Propositional Logics of Overwhelming Truth

Thibaut Antoine, David Baelde

Univ. Rennes

February 12, 2025

The Squirrel proof assistant

Squirrel is a proof assistant for verifying cryptographic protocols in the computational model.
It is based on the CCSA approach.

Gergei Bana & Hubert Comon. *A Computationally Complete Symbolic Attacker for Equivalence Properties.* CCS 2014.

Goal

- Squirrel's logical foundations have grown organically.
- Several completeness issues have occurred in the past.
- Can we get solid logical foundations, at least for a fragment of the logic?
  Yes ! for a modal fragment.

The CCSA logic

In cryptography, security is not perfect but asymptotic.

Local terms and formulas

- Example: $\forall \tau : \text{timestamp}, \text{happens}(\tau) \Rightarrow \text{input}@\tau \neq \text{n}_{\text{secret}}$
- Terms represent names, timestamps...
  Interpreted as η-indexed families of random variables
- Local formulas are boolean terms
  φ is valid when in all models, it is true with overwhelming probability

Global formulas

- First-order formulas over atoms of the form $[\varphi]$ (ow. truth) or $t \sim u$ (indistinguishability)
- Example: $\forall \tau, \text{frame}_{\mathcal{P}}@\tau \sim \text{frame}_{\mathcal{Q}}@\tau \Rightarrow [\varphi]$

In this work: we focus on the $[\,\cdot\,]$ predicate.

Focus on the overwhelming truth predicate

Definition

φ is true in $\mathcal{M}$ with overwhelming probability when $\eta \mapsto \Pr(\llbracket\varphi\rrbracket_\eta^{\mathcal{M}} = 0)$ is asymptotically lower than the inverse of any positive polynomial, i.e. $\eta \mapsto \Pr(\llbracket\varphi\rrbracket_\eta^{\mathcal{M}} = 1)$ is overwhelming.

Example

Let a, b be interpreted as random sequences of length η. Then:

- $\varphi :=$ "$a \neq b$" is ow. true : $\forall\eta, \Pr(\varphi_\eta = 0) = 1/2^\eta$
- $\psi :=$ "a starts with 0" is not ow. true : $\forall\eta, \Pr(\psi_\eta = 0) = \frac{1}{2}$

Focus on the overwhelming truth predicate

Definition

φ is true in $\mathcal{M}$ with overwhelming probability when $\eta \mapsto \Pr(\llbracket\varphi\rrbracket_\eta^\mathcal{M} = 0)$ is asymptotically lower than the inverse of any positive polynomial, i.e. $\eta \mapsto \Pr(\llbracket\varphi\rrbracket_\eta^\mathcal{M} = 1)$ is overwhelming.

Example (some validities)

- $[\varphi \wedge \psi] \Leftrightarrow [\varphi] \wedge [\psi]$
- $[\varphi \vee \psi] \Leftarrow [\varphi] \vee [\psi]$
- $[\varphi \Rightarrow \psi] \Rightarrow ([\varphi] \Rightarrow [\psi])$

Focus on the overwhelming truth predicate

Definition

φ is true in $\mathcal{M}$ with overwhelming probability when $\eta \mapsto \Pr(\llbracket\varphi\rrbracket_\eta^\mathcal{M} = 0)$ is asymptotically lower than the inverse of any positive polynomial, i.e. $\eta \mapsto \Pr(\llbracket\varphi\rrbracket_\eta^\mathcal{M} = 1)$ is overwhelming.

Example (some validities)

- $[\varphi \wedge \psi] \Leftrightarrow [\varphi] \wedge [\psi]$
- $[\varphi \vee \psi] \Leftarrow [\varphi] \vee [\psi]$ ... but $[\varphi \vee \psi] \not\Rightarrow [\varphi] \vee [\psi]$
- $[\varphi \Rightarrow \psi] \Rightarrow ([\varphi] \Rightarrow [\psi])$

Focus on the overwhelming truth predicate

Definition

φ is true in $\mathcal{M}$ with overwhelming probability when $\eta \mapsto \text{Pr}(\llbracket\varphi\rrbracket_\eta^\mathcal{M} = 0)$ is asymptotically lower than the inverse of any positive polynomial, i.e. $\eta \mapsto \text{Pr}(\llbracket\varphi\rrbracket_\eta^\mathcal{M} = 1)$ is overwhelming.

Deterministic inference

Case analysis is invalid in general... But if $[\varphi] \vee [\neg\varphi]$ holds, $[\varphi \vee \psi] \Rightarrow [\varphi] \vee [\psi]$ holds too. In that case, we call φ deterministic.

Creates a new type of inference (needed in Squirrel).

Focus on the overwhelming truth predicate

Definition

φ is true in $\mathcal{M}$ with overwhelming probability when $\eta \mapsto \Pr(\llbracket\varphi\rrbracket_\eta^{\mathcal{M}} = 0)$ is asymptotically lower than the inverse of any positive polynomial, i.e. $\eta \mapsto \Pr(\llbracket\varphi\rrbracket_\eta^{\mathcal{M}} = 1)$ is overwhelming.

Deterministic inference

Case analysis is invalid in general... But if $[\varphi] \vee [\neg\varphi]$ holds, $[\varphi \vee \psi] \Rightarrow [\varphi] \vee [\psi]$ holds too. In that case, we call φ deterministic.
Creates a new type of inference (needed in Squirrel).

What we learned:

- $[\,\cdot\,]$ looks like a modality
- We want the proof system to handle determinism

Our contributions

- Definition of a modal logic for the overwhelming truth predicate
- Characterization of this logic (equivalence with S5)
- Adaptation of a hypersequent calculus for S5
- Development of a proof system for a propositional fragment of CCSA

Modal logic of overwhelming truth

Syntax

$\varphi ::= \bot \mid p \mid \varphi \Rightarrow \varphi \mid \Box\varphi$

Models

Cryptographic structures $\mathcal{S}$, given by :

- for each $\eta \in \mathbb{N}$, a set X_η
- for each $p \in \mathcal{P}, \eta \in \mathbb{N}$, a random variable $\hat{p}_\eta : X_\eta \to \{0, 1\}$

Satisfaction

- $\mathcal{S}, \eta, \rho \models p$ iff $\hat{p}_\eta(\rho) = 1$
- $\mathcal{S}, \eta, \rho \models \varphi \Rightarrow \psi$ iff $\mathcal{S}, \eta, \rho \models \varphi$ implies $\mathcal{S}, \eta, \rho \models \psi$
- $\mathcal{S}, \eta, \rho \models \Box\varphi$ iff φ is ow. true

Characterizing the logic

The following formulas are valid:

$\Box(\varphi \Rightarrow \psi) \Rightarrow (\Box\varphi \Rightarrow \Box\psi)$

$\Box\varphi \Rightarrow \varphi$

$\Box\Box\varphi \Leftrightarrow \Box\varphi$, $\Box\neg\Box\varphi \Leftrightarrow \neg\Box\varphi$

Characterizing the logic

The following formulas are valid:

$$\left.\begin{array}{l} \Box(\varphi \Rightarrow \psi) \Rightarrow (\Box\varphi \Rightarrow \Box\psi) \\ \Box\varphi \Rightarrow \varphi \\ \Box\Box\varphi \Leftrightarrow \Box\varphi,\ \Box\neg\Box\varphi \Leftrightarrow \neg\Box\varphi \end{array}\right] \text{S5 axioms!}$$

Characterizing the logic

The following formulas are valid:

$$\left.\begin{array}{l}\Box(\varphi \Rightarrow \psi) \Rightarrow (\Box\varphi \Rightarrow \Box\psi) \\ \Box\varphi \Rightarrow \varphi \\ \Box\Box\varphi \Leftrightarrow \Box\varphi,\ \Box\neg\Box\varphi \Leftrightarrow \neg\Box\varphi\end{array}\right] \text{S5 axioms!}$$

Theorem

A formula is valid in our sense iff it is a theorem of S5

Proof.

($\Leftarrow$) By definition of S5

($\Rightarrow$) Semantic proof using Kripke frames : from a formula not valid in S5 build a finite clique Kripke counter-model, and transform it into a cryptographic structure. $\Box$

A proof system for S5

S5 enjoys a very nice hypersequent calculus [Poggiolesi 2008].

$$\Gamma_1 \vdash \Delta_1 \mid \cdots \mid \Gamma_n \vdash \Delta_n \quad \text{reads as} \quad \bigvee_i \Box(\wedge\Gamma_i \Rightarrow \vee\Delta_i)$$

Some rules :

$$\frac{}{\cdots \mid \Gamma, \varphi \vdash \varphi, \Delta} \qquad \frac{\cdots \mid \Gamma \vdash \Delta, \varphi \quad \cdots \mid \Gamma, \psi \vdash \Delta}{\cdots \mid \Gamma, \varphi \Rightarrow \psi \vdash \Delta}$$

$$\frac{\cdots \mid \Gamma \vdash \Delta \mid \cdot \vdash \varphi}{\cdots \mid \Gamma \vdash \Delta, \Box\varphi}$$

A proof system for S5

S5 enjoys a very nice hypersequent calculus [Poggiolesi 2008].

$$\Gamma_1 \vdash \Delta_1 \mid \cdots \mid \Gamma_n \vdash \Delta_n \quad \text{reads as} \quad \bigvee_i \Box(\wedge\Gamma_i \Rightarrow \vee\Delta_i)$$

Some rules (slight modification in the paper for termination of proof search):

$$\frac{}{\cdots \mid \Gamma, \varphi \vdash \varphi, \Delta} \qquad \frac{\cdots \mid \Gamma, \varphi \Rightarrow \psi \vdash \Delta, \varphi \quad \cdots \mid \Gamma, \varphi \Rightarrow \psi, \psi \vdash \Delta}{\cdots \mid \Gamma, \varphi \Rightarrow \psi \vdash \Delta}$$

$$\frac{\cdots \mid \Gamma \vdash \Delta, \Box\varphi \mid \cdot \vdash \varphi}{\cdots \mid \Gamma \vdash \Delta, \Box\varphi}$$

A proof system for S5

S5 enjoys a very nice hypersequent calculus [Poggiolesi 2008].

$$\Gamma_1 \vdash \Delta_1 \mid \cdots \mid \Gamma_n \vdash \Delta_n \quad \text{reads as} \quad \bigvee_i \Box(\wedge\Gamma_i \Rightarrow \vee\Delta_i)$$

Some rules (slight modification in the paper for termination of proof search):

$$\frac{}{\cdots \mid \Gamma, \varphi \vdash \varphi, \Delta} \qquad \frac{\cdots \mid \Gamma, \varphi \Rightarrow \psi \vdash \Delta, \varphi \quad \cdots \mid \Gamma, \varphi \Rightarrow \psi, \psi \vdash \Delta}{\cdots \mid \Gamma, \varphi \Rightarrow \psi \vdash \Delta}$$

$$\frac{\cdots \mid \Gamma \vdash \Delta, \Box\varphi \mid \cdot \vdash \varphi}{\cdots \mid \Gamma \vdash \Delta, \Box\varphi}$$

A new axiom gives a complete calculus (via proof search) for S5 with deterministic formulas:

$$\frac{\varphi \text{ deterministic}}{\cdots \mid \Gamma, \varphi \vdash \Delta \mid \Gamma \vdash \Delta, \varphi}$$

What about CCSA?

No need for all this complexity: we only care about formulas with one level of modality.

Propositional fragment of CCSA:

$$\begin{array}{rl} \text{Local formulas} & \varphi ::= \bot \mid p \mid \varphi \Rightarrow \varphi \\ \text{Global formulas} & \Phi ::= \bot \mid [\varphi] \mid \Phi \Rightarrow \Phi \end{array}$$

Two kinds of formulas means two kinds of sequents:

$$\begin{array}{rll} \text{Global sequents} & \overbrace{\Phi_1, \ldots, \Phi_n}^{\Theta} \vdash \overbrace{\Psi_1, \ldots, \Psi_m}^{\Pi} & \text{reads as } \wedge\Theta \Rightarrow \vee\Pi \\ \text{Local sequents} & \Theta\,;\,\Gamma \vdash \Delta & \text{reads as } \wedge\Theta \Rightarrow [\wedge\Gamma \Rightarrow \vee\Delta] \end{array}$$

A sequent calculus for propositional CCSA

Highly inspired by Squirrel's natural deduction-style calculus.

Global rules :

$$\frac{\Theta \vdash \Phi, \Pi \quad G, \Psi \vdash \Pi}{\Theta, \Phi \Rightarrow \Psi \vdash \Pi}$$

Local rules :

$$\frac{\Theta\,;\,\Gamma \vdash \varphi, \Delta \quad \Theta\,;\,\Gamma, \psi \vdash \Delta}{\Theta\,;\,\Gamma, \varphi \Rightarrow \psi \vdash \Delta}$$

Mixed rules :

$$\frac{\Theta\,;\,\cdot \vdash \varphi}{\Theta \vdash [\varphi], \Pi}$$

$$\frac{\Theta\,;\,\Gamma, \varphi \vdash \Delta}{\Theta, [\varphi]\,;\,\Gamma \vdash \Delta}$$

A sequent calculus for propositional CCSA

Highly inspired by Squirrel's natural deduction-style calculus.

Global rules :

$$\frac{\Theta \vdash \Phi, \Pi \quad G, \Psi \vdash \Pi}{\Theta, \Phi \Rightarrow \Psi \vdash \Pi}$$

Local rules :

$$\frac{\Theta\,;\, \Gamma \vdash \varphi, \Delta \quad \Theta\,;\, \Gamma, \psi \vdash \Delta}{\Theta\,;\, \Gamma, \varphi \Rightarrow \psi \vdash \Delta}$$

Mixed rules :

$$\frac{\Theta\,;\, \cdot \vdash \varphi}{\Theta \vdash [\varphi], \Pi}$$

$$\frac{\Theta\,;\, \Gamma, \varphi \vdash \Delta}{\Theta, [\varphi]\,;\, \Gamma \vdash \Delta}$$

Soundness: ✓

A sequent calculus for propositional CCSA

Highly inspired by Squirrel's natural deduction-style calculus.

Global rules :

$$\frac{\Theta \vdash \Phi, \Pi \quad G, \Psi \vdash \Pi}{\Theta, \Phi \Rightarrow \Psi \vdash \Pi}$$

Local rules :

$$\frac{\Theta\,;\,\Gamma \vdash \varphi, \Delta \quad \Theta\,;\,\Gamma, \psi \vdash \Delta}{\Theta\,;\,\Gamma, \varphi \Rightarrow \psi \vdash \Delta}$$

Mixed rules :

$$\frac{\Theta\,;\,\cdot \vdash \varphi}{\Theta \vdash [\varphi], \Pi} \qquad \frac{\Theta\,;\,\Gamma, \varphi \vdash \Delta}{\Theta, [\varphi]\,;\,\Gamma \vdash \Delta}$$

Soundness: ✓

Completeness: Mixed rules are not invertible!!

Proof of completeness

Assume $\bigwedge \Theta \Rightarrow \bigvee \Pi$ is valid.

Step 1. Apply all possible global rules.

$$\dfrac{[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m]}{\begin{array}{c}\vdots\\ \Theta \vdash \Pi\end{array}}$$

Proof of completeness

Assume $\bigwedge \Theta \Rightarrow \bigvee \Pi$ is valid.

Step 1. Apply all possible global rules.

$$\begin{array}{c}[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m] \\ \vdots \\ \Theta \vdash \Pi\end{array}$$

Lemma (Key lemma)

If $[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m]$ is valid,
then there is a k such that $\varphi_1, \ldots, \varphi_n \vdash \psi_k$ is classically valid.

Proof of completeness

Assume $\bigwedge \Theta \Rightarrow \bigvee \Pi$ is valid.

Step 2. Choose a ψ_k to prove.

$$\dfrac{\begin{array}{c}\vdots\\ [\varphi_1], \ldots, [\varphi_n]; \cdot \vdash \psi_k\end{array}}{\begin{array}{c}[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m]\\ \vdots\\ \Theta \vdash \Pi\end{array}}$$

Lemma (Key lemma)

If $[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m]$ is valid, then there is a k such that $\varphi_1, \ldots, \varphi_n \vdash \psi_k$ is classically valid.

Proof of completeness

Assume $\bigwedge \Theta \Rightarrow \bigvee \Pi$ is valid.

Step 3. Transform all global hypotheses into local ones.

$$\dfrac{\dfrac{[\varphi_1], \ldots, [\varphi_{n-1}]; \varphi_n \vdash \psi_k}{\vdots \atop [\varphi_1], \ldots, [\varphi_n]; \cdot \vdash \psi_k}}{\dfrac{[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m]}{\vdots \atop \Theta \vdash \Pi}}$$

Lemma (Key lemma)

If $[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m]$ is valid, then there is a k such that $\varphi_1, \ldots, \varphi_n \vdash \psi_k$ is classically valid.

Proof of completeness

Assume $\bigwedge \Theta \Rightarrow \bigvee \Pi$ is valid.

Step 3. Transform all global hypotheses into local ones.

$$\dfrac{\dfrac{[\varphi_1], \ldots, [\varphi_{n-2}]; \varphi_{n-1}, \varphi_n \vdash \psi_k}{\vdots}\quad}{\dfrac{[\varphi_1], \ldots, [\varphi_n]; \cdot \vdash \psi_k}{[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m]}}$$

$$\vdots$$

$$\Theta \vdash \Pi$$

Lemma (Key lemma)

If $[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m]$ *is valid,*
then there is a k *such that* $\varphi_1, \ldots, \varphi_n \vdash \psi_k$ *is classically valid.*

Proof of completeness

Assume $\bigwedge \Theta \Rightarrow \bigvee \Pi$ is valid.

Step 4. Prove the resulting sequent propositionnally.

$$\dfrac{\begin{array}{c}\varnothing; \varphi_1, \ldots, \varphi_n \vdash \psi_k \\ \vdots \\ [\varphi_1], \ldots, [\varphi_n]; \cdot \vdash \psi_k\end{array}}{\begin{array}{c}[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m] \\ \vdots \\ \Theta \vdash \Pi\end{array}}$$

Lemma (Key lemma)

If $[\varphi_1], \ldots, [\varphi_n] \vdash [\psi_1], \ldots, [\psi_m]$ *is valid,*
then there is a k *such that* $\varphi_1, \ldots, \varphi_n \vdash \psi_k$ *is classically valid.*

Conclusion

Summary

- First completeness results for CCSA logic:
  - ▷ Hypersequents
  - ▷ Global and local sequents
- Compatible with Squirrel's current proof system

Future work

- Compactness for modal logics of ow. truth
- Cut elimination for hypersequents with modified axiom
- Completeness for FO. fragment of CCSA, incorporate indistinguishability predicate

S5 complete w.r.t. our logic

Goal : φ valid in our sense $\implies$ φ derives from **S5**

Proof : Prove the contrapositive i.e.

$$\varphi \text{ doesn't derive from } \mathbf{S5} \implies \neg\varphi \text{ sat. in our sense}$$

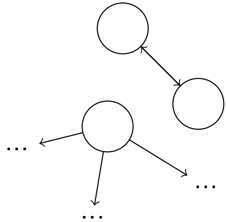
S5 complete w.r.t. our logic

Goal : φ valid in our sense $\implies$ φ derives from **S5**

Step 1. **S5** complete w.r.t. Kripke equivalence models

$\neg\varphi$ has a Kripke equivalence model

φ doesn't derive from **S5** $\implies$

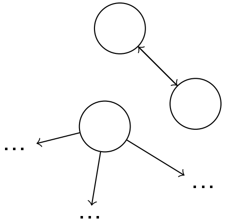


S5 complete w.r.t. our logic

Goal : φ valid in our sense $\implies$ φ derives from **S5**

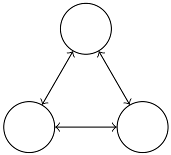
Step 2. Finite clique property

$\neg\varphi$ has a Kripke equivalence model



$\implies$

$\neg\varphi$ has a finite clique model

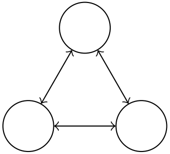


S5 complete w.r.t. our logic

Goal : φ valid in our sense $\implies$ φ derives from **S5**

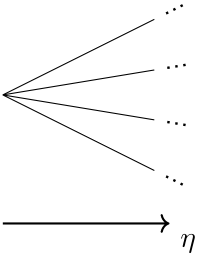
Step 3. Model transformation

$\neg\varphi$ has a finite clique model



$\implies$

$\neg\varphi$ has a crypto. structure model

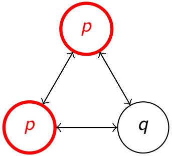


S5 complete w.r.t. our logic

Goal : φ valid in our sense $\implies$ φ derives from **S5**

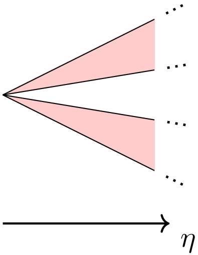
Step 3. Model transformation

$\neg\varphi$ has a finite clique model



$\implies$

$\neg\varphi$ has a crypto. structure model

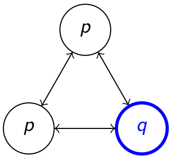


S5 complete w.r.t. our logic

Goal : φ valid in our sense $\implies$ φ derives from **S5**

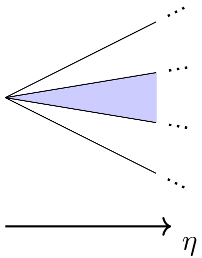
Step 3. Model transformation

$\neg\varphi$ has a finite clique model



$\implies$

$\neg\varphi$ has a crypto. structure model



Validity of disjunctions (proof)

Assumption : $[\varphi_1] \land \cdots \land [\varphi_n] \to [\psi_1] \lor \cdots \lor [\psi_m]$ valid

Goal : There is a k such that $\varphi_1 \land \cdots \land \varphi_n \to \psi_k$ valid

Validity of disjunctions (proof)

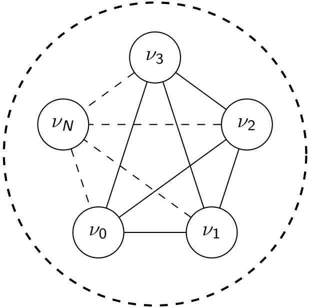
Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid

Goal : There is a k such that $\varphi \to \psi_k$ valid

Validity of disjunctions (proof)

Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid
Goal : There is a k such that $\varphi \to \psi_k$ valid

Proof :



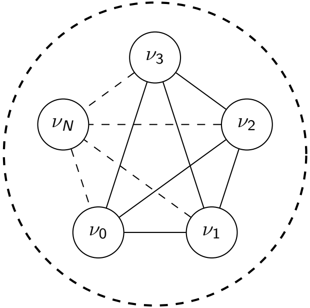
$\mathcal{M} = \mathsf{Mod}(\varphi)$

- $\mathcal{M} \models [\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$

Validity of disjunctions (proof)

Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid
Goal : There is a k such that $\varphi \to \psi_k$ valid

Proof :



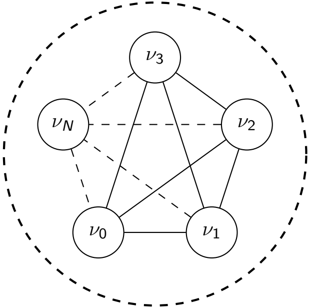
$\mathcal{M} = \mathrm{Mod}(\varphi)$

- $\mathcal{M} \models [\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$
- $\mathcal{M} \models [\varphi]$

Validity of disjunctions (proof)

Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid
Goal : There is a k such that $\varphi \to \psi_k$ valid

Proof :



$\mathcal{M} = \mathsf{Mod}(\varphi)$

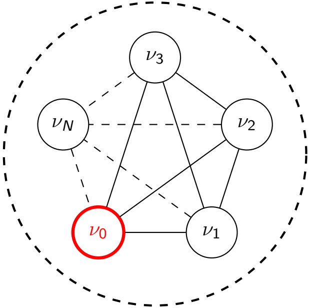
- $\mathcal{M} \models [\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$
- $\mathcal{M} \models [\varphi]$

$\rightsquigarrow$ $\mathcal{M} \models [\psi_1] \vee \cdots \vee [\psi_m]$

Validity of disjunctions (proof)

Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid
Goal : There is a k such that $\varphi \to \psi_k$ valid

Proof :



$\mathcal{M} = \mathrm{Mod}(\varphi)$

- $\mathcal{M} \models [\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$
- $\mathcal{M} \models [\varphi]$

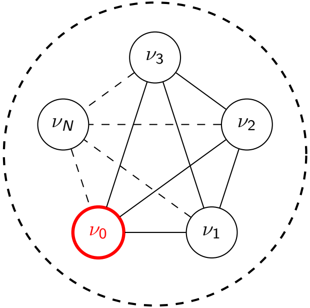
$\rightsquigarrow$ $\mathcal{M} \models [\psi_1] \vee \cdots \vee [\psi_m]$

Then...

Validity of disjunctions (proof)

Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid
Goal : There is a k such that $\varphi \to \psi_k$ valid

Proof :



$\mathcal{M} = \mathrm{Mod}(\varphi)$

- $\mathcal{M} \models [\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$
- $\mathcal{M} \models [\varphi]$

$\rightsquigarrow \mathcal{M} \models [\psi_1] \vee \cdots \vee [\psi_m]$

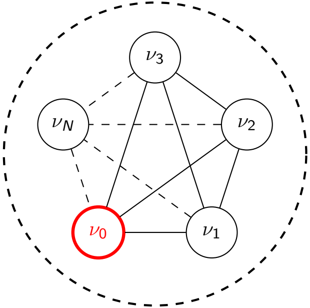
Then...

$$\mathcal{M}, \nu_0 \models [\psi_1] \vee \cdots \vee [\psi_m]$$

Validity of disjunctions (proof)

Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid
Goal : There is a k such that $\varphi \to \psi_k$ valid

Proof :



$\mathcal{M} = \mathrm{Mod}(\varphi)$

- $\mathcal{M} \models [\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$
- $\mathcal{M} \models [\varphi]$

$\rightsquigarrow$ $\mathcal{M} \models [\psi_1] \vee \cdots \vee [\psi_m]$

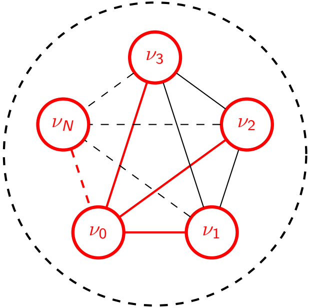
Then...

$$\mathcal{M}, \nu_0 \models [\psi_k]$$

Validity of disjunctions (proof)

Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid
Goal : There is a k such that $\varphi \to \psi_k$ valid

Proof :



$\mathcal{M} = \mathrm{Mod}(\varphi)$

- $\mathcal{M} \models [\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$
- $\mathcal{M} \models [\varphi]$

$\rightsquigarrow$ $\mathcal{M} \models [\psi_1] \vee \cdots \vee [\psi_m]$

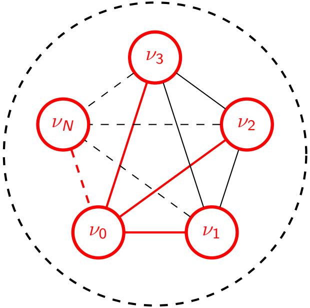
Then...

For all (other) $\nu, \nu \models \psi_k$

Validity of disjunctions (proof)

Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid
Goal : There is a k such that $\varphi \to \psi_k$ valid

Proof :



$\mathcal{M} = \mathrm{Mod}(\varphi)$

- $\mathcal{M} \models [\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$
- $\mathcal{M} \models [\varphi]$

$\rightsquigarrow \mathcal{M} \models [\psi_1] \vee \cdots \vee [\psi_m]$

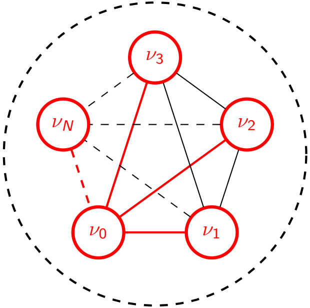
Then...

$$\varphi \models \psi_k$$

Validity of disjunctions (proof)

Assumption : $[\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$ valid
Goal : There is a k such that $\varphi \to \psi_k$ valid

Proof :



$\mathcal{M} = \mathrm{Mod}(\varphi)$

- $\mathcal{M} \models [\varphi] \to [\psi_1] \vee \cdots \vee [\psi_m]$
- $\mathcal{M} \models [\varphi]$

$\rightsquigarrow \mathcal{M} \models [\psi_1] \vee \cdots \vee [\psi_m]$

Then...

$$\models \varphi \to \psi_k$$