Simpson's proof systems for process verification: A fine-tuning

Cosimo Perini Brogi[⋆] Rocco De Nicola[⋆] Omar Inverso[*]

[⋆] IMT School for Advanced Studies Lucca

[*] Gran Sasso Science Institute

Italian Conference on Theoretical Computer Science – ICTCS 2024
Torino, 11-13.09.2024

Finanziato dall'Unione europea NextGenerationEU

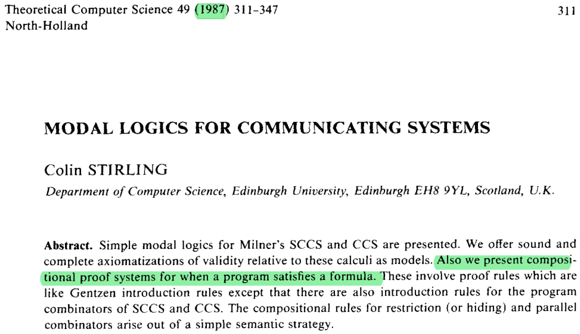
Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

Work supported by the project SERICS - PE0000014, financed within PNRR, M4C2 I.1.3, funded by the European Union - NextGenerationEU

Stirling's research question



Theoretical Computer Science 49 (1987) 311–347 311
North-Holland

MODAL LOGICS FOR COMMUNICATING SYSTEMS

Colin STIRLING

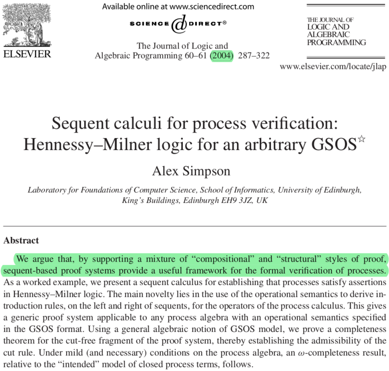
Department of Computer Science, Edinburgh University, Edinburgh EH8 9YL, Scotland, U.K.

Abstract. Simple modal logics for Milner's SCCS and CCS are presented. We offer sound and complete axiomatizations of validity relative to these calculi as models. Also we present compositional proof systems for when a program satisfies a formula. These involve proof rules which are like Gentzen introduction rules except that there are also introduction rules for the program combinators of SCCS and CCS. The compositional rules for restriction (or hiding) and parallel combinators arise out of a simple semantic strategy.

Verification of modular processes *should* be modular

"[C]*ompositional, syntax-directed* proof systems" for verifying properties of concurrent systems expressed in the language of modal logics

Simpson's answer



Available online at www.sciencedirect.com

SCIENCE DIRECT®

The Journal of Logic and Algebraic Programming 60–61 (2004) 287–322

ELSEVIER

THE JOURNAL OF LOGIC AND ALGEBRAIC PROGRAMMING

www.elsevier.com/locate/jlap

Sequent calculi for process verification: Hennessy–Milner logic for an arbitrary GSOS☆

Alex Simpson

Laboratory for Foundations of Computer Science, School of Informatics, University of Edinburgh, King's Buildings, Edinburgh EH9 3JZ, UK

Abstract

We argue that, by supporting a mixture of "compositional" and "structural" styles of proof, sequent-based proof systems provide a useful framework for the formal verification of processes. As a worked example, we present a sequent calculus for establishing that processes satisfy assertions in Hennessy–Milner logic. The main novelty lies in the use of the operational semantics to derive introduction rules, on the left and right of sequents, for the operators of the process calculus. This gives a generic proof system applicable to any process algebra with an operational semantics specified in the GSOS format. Using a general algebraic notion of GSOS model, we prove a completeness theorem for the cut-free fragment of the proof system, thereby establishing the admissibility of the cut rule. Under mild (and necessary) conditions on the process algebra, an ω-completeness result, relative to the "intended" model of closed process terms, follows.

Verification of modular processes *can* be modular *and natural*

"[C]ompositional, structural and naturalness aspects of sequent-based proof follow from properties of the basic sequent calculus [. . .] [It is possible] to relate processes (or programs) to their logical properties [. . .] without breaking the fundamental structural properties of sequent calculus."

Our improvement

A more principled approach

Apply *contemporary* proof-theoretic techniques to enhance Simpson's idea and uniformly obtain a new family of modular sequent calculi for logical verification of concurrent processes: The *motto* is

"Keep left & Geometrize!"

Our improvement

A more principled approach

Apply *contemporary* proof-theoretic techniques to enhance Simpson's idea and uniformly obtain a new family of modular sequent calculi for logical verification of concurrent processes: The *motto* is

"Keep left & Geometrize!"

Results

- Constructive cut-elimination from calculi for Hennessy-Milner logic and GSOS processes
- Substantial simplification of Simpson's proofs for structural and semantic completeness of this kind of calculi

GSOS

Integration in sequents

$$\frac{\{x_i \xrightarrow{\mu_{ij}} y_{ij} \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m_i\} \qquad \cup \qquad \{x_i \overset{\nu_{ik}}{\not\to} \ \mid 1 \leqslant i \leqslant n, 1 \leqslant k \leqslant \ell_i\}}{f(\vec{x}) \xrightarrow{\pi} p(\vec{x},\vec{y})}$$

Consequences of Simpson’s approach

- Cut admissibility and completeness require *ad hoc* conditions on assumable sequents
- Purely *semantic* proof of cut admissibility

GSOS

Our rules

$$\frac{\{x_i \xrightarrow{\mu_{ij}} y_{ij} \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m_i\} \quad \cup \quad \{x_i \overset{\nu_{ik}}{\not\to} \mid 1 \leqslant i \leqslant n, 1 \leqslant k \leqslant \ell_i\}}{f(\vec{x}) \xrightarrow{\pi} p(\vec{x}, \vec{y})}$$

GSOS

Our rules

$$\frac{\{x_i \overset{\mu_{ij}}{\rightarrow} y_{ij} \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m_i\} \qquad \cup \qquad \{x_i \overset{\nu_{ik}}{\not\rightarrow} \mid 1 \leqslant i \leqslant n, 1 \leqslant k \leqslant \ell_i\}}{f(\vec{x}) \overset{\pi}{\rightarrow} p(\vec{x},\vec{y})}$$

Geometrize!

$$(\circ)\ \forall \vec{x}, \vec{y} : \left[\left(\bigwedge_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m_i} (x_i \overset{\mu_{ij}}{\rightarrow} y_{ij}) \ \& \bigwedge_{1\leqslant i\leqslant n, 1\leqslant k\leqslant \ell_i} (x_i \overset{\nu_{ik}}{\not\rightarrow}\ ) \right) \supset (f(\vec{x}) \overset{\pi}{\rightarrow} p(\vec{x},\vec{y})) \right]$$

$$(\circ\circ)\ \forall \vec{r}, \vec{y}, z : \left[(f(\vec{r}) \overset{\pi}{\rightarrow} z) \supset \left(\exists \vec{y} : p(\vec{r},\vec{y}) \equiv z \ \& \bigwedge_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m_i} (r_i \overset{\mu_{ij}}{\rightarrow} y_{ij}) \ \& \bigwedge_{1\leqslant i\leqslant n, 1\leqslant k\leqslant \ell_i} (r_i \overset{\nu_{ik}}{\not\rightarrow}\ ) \right) \right]$$

GSOS

Our rules

$$\frac{\{x_i \xrightarrow{\mu_{ij}} y_{ij} \mid 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m_i\} \quad \cup \quad \{x_i \overset{\nu_{ik}}{\not\rightarrow} \mid 1 \leqslant i \leqslant n, 1 \leqslant k \leqslant \ell_i\}}{f(\vec{x}) \xrightarrow{\pi} p(\vec{x},\vec{y})}$$

Geometrize!

$$(\circ)\ \forall \vec{x},\vec{y} : \left[\left(\bigwedge_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m_i} (x_i \xrightarrow{\mu_{ij}} y_{ij}) \ \& \bigwedge_{1\leqslant i\leqslant n, 1\leqslant k\leqslant \ell_i} (x_i \overset{\nu_{ik}}{\not\rightarrow}\ )\right) \supset (f(\vec{x}) \xrightarrow{\pi} p(\vec{x},\vec{y}))\right]$$

$$(\circ\circ)\ \forall \vec{r},\vec{y},z : \left[(f(\vec{r}) \xrightarrow{\pi} z) \supset \left(\exists \vec{y} : p(\vec{r},\vec{y}) \equiv z \ \& \bigwedge_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m_i} (r_i \xrightarrow{\mu_{ij}} y_{ij}) \ \& \bigwedge_{1\leqslant i\leqslant n, 1\leqslant k\leqslant \ell_i} (r_i \overset{\nu_{ik}}{\not\rightarrow}\ )\right)\right]$$

Keep left!

$$\frac{f(\vec{x}) \xrightarrow{\pi} p(\vec{x},\vec{y}),\ \{x_i \xrightarrow{\mu_{ij}} y_{ij}\}_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m_i},\ \{x_i \overset{\nu_{ik}}{\not\rightarrow}\ \}_{1\leqslant i\leqslant n, 1\leqslant k\leqslant \ell_i},\Gamma \Rightarrow \Delta}{\{x_i \xrightarrow{\mu_{ij}} y_{ij}\}_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m_i},\ \{x_i \overset{\nu_{ik}}{\not\rightarrow}\ \}_{1\leqslant i\leqslant n, 1\leqslant k\leqslant \ell_i},\Gamma \Rightarrow \Delta}\ f\circ$$

$$\frac{}{p \overset{\mu}{\not\rightarrow}\ , p \xrightarrow{\mu} q, \Gamma \Rightarrow \Delta}\ \overset{\mu}{\not\rightarrow}\ \mathit{Def}$$

$$\frac{\left\{p_h(\vec{r},\vec{y}) \equiv z,\ \{r_i \xrightarrow{\mu_{ij}} y_{ij}\}_{1\leqslant i\leqslant n, 1\leqslant j\leqslant m_i},\ \{x_i \overset{\nu_{ik}}{\not\rightarrow}\ \}_{1\leqslant i\leqslant n, 1\leqslant k\leqslant \ell_i}, f(\vec{r}) \xrightarrow{\pi} z, \Gamma \Rightarrow \Delta\right\}_{1\leqslant h\leqslant N}}{f(\vec{r}) \xrightarrow{\pi} z, \Gamma \Rightarrow \Delta}\ f\circ\circ_{(!\vec{y})}$$

+ Rules for ≡-repl.

Main results

Theorem

$\mathsf{G3HML}_{GSOS}$ *satisfies the following properties:*

Soundness: *If the sequent $\Gamma \Rightarrow \Delta$ is derivable, then $\Gamma \vDash \Delta$*

Completeness: *If the sequent $\Gamma \Rightarrow \Delta$ is not derivable, then it is possible to extract from the failed proof search an LTS-countermodel to $\Gamma \Rightarrow \Delta$*

Structural completeness:

- *Generalised initial sequents are derivable*
- *Substitution rule for states over variables are height-preserving admissible*
- *Weakening rules are height preserving admissible*
- *All the rules are height-preserving invertible*
- *Contraction rules are height-preserving admissible*

Cut elimination: *The cut rule can be effectively eliminated*

Put in perspective

- Substantial refinement of Simpson's original labelled sequent calculi for GSOS
- *More principled* formalisation and approach to verification of GSOS processes
- Our cut elimination algorithm as basic result for automation of verification tasks

Put in perspective

- ► Substantial refinement of Simpson's original labelled sequent calculi for GSOS
- ► *More principled* formalisation and approach to verification of GSOS processes
- ► Our cut elimination algorithm as basic result for automation of verification tasks
- ◇ Future extensions with more expressive logics
- ◇ Modular extensions for more general process formats
- ◇ Implementation of certified theorem provers (and countermodel constructors)

Put in perspective

- ► Substantial refinement of Simpson's original labelled sequent calculi for GSOS
- ► *More principled* formalisation and approach to verification of GSOS processes
- ► Our cut elimination algorithm as basic result for automation of verification tasks

- ◇ Future extensions with more expressive logics
- ◇ Modular extensions for more general process formats
- ◇ Implementation of certified theorem provers (and countermodel constructors)

Many thanks for listening!

cosimo.perinibrogi@imtlucca.it