# Propositional Logics of Overwhelming Truth

**Thibaut Antoine**
Univ Rennes, CNRS, IRISA, France

**David Baelde**
Univ Rennes, CNRS, IRISA, France

## Abstract

Cryptographers consider that *asymptotic security* holds when, for any possible attacker running in polynomial time, the probability that the attack succeeds is *negligible*, i.e. that it tends fast enough to zero with the size of secrets. In order to reason formally about cryptographic truth, one may thus consider logics where a formula is satisfied when it is true with overwhelming probability, i.e. a probability that tends fast enough to one with the size of secrets. In such logics it is not always the case that either $\varphi$ or $\neg\varphi$ is satisfied by a given model. However, security analyses will inevitably involve specific formulas, which we call *determined*, satisfying this property – typically because they are not probabilistic. The Squirrel proof assistant, which implements a logic of overwhelming truth, features ad-hoc proof rules for this purpose.

In this paper, we study several propositional logics whose semantics rely on overwhelming truth. We first consider a modal logic of overwhelming truth, and show that it coincides with S5. In addition to providing an axiomatization, this brings a well-behaved proof system for our logic in the form of Poggiolesi's hypersequent calculus. Further, we show that this system can be adapted to elegantly incorporate reasoning on determined atoms. We then consider a logic that is closer to Squirrel's language, where the overwhelming truth modality cannot be nested. In that case, we show that a simple proof system, based on regular sequents, is sound and complete. This result justifies the core of Squirrel's proof system.

**2012 ACM Subject Classification** Security and privacy → Formal methods and theory of security; Theory of computation → Modal and temporal logics; Theory of computation → Proof theory

**Keywords and phrases** Cryptography, Modal Logic, Sequent Calculus

**Digital Object Identifier** 10.4230/LIPIcs.CSL.2025.24

**Funding** This work received funding from the France 2030 program managed by the French National Research Agency under grant agreement No. ANR-22-PECY-0006.

## 1 Introduction

In modern cryptography, one cannot hope for absolute truth. Considering a signature primitive sign with a freshly generated pair of secret and public keys $sk$ and $pk$, it is expected that an attacker cannot forge a valid signature $\mathrm{sign}(m, k)$, even if he has had access to honestly generated signatures $\mathrm{sign}(m_i, k)$ for $i \in [1; n]$ – unless of course $m = m_i$ for some $i$. However, one cannot rule out the possibility that the attacker guesses the secret key: brute force attacks are always possible. Hence, cryptographers must work with a complex notion of truth, restricting attackers to limited resources and admitting a small probability of success. In provable cryptography, a system is said to be *asymptotically secure* when, for any attacker represented as a probabilistic polynomial-time Turing machine, the probability that an attack succeeds is negligible, i.e. asymptotically smaller than the inverse of any positive polynomial in the length of secret keys increases [18]. Dually, we expect that the system remains secure with *overwhelming* probability, i.e. that tends fast enough to one as key lengths increase. In other words, overwhelming truth is the working notion of truth for cryptographers.

In order to ease formal proofs in presence of this complex notion of cryptographic truth, cryptographers have developped specific proof techniques, such as game hopping and reasoning up-to failure [27]. Going further, formal systems have been developed and implemented to mechanize cryptographic proofs [13, 10, 11, 1], successfully bringing together proof techniques coming from both cryptography, program verification and theorem proving – see [9] for a survey. All of the above mentionned systems allow the explicit manipulation of probabilities. This may be desired, e.g. to formalize *concrete security* arguments where precise, explicit bounds are derived for the attacker's advantage. However, this level of detail makes for very tedious proofs, and seems unnecessary to formalize the large body of work on e.g. the asymptotic security of cryptographic protocols. Bana and Comon have proposed to solve this issue with the CCSA approach [7, 8], which builds on the standard framework of first-order logic to provide a formal language that abstracts away probabilities and asymptotic reasoning. After some successful uses on paper [14, 21, 26, 6], the CCSA approach has been mechanized in the Squirrel proof assistant [2, 3, 16], which implements a higher-order version of the CCSA logic [5]. In that logic, one may write e.g. an authentication property as a formula of the form $[\forall \tau.\ \text{happens}(\tau) \Rightarrow \text{condition}@\tau \Rightarrow \exists \tau'.\ \tau' < \tau \wedge \text{event}@\tau']$ which intuitively expresses that, in any execution trace of a protocol, if some participant checks a condition at any time point inside the trace, some event must have happened earlier in the trace. Crucially, the $[\varphi]$ construct expresses that the enclosed formula $\varphi$ holds with overwhelming probability. Such authentication formulas might be consequences of axioms expressing (overwhelmingly true) cryptographic assumptions, e.g. about signatures, and they might have more complex formulas as consequences – the CCSA logics feature a predicate expressing *computational indistinguishability*, which we will leave aside in this work. In typical Squirrel proofs, one often works with formulas of the form $\forall \tau.\ [\text{happens}(\tau)] \Rightarrow \varphi$, where we say that $\varphi$ holds for any time point $\tau$ in the trace. If the considered protocol only features actions $A$ and $B$, an axiom will allow to rewrite this as $\forall \tau.\ [\tau = A \vee \tau = B] \Rightarrow \varphi$. At this point it would be tempting to conclude that our formula holds provided that both $\varphi[\tau := A]$ and $\varphi[\tau := B]$ hold; proving these properties might then rely on the specification of the actions $A$ and $B$. However, such a case analysis is in general unsound due to the probabilistic nature of the logic: $\tau \in \{A, B\}$ might be true with overwhelming probability for a random variable $\tau$ that is equal to $A$ (resp. $B$) with probability $1/2$, in which case neither $\tau = A$ nor $\tau = B$ will be true with overwhelming probability. If relevant, this problem might be worked around by assuming that $\tau$ is actually deterministic, i.e. considering the formula $\forall \tau.\ \det(\tau) \Rightarrow [\tau = A \vee \tau = B] \Rightarrow \varphi$.

Research in the CCSA line of work has been mainly concerned with justifying the soundness of the logic wrt. the cryptographic model, the soundness of the proposed proof systems wrt. the logic, and with concretely verifying cryptographic protocols to justify the practicality of the approach. In comparison, few investigations have looked carefully into the fine structure of the logic and associated proof systems. Scerri and Koutsos have established the decidability of provability for some CCSA systems [15, 22], and a recent work in a variant of the CCSA logic with explicit bounds improves these bounds via proof transformations [4]. However, no completeness result has ever been proved for a CCSA logic, and the proof systems proposed in [2, 3, 5] are just sound collections of rules, some of which may be deemed ad-hoc. Over time, these systems have been structured around notions of local and global sequents [3] which are only justified by their practical usefulness. Moreover, proof systems incorporate a few ad-hoc rules [5] that can take into account the det(_) assumptions: for instance, a rule essentially allows to treat $[\varphi \vee \psi]$ as $[\varphi] \vee [\psi]$ when $\det(\varphi)$. The complexity of the logic, as well as its practical relevance, calls for a more careful design.

In this paper, we provide the first answers to these concerns. We restrict to the propositional fragment of Squirrel's logic [5], which we naturally reframe as a modal logic: we view $[\varphi]$ as $\Box\varphi$, where the $\Box$ modality is interpreted as overwhelming truth. This allows us to apply the well-established concepts and techniques of modal logic and proof theory. We define in Section 2 (several possible variants of) a modal logic of overwhelming truth and show in Section 3 that it coincides with the modal logic S5. This result allows to transfer existing proof systems and model-theoretic techniques from S5 to our modal logic of overwhelming truth. In particular, we show in Section 4 that Poggiolesi's hypersequent calculus can be nicely adapted to incorporate reasoning about determined formulas – a slight variant of the det(_) predicate presented above. We also show that, for the fragment of our logic that most closely corresponds to the language of Squirrel, hypersequents are not necessary: we introduce in Section 5 a sound and complete sequent calculus based on Squirrel's notions of local and global sequents. We conclude in Section 6 with some discussion of related and future works.

## 2 Modal logics of overwhelming truth

We define several *modal logics of overwhelming truth*, whose formulas are standard modal logic formulas, interpreted as families of random variables with the box modality corresponding to overwhelming truth.

We recall that a *probability space* is a triple $X = (S, \Omega, \mu)$ where $S$ is a non-empty set of *samples*, the set of *events* $\Omega \subseteq 2^S$ is a $\sigma$-algebra[1], and $\mu : \Omega \to [0; 1]$ is a measure[2] assigning a probability to each event of $\Omega$, such that $\mu(S) = 1$. A *random variable* $V : X \to Y$ from probability space $X = (S, \Omega, \mu)$ to probability space $Y = (S', \Omega', \mu')$ is a function from $S$ to $S'$ such that the pre-image of any event in $Y$ is an event in $X$: for all $E' \in \Omega'$, $V^{-1}(E') \in \Omega$. This allows us to define $\Pr_{x\in X}\big(V(x) \in E'\big)$ as $\mu(V^{-1}(E'))$ for any event $E' \in \Omega'$.

As is common, we will identify a probability space $X = (S, \Omega, \mu)$ with its sample space, saying for instance that $x \in X$ when $x \in S$. Conversely, we identify a finite set $S$ with the *discrete probability space* $(S, 2^S, \mu)$ where $\mu(E) = |E|/|S|$ – we typically take $S$ to be $\{0, 1\}$ or $\{0, 1\}^k$.

▶ **Definition 1** (Modal formulas). *We assume a set $\mathcal{P}$ of propositional variables. Modal formulas are then built from the following grammar: $\varphi ::= \bot \mid p \mid \varphi \Rightarrow \varphi \mid \Box\varphi$. As usual, we will use other logical connectives as they can be defined from the above ones. For instance, we will write $\varphi \vee \psi$ for $\neg\varphi \Rightarrow \psi$ and $\Diamond\varphi$ for $\neg\Box\neg\varphi$.*

We define next an *abstract* modal logic of overwhelming truth, where validity corresponds to overwhelming truth in a general class of models. Several variants of this logic are then obtained by restricting to particular classes of models. As we shall see in the next section, all these variants are actually equivalent.

### 2.1 The abstract modal logic of overwhelming truth

We will interpret formulas as families of random variables, indexed by the security parameter $\eta \in \mathbb{N}$. To do so, we use an abstract notion of *cryptographic structure* that provides a family of measure spaces, and interprets each variable as a family of random variables over these spaces.

[1] A $\sigma$-algebra must be non-empty and closed under complement, countable unions and intersections.
[2] A measure must satisfy $\mu(\biguplus_{i\in\mathbb{N}} E_i) = \sum_{i\in\mathbb{N}} \mu(E_i)$.

▶ **Definition 2** (Cryptographic structure). *A cryptographic structure $\mathcal{S}$ is given by:*

- *A sequence of probability spaces $(X_\eta^{\mathcal{S}})_{\eta\in\mathbb{N}}$. For $\eta \in \mathbb{N}$, we let $\mathsf{RV}_\eta^{\mathcal{S}}$ be the set of random variables from $X_\eta^{\mathcal{S}}$ to $\{0,1\}$, and $\mathsf{RV}^{\mathcal{S}} = \{\ (U_\eta)_{\eta\in\mathbb{N}} \mid U_\eta \in \mathsf{RV}_\eta^{\mathcal{S}}$ for all $\eta\ \}$.*
- *For each propositional variable $p \in \mathcal{P}$, an interpretation $p^{\mathcal{S}} \in \mathsf{RV}^{\mathcal{S}}$.*

When $U = (U_\eta)_{\eta\in\mathbb{N}} \in \mathsf{RV}^{\mathcal{S}}$, $\eta \in \mathbb{N}$ and $\rho \in X_\eta^{\mathcal{S}}$, we write $U(\eta,\rho)$ for $U_\eta(\rho)$. Conversely, we may define an element $U \in \mathsf{RV}^{\mathcal{S}}$ by defining $U(\eta,\rho)$ for each $\eta \in \mathbb{N}$ and $\rho \in \mathsf{RV}_\eta^{\mathcal{S}}$.

A function $f : \mathbb{N} \to [0,1]$ is *negligible* when $f$ is asymptotically smaller than $\eta \mapsto \eta^{-k}$ for any $k \in \mathbb{N}$. The function is *overwhelming* when $\eta \mapsto 1 - f(\eta)$ is negligible. For conciseness, we will also say that a family of random variables $U \in \mathsf{RV}^{\mathcal{S}}$ (for some cryptographic structure $\mathcal{S}$) is overwhelming when $\eta \mapsto \Pr_{\rho\in X_\eta^{\mathcal{S}}}\big(U(\eta,\rho) = 1\big)$ is overwhelming.

▶ **Definition 3.** *Given a cryptographic structure $\mathcal{S}$ and a formula $\varphi$, we define the interpretation $[\![\varphi]\!]_{\mathcal{S}} \in \mathsf{RV}^{\mathcal{S}}$ as follows, for all $\eta \in \mathbb{N}$ and $\rho \in X_\eta^{\mathcal{S}}$:*

- $[\![p]\!]_{\mathcal{S}}(\eta,\rho) = p^{\mathcal{S}}(\eta,\rho)$ *for $p \in \mathcal{P}$;*
- $[\![\bot]\!]_{\mathcal{S}}(\eta,\rho) = 0$*;*
- $[\![\varphi \Rightarrow \psi]\!]_{\mathcal{S}}(\eta,\rho) = 1$ *iff* $[\![\varphi]\!]_{\mathcal{S}}(\eta,\rho) \le [\![\psi]\!]_{\mathcal{S}}(\eta,\rho)$*;*
- $[\![\Box\varphi]\!]_{\mathcal{S}}(\eta,\rho) = 1$ *iff $[\![\varphi]\!]_{\mathcal{S}}$ is overwhelming.*

▶ **Definition 4** (Validity). *A formula $\varphi$ is* valid *wrt. a class of cryptographic structures when $[\![\varphi]\!]_{\mathcal{S}}$ is overwhelming for any $\mathcal{S}$ in that class. We simply say that $\varphi$ is valid when it is valid wrt. all cryptographic structures.*

We can now define our first logic. As is standard, we define a logic as a set of formulas called the *theorems* of that logic.

▶ **Definition 5.** *The* abstract modal logic of overwhelming truth *is the set of modal formulas that are valid wrt. all cryptographic structures.*

▶ **Example 6.** Let $\varphi$ and $\psi$ be arbitrary modal formulas.

- We have that $\varphi$ is valid iff $\Box\varphi$ is valid: for any $\mathcal{S}$, $[\![\varphi]\!]_{\mathcal{S}}$ is overwhelming iff $[\![\Box\varphi]\!]_{\mathcal{S}}$ is overwhelming.
- The formula $\Box(\varphi \wedge \psi) \Rightarrow \Box\varphi \wedge \Box\psi$ is valid. Indeed, in any $\mathcal{S}$ where $[\![\varphi \wedge \psi]\!]_{\mathcal{S}}$ is overwhelming, so are $[\![\varphi]\!]_{\mathcal{S}}$ and $[\![\psi]\!]_{\mathcal{S}}$.
- The formula $\Box(\varphi \vee \psi) \Rightarrow \Box\varphi \vee \Box\psi$ is not valid. Indeed, $\varphi$ and $\psi$ might both be true with probability $1/2$ (for all $\eta$) in such a way that their disjunction is true with probability 1 (for all $\eta$).

Unlike Squirrel's logic, our modal logic allows the nesting of modal boxes expressing overwhelming truth. Our logic is otherwise much less expressive than Squirrel's, not only because that logic allows (higher-order) quantifications. In our modal logic, propositional variables are interpreted as families of random variables, where the random variables corresponding to different values of $\eta$ might be completely unrelated. In contrast, Squirrel's logic features predicates that allow to restrict to families of random variables that do not vary with $\eta$, or to deterministic families, i.e. families of constant random variables. Finally, Squirrel's logic features the computational indistinguishability predicate, absent from our modal logic, which allows to state, e.g., that two propositional formulas yield probability distributions that are negligibly different.

▶ **Proposition 7.** *The abstract logic of overwhelming truth is a* normal modal logic*: its theorems are closed under substitution and* modus ponens*; they contain classical tautologies and the K axiom $\Box(p \Rightarrow q) \Rightarrow \Box p \Rightarrow \Box q$; moreover, $\Box\varphi$ is a theorem whenever $\varphi$ is.*

This interested reader may find the proof of this result in Section A.

## 2.2 Variants

It is natural to consider several variations on the abstract modal logic of overwhelming truth, obtained by considering validity wrt. restricted classes of cryptographic structures. The first variant is of particular interest to us, since it corresponds to the class of models considered in Squirrel, i.e., to the *term structures* that are suitable for interpreting *names* over *large* types [5].

▶ **Definition 8.** *We say that a cryptographic structure $\mathcal{S}$ is* concrete *when each $X_\eta^{\mathcal{S}} = \{0,1\}^{\ell_\eta}$ for some $\ell_\eta$, with $\eta \mapsto \ell_\eta$ strictly increasing. The* concrete modal logic of overwhelming truth *is the set of modal formulas that are valid wrt. concrete cryptographic structures.*

The next variant is a modal logic of "truth with probability 1", obtained by restricting to a class of structures where overwhelming truth is the same as truth with probability 1.

▶ **Definition 9.** *The* static modal logic of overwhelming truth *is the set of modal formulas that are valid wrt. all cryptographic structures $\mathcal{S}$ such that the same probability space is used for all $\eta$ (i.e., $X_\eta^{\mathcal{S}} = X_{\eta'}^{\mathcal{S}}$ for all $\eta, \eta'$).*

Restricting even further the considered set of structures to discrete probability spaces, we obtain a logic where $\Box\varphi$ reads as "$\varphi$ is true for all samples (with non-zero probability)".

▶ **Definition 10.** *The* static discrete modal logic of overwhelming truth *is the set of modal formulas that are valid wrt. all cryptographic structures $\mathcal{S}$ such that the same* discrete *probability space is used for all $\eta$.*

Note that the observations of Example 6 still hold if one considers validity wrt. any of the above classes. Proposition 7 also holds for all of our variant logics. As we shall see, all of the above variants are actually the same logic. Other variants are possible that would yield the same logic, e.g. considering infinite concrete cryptographic structures where samples are infinite bitstrings. We do not intend to exhaustively list equivalent variants, and believe that the reader should be able to adapt our techniques to handle new variants.

# 3 Soundness and completeness with respect to S5

We now prove that our modal logics of overwhelming truth coincide with S5, the smallest normal modal logic containing the following axioms:

$$\begin{aligned}
&\text{(axiom T)} && \Box p \;\Rightarrow\; p \\
&\text{(axiom 4)} && \Box p \;\Rightarrow\; \Box\Box p \\
&\text{(axiom 5)} && \Diamond p \;\Rightarrow\; \Box\Diamond p
\end{aligned}$$

We can immediately observe that S5 is included in our modal logics; a detailed proof is given in Section B.

▶ **Lemma 11.** *All S5 theorems are theorems of the modal logics of overwhelming truth.*

In order to prove the converse, a model-theoretic characterization of S5 will be useful.

▶ **Definition 12** (Kripke structure)**.** *A Kripke structure $\mathcal{K}$ is given by:*

- *a frame $(W^{\mathcal{K}}, \mathcal{R}^{\mathcal{K}})$ where $W$ is a set of* worlds*, and $\mathcal{R}$ is a binary relation over $W$;*
- *for each world $w \in W$, a set of propositional variables $V^{\mathcal{K}}(w) \subseteq \mathcal{P}$.*

▶ **Definition 13** (Equivalence and clique frames). *A Kripke frame $(W, \mathcal{R})$ is an equivalence relation when $\mathcal{R}$ is symmetric, reflexive and transitive. It is a clique when $\mathcal{R}$ is the full binary relation over $W$. Further, it is a finite clique when $W$ is finite.*

We may omit the $\mathcal{K}$ superscripts when they are clear from the context.

▶ **Definition 14** (Satisfaction). *Given a modal logic formula $\varphi$, a Kripke structure $\mathcal{K}$ and a world $w \in W^{\mathcal{K}}$, we define the satisfaction relation $\mathcal{K}, w \models \varphi$ as follows:*

- $\mathcal{K}, w \models p$ *iff* $p \in V^{\mathcal{K}}(w)$;
- $\mathcal{K}, w \not\models \bot$;
- $\mathcal{K}, w \models \varphi \Rightarrow \psi$ *iff* $\mathcal{K}, w \models \varphi$ *implies* $\mathcal{K}, w \models \psi$;
- $\mathcal{K}, w \models \Box\varphi$ *iff* $\mathcal{K}, w' \models \varphi$ *for all* $w' \in W^{\mathcal{K}}$ *such that* $w \mathcal{R}^{\mathcal{K}} w'$.

A formula is valid wrt. a class of frames when it is satisfied at all worlds of all Kripke structures whose frame belongs to the class. For instance, a formula is valid wrt. clique frames when it is satisfied at all worlds of all Kripke structures whose frame is a clique.

We summarize next some well-known characterizations of S5, proved e.g. in [12]. More details are given in Section B.

▶ **Proposition 15.** *For any modal formula $\varphi$, the following conditions are equivalent:*

1. *$\varphi$ is a theorem of S5;*
2. *$\varphi$ is valid wrt. equivalence frames;*
3. *$\varphi$ is valid wrt. clique frames.*
4. *$\varphi$ is valid wrt. finite clique frames.*

▶ **Lemma 16.** *Our modal logics of overwhelming truth are contained in S5.*

**Proof.** We prove the result for the concrete logic of overwhelming truth, and then explain how the argument can be adapted for the other logics.

By Proposition 15 it suffices to show that, if there is a finite clique counter-model of a modal formula, then there is a concrete cryptographic structure in which the formula is not overwhelmingly true. Let $\mathcal{K}$ be a finite clique Kripke structure, with $W^{\mathcal{K}} = \{w_1, \ldots, w_n\}$. We define a concrete cryptographic structure $\mathcal{S}$ with $X^{\mathcal{S}}_\eta = \{0,1\}^\eta$, for all $\eta$. We can partition each $X^{\mathcal{S}}_\eta$ into $n$ disjoint sets called $X^{\mathcal{S}}_{\eta,i}$ for $i \in [1; n]$, such that asymptotically (in $\eta$) they all have size $\eta/n$. We define the interpretation of propositional variables in $\mathcal{S}$ so that, for each $\eta$, the same variables are true in $w_i$ and $X^{\mathcal{S}}_{\eta,i}$. Formally, for $p \in \mathcal{P}$ in $\mathcal{S}$, we define:

$$p^{\mathcal{S}}(\eta, \rho) = 1 \text{ iff } p \in V^{\mathcal{K}}(w_i) \text{ for the unique } i \in [1; n] \text{ such that } \rho \in X^{\mathcal{S}}_{\eta,i}$$

As a result of our construction, $[\![\psi]\!]_{\mathcal{S}}(\eta, \rho) = [\![\psi]\!]_{\mathcal{S}}(\eta, \rho')$ for any modal formula $\psi$, $\eta \in \mathbb{N}$, and $\rho, \rho' \in X^{\mathcal{S}}_{\eta,i}$. Further, we shall see that, for any modal formula $\psi$, $w_i \in W^{\mathcal{K}}$, $\eta \in \mathbb{N}$ and $\rho \in X^{\mathcal{S}}_{\eta,i}$, we have:

$$\mathcal{K}, w_i \models \psi \text{ iff } [\![\psi]\!]_{\mathcal{S}}(\eta, \rho) = 1.$$

This is proved by induction on $\psi$. The cases where $\psi$ is $\bot$, $\psi \in \mathcal{P}$ or $\psi$ is an implication are easily verified. Assume now that $\psi = \Box\theta$. We have:

$$\begin{array}{lll} \mathcal{K}, w_i \models \psi & \text{iff} & \mathcal{K}, w_j \models \theta \text{ for all } j \in [1; n] \qquad (\mathcal{K} \text{ is a clique}) \\ & \text{iff} & [\![\theta]\!]_{\mathcal{S}}(\eta', \rho') \text{ for all } \eta', \rho' \qquad (\text{induction hypothesis, and } X^{\mathcal{S}}_\eta = \cup_j X^{\mathcal{S}}_{\eta,j}) \end{array}$$

As a result $\mathcal{K}, w_i \models \psi$ does imply that $[\![\theta]\!]_{\mathcal{S}}$ is overwhelming, i.e. $[\![\psi]\!]_{\mathcal{S}}(\eta, \rho) = 1$. Conversely, if $[\![\theta]\!]_{\mathcal{S}}$ is overwhelming in $\mathcal{S}$, then because the $X^{\mathcal{S}}_{\eta,i}$ have asymptotic size $\eta/n$, we must have $[\![\theta]\!]_{\mathcal{S}}(\eta, \rho) = 1$ for $\eta$ large enough and any $\rho \in X^{\mathcal{S}}_\eta$. Hence $\mathcal{K}, w_j \models \theta$ for all $i$, and $\mathcal{K}, w_i \models \psi$.

To conclude, observe that if $\mathcal{K}$ is a finite clique counter-model of a modal formula $\varphi$, then $\mathcal{K}, w_i \not\models \varphi$ for some $i$. By our observation, $[\![\varphi]\!]_{\mathcal{S}}(\eta, \rho) = 0$ for all $\eta$ and $\rho \in X^{\mathcal{S}}_{\eta,i}$. Because $X^{\mathcal{S}}_{\eta,i}$ has asymptotic size $\eta/n$, $[\![\varphi]\!]_{\mathcal{S}}$ is not overwhelming. Hence the concrete modal logic of overwhelming truth is contained in S5.

This argument also shows that the abstract modal logic of overwhelming truth is contained in S5. To obtain the result for the static and static discrete[3] modal logics of overwhelming truth, the argument can be easily adapted: it suffices to take $X^{\mathcal{S}}_{\eta} = \{w_1, \dots, w_n\}$ for each $\eta$, with $X^{\mathcal{S}}_{\eta,i} = \{w_i\}$. ◀

Putting our two lemmas together, we obtain the characterization of our modal logics of overwhelming truth. In the rest of the paper, we shall indiscriminately talk of *the* modal logic of overwhelming truth, and we will interchangeably use this logic and S5.

▶ **Theorem 17.** *S5 coincides with all of our modal logics of overwhelming truth.*

## 4 Hypersequents for overwhelming truth with determined formulas

Having proved that the modal logic of overwhelming truth coincides with S5 directly provides a deductive system for overwhelming truth, in the form of the S5 axioms. More interestingly, it allows to benefit from better structured proof systems for S5, such as Poggiolesi's sound and complete hypersequent calculus for S5 [25]. This system is analytical, enjoys cut elimination and is well-adapted to proof-search. As we shall see, Poggiolesi's system can also be elegantly adapted to incorporate reasoning on determined formulas.

### 4.1 A variant of Poggiolesi's hypersequent calculus for S5

In [25], Poggiolesi introduces the hypersequent calculus CSS5$_s$ and proves that it is complete for S5 using syntactical methods. A semantical proof is also possible, which will provide a more convenient foundation for our needs. We introduce below a slight modification of her calculus that facilitates such a proof – we explain these modifications afterwards. Unlike Poggiolesi, we view sequents and hypersequents as sets rather than multisets.

▶ **Definition 18.** *A* classical *sequent $\Gamma \vdash \Delta$ is composed of two finite sets of formulas $\Gamma$ and $\Delta$. We use the comma to denote the union of sets of formulas, also writing $\Gamma, \varphi$ for $\Gamma \cup \{\varphi\}$.*

▶ **Definition 19.** *A* hypersequent *is a finite set of classical sequents. We use the letter $\mathcal{H}$ to denote hypersequents, and the vertical bar to denote the addition of a sequent to a hypersequent, i.e. $\mathcal{H} \mid \Gamma \vdash \Delta$ stands for $\mathcal{H} \cup \{\Gamma \vdash \Delta\}$.*

*When $\mathcal{H} = (\Gamma_1 \vdash \Delta_1 \mid \dots \mid \Gamma_n \vdash \Delta_n)$ is a hypersequent, we note* $\mathrm{rhs}(\mathcal{H}) = \cup_i \Delta_i$ *the union of the right-hand sides of its sequents. We define similarly* $\mathrm{lhs}(\mathcal{H}) = \cup_i \Gamma_i$.

▶ **Definition 20.** *The* formula interpretation *of a hypersequent $\Gamma_1 \vdash \Delta_1 \mid \dots \mid \Gamma_n \vdash \Delta_n$ is the modal formula $\Box(\bigwedge \Gamma_1 \Rightarrow \bigvee \Delta_1) \vee \dots \vee \Box(\bigwedge \Gamma_n \Rightarrow \bigvee \Delta_n)$.*

We present in Figure 1 a slight variant of Poggiolesi's CCS5$_s$ hypersequent calculus. Rules on the first two lines are immediate embeddings of classical propositional rules of sequent calculus in hypersequents: they apply to any sequent in the hypersequent, and the

[3] The result should not come as a surprise for the static discrete modal logic of overwhelming truth, given the analogy between the S5 characterization in terms of clique Kripke structure and the fact that overwhelming truth in static discrete structures is equivalent to truth for all samplings.

$$\frac{}{\mathcal{H} \mid \Gamma, \varphi \vdash \varphi, \Delta} \qquad \frac{}{\mathcal{H} \mid \Gamma, \bot \vdash \Delta}$$

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

$$\frac{\mathcal{H} \mid \Gamma, \Box\varphi, \varphi \vdash \Delta}{\mathcal{H} \mid \Gamma, \Box\varphi \vdash \Delta} \qquad \frac{\mathcal{H} \mid \Gamma, \Box\varphi \vdash \Delta \mid \Gamma', \varphi \vdash \Delta'}{\mathcal{H} \mid \Gamma, \Box\varphi \vdash \Delta \mid \Gamma' \vdash \Delta'} \qquad \frac{\mathcal{H} \mid \Gamma \vdash \Box\varphi, \Delta \mid \cdot \vdash \varphi}{\mathcal{H} \mid \Gamma \vdash \Box\varphi, \Delta} \; \varphi \notin \mathrm{rhs}(\mathcal{H}), \Delta$$

**Figure 1** Rules of Poggiolesi's (modified) hypersequent calculus for S5.

surrounding hypersequent structure is simply copied in the usual premisses. The axiom rule (top left) derives any hypersequent featuring a sequent that has the same formula on both sides. As usual, this rule can be restricted to the case where $\varphi$ is atomic [25] without loosing completeness. The implication left rule applies to any hypersequent featuring a sequent that has an implication formula $\varphi \Rightarrow \psi$ on its left side; it features two premisses, one where $\varphi$ has moved to the right-hand side of the corresponding sequent and one where $\psi$ has replaced $\varphi \Rightarrow \psi$. In both the left and right implication rules, we keep the principal formula $\varphi \Rightarrow \psi$ (shown in gray) in the premises rather than removing it, as would be more usual. This minor technical difference makes it easier to prove that proof search is terminating, with no negative effect on the efficiency of proof search because the strategies that we will consider can never introduce twice the same formula. Hence, from the proof-search point of view, the grayed out formulas can be seen as pure book-keeping devices.

The system features a right modal rule (bottom right of Figure 1) which, from a (top-down) proof search perspective, creates a new sequent $\vdash \varphi$ when $\Box\varphi$ is found on the right of a sequent – note that formula interpretations of the premise and conclusion hypersequents of this rule are (propositionally) equivalent. Here again, we keep the principal formula $\Box\varphi$ (shown in gray) in the premise. Importantly, the right modal rule can only be applied with principal formula $\Box\varphi$ when the $\varphi$ does not occur (at toplevel) on the right-hand side of any sequent of the conclusion hypersequent. There are two left rules, which may be seen as two versions of the same rule: from a proof-search perspective, it allows to add $\varphi$ on the left-hand side of any sequent in the hypersequent if one sequent features $\Box\varphi$ on its left; the first variant of the rule is for when $\varphi$ is added to the sequent that contains $\Box\varphi$, while the second one if for when $\varphi$ is added to another sequent.

The rules of our system differ from Poggiolesi's [25] in several minor ways. We use (hyper)sequents as sets rather than multisets, due to our focus on proof-search and semantical methods, while Poggiolesi focuses on syntactic methods, including cut elimination. Poggiolesi's calculus also treats conjunction and negation as elementary connectives, while we only consider implication as an elementary connectives. However, our rule for implication is the straightforward combination of her rules for conjunction and negation, applied on $\varphi \Rightarrow \psi$ seen as $\neg(\varphi \wedge \neg\psi)$. The more important difference is our inclusion of the principal formulas $\varphi \Rightarrow \psi$ and $\Box\varphi$ in the premisses of the corresponding rules, i.e. the occurrences shown in gray in Figure 1, and the addition of the side condition on the right modal rule. These modifications allow for a simple proof that proof-search is terminating.

Before providing a proof of this result, let us discuss it in more details. When considering (top-down) proof search in Poggiolesi's calculus, without our gray formulas, the number of logical connectives in a hypersequent decreases strictly with the application of any rule other than the left modal rules. Indeed, it is possible to repeatedly apply a left modal rule, adding

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\Box\neg\Box p \vdash p \mid \cdot \vdash p \mid \cdot \vdash p}}{\Box\neg\Box p \vdash p \mid \cdot \vdash \Box p, p}}{\Box\neg\Box p \vdash p \mid \neg\Box p \vdash p}}{\Box\neg\Box p \vdash p \mid \cdot \vdash p}}{\Box\neg\Box p \vdash \Box p, p}}{\Box\neg\Box p, \neg\Box p \vdash p}}{\Box\neg\Box p \vdash p}$$

**Figure 2** Non-terminating proof-search in $\mathrm{CSS5}_s$.

an even increasing number of copies of $\varphi$ to the left-hand sides of sequents. However, as observed in [25], this behaviour is useless: only a single application of the left rule (for any given $\varphi$ and target sequent) is present in derivations of minimal height. Building on this observation, [25, Theorem6.5] claims that $\mathrm{CSS5}_s$ allows terminating proof-search: while this is true, the proof seems to overlook the non-terminating behaviour induced by the right modal rule. Indeed, non-termination can arise because of the right modal rule (in its original version without the side condition present in Figure 1), despite the parcimonious use of left modal rules, as illustrated in Figure 2.

In order to avoid this issue, proof-search must not only avoid repeated applications of the left modal rules but also forbid the application of the right modal rule on $\Box\varphi$ when $\varphi$ is already present in the right-hand side of some sequent, *but also* when $\varphi$ has been present in a right-hand side of a previously encountered hypersequent. We incorporate this condition in our version of the right modal rule, which can be formulated in a local manner thanks to the inclusion of the (otherwise superfluous) gray formulas.

▶ **Proposition 21.** *The rules of Figure 1 allow terminating top-down proof-search.*

**Proof.** Consider an initial hypersequent $\mathcal{H}$ and an attempt at deriving $\mathcal{H}$ by applying any rule of conclusion $\mathcal{H}$, and then recursively deriving the obtained premisses in the same manner. We only impose a *progress* condition: at any point in this process, the applied rule must produce as premisses hypersequents that are all distinct from the rule's conclusion – this forbids, e.g., the repeated application of a propositional rule on the same formula of the same sequent. This proof-search attempt may eventually succeed by deriving an hypersequent using an initial rule, or stop. Our concern here is to show that it cannot run forever.

It is clear from our rules that any hypersequent $\mathcal{H}'$ arising in this process can only be formed from subformulas of the initial hypersequent $\mathcal{H}$. Moreover, if at any point in the derivation some formula $\varphi$ appears on the left-hand (resp. right-hand) side of a sequent, it will remain present on the left-hand (resp. right-hand) side of some sequent in all hypersequents of that subderivation.

In particular, this means that the right modal rule can only be applied on a finite number of distinct formulas. Applying the rule on $\Box\varphi$ creates a new sequent with $\varphi$ on its right-hand side, which will remain present in the rest of the derivation. Therefore, the right modal rule cannot be applied again on the same formula in that subderivation, due to its side condition. Thus, the number of applications of the right modal rule is bounded in any branch of the proof-search process by the number of boxed subformulas of $\mathcal{H}$.

Now, consider the application of a rule other than the right modal rule, with conclusion $\mathcal{H}'$ and $\mathcal{H}''$ as one of its premise. We observe that $|\mathcal{H}''| \leq |\mathcal{H}'|$ – the inequality can be strict, when the addition of a new formula in a sequent of $\mathcal{H}'$ results in a sequent that was already

present in $\mathcal{H}'$. Moreover, for any sequent $\Gamma' \vdash \Delta'$ of $\mathcal{H}''$, there exists a sequent $\Gamma \vdash \Delta$ of $\mathcal{H}'$ such that $\Gamma \subseteq \Gamma'$ and $\Delta \subseteq \Delta'$. Therefore, the repeated application of rules other than the right modal, subject to our progress condition, can only go on for at most $2 \times n \times k$ where $n$ is the number of sequents in the initial hypersequent $\mathcal{H}$ and $k$ is the number of subformulas of $\mathcal{H}$.

Because proof-search is bounded between any two applications of the right modal rule, and the number of such applications is itself bounded, the whole proof-search process must terminate. ◀

As is standard, we will combine this proof-search termination result with the invertibility of rules to obtain the completeness of our calculus. We rely on *semantic* invertibility, i.e. the validity of the conclusion of a rule implies the validity of all of its premisses. Recall that an hypersequent $\mathcal{H}$ is valid when its formula interpretation is in S5, which is equivalent to saying that it is satisfied in all worlds of all clique Kripke structures. Thus it is not valid iff it has a *counter-model*, that is a clique Kripke structure $\mathcal{K}$ such that, for each sequent $\Gamma \vdash \Delta$ of $\mathcal{H}$, there exists a world $w$ of $\mathcal{K}$ which satisfies all formulas of $\Gamma$ but no formula of $\Delta$ (we say that $w$ falsifies $\Gamma \vdash \Delta$). Such clique counter-models provide a convenient tool for proving the following result, by the contrapositive (see Section C for details).

▶ **Proposition 22.** *The rules of Figure 1 are invertible.*

▶ **Theorem 23.** *The calculus of Figure 1 is sound and complete wrt. S5.*

**Proof.** Soundness is easily verified by checking that each rule is sound – or observing that our rules can be obtained from Poggiolesi's and contraction.

For completeness, we show that, for some appropriate proof-search procedure, proof-search fails on a hypersequent $\mathcal{H}$ only when this hypersequent has a counter-model. To obtain this result we only need to assume that proof-search is progressing (cf. proof of Proposition 21) and that it only stops when no rule applies – we do not even need to assume that it applies initial rules eagerly, though of course this would make proof-search more efficient. By the previous result, this proof-search is terminating. In case of failure, it yields a finite partial derivation, i.e. a proof tree featuring at least one unjustified leaf $\mathcal{H}'$, which cannot be the conclusion of any rule. We shall exhibit a counter-model for $\mathcal{H}'$, which, by invertibility, will prove that $\mathcal{H}$ has a counter-model as expected.

We thus construct a counter-model for $\mathcal{H}'$, exploiting the fact that any rule instance whose conclusion is $\mathcal{H}'$ would also have $\mathcal{H}'$ as one of its premisses. We consider the Kripke clique over worlds $\{w_{\Gamma\vdash\Delta} \mid (\Gamma \vdash \Delta) \in \mathcal{H}'\}$, where $w_{\Gamma\vdash\Delta} \models p$ iff $p \in \Gamma$. We verify, for any world $w_{\Gamma\vdash\Delta}$, that $w_{\Gamma\vdash\Delta} \models \varphi$ for any $\varphi \in \Gamma$, and $w_{\Gamma\vdash\Delta} \not\models \varphi$ for any $\varphi \in \Delta$. This is proved by induction over $\varphi$. The cases for $\bot$ and atoms is immediate. Assume now that $\varphi$ is of the form $\varphi_1 \Rightarrow \varphi_2$:

- If $\varphi \in \Gamma$ then, because the implication left rule would have $\mathcal{H}'$ itself as premise, it must be that either $\varphi_2 \in \Gamma$ or $\varphi_1 \in \Delta$. In either case we conclude, by induction hypotheses on $\varphi_1$ and $\varphi_2$, that $w_{\Gamma\vdash\Delta} \models \varphi$.
- Similarly, if $\varphi \in \Delta$, we obtain that $\varphi_1 \in \Gamma$ and $\varphi_2 \in \Delta$ by hypothesis on $\mathcal{H}'$, and conclude by induction hypotheses on $\varphi_1$ and $\varphi_2$.

Finally, consider the case where $\varphi$ is some $\Box\varphi'$:

- If $\varphi \in \Gamma$, then because the left modal rules yield $\mathcal{H}'$ as a premise, the subformula $\varphi'$ is on the left-hand side of all sequents of $\mathcal{H}'$, thus $w_{\Gamma\vdash\Delta} \models \varphi$.
- If $\varphi \in \Delta$, the right modal rule does not apply without creating a repetition, thus there exists a sequent of $\mathcal{H}'$ which has $\varphi'$ on its right-hand side, providing a world $w'$ which does not satisfy $\varphi'$, hence $w_{\Gamma\vdash\Delta} \not\models \varphi$. ◀

$$\frac{}{\mathcal{H} \mid \Gamma, \varphi \vdash \Delta \mid \Gamma' \vdash \varphi, \Delta'}\ \varphi \text{ determined}$$

**Figure 3** Additional axiom rule for determined formulas.

## 4.2 Reasoning on determined formulas in hypersequent calculus

Now that we have presented Poggiolesi's hypersequent calculus for S5, in a slightly reformulated form, we show that it can easily adapted to elegantly incorporate reasoning on determined formulas. In the context of the logic of overwhelming truth, way say that a formula $\varphi$ is determined if it is either overwhelmingly true or overwhelmingly false (i.e. negligibly true). In our modal language, this can simply be expressed as $\Box\varphi \vee \Box\neg\varphi$. When reasoning about cryptographic protocols, determined formulas often arise, and it is necessary to take this property into account to carry out formal proofs. We are thus interested in designing proof systems that can take the determined character of formulas into account.

To formally define our problem, we first parameterize our logic with a subset of atoms $\mathcal{D}$ that are assumed to be determined – this is a modelling assumption. We consider the problem of deciding whether a formula $\varphi$ is a consequence of $\{\Box d \vee \Box\neg d \mid d \in \mathcal{D}\}$ – of course, this can also be phrased in terms of cryptographic structures or clique Kripke structures by the previous results. More precisely, we would like to find a proof system with nice proof-search behaviour for proving such formulas.

▶ **Example 24.** Take $\mathcal{D} = \{q\}$ for some $q \in \mathcal{P}$. Then $\Box(q \vee \psi) \Rightarrow \Box q \vee \Box\psi$ is valid for any $\psi$. Moreover, for some $p \in \mathcal{P} \setminus \mathcal{D}$, we have $\Box\varphi \vee \Box\neg\varphi$ for $\varphi \in \{q \Rightarrow \bot,\ \Box p,\ q \wedge (p \Rightarrow p)\}$. For $\varphi = (p \Rightarrow q)$, $\Box\varphi \vee \Box\neg\varphi$ is however not valid.

A naive solution to our problem can be obtained from any complete proof system for our modal logic: it suffices to look for proofs of $(\bigwedge_{d\in\mathcal{D}} \Box d \vee \Box\neg d) \Rightarrow \varphi$, using the proof system at hand (assuming wlog. that $\mathcal{D}$ is finite). This is however unsatisfactory, as the addition of the hypotheses $\Box d \vee \Box\neg d$ would yield an explosion of the size of proofs in a typical proof-search, as is the case with our hypersequent calculus.

We propose a better solution, where the determined character of formulas is only used when relevant. Strikingly, it is obtained by adding to the rules of Figure 1 a single rule, shown in Figure 3: instead of adding hypotheses expressing $\mathcal{D}$ in the conclusion hypersequent, we incorporate $\mathcal{D}$ in a modified axiom rule. As with the standard axiom rule, our modified axiom rule can be restricted to the case where $\varphi$ is atomic, without losing completeness – in that case, the side condition is equivalent to requiring that $\varphi \in \mathcal{D}$. In fact, it seems that any reasonable use of this rule in a proof-search would rely on a side condition that is easier to verify than the fact that $\varphi$ is determined: although this is decidable, it is costly; a syntactic criterion for detecting simple determined formulas can be used instead, e.g. checking that the formula is built using propositional connectives from atoms in $\mathcal{D}$ and boxed formulas.

▶ **Theorem 25.** *The proof system of Figure 1 augmented with the rule of Figure 3 is sound and complete for the logic of overwhelming truth with determined formulas in $\mathcal{D}$: a hypersequent $\mathcal{H}$ is derivable in this system iff the formula interpretation of $\mathcal{H}$ is valid in all structures satisfying $\Box\psi \vee \Box\neg\psi$ for all $\psi \in \mathcal{D}$.*

**Proof.** For soundness, it suffices to observe that the conclusion of our new rule cannot have counter-models consistent with $\mathcal{D}$: we would then have a world satisfying $\psi$ and another satisfying $\neg\psi$.

For completeness, we adapt the argument provided for S5 in the previous section, to show that any hypersequent for which proof-search fails admits a counter-model. We do this with a proof-search procedure that makes use of our additional rule, and ensure that in that case the counter-model is consistent with $\mathcal{D}$. Clearly, proof-search still terminates in our system, and rules are still invertible: all we need to do is adapt the counter-model construction for an hypersequent $\mathcal{H}'$ on which proof-search cannot conclude nor progress. We adapt the construction of Theorem 23, taking the same set of worlds as before, but setting $\mathcal{K}, w_{\Gamma\vdash\Delta} \models p$ iff $p \in \Gamma$ or $p \in \mathcal{D} \cap \mathrm{lhs}(\mathcal{H}')$. In this way, we ensure that the atoms in $\mathcal{D}$ are determined in $\mathcal{K}$. We then verify, for any world $w_{\Gamma\vdash\Delta}$, that $w_{\Gamma\vdash\Delta} \models \varphi$ for any $\varphi \in \Gamma$, and $w_{\Gamma\vdash\Delta} \not\models \varphi$ for any $\varphi \in \Delta$. This is proved by induction on $\varphi$ as before, and only the case where $\varphi$ is an atom $p$ is modified:

- If $p \in \Gamma$, we have $w_{\Gamma\vdash\Delta} \models p$ by construction.
- If $p \in \Delta$ and $p \notin \mathcal{D}$, we know that the axiom rule of Figure 1 does not apply, hence $p \notin \Gamma$, from which $w_{\Gamma\vdash\Delta} \not\models p$ follows.
- If $p \in \Delta$ and $p \in \mathcal{D}$, we know that the axiom rules of Figure 1 and Figure 3 do not apply, hence $p \notin \mathrm{lhs}(\mathcal{H}')$ and $w_{\Gamma\vdash\Delta} \not\models p$. ◀

## 5 Sequent calculus for a non-nested logic of overwhelming truth

In this section, we consider a fragment of modal formulas that corresponds to the propositional fragment of the logic underlying Squirrel [5]. Essentially, it is obtained by forbidding nested modalities and requiring that all atoms occur under modalities. In the style of [5], we present these restrictions by organizing formulas into *local* and *global* ones: local formulas may contain atoms but no modalities; global formulas may not contain atoms but can contain $\Box\varphi$ subformulas, under the condition that $\varphi$ is local.

▶ **Definition 26.** *We define local formulas (denoted by $\varphi, \psi$) and global formulas (denoted by $F, G$) by the following grammar:*

$$\varphi, \psi ::= \bot \mid p \mid \varphi \Rightarrow \psi \qquad F, G ::= \bot \mid \Box\varphi \mid F \Rightarrow G$$

▶ **Example 27.** The formula $\Box(p \wedge q) \Rightarrow \Box p$ is a global formula. The formula $\Box p \Rightarrow p$ is neither a local nor a global formula.

To understand why the move to global formulas is not a strong restriction, it is useful to recall the well-known fact that nested modalities do not bring extra expressiveness in S5. The next proposition, proved in Section D, states this result more precisely.

▶ **Proposition 28.** *For any modal formula $\varphi$, there exist families of* propositional *formulas $(\psi_i)_i$, $(\theta_{i,j})_{i,j}$, $(\chi_{i,j})_{i,j}$ such that $\varphi$ and the following formula are equivalent in all cryptographic structures (or, equivalently, in all clique Kripke structures):*

$$\bigwedge_{i=1}^{n} \left( \psi_i \vee \left( \bigvee_{j=1}^{l_i} \Box\chi_{i,j} \right) \vee \left( \bigvee_{k=1}^{m_i} \neg\Box\theta_{i,k} \right) \right)$$

*Moreover, if $\varphi$ is a boxed formula, then $\psi_i = \bot$ for all $i$.*

▶ **Example 29.** The formula $\Box(\Box p \Rightarrow q)$ is equivalent to the global formula $\neg\Box p \vee \Box q$.

Because the validity of $\varphi$ and that of $\Box\varphi$ are equivalent, checking the validity of arbitrary modal formulas can be reduced to checking the validity of global formulas. The catch, however, is that the transformation underlying Proposition 28 may induce an exponential

**Global rules**

$$\frac{}{\Theta, F \vdash F, \Pi} \qquad \frac{}{\Theta, \bot \vdash \Pi}$$

$$\frac{\Theta \vdash F, \Pi \quad \Theta, G \vdash \Pi}{\Theta, F \Rightarrow G \vdash \Pi} \qquad \frac{\Theta, F \vdash G, \Pi}{\Theta \vdash F \Rightarrow G, \Pi}$$

**Local rules**

$$\frac{}{\Theta; \Gamma, \varphi \vdash \varphi, \Delta} \qquad \frac{}{\Theta; \Gamma, \bot \vdash \Delta}$$

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

**Mixed rules**

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

**Figure 4** A sequent calculus for the global logic of overwhelming truth.

blowup. However, this is not a concern in the context of Squirrel, where formulas are given as local and global ones from the beginning: it appears that these fragments are natural for specifying and reasoning about cryptographic protocols.

We now present a simple sequent calculus proof system for global formulas. It involves sequents featuring several kinds of sets of formulas: we will use the letters $\Gamma$ and $\Delta$ to denote a set of *local* formulas, and the letters $\Theta$ and $\Pi$ for sets of *global* formulas.

▶ **Definition 30.** *A* global *sequent* $\Theta \vdash \Pi$ *is formed from two sets of global formulas* $\Theta$ *and* $\Pi$. *A* local *sequent* $\Theta; \Gamma \vdash \Delta$ *is formed from a set of global formulas* $\Theta$ *and two sets of local formulas* $\Gamma$ *and* $\Delta$.

▶ **Definition 31.** *The* formula interpretation *of a global sequent* $\Theta \vdash \Pi$ *is the formula* $\bigwedge_{F \in \Theta} F \Rightarrow \bigvee_{G \in \Pi} G$. *The* formula interpretation *of a local sequent* $\Theta; \Gamma \vdash \Delta$ *is:*

$$\bigwedge_{F \in \Theta} F \Rightarrow \Box \left( \bigwedge_{\varphi \in \Gamma} \varphi \Rightarrow \bigvee_{\psi \in \Delta} \psi \right)$$

The rules of our system are shown in Figure 4. The global rules are the usual rules of classical sequent calculus, and local rules are straightforward adaptations of the same rules for local sequents, occurring under the global context $\Theta$. Mixed rules articulate the two kinds of sequents. The first one allows to derive a global sequent from a local one: considering the formula interpretation of sequents, this rule is a mere weakening; its application requires to choose one formula on the right-hand side, and put it under focus by moving it to a local sequent, forgetting at this point all other formulas from the conclusion's right-hand side. The second mixed rule allows to derive a local sequent with a global hypothesis $\Box\varphi$ from a local sequent with a local hypothesis $\varphi$. Logically speaking, it is essentially the K axiom: focusing on the relevant parts of the formula interpretation of our sequents, we are deriving

$\Box\varphi \Rightarrow \Box(\Gamma \Rightarrow \Delta)$ from $\Box(\varphi \Rightarrow \Gamma \Rightarrow \Delta)$. It is worthwhile to note that the $\Box\varphi$ formula is not kept in this rule's premise. Overall, our rules do not embed any strong principles underlying S5, yet as we shall see they form a complete system for our fragment of S5.

The proof system underlying Squirrel uses global and local sequents similar to ours. One difference is that Squirrel's sequents have a single conclusion, and its proof system is given in a natural deduction style. This choice has been motivated by usability considerations: users of the Squirrel proof assistant may not be experts in logic, and might have found multiple-conclusion sequents confusing. As a consequence, Squirrel's proof system features *reductio ad absurdum* rules at both the local and global levels [5]. Beyond this common difference of style, both proof systems share an apparent weakness. As observed above, our first mixed rule is not invertible. Relatedly, Squirrel's proof system does not allow to perform a mixed *reduction ad absurdum*, shown next:

$$\frac{\Theta, \neg\Box(\Gamma \Rightarrow \varphi) \vdash \bot}{\Theta; \Gamma \vdash \varphi}$$

We do not imply that such a rule should be considered, but its absence essentially forces the same kind of strong choices in Squirrel proofs as our first mixed rule.

We now prove the key lemma explaining the completeness of our proof system.

▶ **Proposition 32.** *Let $\varphi$ and $(\psi_j)_{j\in[1;n]}$ be some propositional formulas such that $\Box\varphi \Rightarrow \vee_{j\in[1;n]}\Box\psi_j$ is valid. There exists $k \in [1;n]$ such that $\varphi \Rightarrow \psi_k$ is a propositional tautology.*

**Proof.** If $\varphi$ is propositionally unsatisfiable, $\varphi \Rightarrow \psi_k$ is a propositional tautology for any $k$, hence the result holds.

Assume now that $\varphi$ is propositionally satisfiable, and consider the clique Kripke structure $\mathcal{K}$ over the non-empty set of worlds $W = \{\ \nu : \mathcal{P} \to \{0,1\} \mid \nu \models \varphi\}$. In words, the worlds of $\mathcal{K}$ are the propositional interpretations $\nu$ that satisfy the (propositional) formula $\varphi$. We set the propositional variables satisfied by the world $\nu$ to be the ones indeed satisfied by $\nu$. It immediately follows that $\mathcal{K}, \nu \models \varphi$ for all $\nu \in W$, and thus $\mathcal{K}, \nu \models \Box\varphi$ for all $\nu \in W$.

Let $F$ be the global formula $\Box\varphi \Rightarrow \vee_{j\in[1;n]}\Box\psi_j$. Let $\nu$ be an arbitrary element of $W$. By hypothesis, $F$ is valid, hence $\mathcal{K}, \nu \models F$. Since $\mathcal{K}, \nu \models \Box\varphi$, we conclude that there exists $k$ such that $\mathcal{K}, \nu \models \Box\psi_k$. This means that $\mathcal{K}, \nu' \models \psi_k$ for all $\nu' \in W$. In other words, the propositional formula $\psi_k$ is satisfied in all propositional interpretations that satisfy $\varphi$: $\varphi \Rightarrow \psi_k$ is propositionally valid. ◀

▶ **Theorem 33.** *The rules of Figure 4 are sound and complete: a global (resp. local) sequent is derivable iff its formula interpretation is a theorem of the modal logic of overwhelming truth (or, equivalently, of S5).*

**Proof.** Soundness is easily verified; we only detail the completeness argument. We proceed by induction on the number of connectives of the sequents. Any (local or global) sequent featuring an implication formula or the $\bot$ constant at toplevel is the conclusion of one of our propositional rules. These rules are invertible and yield premises with one less logical connective, allowing to conclude by induction hypothesis.

Next, consider a valid global sequent of the form $\Box\varphi_1, \ldots, \Box\varphi_m \vdash \Box\psi_1, \ldots, \Box\psi_n$. Note that its formula interpretation is equivalent to $\Box\varphi \Rightarrow \Box\psi_1 \vee \ldots \vee \Box\psi_n$ for $\varphi = \wedge_i\varphi_i$. By Proposition 32, there exists $k$ such that $\varphi \Rightarrow \psi_k$ is a propositional tautology. Equivalently, $\cdot; \varphi_1, \ldots, \varphi_m \vdash \psi_k$ is derivable in our system using only local rules. From there we can derive our initial sequent using the first mixed rule to select $\psi_k$ and $m$ applications of the second mixed rule to transfer the $\Box\varphi_i$ global hypotheses to the local context.

A similar argument can be used to show that any valid local sequent of the form $\Box\varphi_1, \ldots, \Box\varphi_m; \Gamma \vdash \Delta$ can be derived in our system. This concludes the proof. ◀

## 6 Discussion

We have defined the modal logic of overwhelming truth, and shown that it coincides with S5, and that this result remains for several variants of the logic. Next, we have shown that Poggiolesi's CCS5$_s$ hypersequent calculus for S5 can be elegantly adapted to incorporate reasoning over determined formulas – a problem that arises naturally when carrying out formal proof involving both probabilistic and deterministic formulas. In passing, we have refined the analysis of proof-search in Poggiolesi's system, providing clean foundations for semantic proofs of completeness in that setting. Finally, considering the fragment of global formulas (that is, the propositional fragment of Squirrel's logic) we have shown that the hypersequent structure is not necessary, providing instead a sound and complete proof system based on simple (local and global) sequents. Overall, our work provides the first completeness results for logics in the CCSA line of work.

**Related works.** The idea of giving a probabilistic semantics to propositional or modal logics is not new; see e.g. [17] for a survey. For instance, [19] considers a modal logic where a threshold $t \in [0; 1]$ is chosen and $\Box\varphi$ reads as "$\varphi$ holds with probability more than $t$". With this interpretation, $(\Box\varphi \wedge \Box\psi) \Rightarrow \Box(\varphi \wedge \psi)$ is not valid, while it is in our overwhelming truth semantics. Charles G. Morgan also worked on developping a characterization of many logics in terms of conditional probabilities [23, 24]. In particular, he provided an axiomatization of conditional probability measures that is sound and complete wrt. S5. Our approach and motivation is different: we start from a concrete probabilistic semantics and seek to characterize the resulting logic in terms of modal logic axioms.

There has been much work on designing well-structured proof systems for S5, culminating but not ending with Poggiolesi's [25]. While hypersequents provide a satisfying answer to this quest, it appears that this is not possible using simple sequent calculus, at least not without making some sacrifices. We note the work of Indrzejczak [20] which proposes a simple sequent calculus for S5, which he essentially obtains by incorporating into his sequent calculus some rewrite rules that simplify modal formulas to removed nested modalities. This is related in spirit to the results of Section 5, where we propose a simple proof system for formulas that may result from such rewriting. However, our proof system does not feature more rewriting, and thus notably satisfies the subformula property. Indrzejczak's work does not seem to yield a sub-system with such properties, but it would be interesting to try to obtain such a result.

**Directions for future work.** We have only established weak completeness results, at the level of validity, and it would be interesting to investigate whether the modal logic of overwhelming truth coincides with S5 at the level of logical implications. This would yield the strong completeness for the hypersequent calculus wrt. the logic of overwhelming truth, as well as compacity for that logic.

We have used semantical arguments to establish several completeness results, refining in particular Poggiolesi's proof-search analysis to obtain semantical proofs of completeness for hypersequent calculi. It is also possible to establish the completeness of our hypersequent calculus with special axiom for determined formulas, using syntactic methods. Looking for a syntactic proof of completeness for our simple sequent calculus would also be worthwhile.

In both cases, syntactic arguments might provide results that carry over more smoothly to richer fragments, e.g. the first-order case. More generally, it would naturally be desirable to extend our results to richer fragments of the logic of overwhelming truth: one possibility is to extend our language of formulas to the first-order case; it is also possible to stick to the propositional case but incorporate the computational indistinguishability predicate of the CCSA logics. Both directions seem very challenging.

## References


1 Carmine Abate, Philipp G. Haselwarter, Exequiel Rivas, Antoine Van Muylder, Théo Winterhalter, Catalin Hritcu, Kenji Maillard, and Bas Spitters. Ssprove: A foundational framework for modular cryptographic proofs in coq. In *CSF*, pages 1–15. IEEE, 2021. doi:10.1109/CSF51468.2021.00048.

2 David Baelde, Stéphanie Delaune, Charlie Jacomme, Adrien Koutsos, and Solène Moreau. An interactive prover for protocol verification in the computational model. In *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*, pages 537–554. IEEE, 2021. doi:10.1109/SP40001.2021.00078.

3 David Baelde, Stéphanie Delaune, Adrien Koutsos, and Solène Moreau. Cracking the stateful nut: Computational proofs of stateful security protocols using the squirrel proof assistant. In *CSF*, pages 289–304. IEEE, 2022. doi:10.1109/CSF54842.2022.9919665.

4 David Baelde, Caroline Fontaine, Adrien Koutsos, Guillaume Scerri, and Théo Vignon. A Probabilistic Logic for Concrete Security. In *CSF 2024 - 37th IEEE Computer Security Foundations Symposium*, Enschede, Netherlands, July 2024. URL: https://hal.science/hal-04577828.

5 David Baelde, Adrien Koutsos, and Joseph Lallemand. A Higher-Order Indistinguishability Logic for Cryptographic Reasoning. In *LICS'23*. ACM, 2023. URL: https://inria.hal.science/hal-03981949.

6 Gergei Bana, Rohit Chadha, and Ajay Kumar Eeralla. Formal analysis of vote privacy using computationally complete symbolic attacker. In *ESORICS (2)*, volume 11099 of *Lecture Notes in Computer Science*, pages 350–372. Springer, 2018. doi:10.1007/978-3-319-98989-1_18.

7 Gergei Bana and Hubert Comon-Lundh. Towards unconditional soundness: Computationally complete symbolic attacker. In *International Conference on Principles of Security and Trust*, pages 189–208. Springer, 2012. doi:10.1007/978-3-642-28641-4_11.

8 Gergei Bana and Hubert Comon-Lundh. A computationally complete symbolic attacker for equivalence properties. In Gail-Joon Ahn, Moti Yung, and Ninghui Li, editors, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*, pages 609–620. ACM, 2014. doi:10.1145/2660267.2660276.

9 Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno. Sok: Computer-aided cryptography. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 777–795, 2021. doi:10.1109/SP40001.2021.00008.

10 Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, and Santiago Zanella Béguelin. Computer-aided security proofs for the working cryptographer. In *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 71–90. Springer, 2011. doi:10.1007/978-3-642-22792-9_5.

11 David A. Basin, Andreas Lochbihler, and S. Reza Sefidgar. Crypthol: Game-based proofs in higher-order logic. *J. Cryptol.*, 33(2):494–566, 2020. doi:10.1007/S00145-019-09341-Z.

12 Patrick Blackburn, Maarten De Rijke, and Yde Venema. *Modal logic*, volume 53. Cambridge University Press, 2001. doi:10.1017/CBO9781107050884.

13 Bruno Blanchet, Martín Abadi, and Cédric Fournet. Automated verification of selected equivalences for security protocols. *The Journal of Logic and Algebraic Programming*, 75(1):3–51, 2008. doi:10.1016/J.JLAP.2007.06.002.

14 Hubert Comon and Adrien Koutsos. Formal computational unlinkability proofs of RFID protocols. In *CSF*, pages 100–114. IEEE Computer Society, 2017. doi:10.1109/CSF.2017.9.

15 Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. Tractable inference systems: An extension with a deducibility predicate. In Maria Paola Bonacina, editor, *Automated Deduction - CADE-24 - 24th International Conference on Automated Deduction, Lake Placid, NY, USA, June 9-14, 2013. Proceedings*, volume 7898 of *Lecture Notes in Computer Science*, pages 91–108. Springer, 2013. doi:10.1007/978-3-642-38574-2_6.

16 Cas Cremers, Caroline Fontaine, and Charlie Jacomme. A logic and an interactive prover for the computational post-quantum security of protocols. In *SP*, pages 125–141. IEEE, 2022. doi:10.1109/SP46214.2022.9833800.

17 Lorenz Demey, Barteld Kooi, and Joshua Sack. Logic and Probability. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, summer 2019 edition, 2019. URL: https://plato.stanford.edu/archives/sum2019/entries/logic-probability/.

18 Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984. doi:10.1016/0022-0000(84)90070-9.

19 Charles L Hamblin. The modal" probably". *Mind*, 68(270):234–240, 1959.

20 Andrzej Indrzejczak. Simple Decision Procedure for S5 in Standard Cut-Free Sequent Calculus. *Bulletin of the Section of Logic*, 45(2), June 2016. doi:10.18778/0138-0680.45.2.05.

21 Adrien Koutsos. The 5G-AKA authentication protocol privacy. In *EuroS&P*, pages 464–479. IEEE, 2019. doi:10.1109/EUROSP.2019.00041.

22 Adrien Koutsos. Decidability of a sound set of inference rules for computational indistinguishability. In *32nd IEEE Computer Security Foundations Symposium, CSF 2019, Hoboken, NJ, USA, June 25-28, 2019*, pages 48–61. IEEE, 2019. doi:10.1109/CSF.2019.00011.

23 Charles G. Morgan. Simple Probabilistic Semantics for Propositional K, T, B, S4, and S5. *Journal of Philosophical Logic*, 11(4):443–458, 1982. URL: https://www.jstor.org/stable/30226261, doi:10.1007/BF00284979.

24 Charles G. Morgan. There Is a Probabilistic Semantics for Every Extension of Classical Sentence Logic. *Journal of Philosophical Logic*, 11(4):431–442, 1982. URL: https://www.jstor.org/stable/30226260, doi:10.1007/BF00284978.

25 Francesca Poggiolesi. A cut-free simple sequent calculus for modal logic S5. *The Review of Symbolic Logic*, 1(1):3–15, 2008. doi:10.1017/S1755020308080040.

26 Guillaume Scerri and Ryan Stanley-Oakes. Analysis of key wrapping apis: Generic policies, computational security. In *CSF*, pages 281–295. IEEE Computer Society, 2016. doi:10.1109/CSF.2016.27.

27 Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *cryptology eprint archive*, 2004.


## A Proofs of Section 2

▶ **Proposition 7.** *The abstract logic of overwhelming truth is a* normal modal logic*: its theorems are closed under substitution and* modus ponens*; they contain classical tautologies and the K axiom* $\Box(p \Rightarrow q) \Rightarrow \Box p \Rightarrow \Box q$*; moreover,* $\Box\varphi$ *is a theorem whenever* $\varphi$ *is.*

**Proof.** It is clear, by definition of our semantics, that the set of theorems of our logic is closed under substitution. It is also obvious that the validity of $\varphi$ entails that of $\Box\varphi$.

Next, we verify that any classical tautology $\varphi$ is a theorem of our logic. For any $\mathcal{S}$, $\eta$ and $\rho \in X_\eta^{\mathcal{S}}$, notice that $[\![\varphi]\!]_{\mathcal{S}}(\eta,\rho)$ only relies on the interpretation of its subformulas for the same values of $\eta$ and $\rho$. In other words, $[\![\varphi]\!]_{\mathcal{S}}(\eta,\rho)$ can be seen as the classical interpretation of $\varphi$ in the boolean structure $\mathcal{S}(\eta,\rho)$ defined by $p^{\mathcal{S}(\eta,\rho)} = p^{\mathcal{S}}(\eta,\rho)$. Because $\varphi$ is a tautology, we thus have $[\![\varphi]\!]_{\mathcal{S}} = \mathbf{1}$, hence $[\![\varphi]\!]_{\mathcal{S}}$ is overwhelming in any $\mathcal{S}$.

The K axiom is valid: indeed, if both $[\![p \Rightarrow q]\!]_{\mathcal{S}}$ and $[\![p]\!]_{\mathcal{S}}$ are overwhelming in a structure $\mathcal{S}$, then so is $[\![q]\!]_{\mathcal{S}}$ because $\Pr([\![q]\!]_{\mathcal{S}} = 0) \leq \Pr([\![p \Rightarrow q]\!]_{\mathcal{S}} = 0) + \Pr([\![p]\!]_{\mathcal{S}} = 0)$ and the sum of negligible functions is negligible. By the same argument, theorems are closed under modus ponens. ◀

## B Proofs of Section 3

▶ **Lemma 11.** *All S5 theorems are theorems of the modal logics of overwhelming truth.*

**Proof.** Since modal logics of overwhelming truth are normal, it suffices to check that the three axioms defining S5 are valid wrt. arbitrary cryptographic structures.

- Axiom 4 is obvious, as $[\![\Box p]\!]_{\mathcal{S}} = [\![\Box\Box p]\!]_{\mathcal{S}}$ for all $\mathcal{S}$.
- For axiom T, consider an arbitrary $\mathcal{S}$, and proceed by case analysis on whether $[\![p]\!]_{\mathcal{S}}$ is overwhelming. If this is the case, then $[\![\Box p]\!]_{\mathcal{S}} = 1$ thus $[\![\Box p \Rightarrow p]\!]_{\mathcal{S}} = [\![p]\!]_{\mathcal{S}}$, which is overwhelming by hypothesis. Otherwise, $[\![\Box p]\!]_{\mathcal{S}} = 0$ and $[\![\Box p \Rightarrow p]\!]_{\mathcal{S}} = 1$ is overwhelming.
- For axiom 5, note that $[\![\Diamond\varphi]\!]_{\mathcal{S}} = 1$ when $[\![\varphi]\!]$ is non-negligible, and 0 otherwise – in both cases, $[\![\Diamond\varphi]\!]_{\mathcal{S}}(\eta, \rho) = [\![\Diamond\varphi]\!]_{\mathcal{S}}(\eta', \rho')$ for all $\eta, \rho, \eta', \rho'$. Thus $[\![\Box\Diamond p]\!]_{\mathcal{S}} = [\![\Diamond p]\!]_{\mathcal{S}}$, hence the result. ◀

▶ **Proposition 15.** *For any modal formula $\varphi$, the following conditions are equivalent:*

1. *$\varphi$ is a theorem of S5;*
2. *$\varphi$ is valid wrt. equivalence frames;*
3. *$\varphi$ is valid wrt. clique frames.*
4. *$\varphi$ is valid wrt. finite clique frames.*

**Proof sketch.** The equivalence between (1) and (2) is a classic result [12]. Equivalence between (2) and (3) is an easy observation: for any equivalence structure $\mathcal{K}$ and $w \in W^{\mathcal{K}}$, let $\mathcal{K}_w$ be the (clique) substructure corresponding to the equivalence class of $w$ in $\mathcal{K}$; it is easy to see that, for any $\varphi$, $\mathcal{K}, w \models \varphi$ is equivalent to $\mathcal{K}_w, w \models \varphi$. Finally, the equivalence between (3) and (4) is obtained by using the filtration technique [12]: given any initial formula $\varphi$, it allows to extract from a clique structure $\mathcal{K}$ a finite clique structure $\mathcal{K}'$ whose worlds are equivalence classes of worlds of $\mathcal{K}$, such that $\mathcal{K}, w \models \psi$ is equivalent to $\mathcal{K}', [w] \models \psi$ for any subformula $\psi$ of $\varphi$. ◀

## C Proofs of Section 4

▶ **Proposition 22.** *The rules of Figure 1 are invertible.*

**Proof.** We prove the contrapositive: assuming a counter-model of a premise $\mathcal{H}'$ of some rule instance, we build a counter-model of the conclusion $\mathcal{H}$. This is immediate for all rules except the right modal rule. We thus consider the case where $\mathcal{H}$ is of the form $\mathcal{H}_0 \mid \Gamma \vdash \Box\varphi, \Delta$ and $\mathcal{H}'$ is of the form $\mathcal{H}_0 \mid \Gamma \vdash \Box\varphi, \Delta \mid \cdot \vdash \varphi$. By hypothesis, we have a counter-model of $\mathcal{H}$, that is a Kripke structure $\mathcal{K}$ with worlds $\vec{w}$ falsifying the sequents of $\mathcal{H}_0$, and a world $w'$ falsifying $\Gamma \vdash \Box\varphi, \Delta$. In particular, $w' \not\models \Box\varphi$, hence there exists $w''$ such that $w'' \not\models \varphi$. Thus, $\mathcal{K}$, together with the worlds $\vec{w}, w'$ and $w''$, provide a counter-model for $\mathcal{H}'$. ◀

## D Proofs of Section 5

▶ **Lemma 34.** *Let $\varphi$ and $\psi$ be any modal formulas. Then for Kripke equivalence models:*

1. $\Box(\varphi \wedge \psi) \equiv \Box\varphi \wedge \Box\psi$,
2. $\Box(\varphi \vee \Box\psi) \equiv \Box\varphi \vee \Box\psi$,
3. $\Box(\varphi \vee \neg\Box\psi) \equiv \Box\varphi \vee \neg\Box\psi$

**Proof.** Let $\mathcal{S} = (W, R, V)$ be an equivalence Kripke model, $w \in W$.

1. By definition, $(\mathcal{S}, w) \models \Box(\varphi \wedge \psi)$ iff for all successor $v$ of $w$ by $R$, $(\mathcal{S}, v) \models \varphi \wedge \psi$ iff $(\mathcal{S}, v) \models \varphi$ and $(\mathcal{S}, v) \models \psi$.
   This is the case if and only if for all successor $v$ of $w$ by $R$, $(\mathcal{S}, v) \models \varphi$ and for all successor $u$, $(\mathcal{S}, u) \models \psi$, i.e. $(\mathcal{S}, w) \models \Box\varphi$ and $(\mathcal{S}, w) \models \Box\psi$, i.e. $(\mathcal{S}, w) \models \Box\varphi \wedge \Box\psi$, which concludes the proof.
2. Assume $(\mathcal{S}, w) \models \Box(\varphi \vee \Box\psi)$. Then for all successor $v$ of $w$ by $R$, $(\mathcal{S}, v) \models \varphi \vee \Box\psi$. Then there are two cases:
   - Either for all successor $v$ of $w$ by $R$, $(\mathcal{S}, v) \models \varphi$. In this case $(\mathcal{S}, w) \models \Box\varphi$.
   - Either there is a successor $v$ of $w$ by $R$ such that $(\mathcal{S}, v) \not\models \varphi$. In this case, $(\mathcal{S}, v) \models \Box\psi$. Let $u$ be a successor of $w$ for $R$. Then since $R$ is an equivalence relation, $u$ is also a successor of $v$ and $(\mathcal{S}, u) \models \psi$.
     Since this holds for all successors of $w$, $(\mathcal{S}, w) \models \Box\psi$.

   Now for the converse, assume $(\mathcal{S}, w) \models \Box\varphi \vee \Box\psi$. Since $R$ is transitive, $(\mathcal{S}, w) \models \Box\varphi \vee \Box\Box\psi$. It is easy to check next that $(\mathcal{S}, w) \models \Box(\varphi \vee \Box\psi)$.
3. The proof in this case is very similar to the previous one, except in the proof of the converse. We have to use the transitivity as well as the symmetry of $R$ to prove that $(\mathcal{S}, w) \models \Box\varphi \vee \neg\Box\psi$ implies $(\mathcal{S}, w) \models \Box\varphi \vee \Box\neg\Box\psi$. ◀

**Proof of Proposition 28.** We proceed by induction on $\varphi$, considering for this proof that the elementary propositional connectives are negation and conjunction. The case of propositional variables and the inductive case of conjunctions are clear using equivalence 1 of the previous lemma.

- **Case $\varphi = \neg\varphi'$**
  By induction hypothesis on $\varphi'$ and using De Morgan's laws, we know that there are families of propositional formulas $(\psi_i), (\chi_{i,j}), (\theta_{i,j})$ such that

$$\varphi \equiv \bigvee_{i=1}^{n} \left( \neg\psi_i \wedge \left( \bigwedge_{j=1}^{l_i} \neg\Box\chi_{i,j} \right) \wedge \left( \bigwedge_{k=1}^{m_i} \Box\theta_{i,k} \right) \right).$$

  Then, by distributivity of disjunction over conjunction, there is an integer $N$ such that

$$\varphi \equiv \bigwedge_{i=1}^{N} (\omega_{i,1} \vee \cdots \vee \omega_{i,h_i})$$

  where each $\omega_{i,j}$ is either a $\neg\psi_{i'}$, a $\Box\theta_{i',k'}$ or a $\neg\Box\chi_{i',j'}$.
  Finally by grouping for each $i$ the $\neg\psi_{i'}$ into a single propositional formula, the $\Box\theta_{i',k'}$ together and the $\neg\Box\chi_{i',j'}$, we prove $\varphi$ is equivalent to a formula having the desired shape.
- **Case $\varphi = \Box\varphi'$**
  By induction hypothesis on $\varphi'$ and using the first equivalence in the previous lemma, we know there are families of propositional formulas $(\psi_i), (\chi_{i,j}), (\theta_{i,j})$ such that

$$\varphi \equiv \bigwedge_{i=1}^{n} \Box \left( \psi_i \vee \left( \bigvee_{j=1}^{l_i} \Box\chi_{i,j} \right) \vee \left( \bigvee_{k=1}^{m_i} \neg\Box\theta_{i,k} \right) \right).$$

  Then, applying equivalences 2 and 3 of the previous lemma on each one of the $\Box\chi_{i,j}$ and $\neg\Box\theta_{i,k}$, we have that

$$\varphi \equiv \bigwedge_{i=1}^{n} \left( \Box\psi_i \vee \left( \bigvee_{j=1}^{l_i} \Box\chi_{i,j} \right) \vee \left( \bigvee_{k=1}^{m_i} \neg\Box\theta_{i,k} \right) \right)$$

  which is what we wanted since for all $i$, the $\Box\psi_i$ can be grouped with the $\Box\chi_{i,j}$. ◀