Towards a Proper Proof Theory of the Modal μ-Calculus

Gerhard Jäger
University of Bern

Ordinals, subsystems of second order arithmetic, . . .

$$=$$

selling coals to Newcastle (Eulen nach Athen tragen)

Important for

Wilfried βuchholz:

- well-foundedness
- β-models
- München $\hookrightarrow$ μ

μ-calculus, its well-founded derivations and its β-models

Some central questions:

- Is there a cut-free (finite), sound and complete formalization of the modal μ-calculus?
- Is there a cut-elimination procedure for the modal μ-calculus?
- What is the complexity of the model checking problem?

Main references

- C. Dax, M. Hofmann, M. Lange, *A proof system for the linear time μ-calculus*, in: Proceedings 26th Conference on Foundations of software Technology and Theoretical Computer Science, LNCS 4337, Springer, 2006.
- G. Jäger, M. Kretz, T. Studer, *Canonical completeness of infinitary μ*, The Journal of Algebraic and Logic Programming, to appear.
- T. Studer, *On the proof theory of the modal mu-calculus*, Studia Logica, to appear.

The syntax of the modal μ-calculus

Var: set of variables $X, Y, Z, \ldots$

Lab: finite set of labels $a, b, c, \ldots$

Formulas $(A, B, C, \ldots)$:

- $\bot \quad | \quad \top \quad | \quad X \quad | \quad {\sim}X \quad |$
- $(A \vee B) \quad | \quad (A \wedge B) \quad | \quad \langle a \rangle A \quad | \quad [a]A \quad |$
- $(\mu X)A \quad | \quad (\nu X)A$ (both for A positive in X)

The semantics of the modal μ-calculus

A μ-structure $\mathfrak{M}$ consists of

- a non-empty set $|\mathfrak{M}|$, the universe of $\mathfrak{M}$,
- $\mathfrak{M}(X) \subset |\mathfrak{M}|$ for all X from Var
- $\mathfrak{M}(a) \subset |\mathfrak{M}| \times |\mathfrak{M}|$ for all a from Lab

For $S \subset |\mathfrak{M}|$: $\mathfrak{M}[Z{:=}S]$ is the μ-structure which maps Z to S and otherwise agrees with $\mathfrak{M}$.

Definition of the value $\|A\|_{\mathfrak{M}}$ of the μ-formula A:

$$
\begin{aligned}
\|\bot\|_{\mathfrak{M}} &:= \emptyset \\
\|\top\|_{\mathfrak{M}} &:= |\mathfrak{M}| \\
\|X\|_{\mathfrak{M}} &:= \mathfrak{M}(X) \\
\|{\sim}X\|_{\mathfrak{M}} &:= |\mathfrak{M}| \setminus \mathfrak{M}(X) \\
\|A \vee B\|_{\mathfrak{M}} &:= \|A\|_{\mathfrak{M}} \,\cup\, \|B\|_{\mathfrak{M}} \\
\|A \wedge B\|_{\mathfrak{M}} &:= \|A\|_{\mathfrak{M}} \,\cap\, \|B\|_{\mathfrak{M}} \\
\|\langle a\rangle B\|_{\mathfrak{M}} &:= \{s : (\exists t)(\langle s,t\rangle \in \mathfrak{M}(a) \ \&\ t \in \|B\|_{\mathfrak{M}}\} \\
\|[a]B\|_{\mathfrak{M}} &:= \{s : (\forall t)(\langle s,t\rangle \in \mathfrak{M}(a) \ \Rightarrow\ t \in \|B\|_{\mathfrak{M}}\}
\end{aligned}
$$

$$\|(\mu X)A\|_{\mathfrak{M}} := \bigcap\{S \subset |\mathfrak{M}| : \|A\|_{\mathfrak{M}[X:=S]} \subset S\}$$

$$\|(\nu X)A\|_{\mathfrak{M}} := \bigcup\{S \subset |\mathfrak{M}| : S \subset \|A\|_{\mathfrak{M}[X:=S]}\}$$

For all X-positive A, the operator Φ_A, depending on $\mathfrak{M}$,

$$\Phi_A : \mathsf{Pow}(|\mathfrak{M}|) \to \mathsf{Pow}(|\mathfrak{M}|), \qquad \Phi_A(S) := \|A\|_{\mathfrak{M}[X:=S]}$$

is monotone.

Remark 1 Independent of $\mathfrak{M}$, the least and greatest fixed point terms $(\mu X)A$ and $(\nu X)A$ are interpreted as the real least and greatest fixed points, respectively.

Definition 2

1. A formula A is called μ-*valid* if we have $|\mathfrak{M}| \subseteq \|A\|_{\mathfrak{M}}$ for every μ-structure $\mathfrak{M}$; in this case we write $\mu \models A$.

2. A formula A is called μ-*satisfiable* if there exists a μ-structure $\mathfrak{M}$ such that $\|A\|_{\mathfrak{M}} \neq \emptyset$.

Remark 3

1. There exists a natural and trivially sound Hilbert-style axiomatization of the modal μ-calculus due to D. Kozen.

2. According to a result of I. Walukiewicz it is also complete.

3. The completeness proof requires a complicated machinery: tree automata, games, very technical syntactic reductions.

The infinitary calculus $\mathrm{K}_\omega(\mu)$

Extend the language to:

- $\bot \quad | \quad \top \quad | \quad X \quad | \quad {\sim}X \quad |$
- $(A \vee B) \quad | \quad (A \wedge B) \quad | \quad \langle a \rangle B \quad | \quad [a]B \quad |$
- $(\mu X)A \quad | \quad (\nu X)A \quad | \quad (\nu^n X)A \quad$ (A positive in X, $0 < n < \omega$)

μ-formulas are formulas without subformulas of the form $(\nu^n X)B$.

Reduction:

$A^- \quad := \quad$ replace in A all subformulas $(\nu^n X)B$ by $(\nu X)B$

Axioms of $\mathrm{K}_\omega(\mu)$. For all finite formulas sets Γ and all variables X:

$$\Gamma,\ \top \qquad || \qquad \Gamma,\ X,\ {\sim}X$$

Logical rules of $\mathrm{K}_\omega(\mu)$. For all finite formula sets Γ, Δ, all labels a and all formulas A, B:

$$\frac{\Gamma,\ A,\ B}{\Gamma,\ A \vee B}$$

$$\frac{\Gamma,\ A \qquad\qquad \Gamma,\ B}{\Gamma,\ A \wedge B}$$

$$\frac{\Gamma,\ A}{\langle a\rangle\Gamma,\ [a]A,\ \Delta}$$

μ-rules of $\mathbf{K}_\omega(\mu)$. For all finite formula sets Γ and all X-positive formulas $A[X]$:

$$\frac{\Gamma,\ A[(\mu X)A[X]]}{\Gamma,\ (\mu X)A[X]}$$

ν-rules of $\mathbf{K}_\omega(\mu)$. For all finite formula sets Γ and all X-positive formulas $A[X]$:

$$\frac{\Gamma,\ A[\top]}{\Gamma,\ (\nu^1 X)A[X]} \qquad || \qquad \frac{\Gamma,\ A[(\nu^n X)A[X]]}{\Gamma,\ (\nu^{n+1} X)A[X]}$$

$$\frac{\ldots\ \Gamma,\ (\nu^n X)A[X]\ \ldots \quad \text{(for all } 0 < n < \omega)}{\Gamma,\ (\nu X)A[X]}$$

Given a μ-structure $\mathfrak{M}$ and an X-positive formula $A[X]$, the greatest fixed point $gfp(A)$ of the operator

$$\Phi_A \; : \; \mathsf{Pow}(|\mathfrak{M}|) \; \to \; \mathsf{Pow}(|\mathfrak{M}|), \qquad \Phi_A(S) \; := \; \|A\|_{\mathfrak{M}[X:=S]}$$

is approximated by setting

$$J_A^\alpha \; := \; \Phi_A(\bigcap_{\beta<\alpha} J_A^\beta)$$

Then: $$gfp(A) \; = \; \bigcap_\alpha J_A^\alpha \; = \; \bigcap_{\alpha<||A||} J_A^\alpha$$

Typically, the closure ordinal $||A||$ of Φ_A is beyond ω; hence there are two problems with respect to $\mathbf{K}_\omega(\mu)$:

- soundness of $\mathbf{K}_\omega(\mu)$
- completeness of $\mathbf{K}_\omega(\mu)$

Measuring the complexities of formulas

For $\boldsymbol{\sigma} = \langle \sigma_1, \ldots, \sigma_m \rangle$ and $\boldsymbol{\tau} = \langle \tau_1, \ldots, \tau_n \rangle$ we set:

$$\boldsymbol{\sigma} * \boldsymbol{\tau} \ := \ \langle \sigma_1, \ldots, \sigma_m, \tau_1, \ldots, \tau_n \rangle$$

$$\boldsymbol{\sigma} \sqcup \boldsymbol{\tau} \ := \ \begin{cases} \langle \max(\sigma_1, \tau_1), \ldots, \max(\sigma_m, \tau_m), \tau_{m+1}, \ldots, \tau_n \rangle & \text{if } m \leq n, \\ \langle \max(\sigma_1, \tau_1), \ldots, \max(\sigma_n, \tau_n), \sigma_{n+1}, \ldots, \sigma_m \rangle & \text{if } n < m \end{cases}$$

$$<_{lex} := \begin{cases} \text{strict lexicographical ordering of} \\ \text{finite sequences of ordinals} \end{cases}$$

Remark 4 $<_{lex}$ is a well-ordering on any set of sequences of bounded lengths, though not a well-ordering in general.

Definition 5 The *rank* $rk(A)$ of a formula A is inductively defined by:

$$
\begin{array}{rclcll}
rk(A) & := & rk(\sim A) & := & \langle 0 \rangle & (A \text{ atomic}) \\
rk(A \vee B) & := & rk(A \wedge B) & := & (rk(A) \sqcup rk(B)) * \langle 0 \rangle & \\
rk(\langle a \rangle B) & := & rk([a]B) & := & rk(B) * \langle 0 \rangle &
\end{array}
$$

$$
\begin{array}{rcl}
rk((\mu X)A[X]) & := & rk(A[\top]) * \langle 0 \rangle \\
rk((\nu X)A[X]) & := & rk(A[\top]) * \langle \omega \rangle \\
rk((\nu^n X)A[X]) & := & rk(A[\top]) * \langle n \rangle
\end{array}
$$

In addition,

$$lh(A) \ := \ lh(rk(A)).$$

Lemma 6 *We have, e.g.,*

1. $lh(A) = lh(A^-)$; $rk(A)$ *pointwise less than or equal to* $rk(A^-)$.
2. $rk(A[(\nu^n X)A[X]]) <_{lex} rk((\nu^{n+1} X)A[X]) <_{lex} rk((\nu X)A[X])$.

Definition 7 The *Fischer-Ladner closure* $\mathbb{FL}(D)$ of a μ-formula D is inductively defined by:

- $D \in \mathbb{FL}(D)$,
- $(A \vee B) \in \mathbb{FL}(D)$ or $(A \wedge B) \in \mathbb{FL}(D) \quad \Rightarrow \quad A, B \in \mathbb{FL}(D)$,
- $\langle a \rangle B \in \mathbb{FL}(D)$ or $[a]B \in \mathbb{FL}(D) \quad \Rightarrow \quad B \in \mathbb{FL}(D)$,
- $(\mu X)A[X] \in \mathbb{FL}(D) \quad \Rightarrow \quad A[\top], A[(\mu X)A[X]] \in \mathbb{FL}(D)$,
- $(\nu X)A[X] \in \mathbb{FL}(D) \quad \Rightarrow \quad A[\top], A[(\nu X)A[X]] \in \mathbb{FL}(D)$.

Definition 8 The *strong closure* $\mathbb{SC}(D)$ of a μ-formula D is inductively defined by:

- $D \in \mathbb{SC}(D)$,
- $(A \vee B) \in \mathbb{SC}(D)$ or $(A \wedge B) \in \mathbb{SC}(D) \quad \Rightarrow \quad A, B \in \mathbb{SC}(D)$,
- $\langle a \rangle B \in \mathbb{SC}(D)$ or $[a]B \in \mathbb{SC}(D) \quad \Rightarrow \quad B \in \mathbb{SC}(D)$,
- $(\mu X)A[X] \in \mathbb{SC}(D) \quad \Rightarrow \quad A[\top], A[(\mu X)A[X]] \in \mathbb{SC}(D)$,
- $(\nu X)A[X] \in \mathbb{SC}(D) \quad \Rightarrow \quad A[\top], A[(\nu^n X)A[X]] \in \mathbb{SC}(D)$,
- $(\nu^{n+1} X)A[X] \in \mathbb{SC}(D) \quad \Rightarrow \quad A[(\nu^n X)A[X]] \in \mathbb{SC}(D)$,
- $(\nu^1 X)A[X] \in \mathbb{SC}(D) \quad \Rightarrow \quad A[\top] \in \mathbb{SC}(D)$.

Lemma 9 *For any μ-formula D:*

$$A \in \mathbb{SC}(D) \quad \Rightarrow \quad A^{-} \in \mathbb{FL}(D).$$

Lemma 10 *If D is a μ-formula, then the restriction of $<_{lex}$ to the set $\{rk(A) : A \in \mathbb{SC}(D)\}$ is a well-ordering.*

Saturation

Definition 11 Let D be some μ-formula. A finite subset Γ of $\mathbb{SC}(D)$ is called *D-saturated* if the following conditions are satisfied:

$$\mathbf{K}_\omega(\mu) \nvdash \Gamma$$

$$A \vee B \in \Gamma \;\Rightarrow\; A \in \Gamma \text{ and } B \in \Gamma$$

$$A \wedge B \in \Gamma \;\Rightarrow\; A \in \Gamma \text{ or } B \in \Gamma$$

$$(\mu X)A[X] \in \Gamma \;\Rightarrow\; A[(\mu X)A[X]] \in \Gamma$$

$$(\nu X)A[X] \in \Gamma \;\Rightarrow\; (\nu^i X)A[X] \in \Gamma \text{ for some } 0 < i < \omega$$

$$(\nu^{n+1} X)A[X] \in \Gamma \;\Rightarrow\; A[(\nu^n X)A[X]] \in \Gamma$$

$$(\nu^1 X)A[X] \in \Gamma \;\Rightarrow\; A[\top] \in \Gamma$$

Lemma 12 *Let D be some μ-formula. For every finite subset Γ of $\mathbb{SC}(D)$ which is not provable in $\mathbf{K}_\omega(\mu)$ there exists a finite subset Δ of $\mathbb{SC}(D)$ which is D-saturated and contains Γ.*

Definition 13 Let D be some μ-formula. Then $\mathfrak{S}_D$ is the Kripke structure which is defined by the following three conditions:

- $|\mathfrak{S}_D|$:= collection of all D-saturated sets
- For any label a,

$$(\Gamma, \Delta) \in \mathfrak{S}_D(a) \quad :\Leftrightarrow \quad (\Gamma, \Delta) \in |\mathfrak{S}_D|^2 \text{ and } \{ B : \langle a \rangle B \in \Gamma \} \subset \Delta.$$

- For any variable X,

$$\mathfrak{S}_D(X) := \{ \Gamma \in |\mathfrak{S}_D| : X \notin \Gamma \}.$$

Signed truth sets (similar to Streett and Emerson)

Fix a μ-formula D and a $\boldsymbol{\sigma} = \langle \sigma_1, \ldots, \sigma_m \rangle$ of suitable length. Then signed truth sets $\|A\|_D^{\boldsymbol{\sigma}}$ are inductively defined as follows:

$$\|\bot\|_D^{\boldsymbol{\sigma}} := \emptyset \qquad \|\top\|_D^{\boldsymbol{\sigma}} := |\mathfrak{S}_D|$$

$$\|X\|_D^{\boldsymbol{\sigma}} := \mathfrak{S}_D(X) \qquad \|{\sim}X\|_D^{\boldsymbol{\sigma}} := |\mathfrak{M}| \setminus \mathfrak{S}_D(X)$$

$$\|A \vee B\|_D^{\boldsymbol{\sigma}} := \|A\|_D^{\boldsymbol{\sigma}} \cup \|B\|_D^{\boldsymbol{\sigma}} \qquad \|A \wedge B\|_D^{\boldsymbol{\sigma}} := \|A\|_D^{\boldsymbol{\sigma}} \cap \|B\|_D^{\boldsymbol{\sigma}}$$

$$\|\langle a \rangle B\|_D^{\boldsymbol{\sigma}} := \{\Gamma : (\exists \Delta)(\langle \Gamma, \Delta \rangle \in \mathfrak{S}_D(a) \ \& \ \Delta \in \|B\|_D^{\boldsymbol{\sigma}}\}$$

$$\|[a]B\|_D^{\boldsymbol{\sigma}} := \{\Gamma : (\forall \Delta)(\langle \Gamma, \Delta \rangle \in \mathfrak{S}_D(a) \ \Rightarrow \ \Delta \in \|B\|_D^{\boldsymbol{\sigma}}\}$$

For fixed point formulas: Given an X-positive formula $A[X]$ we first introduce the monotone operator

$$\Phi_A : \mathsf{Pow}(|\mathfrak{S}_D|) \to \mathsf{Pow}(|\mathfrak{S}_D|), \quad \Phi_A(S) \ := \ \|A[S]\|_D^{\boldsymbol{\sigma}}.$$

Based on this Φ_A, we now set (σ_m associated to this fixed point)

$$\|(\mu X)A[X]\|_D^{\boldsymbol{\sigma}} \ := \ I_{\Phi_A}^{<\sigma_m}$$

$$\|(\nu^1 X)A[X]\|_D^{\boldsymbol{\sigma}} \ := \ \|A[\top]\|_D^{\boldsymbol{\sigma}}$$

$$\|(\nu^{k+1} X)A[X]\|_D^{\boldsymbol{\sigma}} \ := \ \|A[(\nu^k X)A[X]]\|_D^{\boldsymbol{\sigma}}$$

$$\|(\nu X)A[X]\|_D^{\boldsymbol{\sigma}} \ := \ \bigcap_{i<\omega} \|(\nu^i X)A[X]\|_D^{\boldsymbol{\sigma}}$$

Remark 14 For any μ-formula D there exist suitable $\boldsymbol{\sigma}$ such that for all A: $\|A\|_{\mathfrak{S}_D} \subseteq \|A\|^{\boldsymbol{\sigma}}_D$.

Lemma 15 (Truth lemma) *Let D be some μ-formula. Then for all (suitable) sequences of ordinals $\boldsymbol{\sigma}$, all A from $\mathbb{SC}(D)$ and all D-saturated subsets Γ of $\mathbb{SC}(D)$ we have*

$$A \in \Gamma \quad \Rightarrow \quad \Gamma \notin \|A\|^{\boldsymbol{\sigma}}_D.$$

Theorem 16 (Truth theorem) *Let D be some μ-formula and A from $\mathbb{SC}(D)$. Then for all D-saturated subsets Γ of $\mathbb{SC}(D)$ we have*

$$A \in \Gamma \quad \Rightarrow \quad \Gamma \notin \|A\|_{\mathfrak{S}_D}.$$

Corollary 17 (Completeness) *For all μ-formulas A we have*

$$\mu \models A \quad \Rightarrow \quad \mathbf{K}_\omega(\mu) \vdash A.$$

Finitization of $\mathbf{K}_\omega(\mu)$

Let $\mathbf{K}_{<\omega}(\mu)$ be the variant of $\mathbf{K}_\omega(\mu)$ in which the infinitary rule

$$\frac{\ldots\ \Gamma,\ (\nu^n X)A[X]\ \ldots \quad \text{for all } 0 < n < \omega}{\Gamma,\ (\nu X)A[X]}$$

is replaced by its finite version

$$\frac{\ldots\ \Gamma,\ (\nu^n X)A[X]\ \ldots \quad \text{for all } 0 < n < \ell(\Gamma, (\nu X)A[X])}{\Gamma,\ (\nu X)A[X]}$$

Clearly: $\quad \mathbf{K}_\omega(\mu) \vdash A \quad \Rightarrow \quad \mathbf{K}_{<\omega}(\mu) \vdash A.$

Soundness of $\mathbf{K}_{<\omega}(\mu)$ – and hence also of $\mathbf{K}_{\omega}(\mu)$ – by:

- exploiting the *small model property* of the modal μ-calculus or
- adapting a deductive system originally developed by Dax, Hofmann and Lange for the linear time μ-calculus and extended by Studer to the full μ-calclus and shown to be complete.

The simplified systems S and S_ω

Language of $\mathbf{S}$: language of modal logic (without μ, ν) plus propositional constants P_A and Q_A for all X-positive modal formulas $A[X]$

Language of $\mathbf{S}_\omega$: language of modal logic (without μ, ν) plus propositional constants P_A, Q_A, Q_A^1, Q_A^2, ... for all X-positive modal formulas $A[X]$

Axioms and rules of S_ω

As for $\mathbf{K}_\omega(\mu)$, but with the rules for μ and ν replaced by:

$$\frac{\Gamma,\ A[P_A]}{\Gamma,\ P_A}$$

$$\frac{\Gamma,\ A[\top]}{\Gamma,\ Q_A^1} \qquad || \qquad \frac{\Gamma,\ A[Q_A^n]}{\Gamma,\ Q_A^{n+1}}$$

$$\frac{\ldots\ \Gamma,\ Q_A^n\ \ldots \quad \text{(for all } 0 < n < \omega)}{\Gamma,\ Q_A}$$

Hence $\mathbf{S}_\omega$ is the non-iterated subsystem of $\mathbf{K}_\omega(\mu)$.

Axioms and rules of $\mathbf{S}$

Axioms and rules for disjunction, conjunction and the modal operators as before; in addition

$$\frac{\Gamma,\ A[P_A]}{\Gamma,\ P_A} \qquad || \qquad \frac{\Gamma,\ A[Q_A]}{\Gamma,\ Q_A}$$

Definition 18

1. An $\mathbf{S}$-*preproof* of Γ is a possibly infinite tree whose root is labelled with Γ and which is locally correct with respect to the rules of $\mathbf{S}$.
2. Assume we are given a branch $\Gamma_0, \Gamma_1, \ldots$ within an $\mathbf{S}$-preproof. A *thread* within this branch is a sequence of formulas $A_0, A_1, \ldots$ such that $A_i \in \Gamma_i$ and A_{i+1} corresponds to A_i in the rule which leads from Γ_{i+1} to Γ_i.

Example 19 Consider an $\mathbf{S}$-preproof which contains a rule

$$\frac{\begin{array}{c}\vdots\\ \Gamma,\ B,\ A[Q_A]\end{array}}{\begin{array}{c}\Gamma,\ B,\ Q_A\\ \vdots\end{array}}$$

Then there are, for example, traces

$$\ldots, B, B, \ldots \qquad \text{and} \qquad \ldots, Q_A, A[Q_A], \ldots$$

Definition 20 An $\mathbf{S}$-preproof of Γ is an $\mathbf{S}$-*proof* of Γ if

- every finite branch ends in an axiom of $\mathbf{S}$ and
- every infinite infinite branch contains a thread with infinitely many occurrences of a formula Q_A.

We write $\mathbf{S} \vdash \Gamma$ if there exists an $\mathbf{S}$-proof of Γ.

Theorem 21 *For all Γ we have:*

1. $\mathbf{S} \vdash \Gamma \quad \Rightarrow \quad \mu \models \Gamma$.
2. $\mathbf{S}_\omega \vdash \Gamma \quad \Rightarrow \quad \mathbf{S}_{<\omega} \vdash \Gamma \quad \Rightarrow \quad \mathbf{S} \vdash \Gamma$.