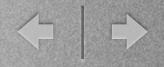


Satisfiability calculus: the semantic counterpart of a proof calculus in general logics

Carlos Gustavo Lopez Pombo University of Buenos Aires, Argentina

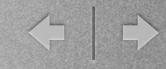
Joint work with:

Tomás Esteban Eduardo Maibaum -- McMaster University, Canada Nazareno Aguirre -- Universidad Nacional de Río Cuarto, Argentina Pablo Castro -- Universidad Nacional de Río Cuarto, Argentina Paula Chocrón -- Universidad de Buenos Aires, Argentina



Intro (Motivation)

- * As proving techniques have proof calculi as formal foundations (in the context of General Logics), semantics-based techniques also require formal foundations
- * Software analysis methodologies, understood as combinations of different verification techniques, also require formal foundations



Institutions and general logics

- ** ***84** Goguen and Burstall formalize the model theory of a logic in category theory by introducing the concept of **institution**
- *'89 Meseguer extends this model theoretical view of a logic to cope with the proof theoretical aspects introducing the concepts of proof calculus, proof sub-calculus and effective proof subcalculus

Institution

Definition . An institution is a structure of the form $(\text{Sign}, \text{Sen}, \text{Mod}, \{\models \Sigma \}_{\Sigma \in |\text{Sign}|})$ satisfying the following conditions:

- Sign is a category of signatures,
- Sen : Sign → Set is a functor. Let Σ ∈ |Sign|, then Sen(Σ) returns the set of Σ-sentences,
- Mod : Sign^{op} → Cat is a functor. Let Σ ∈ |Sign|, then Mod(Σ) returns the category of Σ-models,
- {|=^Σ}_{Σ∈|Sign|}, where |=^Σ⊆ |Mod(Σ)| × Sen(Σ), is a family of binary relations,

and for any signature morphism $\sigma : \Sigma \to \Sigma'$, Σ -sentence $\phi \in \text{Sen}(\Sigma)$ and Σ' -model $\mathcal{M}' \in |\text{Mod}(\Sigma)|$, the following \models -invariance condition holds:

 $\mathcal{M}' \models^{\Sigma'} \operatorname{Sen}(\sigma)(\phi) \quad iff \quad \operatorname{Mod}(\sigma^{\operatorname{op}})(\mathcal{M}') \models^{\Sigma} \phi$.

Entailment system

Definition An entailment system is a structure of the form $(\text{Sign}, \text{Sen}, \{\vdash^{\Sigma}\}_{\Sigma \in |\text{Sign}|})$ satisfying the following conditions:

- Sign is a category of signatures,
- Sen : Sign → Set is a functor. Let Σ ∈ |Sign|; then Sen(Σ) returns the set of Σ-sentences, and
- {⊢Σ}_{Σ∈|Sign|}, where ⊢Σ⊆ 2^{Sen(Σ)} × Sen(Σ), is a family of binary relations such that for any Σ, Σ' ∈ |Sign|, {φ} ∪ {φ_i}_{i∈T} ⊆ Sen(Σ), Γ, Γ' ⊆ Sen(Σ), the following conditions are satisfied:
 - 1. reflexivity: $\{\phi\} \vdash^{\Sigma} \phi$,
 - 2. monotonicity: if $\Gamma \vdash^{\Sigma} \phi$ and $\Gamma \subseteq \Gamma'$, then $\Gamma' \vdash^{\Sigma} \phi$,
 - transitivity: if Γ ⊢^Σ φ_i for all i ∈ I and {φ_i}_{i∈I} ⊢^Σ φ, then Γ ⊢^Σ φ, and
 - +-translation: if Γ ⊢^Σ φ, then for any morphism σ : Σ → Σ' in Sign, Sen(σ)(Γ) ⊢^{Σ'} Sen(σ)(φ).



Logic

Definition A logic is a structure of the form $(\text{Sign}, \text{Sen}, \text{Mod}, \{\vdash^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \{\models^{\Sigma}\}_{\Sigma \in |\text{Sign}|})$ satisfying the following conditions:

- $\langle Sign, Sen, \{\vdash^{\Sigma}\}_{\Sigma \in |Sign|} \rangle$ is an entailment system,
- $(\text{Sign}, \text{Sen}, \text{Mod}, \{\models^{\Sigma}\}_{\Sigma \in |\text{Sign}|})$ is an institution, and
- the following soundness condition is satisfied: for any Σ ∈ |Sign|, φ ∈ Sen(Σ), Γ ⊆ Sen(Σ): Γ ⊢^Σ φ implies Γ ⊨^Σ φ.

A logic is complete if, in addition, the following condition is also satisfied: for any $\Sigma \in |Sign|, \phi \in Sen(\Sigma), \Gamma \subseteq Sen(\Sigma): \Gamma \models^{\Sigma} \phi$ implies $\Gamma \vdash^{\Sigma} \phi$.

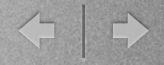
General Logics

A reasonable objection to the above definition of logic⁵ is that it abstracts away the structure of proofs, since we know only that a set Γ of sentences entails another sentence φ , but no information is given about the internal structure of such a $\Gamma \vdash \varphi$ entailment. This observation, while entirely correct, may be a virtue rather than a defect, because the entailment relation is precisely what remains <u>invariant</u> under many equivalent proof calculi that can be used for a logic.

General Logics

A reasonable objection to the above definition of logic⁵ is that it abstracts away the structure of proofs, since we know only that a set Γ of sentences entails another sentence φ , but no information is given about the internal structure of such a $\Gamma \vdash \varphi$ entailment. This observation, while entirely correct, may be a virtue rather than a defect, because the entailment relation is precisely what remains <u>invariant</u> under many equivalent proof calculi that can be used for a logic.

This observation is entirely correct and the result was the formalization of the notion of **proof** calculus, proof sub-calculus and effective proof sub-calculus as an "implementation" or operational view of the entailment relation.



Proof calculus

Definition . A proof calculus is a structure of the form (Sign, Sen, $\{\vdash^{\Sigma}\}_{\Sigma \in |Sign|}, \mathbf{P}, \mathbf{Pr}, \pi$) satisfying the following conditions:

- $(\text{Sign}, \text{Sen}, \{\vdash^{\Sigma}\}_{\Sigma \in |\text{Sign}|})$ is an entailment system,
- **P** : Th₀ → Struct_{PC} is a functor. Let $T \in |\mathsf{Th}_0|$, then $\mathbf{P}(T) \in |\mathsf{Struct}_{PC}|$ is the proof-theoretical structure of T,
- Pr : Struct_{PC} → Set is a functor. Let T ∈ |Th₀|, then Pr(P(T)) is the set of proofs of T; the composite functor Pr ∘ P : Th₀ → Set will be denoted by proofs. and
- $-\pi$: proofs \rightarrow Sen is a natural transformation such that for each $T = \langle \Sigma, \Gamma \rangle \in |\mathsf{Th}_0|$ the image of π_T : proofs $(T) \rightarrow \mathsf{Sen}(T)$ is the set Γ^{\bullet} . The map π_T is called the projection from proofs to theorems for the theory T.

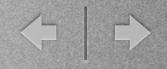
General Logics

A reasonable objection to the above definition of logic⁵ is that it abstracts away the structure of proofs, since we know only that a set Γ of sentences entails another sentence φ , but no information is given about the internal structure of such a $\Gamma \vdash \varphi$ entailment. This observation, while entirely correct, may be a virtue rather than a defect, because the entailment relation is precisely what remains <u>invariant</u> under many equivalent proof calculi that can be used for a logic.

This observation is entirely correct and the result was the formalization of the notion of **proof** calculus, proof sub-calculus and effective proof sub-calculus as an "implementation" or operational view of the entailment relation.

What about the formal aspects of the satisfiability relation?





General Logics

* Many techniques for software verification are based in the semantics of the specification language: tableau techniques, sat-based techniques and many model checking approaches

* In this case what remains invariant is the satisfaction relation

* Thus, Meseguer's argument apply in exactly the same way to satisfiability relations

- * A satisfiability calculus provides an operational views of the satisfiability relation of an institution
- * A satisfiability calculus can be understood as the semantic counterpart of a proof calculus
- * As such, a **satisfiability calculus**, concentrates on the "mechanics" behind the model theoretical aspects of a logic

Definition [Satisfiability Calculus] A satisfiability calculus is a structure of the form $(\text{Sign}, \text{Sen}, \text{Mod}, \{\models^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \mathbf{M}, \text{Mods}, \mu)$ satisfying the following conditions:

- $(\text{Sign}, \text{Sen}, \text{Mod}, \{\models^{\Sigma}\}_{\Sigma \in |\text{Sign}|})$ is an institution,
- M : Th₀ → Struct_{SC} is a functor. Let T ∈ |Th₀|, then M(T) ∈ |Struct_{SC}| is the model structure of T,
- Mods : Struct_{SC} → Cat is a functor. Let T ∈ |Th₀|, then Mods(M(T)) is the category of canonical models of T; the composite functor Mods ∘ M : Th₀ → Cat will be denoted by models, and
- μ: models^{op} → Mod is a natural transformation such that, for each T = ⟨Σ, Γ⟩ ∈ |Th₀|, the image of μ_T : models^{op}(T) → Mod(T) is the category of models Mod(T). The map μ_T is called the projection of the category of models of the theory T.

(Example: Tableau for First Order Predicate Logic)

- the nodes are labeled with sets of formulae (over Σ) and the root node is labeled with S,
- if u and v are two connected nodes in the tree (u being an ancestor of v), then the label of v is obtained from the label of u by applying one of the following rules:

$$\frac{X \cup \{A \land B\}}{X \cup \{A \land B, A, B\}} [\land] \frac{X \cup \{A \lor B\}}{X \cup \{A \lor B, A\}} [\lor]$$

$$\frac{X \cup \{\neg \neg A\}}{X \cup \{\neg \neg A, A\}} [\neg_1] \frac{X \cup \{A\}}{X \cup \{A, \neg \neg A\}} [\neg_2] \frac{X \cup \{A, \neg A\}}{\operatorname{Sen}(\Sigma)} [false]$$

$$\frac{X \cup \{\neg (A \land B)\}}{X \cup \{\neg (A \land B), \neg A \lor \neg B\}} [DM_1] \frac{X \cup \{\neg (A \lor B)\}}{X \cup \{\neg (A \lor B), \neg A \land \neg B\}} [DM_2]$$

$$\frac{X \cup \{(\forall x) P(x)\}}{X \cup \{(\forall x) P(x), P(t)\}} [\forall] \frac{X \cup \{(\exists x) P(x)\}}{X \cup \{(\exists x) P(x), P(c)\}} [\exists]$$

where, in the last rules, c is a new constant and t is a ground term.

(Example: Tableau for First Order Predicate Logic)

Definition : $\mathbf{M} : \mathrm{Th}_0 \to \mathrm{Struct}_{SC}$ is defined as $\mathbf{M}(\langle \Sigma, \Gamma \rangle) = \langle Str^{\Sigma,\Gamma}, \cup, \emptyset \rangle$ and $\mathbf{M}(\sigma : \langle \Sigma, \Gamma \rangle \to \langle \Sigma', \Gamma' \rangle) = \widehat{\sigma} : \langle Str^{\Sigma,\Gamma}, \cup, \emptyset \rangle \to \langle Str^{\Sigma',\Gamma'}, \cup, \emptyset \rangle$, the homomorphic extension of σ to the structures in $\langle Str^{\Sigma,\Gamma}, \cup, \emptyset \rangle$.

Definition 14. Mods : Struct_{SC} \rightarrow Cat is defined as:

$$\begin{split} \mathbf{Mods}(\langle Str^{\Sigma,\Gamma},\cup,\emptyset\rangle) &= \{\langle \Sigma,Cn(\widetilde{\Delta})\rangle \mid (\exists \alpha:\Delta \to \emptyset \in ||Str^{\Sigma,\Gamma}||) \\ (\widetilde{\Delta} \to \emptyset \in \alpha \land (\forall \alpha':\Delta' \to \Delta \in ||Str^{\Sigma,\Gamma}||)(\Delta' = \Delta))\} \end{split}$$

and for all $\sigma : \Sigma \to \Sigma' \in |Sign|$ (and $\hat{\sigma} : \langle Str^{\Sigma,\Gamma}, \cup, \emptyset \rangle \to \langle Str^{\Sigma',\Gamma'}, \cup, \emptyset \rangle \in ||Struct_{SC}||$), the following holds:

 $Mods(\widehat{\sigma})(\langle \Sigma, Cn(\widetilde{\Delta}) \rangle) = \langle \Sigma', Cn(Sen(\sigma)(Cn(\widetilde{\Delta}))) \rangle.$

Definition 15. Let $(\Sigma, \Gamma) \in |Th_0|$, then we define $\mu_{\Sigma} : \text{models}^{op}((\Sigma, \Gamma)) \rightarrow Mod_{FOL}((\Sigma, \Gamma))$ as $\mu_{\Sigma}((\Sigma, \Delta)) = Mod((\Sigma, \Delta))$.

Proposition .

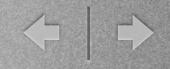
Let $\langle \text{Sign}, \text{Sen}, \{\vdash^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \mathbf{P}, \mathbf{Pr}, \mu \rangle$ be a proof calculus, $\langle \text{Sign}, \text{Sen}, \text{Mod}, \{\vdash^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \{\mid \perp^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \mathbf{M}, \text{Mods}, \pi \rangle$ be a satisfiability calculus, $T = \langle \Sigma, \Gamma \rangle \in |\text{Th}_0|$ and $\alpha \in \text{Sen}(\Sigma)$:

[Soundness] If there exists $\tau \in |\mathbf{proof}(T)|$ such that $\pi_T(\tau) = \alpha$, then for all $M \in |\mathbf{models^{op}}(T)|, \mu_T(M) \models_{\Sigma} \alpha$.

[Completeness] If for all $M \in |\text{models}^{op}(T)|$, $\mu_T(M) \models_{\Sigma} \alpha$, then there exists $\tau \in |\text{proof}(T)|$ such that $\pi_T(\tau) = \alpha$.

Corollary . Let $\langle Sign, Sen, \{\vdash^{\Sigma}\}_{\Sigma \in |Sign|}, \mathbf{P}, \mathbf{Pr}, \mu \rangle$ be a proof calculus, $\langle Sign, Sen, Mod, \{\models^{\Sigma}\}_{\Sigma \in |Sign|}, \mathbf{M}, Mods, \pi \rangle$ be a satisfiability calculus, $T = \langle \Sigma, \Gamma \rangle \in |Th_0|$ and $\alpha \in Sen(\Sigma)$, then

If there exists $M \in |\mathbf{models}^{op}(T)|$ such that $\mu_T(M) \not\models_{\Sigma} \alpha$, then there is no $\tau \in |\mathbf{proof}(T)|$ such that $\pi_T(\tau) = \alpha$.



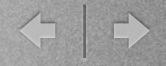
- * A satisfiability sub-calculus is a restriction of a satisfiability calculus
- * Provides the mechanisms for determining a sublanguage (i.e. sub-category of signatures, subset of formulae and sub-category of theories) on which a particular semantics-based method can be applied

Satisfiability sub-calculus

Definition . [Satisfiability subcalculus] A satisfiability subcalculus is a structure of the form $(\text{Sign}, \text{Sen}, \text{Mod}, \text{Sign}_0, ax, \{\models^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \mathbf{M}, \text{Mods}, \mu)$ satisfying the following conditions:

- (Sign, Sen, Mod, {|=^Σ}_{Σ∈|Sign|}) is an institution,
- Sign₀ is a subcategory of Sign called the subcategory of admissible signatures; the restriction of the functor Sen to Sign₀ will be denoted by Sen₀,
- ax : Sign₀ → Set is a subfunctor of the functor obtained by composing Sen₀ with the powerset functor, i.e., there is a natural inclusion ax(Σ) ⊆ P(Sen(Σ)) for each Σ ∈ Sign₀. Each Γ ∈ ax(Σ) is called a set of admissible axioms specified by Q. This defines a subcategory Th_{ax} of Th₀ whose objects are theories T = (Σ, Γ) with Σ ∈ Sign₀ and Γ ∈ ax(Σ), and whose morphisms are axiom-preserving theory morphisms H such that H is in Sign₀.
- M : Th_{ax} → Struct_{SC} is a functor. Let T ∈ |Th_{ax}|, then M(T) ∈ |Struct_{SC}| is the model structure of T,
- Mods : Struct_{SC} → Cat is a functor. Let T ∈ |Th_{ax}|, then Mods(M(T)) is the set of canonical models of T; the composite functor Mods ∘ M : Th_{ax} → Cat will be denoted by models, and
- μ: models^{op} → Mod is a natural transformation such that, for each T = ⟨Σ, Γ⟩ ∈ |Th_{ax}|, the image of μ_T : models^{op}(T) → Mod(T) is the category of models Mod(T). The map μ_T is called the projection of the category of models of the theory T.

Saturday, March 16, 13



Effective Satisfiability sub-calculus

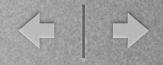
- * A satisfiability sub-calculus is a restriction of a satisfiability calculus
- * Provides the mechanisms for determining a sublanguage (i.e. sub-category of signatures, subset of formulae and sub-category of theories) on which a particular semantics-based method can be applied
- * The sub-language determined must be organized in Spaces

Effective Satisfiability sub-calculus

Definition I. [Effective satisfiability sub-calculus] An effective satisfiability subcalculus is a structure of the form $\langle \text{Sign}, \text{Sen}, \text{Mod}, \text{Sign}_0, \text{Sen}_0, ax, \{\models^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \mathbf{M}, \text{Mods}, \mu \rangle$ satisfying the following conditions:

- $\langle Sign, Sen, Mod, \{\models^{\Sigma}\}_{\Sigma \in |Sign|} \rangle$ is an institution,
- Sign₀ is a subcategory of Sign called the subcategory of admissible signatures; the restriction of the functor Sen to Sign₀ will be denoted by Sen₀,
- Sen₀ : Space \rightarrow Space is a functor such that $\mathcal{U} \circ Sen_0 = Sen \circ J$
- ax : Sign₀ → Space is a sub-functor of the functor obtained by composing Sen₀ with the functor P_{fin} : Space → Space, that sends each space to the space of its finite subsets. This defines a subcategory Th_{ax} of Th₀ whose objects are theories T = (Σ, Γ) with Σ ∈ Sign₀ and Γ ∈ ax(Σ), and whose morphisms are axiom-preserving theory morphisms H such that H is in Sign₀.
- M : Th_{ax} → Struct_{SC} is a functor. Let T ∈ |Th_{ax}|, then M(T) ∈ |Struct_{SC}| is the model structure of T,
- Mods : Struct_{SC} → Space is a functor. Let T ∈ |Th_{ax}|, then Mods(M(T)) is the set of canonical models of T; the composite functor Mods∘M : Th_{ax} → Space will be denoted by models, and
- μ: models^{op} → Mod is a natural transformation such that, for each T = ⟨Σ, Γ⟩ ∈ |Th_{ax}|, the image of μ_T : models^{op}(T) → Mod(T) is the category of models Mod(T). The map μ_T is called the projection of the category of models of the theory T.
- Denoting also by ax, Pr, P and μ the results of composing with U each of the above, the structure is a satisfiability subcalculus.



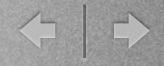


* Software verification techniques are usually divided into two categories, **lightweight** (related to model construction or counterexample searching and usually unassisted) and **heavyweight** (related to theorem proving, usually assisted)

* Software analysis has departed long ago from having to choose one among all the tools available, specially, one of these two categories of tools

* Thus, the key is how to relate them through a methodology, with formal foundations, for software analysis





- * A well known method for software analysis based on the time consumption and expertise required for the technique involved is:
 - * a **lightweight** technique for model searching is used in order to construct a counterexample of the property:
 - * if it exists then the specification and the property are refined,
 - * if not we gained confidence in the specification and the property and then,
 - * a heavyweight technique is applied in order to prove the property

Institution representation

Definition . [Institution representation] Let $(\text{Sign}, \text{Sen}, \text{Mod}, \{\models_{\Sigma}\}_{\Sigma \in |\text{Sign}|})$ and $(\text{Sign}', \text{Sen}', \text{Mod}', \{\models'_{\Sigma}\}_{\Sigma \in |\text{Sign}'|})$ be institutions I and I', respectively. Then, $\langle \gamma^{Sign}, \gamma^{Sen}, \gamma^{Mod} \rangle : I \to I'$ is a representation map of institutions if and only if:

 $\begin{array}{l} - \gamma^{Sign} : \operatorname{Sign} \to \operatorname{Sign}' \ is \ a \ functor, \\ - \gamma^{Sen} : \operatorname{Sen} \to \gamma^{Sign} \circ \operatorname{Sen}', \ is \ a \ natural \ transformation, \\ - \gamma^{Mod} : (\gamma^{Sign})^{\operatorname{op}} \circ \operatorname{Mod}' \to \operatorname{Mod}, \ is \ a \ natural \ transformation, \end{array}$

such that for any $\Sigma \in |\text{Sign}|$, the function $\gamma_{\Sigma}^{Sen} : \text{Sen}(\Sigma) \to \text{Sen}'(\gamma^{Sign}(\Sigma))$ and the functor $\gamma_{\Sigma}^{Mod} : \text{Mod}'(\gamma^{Sign}(\Sigma)) \to \text{Mod}(\Sigma)$ preserves the following satisfaction condition: for any $\alpha \in \text{Sen}(\Sigma)$ and $\mathcal{M}' \in |\text{Mod}(\gamma^{Sign}(\Sigma))|$,

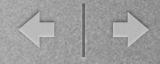
 $\mathcal{M}' \models_{\gamma^{Sign}(\varSigma)} \gamma_{\varSigma}^{Sen}(\alpha) \quad iff \quad \gamma_{\varSigma}^{Mod}(\mathcal{M}') \models_{\varSigma} \alpha \;.$

Definition . [Map of Institution] Let $\langle \text{Sign}, \text{Sen}, \text{Mod}, \{\models_{\Sigma}\}_{\Sigma \in |\text{Sign}|} \rangle$ and $\langle \text{Sign}', \text{Sen}', \text{Mod}', \{\models'_{\Sigma}\}_{\Sigma \in |\text{Sign}'|} \rangle$ be institutions I and I', respectively, and $\gamma = \langle \gamma^{Sign}, \gamma^{Sen}, \gamma^{Mod} \rangle : I \to I'$ an institution representation. Then, if a functor $\gamma^{Th} : \text{Th}_0 \to \text{Th}'_0$ is γ^{Sign} -sensible (see [2, pp. 21]), then $\langle \gamma^{Th}, \gamma^{Sen}, \gamma^{Mod} \rangle : I \to I'$ is said to be a map of institutions.



Theorem . Let $\langle \text{Sign}, \text{Sen}, \{\vdash^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \mathbf{P}, \mathbf{Pr}, \mu \rangle$ be a proof calculus for the logic $\langle \text{Sign}, \text{Sen}, \text{Mod}, \{\vdash^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \{\models^{\Sigma}\}_{\Sigma \in |\text{Sign}|} \rangle$, $T = \langle \Sigma, \Gamma \rangle \in |\text{Th}_0|$ and $\alpha \in \text{Sen}(\Sigma)$. Let $\langle \text{Sign}', \text{Sen}', \text{Mod}', \text{Sign}'_0, \text{Sen}'_0, ax', \{\models'^{\Sigma}\}_{\Sigma \in |\text{Sign}'|}, \mathbf{M}', \text{Mods}', \mu' \rangle$ be an effective satisfiability sub-calculus, $\rho^{Th} : \text{Th}_0 \to \text{Th}'_{ax}$ a functor and $\langle \rho^{Th}, \rho^{Sen}, \rho^{Mod} \rangle$ a map of institutions from $\langle \text{Sign}, \text{Sen}, \text{Mod}, \{\models^{\Sigma}\}_{\Sigma \in |\text{Sign}|} \rangle$ to $\langle \text{Sign}', \text{Sen}', \text{Mod}', \{\models'^{\Sigma}\}_{\Sigma \in |\text{Sign}|} \rangle$, then

If there exists $M \in |\mathbf{models}^{\mathsf{op}}(T)|$, and $\mathcal{M} \in |\mu_{\rho^{Th}(T)}(M)|$ such that $\mathcal{M} \not\models_{\mathbf{Sign} \circ \rho^{Th}(T)}$ $\rho^{Th}(\alpha)$, then there is no $\tau \in |\mathbf{proof}(T)|$ such that $\pi_T(\tau) = \alpha$.



Definition [Negation] An institution $(\text{Sign}, \text{Sen}, \text{Mod}, \{\models_{\Sigma}\}_{\Sigma \in |\text{Sign}|})$ is said to have negation if for all $\Sigma \in |\text{Sign}|, \varphi \in \text{Sen}(\Sigma), \mathcal{M} \in |\text{Mod}(\Sigma)|$ there exists a formula $\psi \in \text{Sen}(\Sigma)$ (usually denoted as $\neg \varphi$) such that $\mathcal{M} \models_{\Sigma} \psi$ if and only if it is not true that $\mathcal{M} \models_{\Sigma} \varphi$.

Corollary Let $\langle \text{Sign}, \text{Sen}, \{\vdash^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \mathbf{P}, \mathbf{Pr}, \mu \rangle$ be a proof calculus for the logic $\langle \text{Sign}, \text{Sen}, \text{Mod}, \{\vdash^{\Sigma}\}_{\Sigma \in |\text{Sign}|}, \{\mid \models^{\Sigma}\}_{\Sigma \in |\text{Sign}|} \rangle, T = \langle \Sigma, \Gamma \rangle \in |\text{Th}_0| \text{ and } \alpha \in \text{Sen}(\Sigma)$. Let $\langle \text{Sign}', \text{Sen}', \text{Mod}', \text{Sign}'_0, \text{Sen}'_0, ax', \{\mid ='^{\Sigma}\}_{\Sigma \in |\text{Sign}'|}, \mathbf{M}', \text{Mods}', \mu' \rangle$ be an effective satisfiability sub-calculus, $\rho^{Th} : \text{Th}_0 \to \text{Th}'_{ax}$ a functor and $\langle \rho^{Th}, \rho^{Sen}, \rho^{Mod} \rangle$ a map of institutions from $\langle \text{Sign}, \text{Sen}, \text{Mod}, \{\mid =^{\Sigma}\}_{\Sigma \in |\text{Sign}|} \rangle$ to $\langle \text{Sign}', \text{Sen}', \text{Mod}', \{\mid ='^{\Sigma}\}_{\Sigma \in |\text{Sign}|} \rangle$, then

If there exists $M \in |\mathbf{models}^{op}(T \cup \neg \alpha)|$, then there is no $\tau \in |\mathbf{proof}(T)|$ such that $\pi_T(\tau) = \alpha$.



(Example: First Order Predicate Logic - Propositional Logic)

Definition 14. γ^{Sign} : Sign_{FOL} $\rightarrow 2^{\mathcal{V}}$ is defined as the functor such that: for all $\Sigma \in |\text{Sign}_{FOL}|, \gamma^{Sign}(\Sigma) = \{v_p | p \text{ is a ground atomic formula in Sen}_{FOL}(\Sigma)\}.$

Definition 15. Let $n \in \mathbb{N}$ and $\Sigma = \langle \{P_j\}_{j \in \mathcal{J}}, \{f_k\}_{k \in \mathcal{K}} \rangle \in |\mathsf{Sign}_{FOL}|$. Then $\gamma_{\Sigma}^{Sen} : \mathbf{Sen}_{FOL}(\Sigma) \to \gamma^{Sign} \circ \mathbf{Sen}_{PL}(\Sigma)$ is defined as:

$$\begin{split} \gamma_{\Sigma}^{Sen}(\alpha) &= Tr_{PL}^{n}(Tr^{n}(\alpha)), \ where: \\ &- \ Tr^{n}((\exists x)A) = \bigvee_{i=1}^{n} Tr^{n}(A|_{x}^{c_{i}}), \\ &- \ Tr^{n}(A \lor B) = Tr^{n}(A) \lor Tr^{n}(B), \\ &- \ Tr^{n}(\neg A) = \neg Tr^{n}(A), \ and \\ &- \ Tr^{n}(P(t_{1}, \ldots, t_{k})) = (fix(P(t_{1}, \ldots, t_{k}))), \ for \ all \ P \in \{P_{j}\}_{j \in \mathcal{J}} \\ &, \ where \ fix(A) = \mu_{X} \begin{bmatrix} \bigvee_{c \in \{c_{1}, \ldots, c_{n}\}} X|_{f(t_{1}, \ldots, t_{k})}^{c} \land c = f(t_{1}, \ldots, t_{k}) \\ &; \ for \ all \ f(t_{1}, \ldots, t_{k}) \in X \ such \ that \\ &t_{1}, \ldots, t_{k} \in \{c_{1}, \ldots, c_{n}\}. \end{bmatrix} (A). \\ &- \ Tr_{PL}^{n}(P(t_{1}, \ldots, t_{k})) = v \ _{e}P(t_{1}, \ldots, t_{k})^{",} \\ &- \ Tr_{PL}^{n}(A \lor B) = Tr_{PL}^{n}(A) \lor Tr_{PL}^{n}(B), \ and \\ &- \ Tr_{PL}^{n}(\neg A) = \neg Tr_{PL}^{n}(A). \end{split}$$

Saturday, March 16, 13



(Example: First Order Predicate Logic - Propositional Logic)

Definition . Let $n \in \mathbb{N}$, $\gamma^{Sign} : \text{Sign}_{FOL} \to 2^{\mathcal{V}}$ be the functor of Def. 14 and $\gamma^{Sen} : \text{Sen}_{FOL} \to \gamma^{Sign} \circ \text{Sen}_{PL}$ be the natural family of functions of Def. 15. Then, we define $\gamma^{\text{Th}_0} : \text{Th}_{FOL0} \to \text{Th}_{PL0}$ as:

 $\gamma^{\mathsf{Th}_0}(\langle \Sigma, \Gamma \rangle) = \langle \gamma^{Sign}(\Sigma), \{\gamma_{\Sigma}^{Sen}(\alpha) | \alpha \in \Gamma \} \rangle .$

Remark . The functor $\gamma^{\mathsf{Th}_0} : \mathsf{Th}_{FOL0} \to \mathsf{Th}_{PL0}$ is γ^{Sign} -sensible.

Definition Let $n \in \mathbb{N}$ and $\Sigma = \langle \{P_j\}_{j \in \mathcal{J}}, \{f_k\}_{k \in \mathcal{K}} \rangle \in |\mathsf{Sign}_{FOL}|$. Then we define $\gamma_{\Sigma}^{Mod} : \gamma^{Sign} \circ \mathsf{Mod}_{PL}(\Sigma) \to \mathsf{Mod}_{FOL}(\Sigma)$ as follows: for all val : $\gamma^{Sign}(\Sigma) \to \{0,1\} \in |\mathsf{Mod}_{PL}(\gamma^{Sign}(\Sigma))|, \gamma_{\Sigma}^{Mod}(val) = \langle S, \mathcal{C}, \mathcal{P}, \mathcal{F} \rangle$ such that:

$$\begin{aligned} &- \mathcal{S} = \{c_1, \dots, c_n\}, \\ &- \mathcal{P} = \{\overline{P} | P \in \{P_j\}_{j \in \mathcal{J}}\}, \text{ where } \\ &\overline{P} = \{\langle c_1, \dots, c_k \rangle | c_1, \dots, c_k \in \mathcal{S}, \text{ val } (v_{P(c_1, \dots, c_k)}) = 1\}, \text{ and } \\ &- \mathcal{F} = \{\overline{f} | f \in \{f_k\}_{k \in \mathcal{K}}\}, \text{ where } \\ &\overline{f} = \{\langle c_1, \dots, c_k \rangle \mapsto c | c_1, \dots, c_k, c \in \mathcal{S}, \text{ val } (v_{c=f(c_1, \dots, c_k)}) = 1\}. \end{aligned}$$



*We provided formal foundations for semantics-based methods for software verification like tableau techniques, sat-based methods and many model-checkers for logical languages

*We provided formal foundations for a well-known methodology for software analysis based on the concept of proof calculus and effective satisfiability sub-calculus

Outro (Further work)

- *Explore conditions under which *map of institutions* reducing the expressive power still allow modular analysis (requires not to loose morphisms)
- *Study relations between structures representing proofs and canonical models in proof calculi and satisfiability calculi, respectively.

:? & :!

dedicated to the memory of Comandante Hugo Chavez Frías ¡Hasta la victoria siempre, patria o muerte!

Saturday, March 16, 13