μ-Calculus with Explicit Points and Approximations

Mads Dam[1] and Dilian Gurov[2]

[1] Dept. of Teleinformatics, Royal Institute of Technology (KTH/IT),
Electrum 204, SE-164 40 Kista, Sweden, E-mail: mfd@sics.se
[2] Corr. author, Swedish Institute of Computer Science (SICS),
Box 1263, SE-164 29 Kista, Sweden, E-mail: dilian@sics.se
tel: (+46 8) 633 1528, fax: (+46 8) 751 7230

Abstract. We present a Gentzen-style sequent calculus for program verification which accomodates both model checking-like verification based on global state space exploration, and compositional reasoning. To handle the complexities arrising from the presence of fixed-point formulas, programs with dynamically evolving architecture, and cut rules we use transition assertions, and introduce fixed-point approximants explicitly into the assertion language. We address, in a game-based manner, the semantical basis of this approach, as it applies to the entailment subproblem. Soundness and completeness results are obtained, and examples are shown illustrating some of the concepts.

1 Introduction

In a number of recent papers [1, 2, 4, 5, 9] proof-theoretical frameworks for compositional verification have been put forward based on Gentzen-style sequents of the shape $\Gamma \vdash \Delta$, where the components of Γ and Δ are correctness assertions $P : \phi$. Several programming or modelling languages have been considered, including CCS [4], the π-calculus [2], CHOCS [1], general GSOS-definable languages [9], and even a significant core fragment of a real programming language, Erlang [5]. An important precursor to the above papers is [10] which used ternary sequents to build compositional proof systems for CCS and SCCS vs. Hennessy-Milner logic [7].

A key idea is that the use of a general sequent format allows correctness properties $P : \phi$ to be stated and proved in a *parametric* fashion. That is, correctness statements ϕ of a composite program $P(Q_1, Q_2)$, say, can be relativized to correctness statements of the components, Q_1, Q_2. A general rule of subterm cut

$$\frac{\Gamma \vdash Q : \psi, \Delta \quad \Gamma, x : \psi \vdash P : \phi, \Delta}{\Gamma \vdash P[Q/x] : \phi, \Delta}$$

allows such subterm assumptions to be introduced and used for compositional verification.

The difficulty with this (as with any other approach to modular verification) is to find a way of supporting temporal properties. In [4] we showed one way of doing this, and built, for the first time, a compositional proof system capable of handling general CCS terms, including those that create new processes dynamically (the only source of infiniteness in CCS). Essentially, recursive formulas are handled using some form of well-founded induction on approximation ordinals. In the absence of the subterm cut rule (or other rules with similar effect, such as the classical cut) approximation ordinals can be guaranteed to occur only in covariant positions, allowing techniques like tagging [12, 3] to be applied. In the presence of cut this can, however, no longer be guaranteed. To be sound, rates of progress for fixed point formulas appearing in different places in a sequent must be related. In our earlier work this caused us to rely on a handling of fixed points which was extremely syntactical, hedged with side conditions, and also unnecessarily restrictive.

The contribution of the present paper is to show that a simpler and more semantical approach is possible, by introducing approximation ordinal variables explicitly into the proof system.

In a previous paper [6] we instantiated our approach to CCS and illustrated the workings of the proof system by means of examples. In this paper we address the semantical basis, as it applies to the entailment subproblem. After briefly introducing the logic and proof system we present a *refutation game* providing a semantical characterisation of validity for cyclic proof structures. We prove soundness of the derived notion of refutation-game provability, and give a completeness result through reduction to Kozen's axiomatisation. For practical proof search the game-based

characterization is unsatisfactory – it does not permit loop closure to be determined effectively. For this reason we introduce (in the full paper) a rule of assumption discharge and show it sound and complete. To illustrate the workings of the proof system we exhibit two examples, of a sequent which is provable and of another sequent which is not.

2 Logic

The standard syntax of the modal μ-calculus is augmented by adding a form of fixed point formula approximation, using ordinal variables. Formulas ϕ are generated by the following grammar, where κ ranges over a set of *ordinal variables*, α over a set of *actions*, and X over a set of *propositional variables*.

$$\phi ::= \phi \vee \phi \;\big|\; \neg\phi \;\big|\; \langle\alpha\rangle\phi \;\big|\; X \;\big|\; \mu X.\phi \;\big|\; (\mu X.\phi)^{\kappa}$$

We assume the standard modal μ-calculus semantics [8], augmented by the clause:

$$\|(\mu X.\phi)^{\kappa}\|\rho = \begin{cases} \emptyset & \text{if } \rho(\kappa) = 0 \\ \|\phi\|\rho[\|(\mu X.\phi)^{\kappa}\|\rho/X, \beta/\kappa] & \text{if } \rho(\kappa) = \beta + 1 \\ \bigcup\{\|(\mu X.\phi)^{\kappa}\|\rho[\beta/\kappa] \mid \beta < \rho(\kappa)\} & \text{if } \rho(\kappa) \text{ is a limit ordinal} \end{cases}$$

where ρ is an interpretation function (environment), mapping ordinal variables to ordinals, and propositional variables to sets of states $P \in \mathcal{S}$.

3 A Proof System for Logical Entailment

An *assertion* is an expression of one of the forms $E : \phi$, $\kappa < \kappa'$, or $E \xrightarrow{\alpha} F$, where E, F are a process terms and ϕ is a propositionally closed formula. Sequents are of the shape $\Gamma \vdash \Delta$, where Γ and Δ are sets of assertions. A sequent is *pure* if it contains satisfaction assertions only. The notion of *validity* is the standard one for such proof systems.

On top of a fairly standard set of rules we add (assuming that $U = \mu X.\phi$):

$$\langle\alpha\rangle\text{-L}\ \frac{\Gamma, E \xrightarrow{\alpha} x, x : \phi \vdash \Delta}{\Gamma, E : \langle\alpha\rangle\phi \vdash \Delta}\, \mathit{fresh}(x) \qquad \langle\alpha\rangle\text{-R}\ \frac{\Gamma \vdash E \xrightarrow{\alpha} E', \Delta \quad \Gamma \vdash E' : \phi, \Delta}{\Gamma \vdash E : \langle\alpha\rangle\phi, \Delta}$$

$$U\text{-L}\ \frac{\Gamma, E : U^{\kappa} \vdash \Delta}{\Gamma, E : U \vdash \Delta}\, \mathit{fresh}(\kappa) \qquad U\text{-R}\ \frac{\Gamma \vdash E : \phi[U/X], \Delta}{\Gamma \vdash E : U, \Delta}$$

$$U^{\kappa}\text{-L}\ \frac{\Gamma, \kappa' < \kappa, E : \phi[U^{\kappa'}/X] \vdash \Delta}{\Gamma, E : U^{\kappa} \vdash \Delta}\ \mathit{fresh}(\kappa') \qquad U^{\kappa}\text{-R}\ \frac{\Gamma \vdash \kappa' < \kappa, \Delta \quad \Gamma \vdash E : \phi[U^{\kappa'}/X], \Delta}{\Gamma \vdash E : U^{\kappa}, \Delta}$$

$$\textsc{OrdTr}\ \frac{\Gamma, \kappa' < \kappa \vdash \kappa'' < \kappa', \Delta}{\Gamma, \kappa' < \kappa \vdash \kappa'' < \kappa, \Delta}$$

Theorem 1 (Local Soundness). *All rules for logical entailment are individually sound: The conclusion of each rule is valid whenever its premises are valid.*

4 The Refutation Game

By themselves the above proof rules are insufficient, as there is no bound on the number of times fixed point formulas need to be unfolded. We devise a simple 1-player game to account for repeating nodes, and for determining when proof construction can safely be terminated, implicitly building in well-founded ordinal induction. We use the notation $N(\Gamma \vdash \Delta)$ to indicate that the node N is labelled by the sequent $\Gamma \vdash \Delta$, and write $N' < N$ if N' appears on the path from the root to N.

Definition 1 (Repeating Node, Arena).

1. *Suppose* $N'(\Gamma' \vdash \Delta') < N(\Gamma \vdash \Delta)$. *Then* N *is a* repeat *of* N' *up to the substitution* σ, *if*
   (a) $A\sigma \in \Gamma$ *whenever* $A \in \Gamma'$, *and*
   (b) $A\sigma \in \Delta$ *whenever* $A \in \Delta'$.

2. *An* arena, $\mathcal{A}$, *is a proof structure for which each leaf node* N *is either an axiom instance or else to* N *is associated some node* N' *and substitution* σ *such that* N *is a repeat of* N' *up to* σ.

Let an arena $\mathcal{A}$ be given, rooted in $N_0(\Gamma \vdash \Delta)$. Initially R picks an interpretation ρ_0 for which $\Gamma \vdash \Delta$ is non-trivial. R's claim is that ρ_0 is a falsifying interpretation for $\Gamma_0 \vdash \Delta_0$. So the *initial configuration* of the game has the shape (N_0, ρ_0). Suppose the game has reached the configuration (N_i, ρ_i). Then R can chose (N_{i+1}, ρ_{i+1}) as a *possible next configuration* if ρ_{i+1} respects the transition assertions and ordinal assertions, and either (1) N_{i+1} is a child node of N_i in $\mathcal{A}$ and ρ_{i+1} agrees with ρ_i on all common free variables, or (2) N_i is a repeat of N' up to some substitution σ in $\mathcal{A}$, and then $N_{i+1} = N'$ and $\rho_{i+1} = \rho_i \circ \sigma$. A game *run*, Π, is a finite or infinite sequence $(N_0, \rho_0), \ldots, (N_i, \rho_i), \ldots$ such that for each $j : 0 \leq j < i$, $\Pi(j+1) = (N_{j+1}, \rho_{j+1})$ is a possible next configuration for $\Pi(j)$.

Definition 2 (Winning Run, Proof).

1. *The refuter* R wins *a game run just in case it is infinite.*
2. *A* proof *is an arena on which* R *has no winning run.*
3. *The sequent* $\Gamma \vdash \Delta$ *is refutation-game provable,* $\Gamma \vdash_r \Delta$, *if there is a proof with root* $\Gamma \vdash \Delta$.

Theorem 2 (Soundness). *The sequent* $\Gamma \vdash \Delta$ *is valid if* $\Gamma \vdash_r \Delta$.

We view transition assertions and ordinal assertions only as an intermediate machinery for proof construction. Therefore, when addressing completeness of the proof system, we are interested in completeness for pure sequents only. Rather than giving a direct completeness proof, which would face well-known complications, we present a completeness result by reduction to Kozen's axiomatisation [8]. This axiomatisation was shown to be complete by Walukiewicz [11].

Theorem 3 (Completeness). *If the pure sequent* $\Gamma \vdash \Delta$ *is valid then* $\Gamma \vdash_r \Delta$.

The refutation game described above gives an abstract condition for when an arena can be considered a proof. For practical proof search the game-based characterization is unsatisfactory – it does not permit loop closure to be determined effectively. For this reason we introduce (in the full paper) a rule of assumption discharge and show it sound and complete as well. To illustrate the workings of the proof system we exhibit two examples, of a sequent which is provable and of another sequent which is not.

References

1. R. Amadio and M. Dam. Reasoning about higher-order processes. In *Proc. CAAP'95,* Lecture Notes in Computer Science, 915:202–217, 1995.
2. R. Amadio and M. Dam. A modal theory of types for the π-calculus. In *Proc. FTRTFT'96,* Lecture Notes in Computer Science, 1135:347–365, 1996.
3. Henrik Reif Andersen, Colin Stirling, and Glynn Winskel. A compositional proof system for the modal μ-calculus. In *Proceedings, Ninth Annual IEEE Symposium on Logic in Computer Science*, pages 144–153, Paris, France, 4–7 July 1994. IEEE Computer Society Press.
4. M. Dam. Proving properties of dynamic process networks. *Information and Computation*, 140:95–114, 1998.
5. M. Dam, L.-å. Fredlund, and D. Gurov. Toward parametric verification of open distributed systems. In *Compositionality: the Significant Difference,* H. Langmaack, A. Pnueli and W.-P. de Roever (eds.), Springer, 1536:150–185, 1998.
6. M. Dam and D. Gurov. Compositional verification of CCS processes. In *Proc. PSI'99,* Lecture Notes in Computer Science, 1755:247–256, 2000.
7. M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the ACM*, **32**:137–162, 1985.
8. D. Kozen. Results on the propositional μ-calculus. *Theoretical Computer Science*, **27**:333–354, 1983.
9. A. Simpson. Compositionality via cut-elimination: Hennessy-Milner logic for an arbitrary GSOS. In *Proc. LICS*, pages 420–430, 26–29 1995.
10. C. Stirling. Modal logics for communicating systems. *Theoretical Computer Science*, 49:311–347, 1987.
11. I. Walukiewicz. Completeness of Kozen's axiomatisation of the propositional mu-calculus. In *Proc. LICS'95,*, pages 14–24, 1995.
12. G. Winskel. A note on model checking the modal ν-calculus. *Theoretical Computer Science*, 83:157–187, 1991.