L}_i$ for every permutation ρ. Labels in $\mathcal{L}_0$ correspond to transitions that do not generate any new name, while labels in $\mathcal{L}_1$ correspond to transitions that generate one new name.[6]

Finally, we do not allow distinct isomorphic transitions between the same states to be present in a HD-automaton, where two transitions $Q \overset{l_1}{\mapsto}_{\zeta_1} Q'$ and $Q \overset{l_2}{\mapsto}_{\zeta_2} Q'$ are isomorphic if there exists some $\rho \in \mathrm{sym}(Q)$ such that

- $l_2 = \rho(l_1)$;
- $\zeta_2^{-1} \circ \rho \circ \zeta_1 \in \mathrm{sym}(Q')$ if $l_1 \in \mathcal{L}_0$ and $\zeta_2^{-1} \circ \rho_{+1} \circ \zeta_1 \in \mathrm{sym}(Q')$ if $l_1 \in \mathcal{L}_1$.

HD Automata with Symmetries, II

Definition 36 (*HD-bisimulation*). Let $\mathcal{A}$ be a HD-automaton. A *HD-simulation* for $\mathcal{A}$ is a set of triples

$$\mathcal{R} \subseteq \{\langle Q_1, \delta, Q_2\rangle \mid Q_1, Q_2 \in \mathcal{S}, \delta \text{ is a finite-kernel permutation}\}$$

such that, whenever $\langle Q_1, \delta, Q_2\rangle \in \mathcal{R}$ then

- for each $\rho_1 \in \mathrm{sym}(Q_1)$ and each $Q_1 \xmapsto{l_1}_{\zeta_1} Q_1'$, there exist some $\rho_2 \in \mathrm{sym}(Q_2)$ and some $Q_2 \xmapsto{l_2}_{\zeta_2} Q_2'$ such that
  - $l_2 = \gamma(l_1)$, where $\gamma = \rho_2^{-1} \circ \delta \circ \rho_1$;
  - $\langle Q_1', \delta', Q_2'\rangle \in \mathcal{R}$, where: $\delta' = \begin{cases} \zeta_2^{-1} \circ \gamma \circ \zeta_1 & \text{if } l_1 \in \mathcal{L}_0, \\ \zeta_2^{-1} \circ \gamma_{+1} \circ \zeta_1 & \text{if } l_1 \in \mathcal{L}_1. \end{cases}$

A *HD-bisimulation* for $\mathcal{A}$ is a set of triples $\mathcal{R}$ such that both $\mathcal{R}$ and $\mathcal{R}^{-1} = \{\langle Q_2, \delta^{-1}, Q_1\rangle \mid \langle Q_1, \delta, Q_2\rangle \in \mathcal{R}\}$ are HD-simulations for $\mathcal{A}$.

HD Automata with Symmetries, III

- Given any HD automata with symmetries, the maximal bisimilarity on its states corresponds to a minimal automaton.
- Coalgebras for the π-calculus on the category of permutation algebras are isomorphic to HD automata with symmetries.
- Each state of an automaton is a concise representation of an orbit of the permutation algebra, and transitions between pairs of HD-states represent all the transitions between the corresponding orbits.
- Finite HD automata with symmetries can be minimized using the list partitioning/ final sequence algorithm.

- Ugo Montanari, Marco Pistore: Pi-Calculus, Structured Coalgebras, and Minimal HD-Automata. MFCS 2000
- Ugo Montanari, Marco Pistore: Structured coalgebras and minimal HD-automata for the pi-calculus. TCS 2005

Roadmap

- History Dependent automata
  - No symmetries
  - Spans of open maps
  - With symmetries
  - For verification
- Named sets vs. presheaves
- Network Conscious π-calculus
- Named graphs
- Conclusion

HD Automata and Verification of Mobile Processes

The HAL environment

- Gian Luigi Ferrari, Gianluigi Ferro, Stefania Gnesi, Ugo Montanari, Marco Pistore, Gioia Ristori: An Automated Based Verification Environment for Mobile Processes. TACAS 1997Gian Luigi Ferrari, Stefania Gnesi, Ugo Montanari, Marco Pistore, Gioia Ristori: Verifying Mobile Processes in the HAL Environment. CAV 1998.
- Gian Luigi Ferrari, Stefania Gnesi, Ugo Montanari, Marco Pistore: A model-checking verification environment for mobile processes. ACM Trans. Softw. Eng. Methodol. 2003.

Named sets and their coalgebras defined type-theoretically

MiHDa minimization algorithm for pi-calculus proved in the finite case and implemented

- Gian Luigi Ferrari, Ugo Montanari, Marco Pistore: Minimizing Transition Systems for Name Passing Calculi: A Co-algebraic Formulation. FoSSaCS 2002
- Gian Luigi Ferrari, Ugo Montanari, Roberto Raggi, Emilio Tuosto: From Co-algebraic Specifications to Implementation: The Mihda Toolkit. FMCO 2002.
- Gian Luigi Ferrari, Ugo Montanari, Emilio Tuosto: Model Checking for Nominal Calculi. FoSSaCS 2005.
- Gian Luigi Ferrari, Ugo Montanari, Emilio Tuosto: Coalgebraic minimization of HD-automata for the Pi-calculus using polymorphic types. TCS 2005.
- Emilio Tuosto, Non-Functional Aspects of Wide Area Network Programming, PhD Thesis, University of Pisa, 2003.

The MIHDA Minimization Tool

- Written in OCAML
- Implements the Kanellakis-Smolka list partitioning algorithm
- Parametric wrt the underlying category
- Most time spent in handling name permutations
- Reasonably efficient execution:
  - handover protocol for GSM Mobile Network
  - the π-calculus specification has 506 states, 745 transitions
  - minimization in 9 seconds on a one-core processor
  - resulting HD-automaton with 105 states and 197 transitions

Roadmap

- History Dependent automata
  - No symmetries
  - Spans of open maps
  - With symmetries
  - For verification
- Named sets vs. presheaves
- Network Conscious π-calculus
- Named graphs
- Conclusion

Three Equivalent Structures

Categorical equivalence between

- the nominal sets of Gabbay and Pitts/permutation algebras
- the Schanuel topos
- the named sets of Montanari and Pistore (whose coalgebras are HD-automata)

Equivalence for Coalgebras

- Marcelo Fiore, Sam Staton, Information and Computation, 2006
- Fabio Gadducci, Marino Miculan, Ugo Montanari, Higher-Order and Symbolic Computation, 2006
- Vincenzo Ciancia, Ugo Montanari: A Name Abstraction Functor for Named Sets, CMCS 2008.
- Vincenzo Ciancia, Accessible Functors and Final Coalgebras for Named Sets, Ph.D. Thesis, 2008.
- Vincenzo Ciancia, Ugo Montanari: Symmetries, Local Names and Dynamic (De)-Allocation of Names. Information and Computation, 2010.

The Category of Named Sets, Revisited, Generalized

- We represent the wide pullback preserving full subcategory of $\mathbf{Set}^{\mathbf{C}}$ as the category $\mathbf{Fam}(\mathbf{Sym}(\mathbf{C})^{op})$
- $\mathbf{Sym}(\mathbf{C})$ is the category of groups of automorphisms of $\mathbf{C}$, representing the **support** and **symmetry** of an element of a presheaf
- Symmetries are the essential information that is needed to reconstruct each represented presheaf: first one reconstructs the presheaf "freely" using representables, then a quotient is made using the symmetry.

For named sets, C is I, the category of finite subsets of natural numbers and injections

Families

Given a **small** category **C**, we define the category **Fam(C)**

- Objects are coproducts in **Set**: indexed collections of objects of **C**

$$\coprod_{i \in I} \{c_i\}$$

- Each $i \in I$ is considered an **element** whose **local interface** is c_i
- An arrow from $\coprod_{i \in I}\{c_i\}$ to $\coprod_{j \in J}\{d_j\}$ is a function $h : i \to j$ and a family of **C** arrows

$$\coprod_{i \in I} \{\mathcal{H}_i : c_i \to d_{h(i)}\}$$

Category Symset = Sym(Set)

Objects:

permutation groups over finite subsets of ω

Morphisms:

$$\mathbf{Symset}[\Phi_1, \Phi_2] :=$$

$$\{ i \circ \Phi_1 \mid i : dom(\Phi_1) \rightarrowtail dom(\Phi_2) \wedge \Phi_2 \circ i \subseteq i \circ \Phi_1 \}$$

Composition:

$$id_\Phi := id_{dom(\Phi)} \circ \Phi = \Phi$$

$$G \circ F = \{ g \circ f \mid g \in G \wedge f \in F \}$$

Can be generalized to automorphism groups of any category

Families vs. Presheaves

Q: what categories of presheaves can be represented as families?

1. Our answer: **small index categories of monos,** all automorphisms are iso, and **(weak) wide pullback preservation** give rise to an **equivalence of categories**

2. **[Adamek, Velebil - TAC 2008]**: **locally presentable index categories** and **weak wide pullback preservation** represent presheaves - natural transformations are not encoded.
   Generalises Joyal's species as representations of analytic functors.

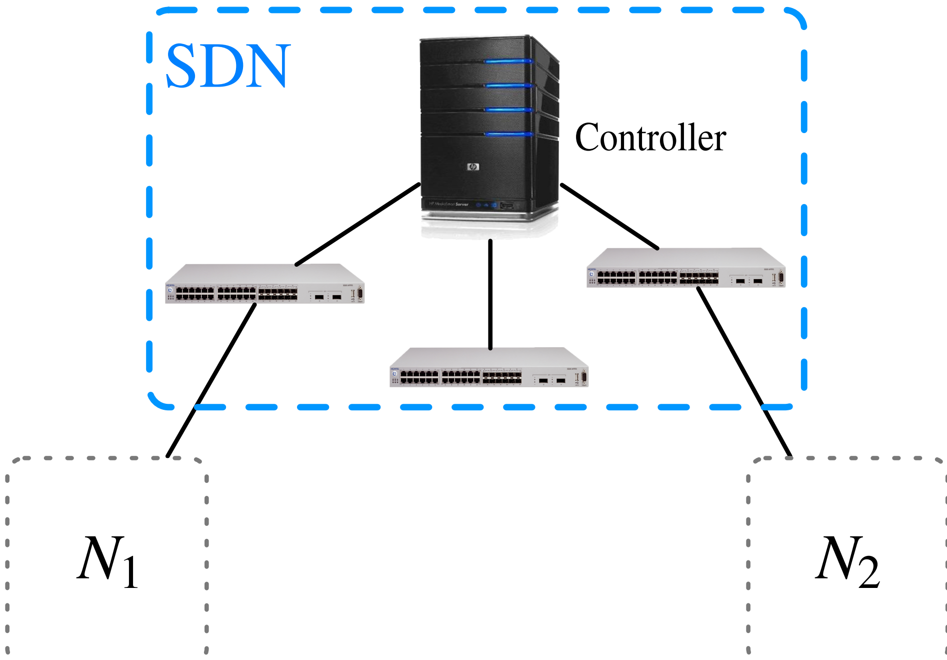
- The two conditions are different: (1) includes coproducts of categories, (2) includes Set
  They obviously overlap (e.g. finite sets and injections).

Vincenzo Ciancia, Alexander Kurz, Ugo Montanari, Families of Symmetries as Efficient Models of Resource Binding. CMCS 2010

Roadmap

- History Dependent automata
  - No symmetries
  - Spans of open maps
  - With symmetries
  - For verification
- Named sets vs. presheaves
- Network Conscious π-calculus
- Named graphs
- Conclusion

Network Conscious π-calculus: Motivating Application



Software Defined Networks

- network administrators can program network services via high level constructs

Network Conscious π-calculus: An Example

Network-aware extension of the π -calculus
Two kinds of names:

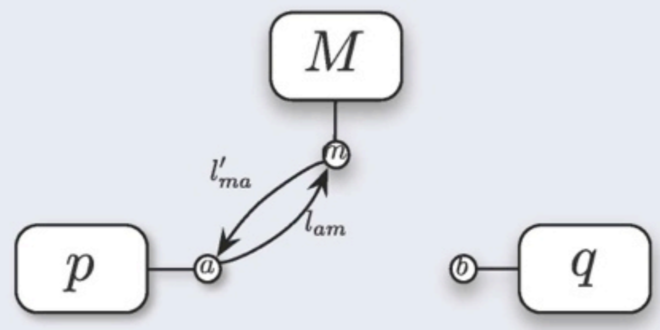
- sites **a,b,c**, i.e. network nodes
- links $\mathbf{l_{ab}}$, connecting two nodes

$$M = m(x).m(y).(l_{xy})(\overline{m}x l_{xy}.M)$$

$$p = \overline{a}ma.\overline{a}mb.a(l_{(xy)}).(L(l_{xy}) \,|\, \overline{a}bc.p')$$

$$q = b(x).q'$$

$$L(l_{xy}) = l_{xy}.L(l_{xy})$$



$$S = p \,|\, M \,|\, q \,|\, L(l_{am}) \,|\, L(l'_{ma})$$

Information Society Technologies

Roadmap

- History Dependent automata
  - No symmetries
  - Spans of open maps
  - With symmetries
  - For verification
- Named sets vs. presheaves
- Network Conscious π-calculus
- Named graphs
- Conclusion

Network Conscious π-calculus: Resources, II

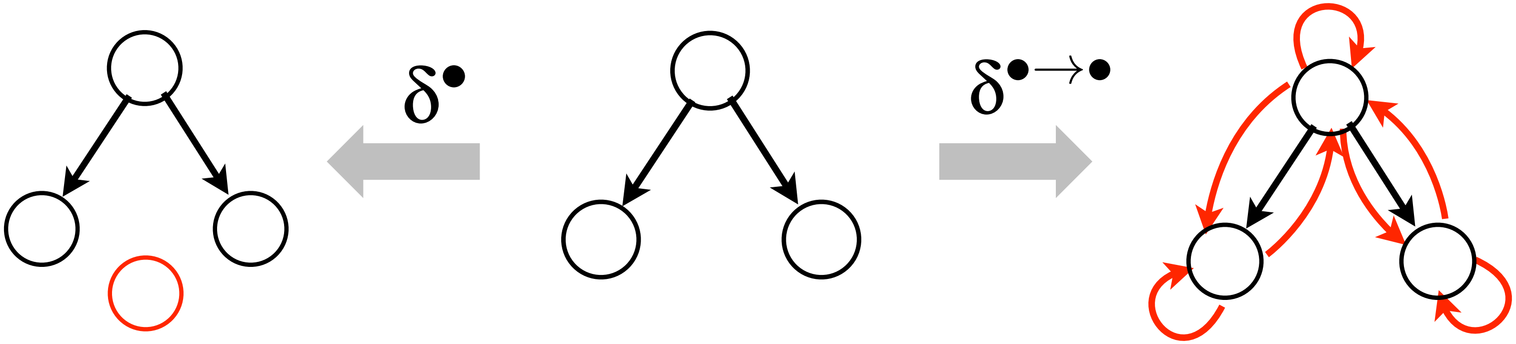
$\mathbf{G}_I$: Directed multigraphs up to isomorphism with injective graph homomorphisms

- Category $\mathbf{Sym}(\mathbb{G}_I)$
  - Objects: for all $g \in |\mathbb{G}_I|$, we take all subgroups of $\mathbb{G}_I[g,g]$ (group operation is composition in $\mathbb{G}_I$)
  - Morphisms and composition as before

- Category **Gset**
  - Objects are $N = (Q_N, S_N)$, where $S_N : Q_N \to |\mathbf{Sym}(\mathbb{G}_I)|$

    $\|q\| \in |\mathbb{G}_I|$ is the local graph of q
  - Morphisms are suitable graph homomorphisms
  - Products $N \times M$ are sets of pairs $n_{g_1} \in N, n_{g_2} \in M$ equipped with an embedding of g_1, g_2 in a bigger graph
  - More abstractly: $\boxed{\mathbf{Fam}(\mathbf{Sym}(\mathbb{G}_I)^{op})}$

Network Conscious π-calculus: Resources, III



Endofunctors for resource allocation

HD Automata for Network Conscious π-calculus

Q: what categories of presheaves can be represented as families?

1. Our answer: **small index categories of monos,** all automorphisms are iso, and **(weak) wide pullback preservation** give rise to an **equivalence of categories**

2. **[Adamek, Velebil - TAC 2008]**: **locally presentable index categories** and **weak wide pullback preservation** represent presheaves - natural transformations are not encoded. Generalises Joyal's species as representations of analytic functors.

G_I satisfies condition 1: thus resource conscious π-calculus has HD automata

Ugo Montanari, Matteo Sammartino: Network Conscious π-calculus: A Concurrent Semantics. MFPS 2012.

Ugo Montanari, Matteo Sammartino, A Network-Conscious Pi-Calculus and Its Coalgebraic Semantics, TCS.

Matteo Sammartino, A Network-Aware Process Calculus for Global Computing and its Categorical Framework, PhD Thesis, University of Pisa, December 2013.

Roadmap

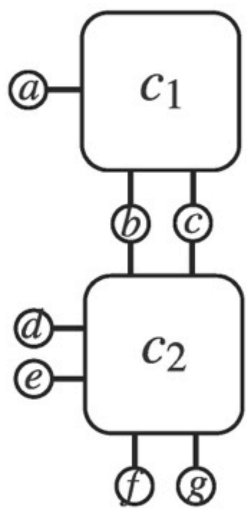
- History Dependent automata
  - No symmetries
  - Spans of open maps
  - With symmetries
  - For verification
- Named sets vs. presheaves
- Network Conscious π-calculus
- Named graphs
- Conclusion

Information Society Technologies

What’s Next: Software Architectures

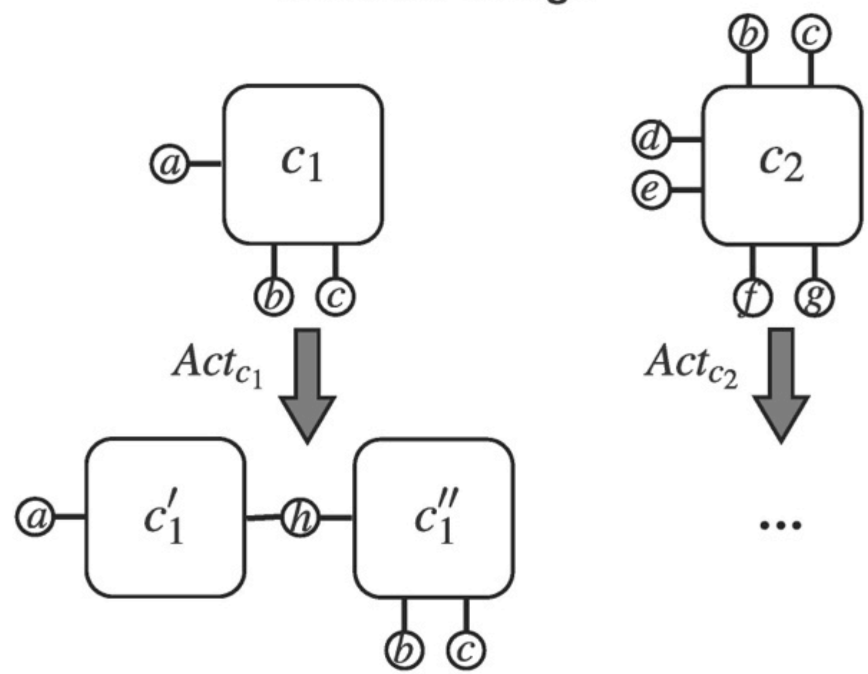
Synchronized hyperedge replacement (CCS-like, i.e. without mobility) to describe

Software architecture



synchronization rules

Detailed design



productions for single hyperedges

Architectures as Resources

Model of resources

- Architectures as a category of hypergraphs
- δs add new components (hyperedges) and connections (nodes)
- Presheaves index systems by their architecture

Two levels of behavior

1. *In the large*
   Algebra of parallel composition of components
   Coalgebra of component synchronization
2. *in the small*
   Syntax of sequential programs/processes
   Coalgebra of process actions

(1) + (2) = Composition of bialgebras to define the whole system

Similar structure for BI(P): **B**ehavior of atomic components + **I**nteractions among them