Semantics for "Enough-Certainty" and Fitting's Embedding of Classical Logic in S4

Gergei Bana[*1] **and Mitsuhiro Okada**[†2]

1 **INRIA de Paris, Paris, France**
bana@math.upenn.edu
2 **Department of Philosophy, Keio University, Tokyo, Japan**
mitsu@abelard.flet.keio.ac.jp

Abstract

In this work we look at how Fitting's embedding of first-order classical logic into first-order S4 can help in reasoning when we are interested in satisfaction "in most cases", when first-order properties are allowed to fail in cases that are considered insignificant. We extend classical semantics by combining a Kripke-style model construction of "significant" events as possible worlds with the forcing-Fitting-style semantics construction by embedding classical logic into S4. We provide various examples. Our main running example is an application to symbolic security protocol verification with complexity-theoretic guarantees. In particular, we show how Fitting's embedding emerges entirely naturally when verifying trace properties in computer security.

1998 ACM Subject Classification F.3.1 Logics and Meanings of Programs

Keywords and phrases first-order logic, possible-world semantics, Fitting embedding, asymptotic probabilities, verification of complexity-theoretic properties

Digital Object Identifier 10.4230/LIPIcs.CSL.2016.34

1 Introduction

Recently Bana and Comon in [3] – with others in followup papers [1, 4] – used a non-Tarskian semantics for first-order logic to formalize security properties of cryptographic primitives and of protocols, and to deduce the latter from the former with first-order deduction rules. By "non-Tarskian" we mean that disjunction, negation, and the existential quantifier were interpreted in a way different from usual, but nevertheless first-order deduction rules turned out to be sound for this interpretation. The non-Tarskian semantics emerged entirely naturally while they were trying to define what it means that a probabilistic polynomial-time attacker can compute a secret, what it means that it can either compute something (on certain random inputs) *or* something else (on other random inputs), and so on. Once they verified directly that despite the non-standard semantics first-order deduction rules hold, they realized that there might be some more general logical idea behind their result. And indeed, the result turned out (see [4]) to be a special case of Fitting's embedding of classical logic in S4 [7]. Fitting's embedding consists of applying $\Box\Diamond$ recursively on each sub-formula of a first-order formula. The resulting formula is deducible in first-order S4 if and only if the original is deducible in classical first-order logic. A non-Tarskian semantics to first-order

* Partially supported by ERC Consolidator Grant CIRCUS (683032).
† Partially supported by MEXT-Grant-in-Aid for Scientific Research on Innovative Areas (Grant number 23120002) and MEXT-JSPS Grant-in-Aid for Scientific Research (B) (Grant number 26284005). Also partially supported by the Next Generation Research Project Promotion Program of Keio University.

logic is obtained by composing Fitting's embedding with a standard Kripke-semantics to first-order S4, and such is the one given by Bana and Comon. Fitting's work is in turn closely related to Cohen's forcing [5], as Fitting and Smullyan stated in [7, 15]. Forcing, and Fitting's technique allow to generate new models for first-order logic from given ones. The idea of generating new models is used in a special way in computer security: namely, generating attacker models for security protocols that are executable for probabilistic polynomial-time attackers. In this paper, we shall call a model that is generated by Fitting's embedding, a Fitting-twisted model.

The aim of this paper is to look (in a self-contained manner) at what aspects of the computability model considered in [3] are essential for the Fitting embedding to rise naturally, and explore a more general contexts in which the use of Fitting-twisted models may be the most suitable. One such aspect is the need for the following non-standard interpretation of disjunction and negation (and hence classical implication): Roughly speaking, imagine that there is a set W on which satisfaction $w \models \phi$ of first-order formulas is defined for each $w \in W$, when quantification runs over a single domain (variables in ϕ are interpreted over some domain $\mathcal{D}_w$ as usual in first-order logic, and we take $\mathcal{D}_w$ to be the same $\mathcal{D}$ for all $w \in W$)[1]. From this we want to define another satisfaction $W \models' \phi$ of the same first-order formulas. Instead of defining the satisfaction of a disjunction on W as usual so that either one of the disjuncts or the other is satisfied on W, it may be more natural (for example, as in case of the team semantics in [16]) to require that W can be split in two parts, on one of which one of the disjuncts is satisfied, and on the other, the other disjunct: $W \models' \phi_1 \vee \phi_2$ iff $W = W_1 \cup W_2$ and for both $i = 1, 2$, for all $w \in W_i$, $w \models \phi_i$. Negation on the other hand can mean that the negated predicate holds nowhere: $W \models' \neg\phi$ iff for all $w \in W$, $w \not\models \phi$. Then the first-order material implication $\phi \to \psi \equiv \neg\phi \vee \psi$ turns out to mean under $\models'$ that on the part where ϕ holds, ψ also must hold. This in itself would not require Fitting embedding, only an embedding of classical logic in S5 by applying $\Box$ recursively on each sub-formula (as touched upon in [7]) as $W \models' \phi$ would just mean $W \models' \phi$ if and only if $w \models \phi$ for all $w \in W$. The other aspect of computability in [3] that warrants the need for the Fitting-embedding to appear is the importance of random sets with "non-negligible" probabilities. Non-negligible sets can be looked at as generalized non-zero-measure sets. In computing, just as in measure theory, we are often not interested in what happens on negligible or measure-zero sets. So there is a notion of "significant" sets and "insignificant" sets, and we are only interested in what happens up to an error of insignificant sets. On insignificant sets, anything is allowed. When looking at implication, we do not want to mean that whenever the premise holds, the conclusion also holds, but we only want to mean that whenever the premise holds on a significant set, the conclusion also holds there with at most insignificant error. This makes it necessary to switch from W as the set of possible worlds to the significant sets of W as possible worlds, on which now we have a transitive accessibility relation: inclusion. This creates an S4 Kripke-model situation, leaving the S5 model.

In fact, in the case of computability, there is a further aspect that makes taking non-negligible sets to be the possible worlds necessary: There are important properties the satisfaction of which cannot be considered pointwise by $\models$ on W, but only on non-negligible sets. (This is similar to that in probability theory, conditionalization only makes sense on sets with non-zero measure. Or, in function analysis, differentiability only makes sense on open sets.) A single bit string is always computable from another bit string. However, when we talk about distributions of bit strings parametrized by some size, then we can

[1] This is sufficient for us, but Fitting's theorem works for varying domains as well.

ask if there exist algorithms within some complexity class that compute one parametrized distribution from another on a set that has non-negligible probability. The satisfaction of this property cannot be considered under $w \models$. This aspect reinforces the necessity to distinguish significant and insignificant sets.

Besides the applicability of the Fitting-embedding to the situation when we are interested in satisfaction of first-order properties on significant sets only, there may be another important aspect of this connection going in the other direction, from deduction system to semantics. This significant sets construction is also an extension of standard first-order Tarski semantics, just as the Fitting twist, and forcing. But it is less general, more concrete, and hence perhaps more intuitive. One wonders, can this significant sets construction be directly used for model construction in first-order logic to investigate consistency of formulas, other than for finding attacks to protocols, in situations more important for logic itself. We do not have such examples yet.

In Section 2 and 3 we motivate and build up the Fitting-twisted semantics. In this, we shall keep in mind the application to computer security, but we shall also consider other examples, conditional implication, and the ϵ-semantics of "typically" [11, 8]. In Section 4 we shall explain the connection with Fitting's embedding, and mention when and how first-order deduction is sound in the concrete examples of conditional implication and computer security.

2 Semantics for Enough-Certainty

Suppose that we have a set of possible worlds W. Suppose also that we are interested in first-order statements the terms of which are interpreted in a domain $\mathcal{D}$ and the satisfaction of its predicates are defined for all $w \in W$ with the single domain $\mathcal{D}$. Hence satisfaction of first-order formulas is defined for all $w \in W$ in the usual way. Now suppose also that we are interested in the satisfaction of the same formulas over subsets of W allowing some possible insignificant error. Think for example of measure theory: Measure zero sets are considered insignificant. Equality of functions over this measure space can be considered at each point, but it can also be considered over sets of the measure space, "almost everywhere", that is, except for a measure-zero set. We shall see more complex examples later. Motivated by this simple measure-theoretic example, we also allow sets of possible worlds for which we cannot tell if it is significant or insignificant.

Accordingly, consider the following definitions:

▶ **Definition 1.** Let W be a set, $\Sigma \subseteq 2^W$ be a σ-algebra, and let Σ_i be a non-trivial ideal of Σ, namely:

- if $S \in \Sigma_\mathrm{i}$, and $S' \in \Sigma$, and $S' \subseteq S$, then $S' \in \Sigma_\mathrm{i}$;
- if $S \in \Sigma_\mathrm{i}$, and $S' \in \Sigma_\mathrm{i}$, then then $S \cup S' \in \Sigma_\mathrm{i}$;
- $\Sigma_\mathrm{i} \neq \Sigma$.

We call Σ_i the set of insignificant sets and we call $\Sigma_\mathrm{s} := \Sigma \setminus \Sigma_\mathrm{i}$ the set of significant sets. We shall refer to elements of Σ as events. If the complement of S, $S^\perp \in \Sigma_\mathrm{i}$, then we call S a certain enough set. Note, the set of certain enough sets is the filter complementary to Σ_i.

We shall also use the term insignificant set implicitly meaning that it is an insignificant event. In other words, sub-events of insignificant events (sets) are insignificant, this is a rather obvious condition. It is also rather obvious that the full space W should be significant, that is, $\Sigma_\mathrm{i} \neq \Sigma$ should be required, otherwise we have nothing significant. We also assume that the union of two insignificant events are also insignificant; this is just an assumption that insignificant sets are indeed insignificant enough not to turn into significant ones so easily as taking finite unions.

To see more complex examples of insignificant sets than the measure zero sets, consider the following definitions.

Let $\mathbb{R}^+$ denote the non-negative real numbers. Let $\mathcal{C}$ be a convergence class in the following sense:

▶ **Definition 2** (Convergence Class)**.** We call $\mathcal{C}$, a set of $\mathbb{N} \to \mathbb{R}^+$ sequences a *convergence class*, if

- for each $s \in \mathcal{C}$, all subsequences of s are also in $\mathcal{C}$,
- for all $s \in \mathcal{C}$, $\lim_{i\to\infty} s_i = 0$;
- if $s \in \mathcal{C}$, and $s' : \mathbb{N} \to \mathbb{R}^+$, and for all $i \in \mathbb{N}$, $s'_i \leq s_i$, then $s' \in \mathcal{C}$;
- if $s, s' \in \mathcal{C}$, then $s + s' \in \mathcal{C}$.

Note that $\mathcal{C}$ is an ideal of sequences of the form $\mathbb{N} \to \mathbb{R}^+$ if the partial order $\leq$ on the set of such sequences is defined to hold if all elements of the sequence on the left are less than or equal to the corresponding elements of the sequence on the right. Note also, these conditions imply that if $s \in \mathcal{C}$, and $r \in \mathbb{R}^+$, then $r \cdot s \in \mathcal{C}$, because $r \leq n$ for some n natural, and then $r \cdot s \leq n \cdot s = s + \ldots + s$.

$\mathcal{C}$ can be for example the set of all positive sequences converging to 0, or the set of sequences super-polynomially converging to 0, and so on. In this latter case, the elements of $\mathcal{C}$ are called *negligible functions*. We shall define them later precisely.

▶ **Definition 3** (Parametric Probability Space)**.** Let Ω be a set of elementary events with $\Sigma \subseteq 2^\Omega$ a σ-algebra on Ω. For each $i \in \mathbb{N}$, let P_i be a (σ-additive) probability measure on Σ, and let $\mathcal{P}$ denote the sequence $(P_i)_{i\in\mathbb{N}}$. We call $(\Omega, \Sigma, \mathcal{P})$ a parametric probability space.

▶ **Definition 4** ($\mathcal{C}$-Asymptotically Possible/Impossible/Certain Sets)**.** Let $\mathcal{C}$ be a convergence class, and let $(\Omega, \Sigma, \mathcal{P})$ be a parametric probability space. We call a set $S \in \Sigma$ a $\mathcal{C}$-asymptotically possible set if $(P_i(S))_{i\in\mathbb{N}} \notin \mathcal{C}$ and we call it a $\mathcal{C}$-asymptotically impossible set if the sequence $(P_i(S))_{i\in\mathbb{N}} \in \mathcal{C}$. Let $\mathcal{S}_{\mathcal{C}\text{-p}}$ denote the set of $\mathcal{C}$-asymptotically possible elements of Σ, and let $\mathcal{S}_{\mathcal{C}\text{-i}}$ denote the set of $\mathcal{C}$-asymptotically impossible elements of Σ. We call a set S $\mathcal{C}$-asymptotically certain if its complement, $S^\perp$ is $\mathcal{C}$-asymptotically impossible, that is, if $(1 - P_i(S))_{i\in\mathbb{N}} \in \mathcal{C}$.

Clearly, a $\mathcal{C}$-asymptotically impossible set is a special insignificant set, a $\mathcal{C}$-asymptotically possible set is a significant set and a $\mathcal{C}$-asymptotically certain set is a certain enough set.

▶ **Example 5.** The simplest examples of parametric probability spaces are when all P_i coincide. In that case there is only one probability, and it can only converge to 0 if it is 0. Accordingly, in that special case, the asymptotically impossible sets are the measure zero sets, the asymptotically certain sets are the sets with measure 1. ◀

▶ **Example 6.** We can imagine the sequence of probability distributions $P_1, P_2, \ldots$ as change corresponding to time. For example, when one considers a Markov chain. In that case, a $\mathcal{C}$-asymptotically impossible set is one for which the probability goes to 0 in a way characterized by $\mathcal{C}$ as time progresses. ◀

▶ **Example 7.** The example which we elaborate mostly in this paper is when the sequence $P_1, P_2, \ldots$ corresponds to some size parameter. This is the case for the mathematical formalization of hardness assumptions such as the discrete logarithm problem, Diffie-Hellman problem etc. In this case, we consider $\{0,1\}^*$ with Σ_0 the σ-algebra generated by those sets for which the first n bits are fixed. For example, elements of the form 01001ω where

$\omega \in \{0,1\}^*$ make up such a set, with $n = 5$. Let P^c be the probability distribution that gives $1/2^n$ on such sets: fair coin tosses. Let

$$\Omega^c := \mathbb{N} \times \{0,1\}^*$$

with the product σ-algebra Σ^c (where $2^{\mathbb{N}}$ is taken on $\mathbb{N}$ and Σ_0 on $\{0,1\}^*$). That is, Σ^c is generated by sets of the form $S_1 \times S_2$ where $S_1 \in 2^{\mathbb{N}}$ and $S_2 \in \Sigma_0$. Clearly, each $S \in \Sigma^c$, can be written as

$$S = \bigcup_{i=0}^{\infty} \{i\} \times S_i$$

for some $S_i \in \Sigma_0$. We define $\mathcal{P}^c = (P_i^c)_{i\in\mathbb{N}}$ such that for all $S = \bigcup_{i=0}^{\infty}\{i\} \times S_i$,

$$P_i^c(S) := P^c(S_i).$$

That is, $P_i^c(S)$ gives the probability of the i'th section of S according to P^c. Let $\mathcal{C}^c$ denote the set of those sequences that go to 0 faster than the inverse of any polynomial: for each $s \in \mathcal{C}^c$ and $n \in \mathbb{N}$, there is an $i \in \mathbb{N}$ such that for all $j \in \mathbb{N}$ with $j \geq i$, we have $s_j \leq 1/j^n$. Then the $\mathcal{C}^c$-asymptotically impossible elements of Σ_{i}^c are called *negligible events* (or sets with negligible probability) in the literature and $\mathcal{C}^c$-asymptotically possible sets in Σ_{s}^c are called *non-negligible*.

▶ **Example 8.** Another example comes from natural language, to interpret the meaning of "typically". For example, "Typically birds can fly". Sequences of probability distributions were used for example in [11, 8] for giving semantics to such statements (ϵ-semantics). In this case, $\mathcal{C}$ contains all sequences converging to 0. Something typically holds, if it holds outside an asymptotically impossible set.

Consider now the first-order signature $(\mathfrak{f}, \mathfrak{p})$ with $\mathfrak{f}$ a set of function symbols and $\mathfrak{p}$ a set of predicates. Let $A_{(\mathfrak{f},\mathfrak{p})}$ denote the atomic formulas built on $(\mathfrak{f}, \mathfrak{p})$ with some countable set of variables. Let $\Phi_{(\mathfrak{f},\mathfrak{p})}$ denote the first order formulas built on $(\mathfrak{f}, \mathfrak{p})$ with the same countable set of variables. Let $\mathcal{D}$ be a domain of interpretation, that is, terms are interpreted as elements of $\mathcal{D}$, and predicates are interpreted as relations on $\mathcal{D}$. Let W be a set of possible worlds with the fixed domain $\mathcal{D}$; each $w \in W$ defines an interpretation of the function symbols and the predicates on $\mathcal{D}$. Let $\mathcal{V}$ denote the set of valuations of variables in $\mathcal{D}$. Then a relation $\models$ is defined on $\mathcal{V} \times W \times \Phi$ the standard first-order way; for all $V \in \mathcal{V}$, $w \in W$, and $\phi \in \Phi_{(\mathfrak{f},\mathfrak{p})}$, either $V, w \models \phi$ or $V, w \not\models \phi$.

In the following, we shall also assume that a σ-algebra Σ and a set of insignificant events Σ_{i} and hence significant events Σ_{s} are also defined on W. Let us call such a $(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \mathfrak{f}, \mathfrak{p}, \models)$ a *possible world model with significant events*.

Coming back to our question at the beginning of this section, using the possible-world-wise satisfaction $w \models \phi$, how should we define $W \models' \phi$? Or, more generally, how should we define $S \models' \phi$ for a set $S \in \Sigma$ and $\phi \in \Phi_{(\mathfrak{f},\mathfrak{p})}$ using the pointwise satisfaction $w \models \phi$? One obvious answer is the following.

▶ **Definition 9** (Absolute Certainty Semantics)**.** Let $(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \mathfrak{f}, \mathfrak{p}, \models)$ be a possible world model with significant events. Let $\mathcal{V}$ denote the set of valuations of variables in $\mathcal{D}$. We can define the relation $\models_{\mathrm{AC}}$ on $\mathcal{V} \times \Sigma \times A_{(\mathfrak{f},\mathfrak{p})}$:

$$V, S \models_{\mathrm{AC}} \phi \quad \Leftrightarrow \quad \forall w \in S.\ (V, w \models \phi)\,.$$

Then $\models_{\mathrm{AC}}$ can be extended to $\mathcal{V} \times \Sigma \times \Phi_{(\mathfrak{f},\mathfrak{p})}$ as usual for first-order semantics. We call this *absolute certainty semantics* of the first-order formulas as satisfaction is required everywhere on S.

Here, and in what follows we use bold face $\forall$, $\exists$, $\wedge$, $\vee$, $\neg$ for meta expressions, while we use the standard ones for our first order formulas.

But in this work, we shall not care what happens on insignificant sets. Just as in measure theory, one does not care what happens on 0-measure sets, and in complexity theory we do not care what happens on negligible sets. We only care about properties satisfied up to an error of insignificant set. Then it makes sense to define the following satisfaction for any $S \in \Sigma_{\mathrm{s}}$.

▶ **Definition 10** (Enough-Certainty Semantics)**.** Let $(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \mathfrak{f}, \mathfrak{p}, \models)$ be a possible world model with significant events. Let $\mathcal{V}$ denote the set of valuations of variables in $\mathcal{D}$. We can define the relation $\models_{\mathrm{EC}}$ on $\mathcal{V} \times \Sigma_{\mathrm{s}} \times A_{(\mathfrak{f},\mathfrak{p})}$:

$$V, S \models_{\mathrm{EC}} \phi \quad \Leftrightarrow \quad \exists S' \in \Sigma_{\mathrm{s}}.\ (S' \subseteq S \ \ \wedge \ \ S \setminus S' \in \Sigma_{\mathrm{i}} \ \ \wedge \ \ V, S' \models_{\mathrm{AC}} \phi)\,.$$

Again, $\models_{\mathrm{EC}}$ can be extended to $\mathcal{V} \times \Sigma_{\mathrm{s}} \times \Phi_{(\mathfrak{f},\mathfrak{p})}$ as usual for first-order semantics. We call this *enough-certainty semantics* of the first-order formulas as satisfaction is required up to an error of an insignificant subset $S \setminus S'$ of S.

▶ **Example 11.** Given a parametrized probability space $(\Omega, \Sigma, \mathcal{P})$, let the $\mathcal{C}$-asymptotically impossible sets be the insignificant sets. For two random variables $X, Y : \Omega \to \mathbb{R}$, for each ω, we can define $\omega \models X = Y$ iff $X(\omega) = Y(\omega)$. Similarly, we can define $\omega \models X \leq Y$ iff $X(\omega) \leq Y(\omega)$. According to the above definition, $\Omega \models_{\mathrm{AC}} X = Y$ iff $X(\omega) = Y(\omega)$ for all ω. Similarly for $\leq$. Also, $\Omega \models_{\mathrm{EC}} X = Y$ if $X(\omega) = Y(\omega)$ for all ω except possibly on a $\mathcal{C}$-asymptotically impossible set. Moreover, for other two random variables $U, W : \Omega \to \mathbb{R}$, we have that $\Omega \models_{\mathrm{AC}} X = Y \vee U = W$ if either $X = Y$ on all of Ω, or $U = W$ on all of Ω.

Now this may not be the best definition on a probability field. When we say that either $X = Y$ or $U = W$, we might want to mean that on a part of Ω (that is, for certain randomness) $X = Y$ holds, and on its complement $U = W$ holds, not necessarily one of them everywhere. The same can be said about $\models_{\mathrm{EC}}$ up to a $\mathcal{C}$-asymptotically impossible sets.

▶ **Example 12.** Coming back to Example 8, the semantics of "typically, birds can fly or birds are sick" should not be the same as "typically birds can fly or typically birds are sick". Similarly, "typically monkeys do not fly" is not the same as "it is not true that typically monkeys fly". The latter would allow monkeys to fly often enough, maybe in 1/3 of the cases, but not typically. The former only allows monkeys to fly very rarely. On the other hand, "typically, birds can fly or birds are sick" can be the same as "typically, typically birds can fly or typically birds are sick" if we assume (and we do) that the union of two atypical sets is also atypical.

The the above examples show that for a $(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \mathfrak{f}, \mathfrak{p}, \models)$ possible world model, although $\models_{\mathrm{AC}}$ and $\models_{\mathrm{EC}}$ interpret connectives and quantifiers as usual in first-order logic, they are not necessarily what we expect from a good semantics. It is intuitive to define another semantics as well. In this new semantics, for an $S \in \Sigma_{\mathrm{s}}$, $S \models \phi_1 \vee \phi_2$, that is, on S, either ϕ_1 or ϕ_2 is satisfied, could mean that S can be divided into (or covered by) two parts, one on which ϕ_1 holds, one on which ϕ_2 holds. As the existential quantifier is a generalized disjunction, the analogous definition for the semantics of $\exists$ would be that S can be covered by elements in Σ_{s} on each of which there is a witness. Coming back to our Example 11,

let us consider $X = Y \vee X \neq Y$. Having accepted that $\vee$ is interpreted as a division of S into two parts, one on which $X = Y$ holds, another on which $X \neq Y$ holds, clearly, $X \neq Y$ should be interpreted as $X = Y$ holds nowhere on the part where $X \neq Y$ holds.

One can also think of coin tosses: The statement that the result of a coin toss is either heads or tails means that on certain part of the underlying probability field, the coin comes down heads, on the other part it comes down tails. There is no other option. When we say that the result of throwing the dice is either 1 or not 1, we mean that on a part of the underlying probability field, it is 1, on the other part it is nowhere 1.

Accordingly, adding that we do not care what happens on insignificant sets, we need the following:

▶ **Definition 13** (Covering Enough-Certainty Semantics)**.** Let $(\mathcal{D}, W, \Sigma, \Sigma_s, \mathfrak{f}, \mathfrak{p}, \models)$ be a possible world model with significant events. Let $\mathcal{V}$ denote the set of valuations of variables ranging over $\mathcal{D}$. We define the relation $\models_{\text{CEC}}$ on $\mathcal{V} \times \Sigma_s \times \Phi_{(\mathfrak{f},\mathfrak{p})}$ in the following way:

- If $\phi \in A_{(\mathfrak{f},\mathfrak{p})}$, then $V, S \models_{\text{CEC}} \phi$ iff $V, S \models_{\text{EC}} \phi$.
- The semantics of $\wedge$ and $\forall$ are the usual ones.
- $V, S \models_{\text{CEC}} \phi_1 \vee \phi_2 \Leftrightarrow \exists S_1, S_2 \in \Sigma_s.\big(S \setminus (S_1 \cup S_2) \in \Sigma_i \ \wedge\ V, S_1 \models_{\text{CEC}} \phi_1 \ \wedge\ V, S_2 \models_{\text{CEC}} \phi_2\big)$
- $V, S \models_{\text{CEC}} \neg\phi \Leftrightarrow \forall S' \in \Sigma_s.\big(S' \subseteq S \Rightarrow V, S' \not\models_{\text{CEC}} \phi\big)$
- $V, S \models_{\text{CEC}} \phi_1 \to \phi_2 \Leftrightarrow \forall S' \in \Sigma_s.\big(S' \subseteq S \ \wedge\ V, S' \models_{\text{CEC}} \phi_1 \Rightarrow V, S' \models_{\text{CEC}} \phi_2\big)$
- $V, S \models_{\text{CEC}} \exists x\phi[x] \Leftrightarrow \forall S' \in \Sigma_s.\Big(S' \subseteq S \Rightarrow$
  $\exists \mathcal{S} \subseteq \Sigma_s.\Big(S' \setminus \bigcup_{S'' \in \mathcal{S}} S'' \in \Sigma_i$
  $\wedge\ \forall S'' \in \mathcal{S}.\big(\exists V' \in \mathcal{V} \text{ differing from } V \text{ only on } x.\ (V', S'' \models_{\text{CEC}} \phi[x])\big)\Big)\Big)$

We call this *covering enough-certainty semantics* of the first-order formulas.

▶ Remark. Note, the first thought would be to define satisfaction of the existential quantifier as

$$V, S \models_{\text{CEC}} \exists x\phi[x] \Leftrightarrow \exists \mathcal{S} \subseteq \Sigma_s.\Big(S \setminus \bigcup_{S'' \in \mathcal{S}} S'' \in \Sigma_i \wedge \forall S'' \in \mathcal{S}.\big(\exists V' \in \mathcal{V} \text{ differing from } V \text{ only on } x.\ (V', S'' \models_{\text{CEC}} \phi[x])\big)\Big).$$

However, this is not good, because the insignificant parts in the S''s where $\phi[x]$ is not satisfied, may add up to a significant subset of S. Hence the above definition.

If $\mathcal{D}$ only has countably many elements, and if $\{w \in W : w \models \phi\}$ is measurable for all $\phi \in A_{(\mathfrak{f},\mathfrak{p})}$, then although the semantics of compound formulas with respect to $\models_{\text{CEC}}$ is not defined the usual Tarski way, first order logical deduction rules are valid with respect to $\models_{\text{CEC}}$. We shall see the proof of this in Section 4. In particular, when these conditions are satisfied, the usual distributivity holds for disjunction and conjunction, $\neg\exists$ is the same as $\forall\neg$ and so on. We shall also see in Section 4 that it is possible to give a better general semantics, namely Definition 21, for which first order deduction rules work even when $\mathcal{D}$ is not countable or when $\{w \in W : w \models \phi\}$ is not measurable.

▶ Remark. Note that for ϕ without quantifiers, we have

$$V, S \models_{\text{CEC}} \phi \Leftrightarrow \exists S' \in \Sigma_s.\big(S \setminus S' \in \Sigma_i \ \wedge\ V, S' \models_{\text{AC}} \phi\big) \tag{1}$$

For any ϕ without quantifiers, let

$$[\phi]_V := \big\{w \big| w \in W \ \wedge\ V, w \models \phi\big\}$$

When ϕ and ψ have no quantifiers, and $[\psi]_V$ (and hence $[\neg\psi]_V$) and $[\phi]_V$ are measurable, and in that case,

$$V, S \models_{\mathrm{CEC}} \phi \to \psi \quad \Leftrightarrow \quad [\neg\psi]_V \wedge [\phi]_V \in \Sigma_{\mathrm{i}} \tag{2}$$

also holds. In other words, on $[\phi]_V$, ψ may fail only on an insignificant set.

▶ **Example 14.** When insignificant sets are the $\mathcal{C}$-asymptotically impossible sets of a parametric probability field $(\Omega, \Sigma, \mathcal{P})$, then for ϕ and ψ without quantifiers, if $[\phi]_V$ and $[\psi]_V$ are measurable, then we have

$$V, S \models_{\mathrm{CEC}} \phi \to \psi \quad \Leftrightarrow \quad \Big(1 - P_i\big(\ [\psi]_V \ \big|\ [\phi]_V\ \big)\Big)_{i\in\mathbb{N}} \in \mathcal{C} \tag{3}$$

where $P_i(\ [\psi]_V \mid [\phi]_V\ )$ is the probability of $[\psi]_V$ conditioned on $[\phi]_V$. This is again because $V, S \models_{\mathrm{CEC}} \neg\phi\vee\psi$ means exactly that on the part of S where ϕ holds, ψ also has to hold except for an $\mathcal{C}$-asymptotically impossible set, which exactly means that $(1-P_i(\ [\psi]_V \ \big|\ [\phi]_V\ ))_{i\in\mathbb{N}} \in \mathcal{C}$. In other words, $[\psi]_V$ is $\mathcal{C}$-asymptotically certain conditioned on $[\phi]_V$.

For this conditional implication however, another connective $\to'$ is introduced in [11, 8] with the above semantics in (3). That is, a conditional implication that holds "typically". One of the conclusions of this paper in Example 26 will be that when the sets of the form $[\phi]_V$ are measurable for atomic formulas, and we are only interested in what is satisfied on $\mathcal{C}$-asymptotically possible sets, then we do not need to introduce a new implication for this, the usual one together with the Fitting twist provides this semantics for $\phi \to \psi$ where ϕ and ψ are formulas without quantifiers, and classical first-order deduction rules are sound.

▶ **Example 15.** Consider $[0, 1] \subset \mathbb{R}$ with Lebesgue measurability and the uniform distribution. For the random variable X that is 0 before $1/2$ and 1 from $1/2$, according to the above definition, $X = 0 \vee X = 1$ is satisfied. Which is intuitive. Let Y be the random variable for which $Y(\omega) = n$ for $1/(n + 1) < \omega \leq 1/n$. Then according to $\models_{\mathrm{CEC}}$, it is satisfied that "There is a constant random variable Z such that $Z = Y$". That is because Y is locally constant, we can cover the space with measurable sets on each of which Y is constant. If we make equality a congruence, then this constant predicate cannot distinguish between globally constant and locally constant notions.

The same statement "There is a constant random variable Z such that $Z = W$" fails to hold for $W(\omega) = \omega$. This shows that it is easy to come up with formulas for which it is not good to define satisfaction on S by pointwise satisfaction for quantifiers: For this W, obviously, all ω satisfies that there is a constant c such that $W(\omega) = c$. So had we defined $\models_{\mathrm{CEC}}$ such that (1) hold for ϕ with existential quantifier as well, S would satisfy for any random variable that there is a constant equaling the random variable, which we do not want.

▶ **Example 16.** In case of continuous distributions, if we are only interested in satisfaction of properties up to an error of zero probability – which is the standard in measure theory and probability theory – then it is useless to require existence with satisfaction at each point when the points have zero measure. A formula of the sort $\exists f$. (f satisfies some property except on a set with zero probability) cannot be made sense pointwise on each ω for continuous distributions. Only on sets with non-zero probability can we have statements that hold up to zero-probability.

▶ **Example 17.** Considering "typically", similarly to up to zero probability, we might need more than a single point to evaluate statements. Such are those that have the form "typically

exists ... that typically ... ". For example, "Typically there are chain shops that typically sell pens." meaning that typically in every region there is a chain shop that typically (in that region) sells pens. It is possible that there are some atypical regions where there are no chain shops selling pens. It is also possible that a chain shop that typically sells pens in a region does not do so in another region. In that other region another chain shop sells it. It is clear that this existence cannot be defined pointwise.

In [11], the authors define a conditional entailment $\phi \mid\!\sim \psi$ for atomic formulas exactly as $(1 - P_i(\ [\psi]_V \mid [\phi]_V\ ))_{i\in\mathbb{N}} \in \mathcal{C}$, which is the same what we have in Equation (2). As the authors note, $\phi \mid\!\sim \psi$ does not imply $\phi \wedge \phi' \mid\!\sim \psi$ in general. For example, "typically birds fly" does not mean that "typically penguin birds fly". That is because penguins are atypical. However, if we are only interested in statements on typical sets, then, as we shall see, first order deduction rules can be made to work even when the domain is not countable. In that case, $\phi \wedge \phi' \mid\!\sim \psi$ is implied because $\phi \wedge \phi'$ is atypical, that is, insignificant.

▶ Remark. Note that when W has only one element (and hence the probability distributions all agree), $\models_{\mathrm{AC}}$, $\models_{\mathrm{EC}}$, $\models_{\mathrm{CEC}}$ all coincide with $\models$. In other words, $\models_{\mathrm{AC}}$, $\models_{\mathrm{EC}}$, $\models_{\mathrm{CEC}}$ can be considered extensions of the Tarski-semantics for first-order logic.

The three semantics of the previous section are defined using a basic satisfaction notion $\models$ on possible worlds $w \in W$. Sometimes we need something more general, when the satisfaction of some predicate does not come from pointwise satisfaction.

▶ **Definition 18** (Significant Sets Semantics)**.** Let $(W, \Sigma, \Sigma_{\mathrm{s}})$ such that W is a set, Σ is a σ-algebra on W, and Σ_{s} is a subset of significant sets in σ. Let $(\mathfrak{f}, \mathfrak{p})$ be a first-order language. Let $\mathcal{D}$ be a domain for interpretation. Let $\mathcal{V}$ denote the set of valuations of first-order variables with codomain $\mathcal{D}$. Suppose for each Σ_{s}, the predicates are interpreted on $\mathcal{D}$, and hence a relation $\models_{\mathrm{SiS}}$ on $\mathcal{V} \times \Sigma_{\mathrm{s}} \times A_{(\mathfrak{f},\mathfrak{p})}$ is given, which we call a *significant sets semantics*. $\models_{\mathrm{SiS}}$ can be extended to $\mathcal{V} \times \Sigma_{\mathrm{s}} \times \Phi_{(\mathfrak{f},\mathfrak{p})}$ as usual for first-order semantics.

Clearly, $\models_{\mathrm{AC}}$ and $\models_{\mathrm{EC}}$ are special cases of $\models_{\mathrm{SiS}}$ for $\Phi_{(\mathfrak{f},\mathfrak{p})}$.

3 Kripke Semantics and Fitting-Twisted Semantics for Enough-Certainty

In this section, we exploit the fact that there is a transitive reachability relation on Σ_{s} such that S' is reachable from S if and only if $S' \subseteq S$. Let $\Phi^K_{(\mathfrak{f},\mathfrak{p})}$ denote the set of modal formulas with the addition of $\Box$ and $\Diamond$ operators to $\Phi_{(\mathfrak{f},\mathfrak{p})}$.

▶ **Definition 19** (Kripke Absolute Certainty, Kripke Enough Certainty, Kripke Significant Sets Semantics)**.** With $\subseteq$ as a reachability (also called accessibility) relation, all of $\models_{\mathrm{AC}}$, $\models_{\mathrm{EC}}$, and $\models_{\mathrm{SiS}}$ can be extended to $\models_{\mathrm{KAC}}$, $\models_{\mathrm{KEC}}$, and $\models_{\mathrm{KSiS}}$ respectively on $\mathcal{V} \times \Sigma_{\mathrm{s}} \times \Phi^K_{(\mathfrak{f},\mathfrak{p})}$ interpreting $\Box$ and $\Diamond$ as usual for first-order Kripke semantics. This makes three different S4 semantics because the set-inclusion is reflexive and transitive.

$\models_{\mathrm{KAC}}$, $\models_{\mathrm{KEC}}$, are special instances of $\models_{\mathrm{KSiS}}$. We shall use these Kripke semantics later to obtain the Fitting-twisted first-order semantics.

▶ **Example 20.** Now we show an example in which the interpretation of a predicate cannot be defined point-wise on each $w \in W$. We also use this example to motivate our targeted semantics. Bana and Comon in [3] presented a technique for the verification of trace properties of cryptographic protocols. They used a predicate $t_1, \ldots, t_n \rhd t$ with the intuitive meaning that an attacker can compute t from $t_1, \ldots, t_n$ with a probabilistic polynomial-time

algorithm, while $t_1, \ldots, t_n \not\rhd t$ (that is, $\neg(t_1, \ldots, t_n \rhd t)$) means intuitively that there is no such algorithm. When t is a nonce N,[2] and $t_1, \ldots, t_n$ represent the messages sent by the honest agents, $t_1, \ldots, t_n \not\rhd N$ means that N remains secret: there is no probabilistic polynomial-time algorithm that computes it from the messages of the honest agents. But when they wanted to make this intuition formal, it turned out to be a difficult task. They tried several possibilities first, both for the interpretation of $t_1, \ldots, t_n \rhd t$ and various non-Tarskian interpretations of connectives, which all failed before arriving to the final definitions. This process was never actually published, but here we do that to illustrate how the non-Tarskian semantics naturally emerges in security. In fact the one presented in [3] still worked only for a fragment of the formulas, the final correct definitions only appeared in eprint [2] and in subsequent works such as [4].

Take $(\Omega^c, \Sigma^c, \Sigma^c_{\mathrm{s}}, \mathcal{P}^c)$ as in Example 7. We take the domain $\mathcal{D}^c$ to be probabilistic polynomial-time (PPT) algorithms such that for each $a \in \mathcal{D}^c$ the input is of the form $(1^\eta, \omega)$, where $\eta \in \mathbb{N}$, $\omega \in \{0,1\}^*$, and 1^η means a bit string with η many 1's. That is, the inputs of a are in Ω^c and the first component of elements of Ω^c are fed to a in the form of a string of 1's. The requirement that a is PPT means that a has to stop in polynomial number of steps $p(\eta)$ as a function of η. This means that a can only use an initial section of ω, its second input, namely at most $p(\eta)$ number of random bits.

The interpretations of terms $t_1, \ldots, t_n, t$ take values in this $\mathcal{D}^c$. For a $V \in \mathcal{V}$ valuation of variables in $\mathcal{D}$, let $[\![t_1]\!]_V, \ldots, [\![t_n]\!]_V, [\![t]\!]_V$ denote the interpretations in $\mathcal{D}$. How should the semantics of $t_1, \ldots, t_n \rhd t$ be defined to correspond to the intuition that a PPT attacker can compute t from $t_1, \ldots, t_n$? That is, taking an $S \in \Sigma^c_{\mathrm{s}}$, what should be the definition of $V, S \models^c t_1, \ldots, t_n \rhd t$? The first thought would be to say that $V, S \models^c t_1, \ldots, t_n \rhd t$ if and only if there is a PPT algorithm $\mathcal{A}$ that computes $[\![t]\!]_V$ from $[\![t_1]\!]_V, \ldots, [\![t_n]\!]_V$ except on a negligible set. That is, $\mathcal{A}([\![t_1]\!]_V(1^\eta, \omega), \ldots, [\![t_n]\!]_V(1^\eta, \omega), \omega) = [\![t]\!]_V(1^\eta, \omega)$ for all (η, ω), except on a negligible set of Ω^c (making sure that the bits in ω used by $\mathcal{A}$ in its last argument are disjoint from those used by $[\![t_1]\!]_V, \ldots, [\![t_n]\!]_V, [\![t]\!]_V$). This however does not work. The reason is that if there are two algorithms, $\mathcal{A}_1$ and $\mathcal{A}_2$, and $\mathcal{A}_1$ computes the RHS of $\rhd$ from the LHS of $\rhd$ for parts of the (η, ω) and $\mathcal{A}_2$ computes the RHS from the LHS for the rest of the (η, ω) pairs except maybe on a negligible set, that is a win for the attacker as well, although there may not be a single algorithm for the whole Ω^c. Furthermore, when in computer security we prove that $t_1, \ldots, t_n \not\rhd t$, we want the meaning to be such that there is no $\mathcal{A}$ PPT algorithm that computes the RHS from the LHS on a non-negligible set.

So let us fix the meaning of $V, S \models^c t_1, \ldots, t_n \not\rhd t$ first. We shall say that $V, S \models^c t_1, \ldots, t_n \not\rhd t$ if and only if for all $\mathcal{A}$ PPT, and all $S' \in \Sigma^c_{\mathrm{s}}$ with $S' \subseteq S$, there is an $(\eta, \omega) \in S'$ such that $\mathcal{A}([\![t_1]\!]_V(1^\eta, \omega), \ldots, [\![t_n]\!]_V(1^\eta, \omega), \omega) \neq [\![t]\!]_V(1^\eta, \omega)$. Note that in fact the inequality must be true for all elements in S' except for some with negligible probability, otherwise there would be a non-negligible subset of S' where the equality would be satisfied, that would contradict this definition. Hence, $V, S \models^c t_1, \ldots, t_n \not\rhd t$ if and only if for all $\mathcal{A}$ PPT, the set

$$\{(\eta, \omega) \in S : \mathcal{A}([\![t_1]\!]_V(1^\eta, \omega), \ldots, [\![t_n]\!]_V(1^\eta, \omega), \omega) = [\![t]\!]_V(1^\eta, \omega)\}$$

is negligible.

So then if we want the negation to be standard, $V, S \models^c t_1, \ldots, t_n \rhd t$ should be defined such that there is a PPT algorithm $\mathcal{A}$ that can compute the RHS from the LHS on some S' non-negligible subset of S. But the problem is that this definition has bad properties! For

[2] A nonce in security is a freshly, randomly generated bit string that can only be guessed with negligible probability

example $V, S \models^c t_1, \ldots, t_n \rhd t \wedge t_1, \ldots, t_n \rhd t'$ would not imply that $V, S \models^c t_1, \ldots, t_n \rhd (t, t')$, because the non-negligible set on which t can be computed may be disjoint from the non-negligible set on which t' can be computed, and then there is no non-negligible set on which both t and t' can be computed from the LHS of $\rhd$. Hence it looks like we either have to give up the standard Tarski definition of the semantics of negation, or we have to deal with bad properties. Giving up Tarski definition of the semantics of negation, likely means giving up the use of first-order deduction. But as we shall see this is not the case! We can give up Tarskian semantics and still keep first-order deduction.

So let us keep the definition of $V, S \models^c t_1, \ldots, t_n \not\rhd t$, give up Tarski's semantics for negation, and continue thinking what $V, S \models^c t_1, \ldots, t_n \rhd t$ should be. The next idea is that we require the RHS to be computable from the LHS except maybe for negligible subset of S not by one algorithm, but many. That is, maybe we should define $V, S \models^c t_1, \ldots, t_n \rhd t$ so that S can be covered by non-negligible sets $S_i \in \Sigma_{\mathrm{s}}^c$ such that $S \setminus \bigcup_i S_i \in \Sigma_{\mathrm{i}}^c$, and for each S_i there is an algorithm $\mathcal{A}_i$ that computes the RHS from the LHS. This however is still problematic, $V, S \models^c t_1, \ldots, t_n \rhd t \wedge t_1, \ldots, t_n \rhd t'$ still would not imply $V, S \models^c t_1, \ldots, t_n \rhd (t, t')$. That is because although the sets on which both t and t' can be computed, that is, the intersections of the covering for t and the covering for t' still covers S except maybe for negligible probability, but those intersections may all be negligible!

So let us try to make the definition of $V, S \models^c t_1, \ldots, t_n \rhd t$ stronger than just a covering. Namely, for each covering of S, there is a refinement covering such that on this new covering there is an algorithm for each covering set that computes the RHS from the LHS on that set. This is equivalent with the following: $V, S \models^c t_1, \ldots, t_n \rhd t$ if and only if for all $S' \in \Sigma_{\mathrm{s}}^c$, $S' \subseteq S$, there is an $S'' \in \Sigma_{\mathrm{s}}^c$, $S'' \subseteq S'$, and an algorithm $\mathcal{A}$ such that for all $(\eta, \omega) \in S''$, $\mathcal{A}(\llbracket t_1 \rrbracket_V(1^\eta, \omega), \ldots, \llbracket t_n \rrbracket_V(1^\eta, \omega), \omega) = \llbracket t \rrbracket_V(1^\eta, \omega)$ (where $\mathcal{A}$ uses fresh part of ω). It is easy to check that $V, S \models^c t_1, \ldots, t_n \rhd t \wedge t_1, \ldots, t_n \rhd t'$ does imply $V, S \models^c t_1, \ldots, t_n \rhd (t, t')$, because for all non-negligible $S' \subseteq S$, there is a non-negligible $S'' \subseteq S'$ on which t can be computed, and S'' has a non-negligible subset S''' on which t' can be computed. Since on S''' both t and t' can be computed, S' has such a subset S''', and $V, S \models^c t_1, \ldots, t_n \rhd (t, t')$ is satisfied.

In the previous paragraph, we implicitly assumed that for conjunction, $V, S \models^c t_1, \ldots, t_n \rhd t \wedge t'_1, \ldots, t'_n \rhd t'$ is defined as usual. Let us keep this definition.

Now how should we define $V, S \models^c t_1, \ldots, t_n \rhd t \vee t'_1, \ldots, t'_n \rhd t'$? The first idea would of course be that S can be covered by two sets S_1 and S_2 such that $V, S_1 \models^c t_1, \ldots, t_n \rhd t$ and $V, S_2 \models^c t'_1, \ldots, t'_n \rhd t'$. But there is a better one. We have already defined negation and conjunction, so let us try that $V, S \models^c t_1, \ldots, t_n \rhd t \vee t'_1, \ldots, t'_n \rhd t'$ if and only if $V, S \models^c \neg(\neg t_1, \ldots, t_n \rhd t \wedge \neg t'_1, \ldots, t'_n \rhd t')$. By the definition of the interpretation of negation and of conjunction is easy to check that this turns out to be the following: $V, S \models^c t_1, \ldots, t_n \rhd t \vee t'_1, \ldots, t'_n \rhd t'$ if and only for all non-negligible set $S' \subseteq S$, there is a non-negligible $S'' \subseteq S'$ such that either $V, S'' \models^c t_1, \ldots, t_n \rhd t$ or $V, S'' \models^c t'_1, \ldots, t'_n \rhd t'$. This definition is not so far from the above splitting into S_1 and S_2, except that the unions of the sets on which one disjunct is satisfied and the unions of those on which the other may not be in Σ.

With a bit of similar considerations, defining the interpretation of $\forall$ as usual, and then the interpretation of $\exists$ through $\forall$ and negation, we arrive at a similar definition. These considerations motivate our next definition.

Motivated by the above example, we introduce the following notion, named after Melvin Fitting (it will be clear in Section 4.1 why):

▶ **Definition 21** (Fitting Twisted Enough-Certainty Semantics). Let $(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \models_{\mathrm{SiS}})$ be a significant sets semantics for $\Phi_{(\mathfrak{f},\mathfrak{p})}$. Let $\mathcal{V}$ denote the set of valuations of first-order variables

with codomain $\mathcal{D}$. We can define the relation $\models_{\mathrm{FEC}}$ on $\mathcal{V} \times \Sigma_{\mathrm{s}} \times \Phi_{(\mathfrak{f},\mathfrak{p})}$ in the following way:

- $\phi \in A_{(\mathfrak{f},\mathfrak{p})}$, then

$$V, S \models_{\mathrm{FEC}} \phi \;\Leftrightarrow \forall S' \in \Sigma_{\mathrm{s}}.\, \Big(S' \subseteq S \Rightarrow \exists S'' \in \Sigma_{\mathrm{s}}.\, (S'' \subseteq S' \wedge V, S'' \models_{\mathrm{SiS}} \phi)\Big)$$

- The semantics of $\wedge$ and $\forall$ are the usual ones.
- $V, S \models_{\mathrm{FEC}} \neg\phi \;\Leftrightarrow\; \forall S' \in \Sigma_{\mathrm{s}}.\, \Big(S' \subseteq S \Rightarrow V, S' \not\models_{\mathrm{FEC}} \phi\Big)$
- $V, S \models_{\mathrm{FEC}} \phi_1 \vee \phi_2$
  $\Leftrightarrow\; \forall S' \in \Sigma_{\mathrm{s}}.\, \Big(S' \subseteq S \;\Rightarrow\; \exists S'' \in \Sigma_{\mathrm{s}}.\, \big(S'' \subseteq S' \;\wedge\; (V, S'' \models_{\mathrm{FEC}} \phi_1 \;\vee\; V, S'' \models_{\mathrm{FEC}} \phi_2)\big)\Big)$
- $V, S \models_{\mathrm{FEC}} \exists x \phi[x]$
  $\Leftrightarrow\; \forall S' \in \Sigma_{\mathrm{s}}.\, \Big(S' \subseteq S$
  $\Rightarrow\; \exists S'' \in \Sigma_{\mathrm{s}}.\, \big(S'' \subseteq S' \wedge (\exists V' \in \mathcal{V}$ differing from V only on $x.\, (V', S'' \models_{\mathrm{FEC}} \phi[x]))\big)\Big)$

We call this *Fitting twisted enough-certainty semantics* of the first-order formulas.

In the next section we shall see that the deducibility/provability of classical first-order logic is sound with respect to this semantics.

▶ Remark. Let us introduce the abbreviation

$$\phi \to \psi \equiv \neg\phi \vee \psi$$

then it is easy to check that

- $V, S \models_{\mathrm{FEC}} \phi \to \psi \;\Leftrightarrow\; \forall S' \in \Sigma_{\mathrm{s}}.\, \Big(S' \subseteq S \wedge V, S' \models_{\mathrm{FEC}} \phi \Rightarrow V, S' \models_{\mathrm{FEC}} \psi\Big)$

In other words, $\phi \to \psi$ means that if ϕ is satisfied on a significant subset of S, then ψ also has to by satisfied there.

▶ **Proposition 22.** *Let $(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \models_{SiS})$ and $(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \models'_{SiS})$ be two significant sets semantics such that for each $\phi \in A_{(\mathfrak{f},\mathfrak{p})}$ and $S \in \Sigma_{\mathrm{s}}$, $S \models_{SiS} \phi$ if and only if there is an $S' \in \Sigma_{\mathrm{s}}$ with $(S \setminus S') \cup (S' \setminus S) \in \Sigma_{\mathrm{i}}$ and $S' \models'_{SiS} \phi$. Then$(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \models_{SiS})$ and $(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \models'_{SiS})$ result the exact same Fitting twisted enough-certainty semantics.*

Proof. The proof of this is rather obvious from the definitions. The idea is that if for a significant set S, it is true that for all significant $S' \subseteq S$ there is a significant $S'' \subseteq S'$ such that $V, S'' \models_{\mathrm{SiS}} \phi$ with ϕ atomic, then there is a significant $S''' \subseteq S''$ such that $V, S''' \models'_{\mathrm{SiS}} \phi$ and vice versa by the conditions of the proposition. Then for compound formulas induction can be applied with the same idea. ◀

As a consequence of this, it does not matter if in Example 20 we require that $\mathcal{A}$ succeeds on the S'' sets completely or with a negligible error because they result the same exact definition. Moreover, if we apply the Fitting twist to $\models_{\mathrm{KAC}}$ and $\models_{\mathrm{KEC}}$ (as special instances of $\models_{\mathrm{SiS}}$), the resulting semantics is the same.

The theorem below shows that the covering enough-certainty semantics in certain cases is just a special case of the Fitting twist.

▶ **Proposition 23.** *Let $(\mathcal{D}, W, \Sigma, \Sigma_{\mathrm{s}}, \mathfrak{f}, \mathfrak{p}, \models)$ be a possible world model with significant events. If $\mathcal{D}$ only has countably many elements, and if $\{w : w \models \phi\} \in \Sigma$ for all $\phi \in A_{(\mathfrak{f},\mathfrak{p})}$, and if Σ_{i} is a σ-subalgebra then covering enough-certainty semantics is a special case of Fitting twisted enough-certainty semantics. In other words, when for the Kripke semantics $\models_{KSiS}$, the special case $\models_{KAC}$ is taken, then the Fitting twisted semantics $\models_{FEC}$ is the same as $\models_{CEC}$.*

Outline of the proof: It is shown first that with the conditions of the theorem, for any formula ϕ, and valuation V, there is a maximal $S \in \Sigma_s$ such that $V, S \models_{\text{CEC}} \phi$. With this idea, the proof is rather straightforward induction on the size of the formulas, and it is important that countable unions of insignificant sets are still insignificant with the conditions.

4 Soundness Of Classical Logic With Respect To Enough-Certainty Semantics

In this section we relate our semantics introduced in Section 2 and 3 to the syntactic deducibility/provability notion of classical (first order) predicate logic, in terms of soundness. Then we reconsider the examples we saw earlier to show the usage of this soundness theorem. First-order logic is sound and complete with respect to the standard first-order semantics (that is, Tarskian semantics, when the interpretation of connectives and quantifiers are defined the usual way), which has been well known since Gödel (1930). It has also been explored from time to time that soundness of first-order logic can be maintained for various ranges of semantics which are wider than the standard Tarskian semantics. For example, Rasiowa and Sikorski [13] introduced Boolean valued models for which first order logic is sound. The Boolean-valued classical semantics was used later by Scott-Solovay [14] for a semantic framework of Cohen's forcing model-construction in set theory; we can view this as an example of the usefulness of such extended classical semantics. As we shall discuss later in detail, Fitting introduced in [7] a possible world semantics for classical logic, which corresponds to "necessity-possibility" (or box-diamond) interpretation in terms of S4-modal logical syntactic interpretation. Fitting's interpretation uses double modalities (we can say "twisted" interpretation), which is effectively constructing from standard classical semantics a new semantics that is still classical in the sense that first-order deduction rules are sound, but not standard as some connectives and quantifications are not interpreted as usual. Note, when we say first-order deduction rules are sound, we mean *any* first-order deduction system, including natural deduction, that is sound for standard interpretations.

A different way to obtain from standard classical semantics a new classical semantics via S4 is to combine the Gödel's modal embedding of intuitionistic logic in S4 [9] and the Gödel-Kolmogorov embedding of classical logic into intuitionistic logic [10, 12]. These and various other embedding theorems are ways of constructing new classical semantics from some base classical semantics.

In Section 4.1, we use Fitting's theorem to show that soundness holds for our Fitting-twisted semantics. One natural way to extend the classical semantics is to introduce a new semantic notion. In our case, we are motivated to introduce "enough-certainty" and its variations. In Section 2 and 3, we reached such a new semantics and here we confirm that the new semantics is still classical semantics. We then finish this section by illustrating the use of this new semantics on the examples we have introduced.

4.1 Soundness Theorems

In this section we discuss the relationship of our Fitting-twisted semantics and Fitting's embedding of first-order logic into first-order S4.

In 1970, Melvin Fitting published a paper [7] that is about embedding first order logic into first-order S4. He does this in the following way. For any first-order formula θ, consider the transformation $\theta \to \theta^*$, where θ^* is a formula of S4 (with Barcan formulas), and is defined recursively as follows:

- For any atomic formula θ, let $\theta^* \equiv \Box\Diamond\theta$.
- $(\neg\theta)^* \equiv \Box\neg\theta^*$

- $(\theta_1 \to \theta_2)^* \equiv \Box(\theta_1^* \to \theta_2^*)$
- $(\theta_1 \wedge \theta_2)^* \equiv (\theta_1^* \wedge \theta_2^*)$
- $(\theta_1 \vee \theta_2)^* \equiv \Box\Diamond(\theta_1^* \vee \theta_2^*)$
- $(\forall x\theta)^* \equiv \forall x\theta^*$
- $(\exists x\theta)^* \equiv \Box\Diamond\exists x\theta^*$

Fitting in [7] put $\Box\Diamond$ everywhere and noted that it is redundant in front of the conjunction. It is also easy to check that if the Barcan formula and its converse ($\forall x\Box\theta \leftrightarrow \Box\forall x\theta$) are assumed (that is, when the domain does not change from possible world to possible world in the Kripke structure), then $\Box\Diamond$ is also redundant in front of the universal quantification (as $\theta^* \leftrightarrow \Box\Diamond\theta^*$ holds in our definitions for all θ). For us it is sufficient to only consider a single domain for each possible world, so we assume the Barcan formula and its converse. Fitting's original theorem works for varying domains as well. Fitting's theorem says the following:

- **Fitting's Embedding.** Any formula θ is derivable in first-order logic if and only if θ^* it is derivable in S4 with the Barcan formulas. (Without the Barcan formulas, the theorem still holds, but $(\forall x\theta)^* \equiv \Box\Diamond\forall x\theta^*$ has to be written above).

Fitting's result is closely related to forcing, and a satisfaction relation in S4, $\Gamma \models \Box\Diamond\theta$ is analogous to "θ is weakly forced". While forcing is used in logic to find models of certain formulas, as we showed in the previous section, the above construction naturally arises in the field of computer security when formalizing and deriving properties are based on computational complexity. Let $\vdash_{FOL}$ denote the usual first-order deduction.

▶ **Theorem 24.** *For any first-order formula ϕ, we have that $\vdash_{FOL} \phi$ if and only if it is satisfied by all Fitting-twisted enough-certainty models.*

Proof. The if part follows from the completeness of first-order logic: as a first-order model is a trivial Fitting twisted enough-certainty model, a formula that is satisfied by all Fitting twisted enough-certainty models is also satisfied by all first-order models.

The only if part follows from Fitting's theorem for his embedding. The satisfaction of $\models_{\text{FEC}}$ is the combination of Fitting embedding with $\models_{\text{KSiS}}$: if for a $\phi \in \Phi_{(\mathfrak{f},\mathfrak{p})}$, ϕ^* denotes the Fitting interpretation of ϕ, then it is immediate from the definitions that

$$V, S \models_{\text{FEC}} \phi \Leftrightarrow V, S \models_{\text{KSiS}} \phi^*$$

Since $\models_{\text{KSiS}}$ is a special Kripke semantics and hence S4 deduction rules are sound, and since by Fitting's theorem a formula of the form ϕ^* can be deduced in $S4$ if and only if it can be deduced in first-order logic, we have that if ϕ^* can be deduced in first-order logic then $V, S \models_{\text{KSiS}} \phi^*$ and hence $V, S \models_{\text{FEC}} \phi$ holds. ◀

▶ **Corollary 25.** *Let $(\mathcal{D}, W, \Sigma, \Sigma_{\text{s}}, \mathfrak{f}, \mathfrak{p}, \models)$ be a possible world model with significant events. If $\mathcal{D}$ is countable, if $\{w \in W : w \models \phi\}$ is measurable for all $\phi \in A_{(\mathfrak{f},\mathfrak{p})}$, and if Σ_{i} is a σ-subalgebra, then although the semantics of compound formulas with respect to $\models_{CEC}$ is not defined the usual Tarski way, first order deduction rules are valid with respect to $\models_{CEC}$.*

Proof. This is a direct consequence of Theorem 24 and Proposition 23 ◀

4.2 Applications to the Examples

In this section we come back to the examples that we introduced earlier, and see how Fitting's embedding can be applied there and use classical logic for the deduction of desirable properties.

▶ **Example 26.** In Example 14, we looked at how $\to$ becomes interpreted as conditional implication under $\models_{\mathrm{CEC}}$. We also saw in Corollary 25 that when $\mathcal{D}$ is countable, then the first-order deduction rules are sound for $\models_{\mathrm{CEC}}$. However, even when $\mathcal{D}$ is not countable, the Fitting-twisted semantics obtained from $\models_{\mathrm{AC}}$, as a special case of $\models_{\mathrm{FEC}}$ also gives conditional implication for formulas without quantifiers: When $\models_{\mathrm{FEC}}$ is a Fitting-twisted $\models_{\mathrm{AC}}$, then

$$V, S \models_{\mathrm{FEC}} \phi \to \psi \quad \Leftrightarrow \quad [\neg\psi]_V \wedge [\phi]_V \in \Sigma_{\mathrm{i}}$$

as long as $[\neg\psi]_V, [\phi]_V \in \Sigma$.

In case of a parametrized probability space $(\Omega, \Sigma, \mathcal{P})$, it is easy check that for $S \in \Sigma_{\mathrm{s}}$,

$$V, S \models_{\mathrm{FEC}} \phi \to \psi \quad \Leftrightarrow \quad \Big(1 - P_i\big(\ [\psi]_V \ \big|\ [\phi]_V\ \big)\Big)_{i\in\mathbb{N}} \in \mathcal{C}$$

As a result, even if $\mathcal{D}$ is not countable, it is possible to use first-order logic for conditional implication, when we are only interested in this implication on significants sets.

▶ **Example 27.** As it was worked out in [3, 1, 4], when a security protocol is executed, there are random inputs, coins are tossed by both the attacker and the honest agents. Random nonces are generated, encryptions usually use random inputs, the attacker is also allowed to toss coins. The agents' and the attacker's actions may be different for the various random inputs. A property that may hold for some of the random inputs may fail for others. The security property of a protocol takes the form $\phi \to \psi$, which, in the Fitting-twisted semantics means, as we mentioned in the Remark after Definition 21, that if ϕ is satisfied on a non-negligible part of a protocol execution, then ψ is also satisfied on that non-negligible part (except maybe for negligible probability). That is, whenever the properties expressed by ϕ are satisfied on a part of the execution, the properties expressed by ψ are also satisfied. On other parts, were ϕ is not satisfied, ψ is not required to be satisfied either.

For example ϕ could be expressing that a random secret (nonce) was communicated between two honest agents and ψ expressing that this nonce cannot be computed by the attacker. In this case ψ has the form $t_1, \ldots, t_n \not\rhd N$ (see Example 20) where N is the nonce, $t_1, \ldots, t_n$ are the messages the attacker has seen. Then such a security property is deduced from the axioms on the predicate $\rhd$. Some axioms are general axioms, such as $t_1, \ldots, t_n \rhd t \to t_1, \ldots, t_n, u \rhd t$ (expressing that if the attacker can compute t without u, then it can also compute t with u), while some express the security of the cryptographic primitives such as (roughly) $t_1, \ldots, t_n, \{u\}_k^r \rhd t \to t_1, \ldots, t_n \rhd t$ (expressing that the encryption $\{u\}_k^r$ cannot help computing t).

Because of the soundness theorem Theorem 24, first order deduction rules can be used to deduce the security property from the axioms, and as a result, complexity theoretic guarantees will be obtained. Verifying complexity-theoretic properties of security protocols is a difficult problem and although various research groups have put large efforts to create automated tools for this purpose, there has not been real breakthrough in this area. The aim of this technique is to allow the use of a fragment of first-order logic, the automation of which is well researched and hence open the possibility of fully automated proofs with complexity-theoretic guarantees.

If the semantics of $\to$ were the usual Tarski semantics, then it would mean that if the premise is satisfied over the entire execution space then the conclusion is also satisfied over the entire space. This however is not appropriate because we need to be able to reason about parts of the execution space. The solution of the authors of [6] was to introduce two kinds of implication: one that has the usual Tarski interpretation and one $\to'$ that has a conditional interpretation coming from ϵ-semantics. However, their conditional implication has some

undesirable non-classical properties such as $(\phi \rightarrow' \psi) \not\rightarrow (\phi \wedge \phi' \rightarrow' \psi)$, which we would only need if we cared what happened on negligible sets. And why use two implications when one is sufficient?

5 Conclusion

In this work we have introduced a semantics for "enough-certainty" that allows us to argue with first-order logic about satisfaction of properties on significant sets of possible worlds while ignoring what happens on insignificant sets of possible worlds. We were motivated by an application to computer security and complexity theory, we showed how this non-Tarskian semantics emerged entirely naturally in the context of computer security, and presented a more general framework shifting from non-negligible sets of complexity theory to a notion of significant sets. The trick that ensures the soundness of first-order deduction rules is to combine an S4 Kripke-semantics based on the significant sets as possible worlds with Fitting's embedding of first-order logic in first-order S4. We also showed how the Fitting twist turns material implication into conditional implication.

References

1 G. Bana, P. Adão, and H. Sakurada. Computationally Comlete Symbolic Attacker in Action. In *Proceedings of the 32nd International Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'12)*, LIPIcs, pages 546–560. Schloss Dagstuhl, 2012.

2 G. Bana and H. Comon-Lundh. Towards unconditional soundness: Computationally complete symbolic attacker. Available at IACR ePrint Archive, Report 2012/019.

3 G. Bana and H. Comon-Lundh. Towards unconditional soundness: Computationally complete symbolic attacker. In *Proceedings of the 1st International Conference on Principals of Security and Trust (POST'12)*, LNCS, pages 189–208. Springer, 2012.

4 G. Bana, K. Hasebe, and M. Okada. Computationally complete symbolic attacker and key exchange. In *Proceedings of the 20th ACM SIGSAC Conference on Computer and Communications Security (CCS'13)*, pages 1231–1246. ACM, 2013.

5 P. J. Cohen. *Set theory and the continuum hypothis*. W. A. Benjamin, Inc., New York, 1966.

6 A. Datta, A. Derek, J. C. Mitchell, and B. Warinschi. Computationally sound compositional logic for key exchange protocols. In *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06)*, pages 321–334. IEEE, 2006.

7 M. Fitting. An embedding of classical logic in s4. *The Journal of Symbolic Logic*, 35(4):529–534, 1970.

8 N. Friedman, J. Y. Halpern, and D. Koller. First-order conditional logic for default reasoning revisited. *ACM Transactions on Computational Logic*, 1(2):175–207, 2000.

9 K. Gödel. Eine interpretation des intuitionistischen aussagenkalküls. *Ergebnisse eines Mathematischen Kolloquiums*, 4:39–40, 1933.

10 K. Gödel. Zur intuitionistischen arithmetik und zahlentheorie. *Ergebnisse eines Mathematischen Kolloquiums*, 4:34–38, 1933.

11 M. Goldszmidt, P. Morris, and J. Pearl. A maximum entropy approach to nonmonotonic reasoning. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(3):220–232, March 1993.

12 A. N. Kolmogorov. O principe tertium non datur (russian). *Matematiceskij Sbornik*, 32:646–667, 1925.

13 H. Rasiowa and R. Sikorski. *The Mathematics of Metamathematics*. Polish Scientific Publishers, 1963.

14 D. Scott and R. Solovay. Boolean-valued models of set theory. *unpublished and circulated*, 1967.

15 R. M. Smullyan and M. Fitting. *Set Theory and the Continuum Problem*. Oxford University Press, 1996. revised addition by Dover, 2006.

16 J. Väänänen. *Dependence Logic: A New Approach to Independence Friendly Logic*. Cambridge University Press, 2007.