# Proof Complexity of Non-Classical Logics*

Olaf Beyersdorff[1] and Oliver Kutz[2]

[1] Institut für Theoretische Informatik, Leibniz-Universität Hannover, Germany
beyersdorff@thi.uni-hannover.de
[2] Research Center on Spatial Cognition (SFB/TR 8), Universität Bremen, Germany
okutz@informatik.uni-bremen.de

**Abstract.** Proof complexity is an interdisciplinary area of research utilising techniques from logic, complexity, and combinatorics towards the main aim of understanding the complexity of theorem proving procedures. Traditionally, propositional proofs have been the main object of investigation in proof complexity. Due their richer expressivity and numerous applications within computer science, also non-classical logics have been intensively studied from a proof complexity perspective in the last decade, and a number of impressive results have been obtained.
In these notes we give an introduction to this recent field of proof complexity of non-classical logics. We cover results from proof complexity of modal, intuitionistic, and non-monotonic logics. Some of the results are surveyed, but in addition we provide full details of a recent exponential lower bound for modal logics due to Hrubeš [60] and explain the complexity of several sequent calculi for default logic [16, 13]. To make the text self-contained, we also include necessary background information on classical proof systems and non-classical logics.

* Part of these notes are based on the survey [12] and the research paper [13]. This paper was produced while the first author was visiting Sapienza University of Rome under support of grant N. 20517 by the John Templeton Foundation.

# Table of Contents

# 1 Introduction

These notes originate in an ESSLLI course held in August 2010 at the University of Copenhagen. The aim of this course was—and is of these notes—to present an up-to-date introduction to proof complexity with emphasis on non-classical logics and their applications. The ESSLLI course started with a first lecture introducing central concepts from classical proof complexity and then concentrated in the remaining four lectures on proof complexity of non-classical logics. The material here is organised slightly differently, but again we will start with some remarks on the motivations for proof complexity, first for classical propositional proofs and then for proof complexity of non-classical logics.

## 1.1 Propositional Proof Complexity

One of the starting points of propositional proof complexity is the seminal paper of Cook and Reckhow [34] where they formalised propositional proof systems as polynomial-time computable functions which have as their range the set of all propositional tautologies. In that paper, Cook and Reckhow also observed a fundamental connection between lengths of proofs and the separation of complexity classes: they showed that there exists a propositional proof system which has polynomial-size proofs for all tautologies (a *polynomially bounded* proof system) if and only if the class $\mathsf{NP}$ is closed under complementation. From this observation the so called *Cook-Reckhow programme* was derived which serves as one of the major motivations for propositional proof complexity: to separate $\mathsf{NP}$ from $\mathsf{coNP}$ (and hence $\mathsf{P}$ from $\mathsf{NP}$) it suffices to show super-polynomial lower bounds to the size of proofs in all propositional proof systems.

Although the first super-polynomial lower bound to the lengths of proofs had already been shown by Tseitin in the late 60's for a sub-system of Resolution [105], the first major achievement in this programme was made by Haken in 1985 when he showed an exponential lower bound to the proof size in Resolution for a sequence of propositional formulae describing the pigeonhole principle [55]. In the last two decades these lower bounds were extended to a number of further propositional systems such as the Nullstellensatz system [7], Cutting Planes [18, 91], Polynomial Calculus [32, 95], or bounded-depth Frege systems [1, 8, 9, 78]. For all these proof systems we know exponential lower bounds to the lengths of proofs for concrete sequences of tautologies arising mostly from natural propositional encodings of combinatorial statements.

For proving these lower bounds, a number of generic approaches and general techniques have been developed. Most notably, there is the method of feasible interpolation developed by Krajíček [73], the size-width trade-off introduced by Ben-Sasson and Wigderson [10], and the use of pseudorandom generators in proof complexity [2, 74, 75].

Despite this enormous success many questions still remain open. In particular Frege systems currently form a strong barrier [17], and all current lower bound methods seem to be insufficient for these strong systems. A detailed survey of recent advances in propositional proof complexity is contained in [101].

Let us mention that the separation of complexity classes is not the only motivation for studying lengths of proofs. In particular concerning strong systems such as Frege and its extensions there is a fruitful connection to bounded arithmetic which adds insights to both subjects (cf. [72]). Further, understanding weak systems such as Resolution is vital to applications as for example the design of efficient SAT solvers (see e. g. [90] for a more elaborate argument). Last but not least, propositional proof complexity has over the years grown into a mature field and many researchers believe that understanding propositional proofs and proving lower bounds—arguably the hardest task in complexity—is a very important and beautiful field of logic which is justified in its own right.

## 1.2 Proof Complexity of Non-Classical Logics

Besides the vivid research on propositional proof complexity briefly mentioned above, the last decade has also witnessed intense investigations into the complexity of proofs in non-classical logics. Before describing some of the results, let us comment a bit on the motivation for this research. Rudolf Carnap formulated his *Principle of Logical Tolerance* in 1934 [30], endorsing a pragmatic choice of logical formalism that is most beneficial for a given scientific endeavour. Since then, computing science has gone a long way, and logical methods are being employed in almost all areas of modern computer science. As a consequence, *logical pluralism* understood pragmatically is today common sense. Here is one such voice [85] articulating this position:

> [. . . ] it is a fact of life that no single perspective, no single formalisation or level of abstraction suffices to represent a system and reason about its behaviour. [. . . ] no logical formalism (specification language, prototyping language, etc.) will be best for all purposes. What exists is a space of possibilities (the universe of logics) in which careful choice of the formalisms that best suit some given purposes can be exercised.

Non-classical logics can therefore be considered even more important for computer science than classical logic as they adapt to needed expressive capabilities and hence are often more suitable for concrete applications.

Whilst such heterogeneity might be rather obvious when considering quite different application areas across computer science, say formal verification vs. database theory, it materialises also *within* a single domain. Consider the case of formal ontology engineering. Here, ontologies are being designed in lightweight description logics (DLs) suitable e.g. for very large biomedical ontologies, expressive DLs (for smaller more expressive domain ontologies), and first-order logic (e.g. foundational ontologies). However, also intuitionistic logic is being used (e.g. concerning legal ontologies) as well as paraconsistent logic for handling inconsistent information, and non-monotonic and default logic for handling rules and exceptions. Of course, each such logic comes with specialised reasoning support and quite distinct proof systems.[3]

Given this situation, it is therefore rather important to enhance our understanding of theorem proving procedures in these logics, in particular, given the impact that lower bounds to the lengths of proofs have on the performance of proof search algorithms. From the list of logics just mentioned, besides classical logic we will consider here in detail the modal logic **K** (and some of its extensions), intuitionistic logic **INT**, as well as Reiter's default logic.

Another motivation comes from complexity theory. As non-classical logics are often more expressive than propositional logic, they are usually associated with large complexity classes like PSPACE. The satisfiability problem in the modal logic **K** was shown to be PSPACE-complete by Ladner [82], and this was subsequently also established for many other modal and intuitionistic logics.[4] Thus, similarly as in the Cook-Reckhow programme mentioned above, proving lower bounds to the lengths of proofs in non-classical logics can be understood as an attempt to separate complexity classes, but this time we are approaching the NP vs. PSPACE question. Intuitively therefore, lower bounds to the lengths of proofs in non-classical logic should be easier to obtain, as they "only" target at separating NP and PSPACE. In some sense the results of Hrubeš [60] and Jeřábek [65] on non-classical Frege systems (see Section 5) confirm this intuition: they obtain exponential lower bounds for modal and intuitionistic Frege systems (in fact, even extended Frege) whereas to reach such results in propositional proof complexity we have to overcome a strong current barrier [17].

Last not least, research in non-classical proof complexity will also advance our understanding of propositional proofs as we see a number of phenomena which do not appear in classical logic (as e. g. with respect to the question of Frege vs. *EF* and *SF*, see Section 6). These results are very interesting to contrast with our knowledge on classical Frege as they shed new light on this topic from a different perspective.

### 1.3 Organisation of the Paper and Guidelines for Reading

The remaining part of these notes is organised as follows. We start with two preliminary sections on classical propositional proof systems and non-classical logics, respectively. These two sections contain all definitions and notions that are used in the text. In particular, Section 2 on proof complexity contains definitions and results on propositional proof systems such as Resolution, Frege, and *LK*. In Section 3, we provide background material for modal, intuitionistic, and default logic. In Section 4, we explain interpolation, both in classical logic

[3] The broad logical landscape found in contemporary ontology engineering is described in detail in [81].

[4] In fact, PSPACE seems to be the "typical" complexity of monomodal logics and similar systems which we will consider here. The complexity often gets higher for logics in richer languages, e. g., PDL or the modal $\mu$-calculus, but we are not aware of any proof complexity research on these, though.

and in modal and intuitionistic logics. Building on interpolation, the feasible interpolation technique is one of the main techniques for lower bounds in proof complexity. This technique is described in Section 4.2.

Proof complexity of non-classical logics properly starts in Section 5. In Section 5, we discuss strong lower bounds for modal and intuitionistic logics. In particular, we give full details on the exponential lower bound for **K** due to Hrubeš [60]. In Section 6, we survey simulations between modal and intuitionistic Frege systems. Section 7 is devoted to the proof complexity of propositional default logic where again we give full details. Finally, we conclude in Section 8 with some open problems.

The reader familiar with proof complexity and/or non-classical logic may skip Sections 2 and 3 (and possibly even Section 4 on interpolation) and directly proceed to the main material in Sections 5 to 7. Sections 5–7 are almost independent and can be read in any order.

## 2 Preliminaries I: Classical Proof Complexity

We fix a language of propositional connectives. In most places the actual choice of these connectives is not important as long as they form a basis for the set of all boolean functions. In the following, we will allow the connectives $\wedge, \vee, \rightarrow, \neg$ and constants 0,1. The set TAUT is defined as the set of all propositional tautologies over these connectives. Sometimes we will also consider proof systems for tautologies over a restricted propositional language. To better distinguish propositional tautologies from tautologies in other logics we will also alternatively denote TAUT by **PL**.

Propositional proof systems were defined in a very general way by Cook and Reckhow in [34] as polynomial-time computable functions $P$ which have as its range the set of all tautologies. In fact, their definition applies to arbitrary languages.

**Definition 1 (Cook, Reckhow [34]).** *A proof system for an arbitrary language $L$ is a polynomial-time computable function $P$ with* $\operatorname{rng}(P) = L$. *Proof systems for $L =$* TAUT *are called* propositional proof systems. ■

A string $\pi$ with $P(\pi) = \varphi$ is called a $P$-proof of the element $\varphi$. The intuition behind this definition is that given a proof it should be easy to determine which formula is actually proven and to verify the correctness of the proof. Nevertheless it might be difficult to generate proofs for a given formula and proofs might be very long compared to the size of the formula proven.

Probably the simplest propositional proof system is the *truth-table system* that proves formulae by checking all propositional assignments. In the sense of Definition 1 proofs in the truth-table system consist of the proven formula $\varphi$ together with a string $1^{2^{|\mathrm{Var}(\varphi)|}}$. As most formulae require exactly exponential proof size in this system it is neither very interesting from the application oriented nor from the proof complexity perspective.

But also all the usually studied proof systems are captured by the above definition. Let us illustrate this by an example. One of the most widely used proof systems is the *Resolution calculus* and its variants introduced by Davis and Putnam [37] and Robinson [99]. Resolution is a refutation system that operates with clauses which are finite sets of negated or unnegated variables called literals. A clause is associated with the disjunction of the literals it contains and a set of clauses is associated with the conjunction of its clauses. Therefore finite sets of clauses correspond to propositional formulae in conjunctive normal form.

A clause is satisfied by a propositional assignment if at least one literal of the clause is satisfied by the assignment. Therefore by definition the empty clause is unsatisfiable. A Resolution proof shows the unsatisfiability of a set of clauses by starting with these clauses and deriving new clauses by the Resolution rule

$$\frac{C \cup \{p\} \qquad D \cup \{\neg p\}}{C \cup D}$$

until the empty clause is derived.

At first glance the Resolution system does not seem to fit into the Cook-Reckhow framework of propositional proof systems because it is a refutation system and can furthermore only refute formulae in CNF. But we can associate with Resolution the following function *Res*:

$$Res(\pi) = \begin{cases} \varphi & \text{if } \pi = (\varphi, C_1, \dots, C_k) \text{ where } \varphi \text{ is a formula in DNF} \\ & \text{and } C_1, \dots C_k \text{ is a Resolution refutation of the set} \\ & \text{of clauses for } \neg\varphi \\ \top & \text{otherwise.} \end{cases}$$

The second line of the definition is incorporated because by definition every string $\pi$ has to be interpreted as a proof of some formula. Clearly, *Res* is computable in polynomial time. Hence in accordance with the above general definition, *Res* is a proof system for all propositional tautologies in DNF. A common way to extend the Resolution system from a proof system for formulae in DNF to a proof system for all propositional tautologies is to transfer the formula to an equivalent formula in DNF, either by direct translation or by using new auxiliary variables (cf. [26] for the details).

Proof systems can be compared according to their strength by the notion of simulation. In proof complexity, simulations play a similar role as reductions in computational complexity. Given two proof systems $P$ and $S$ for the same language $L$, we say that $S$ **simulates** $P$ (denoted by $P \leq S$) if there exists a polynomial $p$ such that for all $x$ and $P$-proofs $\pi$ of $x$ there is a $S$-proof $\pi'$ of $x$ with $|\pi'| \leq p(|\pi|)$ [76]. If such a proof $\pi'$ can even be computed from $\pi$ in polynomial time we say that $S$ **p-simulates** $P$ and denote this by $P \leq_p S$ [34]. If $P \leq S$, then we will often simply say that $S$ is stronger than $P$. As usual we say that $P$ and $S$ are equivalent (denoted by $P \equiv S$) if $P \leq S$ and $S \leq P$. The relation $\equiv_p$ is defined similarly. It is clear that $\equiv$ and $\equiv_p$ are equivalence relations on the set of all proof systems. Their equivalence classes are called *degrees*.

A proof system is called **(p-)optimal** if it (p-)simulates all proof systems. Whether or not optimal proof systems exist is an open problem posed by Krajíček and Pudlák [76].

The central objective in proof complexity is to understand how long proofs have to be for a given formula. There are two measures which are of primary interest. The first is the minimal **size** of an $f$-proof for some given element $x \in L$. To make this precise, let

$$s_f(x) = \min\{\, |w| \mid f(w) = x \,\} \quad \text{and} \quad s_f(n) = \max\{\, s_f(x) \mid |x| \leq n, x \in L \,\} \ .$$

We say that the proof system $f$ is **$t$-bounded** if $s_f(n) \leq t(n)$ for all $n \in \mathbb{N}$. If $t$ is a polynomial, then $f$ is called **polynomially bounded**. Another interesting parameter of a proof is the **length** defined as the number of proof steps. This measure only makes sense for proof systems where proofs consist of lines containing formulae or sequents. This is the case for most systems studied in this paper. For such a system $f$, we let

$$t_f(\varphi) = \min\{\, k \mid f(\pi) = \varphi \text{ and } \pi \text{ uses } k \text{ steps} \,\}$$

and $t_f(n) = \max\{\, t_f(\varphi) \mid |\varphi| \leq n, \varphi \in L \,\}$. Obviously, it holds that $t_f(n) \leq s_f(n)$, but the two measures are even polynomially related for a number of natural systems as extended Frege (cf. [72]).

Given the general notion of a proof system from Definition 1, a proof system for a language $L$ is simply a nondeterministic procedure that accepts $L$. Hence polynomially bounded proof systems correspond to $\mathsf{NP}$-algorithms for $L$. This connection to complexity theory is made precise by the following theorem of Cook and Reckhow from their seminal paper [34].

**Theorem 2 (Cook, Reckhow [34]).** *Let $L$ be an arbitrary nonempty language. Then there exists a polynomially bounded proof system for $L$ if and only if $L \in \mathsf{NP}$.*

*Proof.* For the first direction let $P$ be a polynomially bounded proof system for $L$ with bounding polynomial $p$. Consider the following algorithm:

```
Input: a string $x$
guess $\pi \in \Sigma^{\leq p(|x|)}$
IF $P(\pi) = x$ THEN accept ELSE reject
```

Obviously the above algorithm is a nondeterministic polynomial-time algorithm for $L$, hence $L \in \mathsf{NP}$.

For the other direction assume that $L \in \mathsf{NP}$. Hence there exists a nondeterministic polynomial time Turing machine $M$ that accepts $L$. Let the polynomial $p$ bound the running time of $M$. Consider the function

$$P(\pi) = \begin{cases} x & \text{if } \pi \text{ codes an accepting computation of } M(x) \\ x_0 & \text{otherwise} \end{cases}$$

where $x_0 \in L$ is some fixed element. Then $P$ is a proof system for $L$ which is polynomially bounded by $p$. ■

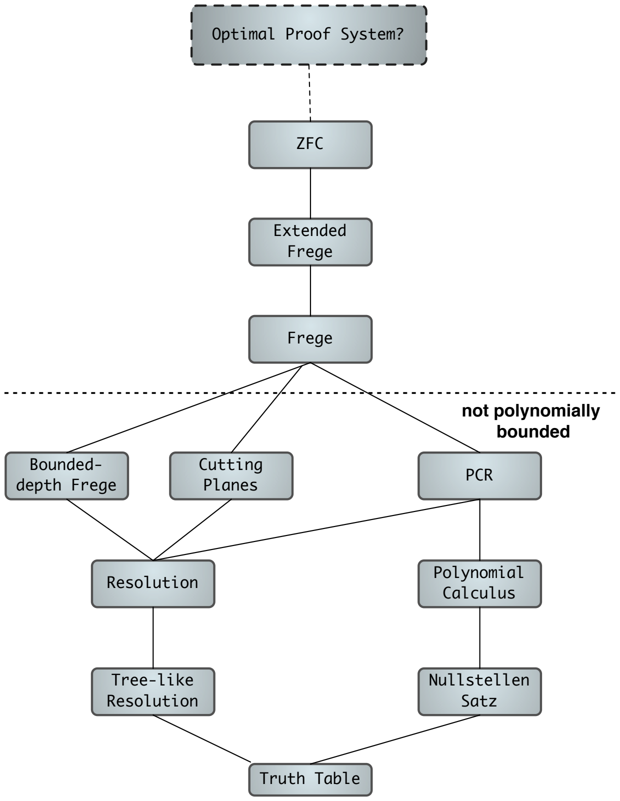


**Fig. 1.** The simulation order of propositional proof systems

By the coNP-completeness of TAUT, this means that there exists a polynomially bounded propositional proof system if and only if NP = coNP. From this result the Cook-Reckhow programme is derived which we already mentioned in the introduction. To separate NP from coNP (and hence also P from NP) it is sufficient to establish for stronger and stronger propositional proof systems that they are not polynomially bounded.

Figure 1 depicts some of the most common propositional proof systems together with their simulation relations. A line between proof systems indicates that the lower proof system is simulated by the higher system in Fig. 1. Moreover all the proof systems below the dashed line have also been separated, i.e. the simulations do not hold in the opposite direction. The dashed line shows the current frontier in the search for super-polynomial lower bounds to the proof length, i.e. for all systems below the line sequences of formulae are known that do not admit polynomial size proofs in the respective proof systems, whereas for the systems above the line there is currently no information about non-trivial lower bounds to the proof size available. A detailed description of the proof systems depicted in Fig. 1 together with information on lower bounds can be found in the surveys [92], [101], and [106].

## 2.1 Frege Systems and Their Extensions

In this section we will describe Frege systems and their extensions. These are strong proof systems that will play a central role for the rest of these notes.

Frege systems derive formulae using axioms and rules. In texts on classical logic these systems are usually referred to as Hilbert-style systems but in propositional proof complexity it has become customary to call them Frege systems [34].

A **Frege rule** is a $(k+1)$-tuple $(\varphi_0, \varphi_1 \dots, \varphi_k)$ of propositional formulae such that

$$\{\varphi_1, \varphi_2, \dots, \varphi_k\} \models \varphi_0 \ .$$

The standard notation for rules is

$$\frac{\varphi_1 \quad \varphi_2 \quad \dots \quad \varphi_k}{\varphi_0} \ .$$

A Frege rule with $k = 0$ is called a **Frege axiom**.

A formula $\psi_0$ can be derived from formulae $\psi_1, \dots, \psi_k$ by using the Frege rule $(\varphi_0, \varphi_1 \dots, \varphi_k)$ if there exists a substitution $\sigma$ such that

$$\sigma(\varphi_i) = \psi_i \quad \text{for } i = 0, \dots, k \ .$$

Let $\mathcal{F}$ be a finite set of Frege rules. An **$\mathcal{F}$-proof** of a formula $\varphi$ from a set of propositional formulae $\Phi$ is a sequence $\varphi_1, \dots, \varphi_l = \varphi$ of propositional formulae such that for all $i = 1, \dots, l$ one of the following holds:

1. $\varphi_i \in \Phi$ or
2. there exist numbers $1 \le i_1 \le \dots \le i_k < i$ such that $\varphi_i$ can be derived from $\varphi_{i_1}, \dots, \varphi_{i_k}$ by a Frege rule from $\mathcal{F}$.

We denote this by $\mathcal{F} : \Phi \vdash \varphi$.

$\mathcal{F}$ is called **complete** if for all formulae $\varphi$

$$\models \varphi \quad \Longleftrightarrow \quad \mathcal{F} : \varnothing \vdash \varphi \ .$$

$\mathcal{F}$ is called **implicationally complete** if for all $\varphi \in$ Form and $\Phi \subseteq$ Form

$$\Phi \models \varphi \quad \Longleftrightarrow \quad \mathcal{F} : \Phi \vdash \varphi \ .$$

$\mathcal{F}$ is a **Frege system** if $\mathcal{F}$ is implicationally complete.

Without proof we note that the set of axioms and rules in Table 1, taken from [26], constitute an example of a Frege system for classical propositional logic **PL**. In the formulas in Table 1, we associate brackets from right to left, i.e. $p_1 \to p_2 \to p_1$ abbreviates $p_1 \to (p_2 \to p_1)$.

This definition leaves much freedom to design individual Frege systems but if we are only interested in the lengths of proofs there is only one Frege system $F$ as already noted by Cook and Reckhow [34] (cf. also Section 6).

| | |
|---|---|
| Axioms | $p_1 \to p_2 \to p_1$ |
| | $(p_1 \to p_2) \to (p_1 \to (p_2 \to p_3)) \to (p_1 \to p_3)$ |
| | $p_1 \to p_1 \vee p_2$ |
| | $p_2 \to p_1 \vee p_2$ |
| | $(p_1 \to p_3) \to (p_2 \to p_3) \to (p_1 \vee p_2 \to p_3)$ |
| | $(p_1 \to p_2) \to (p_1 \to \neg p_2) \to \neg p_1$ |
| | $\neg\neg p_1 \to p_1$ |
| | $p_1 \wedge p_2 \to p_1$ |
| | $p_1 \wedge p_2 \to p_2$ |
| | $p_1 \to p_2 \to p_1 \wedge p_2$ |
| Rules | $\dfrac{p_1 \qquad p_1 \to p_2}{p_2}$ |

**Table 1.** A Frege system for propositional logic **PL**.

**Theorem 3 (Cook, Reckhow [34]).** *Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be Frege systems. Then $\mathcal{F}_1 \equiv_p \mathcal{F}_2$.* ■

Now we describe the extensions of Frege systems as introduced in [34]. Let $\mathcal{F}$ be a Frege system. An **extended Frege proof** of $\varphi$ from a set $\Phi$ of formulae is a sequence $(\varphi_1, \dots, \varphi_l = \varphi)$ of propositional formulae such that for each $i = 1, \dots, l$ one of the following holds:

1. $\varphi_i \in \Phi$ or
2. $\varphi_i$ has been derived by an $\mathcal{F}$-rule or
3. $\varphi_i = q \leftrightarrow \psi$ where $\psi$ is an arbitrary propositional formula and $q$ is a new propositional variable that does not occur in $\varphi$, $\Phi$, $\psi$, and $\varphi_j$ for $1 \leq j < i$.

The introduction of the extension rule 3 allows the abbreviation of possibly complex formulae by variables. Hence using this rule for formulae which appear very often in an $\mathcal{F}$-proof can substantially reduce the proof size.

Analogously as in Theorem 3 it follows that all extended Frege systems are polynomially equivalent. It is clear that *EF* simulates Frege systems but whether *EF* is indeed a strictly stronger system is an open problem.

Another way to enhance the power of Frege systems is to allow substitutions not only for axioms but also for all formulae that have been derived in Frege proofs. This is accomplished by introducing the **substitution rule**

$$\frac{\varphi}{\sigma(\varphi)}$$

which allows to derive $\sigma(\varphi)$ for an arbitrary substitution $\sigma$ from the earlier proven formula $\varphi$. Augmenting Frege systems by this substitution rule we arrive at the **substitution Frege system** *SF*.

*SF* is polynomially equivalent to *EF*. While $EF \leq_p SF$ is relatively easy to see [34] the transformation of *SF*-proofs to *EF*-proofs on the propositional level is quite involved [76]. We will discuss this in more detail in Section 6.

## 2.2 The Propositional Sequent Calculus

Historically one of the first and best analysed proof systems is Gentzen's sequent calculus [48]. The sequent calculus is widely used both for propositional and first-order logic. Here we will describe the propositional sequent calculus *LK*. The basic objects of the sequent calculus are **sequents**

$$\varphi_1, \dots, \varphi_m \longrightarrow \psi_1, \dots, \psi_k \ .$$

Formally these are ordered pairs of two sequences of propositional formulae separated by the symbol $\longrightarrow$. The sequence $\varphi_1, \dots, \varphi_m$ is called the **antecedent** and $\psi_1, \dots, \psi_k$ is called the **succedent**. These cedents are usually denoted by letters like $\Gamma$ and $\Delta$. An assignment $\alpha$ satisfies a sequent

$$\Gamma \longrightarrow \Delta$$

if

$$\alpha \models \bigvee_{\varphi \in \Gamma} \neg\varphi \vee \bigvee_{\psi \in \Delta} \psi \ .$$

The sequence $\varnothing \longrightarrow \Delta$ having empty antecedent is abbreviated as $\longrightarrow \Delta$. Likewise $\Gamma \longrightarrow$ abbreviates $\Gamma \longrightarrow \varnothing$. Sequences of the form

$$A \longrightarrow A, \quad 0 \longrightarrow, \quad \longrightarrow 1$$

are called *initial sequents*. The sequent calculus *LK* uses the following set of rules:

1. weakening rules

$$\frac{\Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta} \quad \text{and} \quad \frac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, A}$$

2. exchange rules

$$\frac{\Gamma_1, A, B, \Gamma_2 \longrightarrow \Delta}{\Gamma_1, B, A, \Gamma_2 \longrightarrow \Delta} \quad \text{and} \quad \frac{\Gamma \longrightarrow \Delta_1, A, B, \Delta_2}{\Gamma \longrightarrow \Delta_1, B, A, \Delta_2}$$

3. contraction rules

$$\frac{\Gamma_1, A, A, \Gamma_2 \longrightarrow \Delta}{\Gamma_1, A, \Gamma_2 \longrightarrow \Delta} \quad \text{and} \quad \frac{\Gamma \longrightarrow \Delta_1, A, A, \Delta_2}{\Gamma \longrightarrow \Delta_1, A, \Delta_2}$$

4. $\neg$ : introduction rules

$$\frac{\Gamma \longrightarrow \Delta, A}{\neg A, \Gamma \longrightarrow \Delta} \quad \text{and} \quad \frac{A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \neg A}$$

5. $\wedge$ : introduction rules

$$\frac{A, \Gamma \longrightarrow \Delta}{A \wedge B, \Gamma \longrightarrow \Delta} \quad \text{and} \quad \frac{A, \Gamma \longrightarrow \Delta}{B \wedge A, \Gamma \longrightarrow \Delta}$$

$$\text{and} \quad \frac{\Gamma \longrightarrow \Delta, A \qquad \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \wedge B}$$

6. $\vee$ : introduction rules

$$\frac{A, \Gamma \longrightarrow \Delta \qquad B, \Gamma \longrightarrow \Delta}{A \vee B, \Gamma \longrightarrow \Delta}$$

$$\text{and} \quad \frac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, A \vee B} \quad \text{and} \quad \frac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, B \vee A}$$

7. cut-rule

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

Similarly as in Frege systems an *LK-proof* of a propositional formula $\varphi$ is a derivation of the sequent

$$\longrightarrow \varphi$$

from initial sequents by the above rules. Without proof we note that the above set of rules specifies a proof system that is complete for the set of all tautologies (see [72]).

As Frege systems can be easily transformed into the sequent formulation a straightforward analysis shows that Frege systems and the Gentzen calculus *LK* polynomially simulate each other.

**Proposition 4 (Cook, Reckhow [34]).** *Frege systems and the propositional sequent calculus LK are polynomially equivalent.* ■

## 3 Preliminaries II: Non-classical Logics

In this section, we cover the basics of the non-classical logics whose proof-complexity we analyse subsequently. This comprises basic syntax and semantics, as well as some meta-theoretical results that are of relevance. We concentrate on three different branches of non-classical logics, namely (i) modal logics, i.e. *extensions* of classical logic which keep all classical tautologies but add new sentence forming operators, namely the modalities; (ii) intuitionistic logic, a *restriction* of classical logic giving up some classical principles, but being formulated in the same language; and (iii) Reiter's default logic, i.e. a member of the family of *non-monotonic logics* being able to handle default rules and exceptions.

### 3.1 Modal Logic and Kripke Semantics

Historically, modern modal logic is typically seen to begin (see e.g. [53]) with the systems devised by C. I. Lewis [83], intended to model strict implication and avoid the paradoxes of material implication, such as the *ex falso quodlibet*. Here is an example for such a 'paradox':

> If it never rains in Copenhagen, then Elvis never died.

Lewis' systems, however, were mutually incompatible, and no base logic was given of which the other logics were extensions of. The modal logic **K**, by contrast, is such a base logic, named after Saul Kripke, and which serves as a minimal logic for the class of all its (normal) extensions—defined below via its standard Frege system.

**Proof Systems for Modal Logics.** While most lower bounds for classical propositional proofs are shown for weak systems like Resolution, Cutting Planes, or Polynomial Calculus, researchers in non-classical logics have mostly investigated Frege style systems. This is quite natural as many modal logics are even defined via derivability in these systems.

In addition to the propositional connectives (chosen such that they form a basis for the set of all boolean functions), the **modal language** contains the unary connective $\Box$. We will also use the connective $\Diamond$ which we treat as an abbreviation of $\neg\Box\neg$.

As mentioned, non-classical logics are very often defined via an associated Frege system. As an example, a Frege system for the modal logic **K** is obtained by augmenting the propositional Frege system from the previous section by the modal axiom of distributivity

$$\Box(p \to q) \to (\Box p \to \Box q)$$

and the rule of necessitation

$$\frac{p}{\Box p} \ .$$

The complete Frege system for the modal logic **K** is shown in Table 2.

The modal logic **K** can then simply be defined as the set of all modal formulae derivable in this Frege system. Other modal logics can be obtained by adding further axioms, e. g., **K4** is obtained by adding the axiom $\Box p \to \Box\Box p$, **KB** by adding $p \to \Box\Diamond p$, and **GL** by adding $\Box(\Box p \to p) \to \Box p$. A list of important modal logics is depicted in Table 3.

Other popular proof systems that are used in practise are systems based on semantic tableaux [43] as well as systems based on Resolution (see e.g. [38, 6]). Tableaux are refutation based proof systems, and more straightforwardly admit various optimisation techniques compared to using Frege systems, as can also be witnessed by the highly optimised tableaux systems that are being employed for e.g. contemporary reasoners for the web ontology language OWL 2 that

| | |
|---|---|
| Axioms | $p_1 \to (p_2 \to p_1)$ |
| | $(p_1 \to p_2) \to (p_1 \to (p_2 \to p_3)) \to (p_1 \to p_3)$ |
| | $p_1 \to p_1 \vee p_2$ |
| | $p_2 \to p_1 \vee p_2$ |
| | $(p_1 \to p_3) \to (p_2 \to p_3) \to (p_1 \vee p_2 \to p_3)$ |
| | $(p_1 \to p_2) \to (p_1 \to \neg p_2) \to \neg p_1$ |
| | $\neg\neg p_1 \to p_1$ |
| | $p_1 \wedge p_2 \to p_1$ |
| | $p_1 \wedge p_2 \to p_2$ |
| | $p_1 \to p_2 \to p_1 \wedge p_2$ |
| | $\Box(p \to q) \to (\Box p \to \Box q)$ |
| Rules | $\dfrac{p \qquad p \to q}{q} \qquad \dfrac{p}{\Box p}$ |

**Table 2.** A Frege system for the modal logic **K**

| modal logic | axioms | | |
|---|---|---|---|
| **K4** | **K** | + | $\Box p \to \Box\Box p$ |
| **KB** | **K** | + | $p \to \Box\Diamond p$ |
| **GL** | **K** | + | $\Box(\Box p \to p) \to \Box p$ |
| **S4** | **K4** | + | $\Box p \to p$ |
| **S4.Grz** | **S4** | + | $\Box(\Box(p \to \Box p) \to p) \to p$ |

**Table 3.** Frege systems for important modal logics

implement the expressive DL $\mathcal{SROIQ}$ [57] which is N2ExpTime-complete [68].[5] Tableaux are also often used for establishing upper bounds for the complexity of a SAT problem for a logic.

**Semantics of Modal Logic.** A large class of modal logics can be characterised semantically via Kripke frames, including all the ones that are introduced here.[6]

**Definition 5.** *A **Kripke frame**[7] (or simply a **frame**) is a pair $(W, R)$ where*

- *$W$ is a set (the set of **worlds**) and*
- *$R$ is a binary relation on $W$.* ■

As in classical logic, if we augment frames with assignments, we arrive at the notion of a model.

**Definition 6.** *A **Kripke model** (or simply a **model**) for the modal language is a pair $(F, V)$ where*

- *$F = (W, R)$ is a frame and*
- *$V : \mathsf{Var} \mapsto \mathcal{P}(W)$ is a mapping assigning to each propositional variable $x$ a set $V(x)$ of worlds ($\mathcal{P}(W)$ denotes the power set of $W$).* ■

With the notion of models in place we can now define the notion of satisfaction or truth for modal formulae which is defined with respect to pointed models as follows:

**Definition 7.** *Let $\varphi, \psi$ be modal formulae, let $M = (W, R, V)$ be a model and $w \in W$ be a world. Inductively we define the notion of a formula to be **satisfied** in $M$ at world $w$:*

- *$M, w \models x$ if $w \in V(x)$ where $x \in \mathsf{Var}$,*
- *$M, w \models \neg\varphi$ if not $M, w \models \varphi$,*
- *$M, w \models \varphi \wedge \psi$ if $M, w \models \varphi$ and $M, w \models \psi$*
- *$M, w \models \varphi \vee \psi$ if $M, w \models \varphi$ or $M, w \models \psi$*
- *$M, w \models \Box\varphi$ if for all $v \in W$ with $(w, v) \in R$ we have $M, v \models \varphi$.* ■

[5] Compare http://www.cs.man.ac.uk/ sattler/reasoners.html for a comprehensive list of implemented DL reasoners.

[6] When giving a general definition of *normal modal logic* as any set of modal formulae containing the distributivity axiom and being closed under necessitation, modus ponens, and uniform substitution, the more abstract notion of *general frames* is needed to give general semantics [31, 70].

[7] Most textbooks present a slightly more restrictive definition, assuming a *non-empty* set of worlds, which would also suffice for our purposes. However, in some contexts allowing also empty sets of worlds is more natural from a technical point of view. Examples are multiple-conclusion rules, and duality theory: the empty frame is dual to the one-element modal (or Heyting, in the intuitionistic case) algebra (see e.g. [70]).

A modal formula $\varphi$ is **satisfiable** if there exists a model $M = (W, R, V)$ and a world $w \in W$ such that $M, w \models \varphi$. Dually, $\varphi$ is a **modal tautology** if for every model $M = (W, R, V)$ and every $w \in W$ we have $M, w \models \varphi$. Given a frame $F$, a formula $\varphi$ is moreover said to be **valid on** $F$ if $\varphi$ is satisfied in every pointed model based on $F$.

It can be shown that the Frege system from the previous section is indeed a proof system for the modal logic **K**, i.e. it is sound and complete for all modal tautologies.

More generally, let $\mathfrak{F}$ be some class of frames, and let $L(\mathfrak{F})$ be the set of formulae that are valid on all frames in $\mathfrak{F}$. It is easily seen that this defines a normal modal logic, i.e. a set of formulae that contains all axioms of **K** and which is closed under the rules of **K** as well as substitution.

The semantics of other modal logics can therefore conveniently be defined via suitable restrictions on the class of all Kripke frames and by imposing frame validity with respect to these classes of frames. More formally, we say that a logic $L$ is characterised by a class $\mathfrak{F}$ of frames if all $\varphi \in L$ are valid in $\mathfrak{F}$, and any non-theorem $\varphi \notin L$ can be refuted in a model based on a frame in $\mathfrak{F}$. For example, **K4** consists of all modal formulae which are valid over all transitive frames (i.e. the relation $R$ is transitive) and **KB** is the class modal formulae which are valid over all symmetric frames. See Table 4 for an overview.

| modal logic | characterising class of frames |
|---|---|
| **K** | all frames |
| **K4** | all transitive frames |
| **KB** | all symmetric frames |
| **GL** | $R$ transitive and $R^{-1}$ well-founded |
| **S4** | all reflexive and transitive frames |
| **S4.Grz** | $R$ reflexive and transitive; $R^{-1} \setminus \mathrm{Id}$ well-founded |

**Table 4.** Characterising classes of frames

This kind of characterisation gives rise to the field of *modal correspondence theory* (see [70] for a comprehensive overview) culminating in the Sahlqvist Correspondence Theorem that systematically characterises a class of modal axioms and corresponding characterising first-order frame conditions. To illustrate this idea, we show the example of the modal logic axiom defining the logic **K4** and the first-order axiom that characterises the class of transitive frames. Let $(W, R)$ be a frame, $R$ is **transitive** if $\forall x, y, z \in W. xRy$ and $yRz$ imply $xRz$.

**Proposition 8.** *For any frame $F = (W, R)$:*

$$\Box p \to \Box\Box p \textit{ is valid on } F \iff R \textit{ is transitive}$$

*Proof.* We first show that the 4-axiom is valid in transitive frames. By contraposition, assume $F = (W, R)$ is a frame such that $\Box p \to \Box\Box p$ is not valid on $F$, i.e. there is a model $M$ based on $F$ and a point $x \in W$ such that $M, x \not\models \Box p \to \Box\Box p$, i.e. $M, x \models \Box p \wedge \Diamond\Diamond\neg p$. Then there are points $y, z$ such that $xRyRz$, $M, y \models p \wedge \Diamond\neg p$ and $M, z \models \neg p$ . Clearly, $F$ cannot be transitive.

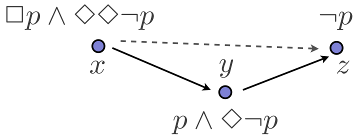


**Fig. 2.** A non-transitive frame refuting the 4-axiom.

Conversely, assume we are given an intransitive frame $F$, i.e. we have $xRy$, $yRz$, but $\neg xRz$. Define a model on $F$ as in Fig. 2 ($p$ holds everywhere except $z$). Clearly, $\Box p \to \Box\Box p$ is refuted in $x$.

■

For more information on modal logics we refer the reader to the monographs [31, 70, 14, 46], or the thorough introduction in [65].

### 3.2 Intuitionistic Logic and Semantics

While modal logics extend the classical propositional calculus with new sentence-forming operators (i.e. the modal operators), *intuitionistic logic* is a restriction thereof.[8]

Intuitionistic propositional logic **INT** is an attempt to provide a formal explication of Luitzen Egbertus Jan Brouwer's philosophy of intuitionism (1907/8) [20, 21]. One of Brouwer's main positions was a rejection of the tertium non datur:

> [. . . ] [To the Intuitionist] the dogma of the universal validity of the principle of excluded third is a phenomenon in the history of civilisation, like the former belief in the rationality of $\pi$, or in the rotation of the firmament about the earth. [22, p. 141–42]

A main idea in Heyting's formalisation was to preserve not truth (as in classical logic), but *justifications*. Indeed, one of the main principles of intuitionism is that the truth of a statement can only be established by giving a constructive proof. When reading intuitionistic formulae, it is therefore instructive to read the connectives in terms of 'proofs' or 'constructions'. The following interpretation of the intuitionistic connectives is often called the **Brouwer-Heyting-Kolmogorov interpretation** (or BHK-interpretation):

[8] The exposition of intuitionistic logic and its semantics based on possible worlds presented here largely follows [31].

- A proof of a proposition $\varphi \wedge \psi$ consists of a proof of $\varphi$ and a proof of $\psi$.
- A proof of $\varphi \vee \psi$ is given by presenting either a proof of $\varphi$ or a proof $\psi$, and by telling which of the two is presented.
- A proof of $\varphi \to \psi$ is a construction which, given a proof of $\varphi$, returns a proof of $\psi$.
- $\perp$ has no proof and a proof of $\neg\varphi$ is a construction which, given a proof of $\varphi$, would return a proof of $\perp$.

The tertium, i.e. the law of excluded middle, clearly, is not valid in the BHK-interpretation.

**Frege Systems for Intuitionistic Logics.** The intuitionistic propositional calculus in the form of a Hilbert (Frege) calculus was devised by Kolmogorov (1925) [69], Orlov (1928) [89], and Glivenko (1929) [51]. The first-order version, which we won't discuss here in detail, by Arend Heyting (1930) [56].

A typical Frege system for intuitionistic logic is the system depicted in Table 5 which is derived from the classical Frege system in Section 2.1.

| | |
|---|---|
| Axioms | $p_1 \to (p_2 \to p_1)$ |
| | $(p_1 \to p_2) \to (p_1 \to (p_2 \to p_3)) \to (p_1 \to p_3)$ |
| | $p_1 \to p_1 \vee p_2$ |
| | $p_2 \to p_1 \vee p_2$ |
| | $(p_1 \to p_3) \to (p_2 \to p_3) \to (p_1 \vee p_2 \to p_3)$ |
| | $\perp \to p_1$ |
| | $p_1 \wedge p_2 \to p_1$ |
| | $p_1 \wedge p_2 \to p_2$ |
| | $p_1 \to p_2 \to p_1 \wedge p_2$ |
| Modus Ponens | $\dfrac{p \qquad p \to q}{q}$ |

**Table 5.** A Frege system for intuitionistic logic **INT**.

Note that the axiom $\perp \to p_1$ here replaces two classical axioms. An important property of this Frege system (and of intuitionistic logic generally) is the so-called **disjunction property**. It can be read in a constructive fashion as follows:

for every *proof* of a disjunction $A \vee B$
there *exists a proof* of either $A$ or $B$.

Clearly, this does not hold classically. From a proof of the (classical) tautology $p \vee \neg p$ in **PL** we cannot find a proof of either of $p$ or $\neg p$.[9]

[9] Indeed, neither of $p$ or $\neg p$ are provable in **PL** ($p$ a propositional variable), and any (substitution-invariant) proper extension of **PL** with axioms $p$ or $\neg p$ is inconsistent.

**Intuitionistic Kripke Semantics.** The interpretation of intuitionism in terms of justifications or proofs is particularly well-reflected in the possible worlds semantics for **INT**, first given by Saul Kripke in 1965 [80], that we present next. In this semantics, we interpret this intuition in an epistemic way as follows (see [31]):

- possible worlds are understood as '*states of knowledge*';
- moving from one world to the next *preserves the current knowledge*;
- a proposition not true now can *become true* at a later stage

More formally, then, the connectives are interpreted as follows:

- $\varphi \wedge \psi$ is true at a state $x$ if both $\varphi$ and $\psi$ are true at $x$.
- $\varphi \vee \psi$ is true at $x$ if either $\varphi$ or $\psi$ is true at $x$.
- $\varphi \rightarrow \psi$ is true at a state $x$ if, for every subsequent possible state $y$, in particular $x$ itself, $\varphi$ is true at $y$ only if $\psi$ is true at $y$.
- $\perp$ is true nowhere.

To define possible worlds semantics that reflect this reading, define a **Kripke frame for INT** as a frame $\langle W, \leq \rangle$, where $\leq$ is a partial order (i.e. reflexive, antisymmetric, and transitive). Whilst the notion of a pointed model is the same as in standard modal logic, the notions of valuation and satisfaction have to be adapted. We first define **intuitionistic valuations** as *upward closed valuations* as follows: $\beta(p) \subseteq W$ such that: for every $x \in \beta(p)$ and $y \in W$ with $xRy$ we have $y \in \beta(p)$.

We can now formally define **intuitionistic satisfaction** of propositional formulae:

$$\begin{aligned}
M, x &\not\models \perp \\
M, x \models p \wedge q &\iff M, x \models p \text{ and } M, x \models q \\
M, x \models p \vee q &\iff M, x \models p \text{ or } M, x \models q \\
M, x \models p \rightarrow q &\iff \text{for any } y \geq x : \text{if } M, y \models p \text{ then } M, y \models q \\
M, x \models \neg p &\iff \text{for no } y \geq x : M, y \models p \; ( \iff M, x \models p \rightarrow \perp)
\end{aligned}$$

This semantics can be shown to be sound and complete for the Frege system for **INT** given in the previous section.

To understand the relationship between classical and intuitionistic logic, it is instructive to see that we can embed **PL** into **INT** by simply adding a double negation in front of classical tautologies: the following is called Glivenko's Theorem. For the proof, note that the so-called *generation theorem* states that, informally, to determine whether a formula is satisfied in a point $x$, it is sufficient to consider the frame generated by the point $x$. Therefore, by $x \uparrow$ we denote the upward-closed set generated by $x$, i.e. $x \uparrow = \{y \mid y \geq x\}$ (note that this is upward-closed by transitivity).

**Theorem 9 (Glivenko).** *For every formula $\varphi$: $\varphi \in$* **PL** $\iff$ $\neg\neg\varphi \in$ **INT**.

*Proof.* The easy direction, from right to left, is as follows. Suppose $\neg\neg\varphi \in \mathbf{INT}$. Then $\neg\neg\varphi \in \mathbf{PL}$. Thus, by the classical law of double negation, i.e. $\neg\neg\varphi \leftrightarrow \varphi \in \mathbf{PL}$, we obtain $\varphi \in \mathbf{PL}$.

Now, for the opposite direction, by contraposition, assume $\neg\neg\varphi \notin \mathbf{INT}$. Then, since **INT** enjoys the finite-model property (see e.g. [31]), there are a finite model $M$ and a point $w$ in $M$ such that $M, w \not\models \neg\neg\varphi$. Hence there is a $v \in w\uparrow$ for which $v \models \neg\varphi$. Let $u$ be some final point in the set $w\uparrow$. Because truth is propagated upwards, we have: $u \models \neg\varphi$ and so $u \not\models \varphi$. Let $M'$ be the submodel of $M$ generated by $u$, i.e., $M', u \models p \iff M, u \models p$, for every variable $p$. According to the generation theorem, $M$ refutes $\varphi$. It follows that $\varphi \notin \mathbf{PL}$. ■

Such embeddings[10] from $L_1$ to $L_2$ have several useful features, e.g.:

1. logical connectives in $L_1$ can be understood in terms of those of $L_2$.
2. various properties of logics may be preserved along an embedding, e.g.: if $L_2$ is a decidable logic, then so is $L_1$.

We have seen how intuitionistic and classical logic can be related in this way. Let us next look at a similar result relating modal logic and intuitionistic logic using the famous Gödel-Tarski-McKinsey, or simply Gödel translation, embedding **INT** into **S4** (see [52, 102]). The main insight here is that the modality $\Box$ can alternatively be read as 'it is provable' or as 'it is constructable'. The translation $\mathsf{T} : \mathsf{For}(\mathbf{INT}) \to \mathsf{For}(\mathbf{S4})$ (where $\mathsf{For}(\cdot)$ denotes the sets of well-formed formulae) is defined as follows:

$$\begin{aligned}
\mathsf{T}(p) &= \Box p\\
\mathsf{T}(\bot) &= \bot\\
\mathsf{T}(\varphi \wedge \psi) &= \mathsf{T}(\varphi) \wedge \mathsf{T}(\psi)\\
\mathsf{T}(\varphi \vee \psi) &= \mathsf{T}(\varphi) \vee \mathsf{T}(\psi)\\
\mathsf{T}(\varphi \to \psi) &= \Box(\mathsf{T}(\varphi) \to \mathsf{T}(\psi))
\end{aligned}$$

Now the connection established by $\mathsf{T}$ is as follows:

**Theorem 10 (Gödel-Tarski-McKinsey Translation).**
*For every formula $\varphi \in \mathsf{For}(\mathbf{INT})$ we have*

$$\varphi \in \mathbf{INT} \iff \mathsf{T}(\varphi) \in \mathbf{S4} \iff \mathsf{T}(\varphi) \in \mathbf{S4.Grz}$$

The Gödel translation has several important applications, some of which are directly relevant for the area of proof complexity. First, $\mathsf{T}$ is being used to define the notion of a **modal companion** of a given superintuitionistic logic, i.e. for any modal logic $M$ that is a normal extension of **S4**, $M$ is a **modal companion** of the superintuitionistic logic $L$ if for any intuitionistic formula $\varphi$ we have:

$$\varphi \in L \iff \mathsf{T}(\varphi) \in M.$$

[10] We here only use a 'naive' form of embedding. For a full analysis of the notion of 'logic translation', consult [87].

In fact, there is an exact correspondence between the normal extensions of **S4** and superintuitionistic logics, see e.g. [31, 70] for details. This allows to transfer various meta-logical properties concerning **INT** to those of **S4**, and conversely. For instance, the admissibility of rules in **INT** can be reduced to the admissibility in **S4**.**Grz** or **S4**. Moreover, the equivalence of Frege systems **INT** [86] can be generalised to **S4** [63]. These issues will be discussed in greater detail in Section 6.

### 3.3 Default Logic

Besides modal and intuitionistic logics there are many other important non-classical logics. One example of such logics are non-monotonic logics which became an important new research field in logic after a seminal issue of the Artificial Intelligence journal in 1980. In one of these papers, Raymond Reiter defined what is now called Reiter's *default logic* [97], which is still one of the most popular systems under investigation in this branch of logic.[11] In a nutshell, non-monotonic logics are a family of knowledge representation formalisms mostly targeted at modelling *common-sense* reasoning. Unlike in classical logic, the characterising feature of such logics is that an *increase in information* may lead to the *withdrawal* of previously accepted information or may *blocks* previously possible inferences.
Some typical examples, involving incomplete information and 'jumping to conclusions', are the following:

- Medical diagnosis: Make a best guess at a diagnosis. Given a new symptom, revise the diagnosis.
- Databases: the closed world assumption: what we don't know explicitly, we assume to be false.
- Default rules: in the absence of conflicting information, apply a given rule of inference.

Reiter's default Logic is a special kind of non-monotonic logic, aiming at reasoning with exceptions without listing them and to model certain forms of common-sense reasoning. It adds to classical logic new logical inference rules, so-called defaults. Default logic is undecidable for first-order rules, and we here work with propositional logic only.

A **default theory** $\langle W, D\rangle$ consists of a set $W$ of propositional sentences and a set $D$ of **defaults** (or *default rules*). A default (rule) $\delta$ is an inference rule of the form $\dfrac{\alpha\colon\beta}{\gamma}$ , where $\alpha$ and $\gamma$ are propositional formulae and $\beta$ is a set of propositional formulae. The **prerequisite** $\alpha$ is also referred to as $p(\delta)$, the formulae in $\beta$ are called **justifications** (referred to as $j(\delta)$), and $\gamma$ is the **conclusion** that is referred to as $c(\delta)$. Informally, the idea is that we shall infer a consequent $\gamma$ from a set of formulae $W$ via a default rule $\dfrac{\alpha\colon\beta}{\gamma}$ , if

[11] An overview of the first 30 years of non-monotonic logic research might be found in [49].

the prerequisite $\alpha$ *is known* (i.e. belongs to $W$ and the justification $\beta$ is not inconsistent with the information in $W$. Here is a simple example.[12]

*Example 11.* Assume we want to formalise common-sense rules concerning the game of football. One such rule might say that 'A game of football takes place unless there is snow.' Let

$$W := \{\mathsf{football}, \mathsf{precipitation}, \mathsf{cold} \wedge \mathsf{precipitation} \rightarrow \mathsf{snow}\}$$

$$D := \left\{ \frac{\mathsf{football}\colon \neg\mathsf{snow}}{\mathsf{takesPlace}} \right\}$$

Because $W$ contains precipitation, but not cold, ¬snow is consistent with $W$ (i.e. it may rain, but not snow). Hence we *can* infer takesPlace. Now if cold is added to $W$, ¬snow becomes inconsistent with $W$, and so the inference is blocked. I.e., the rule is non-monotonic. Note that for being able to apply the rule, we do not need *to know* that it does not snow (i.e. ¬snow being a member of $W$), but we must be able *to assume* that it does not snow (consistency of information). ■

Another instructive example is given by considering the so-called *closed world assumption* from database theory.

*Example 12.* The closed world assumption typically underlies database querying:

> When database $D$ is queried whether $\varphi$ holds, it looks up the information and answers 'Yes' if it finds (or can deduce) $\varphi$. If it does not find it, it will answer 'No'.

This corresponds to the application of a particular type of default rule:

$$\frac{\mathsf{true}\colon \neg\varphi}{\neg\varphi}$$

This means that we can assume a piece of information to be false whenever it is consistent to do so. As an effect: we only need to record positive information in a knowledge base, all negative information can be derived by default rules. ■

Note that we have so far not formally defined the semantics of what it means 'to be known' and with respect to which theory we have to check for consistency relative to the justifications. The first idea would be to check consistency with respect to the set of facts, i.e. the members of $W$. However, consider the following example:

*Example 13.* Consider the default formalising the rule 'Usually my friend's friends are also my friends.':

$$\frac{\mathsf{friends}(x, y) \wedge \mathsf{friends}(y, z)\colon \mathsf{friends}(x, z)}{\mathsf{friends}(x, z)}$$

Clearly, from friends(tom, bob), friends(bob, sally) and friends(sally, tina), we want to be able to infer friends(tom, tina). However, note that this is possible only after an intermediate step that derives: friends(tom, sally), i.e., possible inferences depend on previously applied rules and expansion of known facts. ■

[12] Most of the examples and discussion below is extracted from [5].

Moreover, we can have default rules with conflicting information, which is one way to get around logical explosion found in classical logic: if the 'certain knowledge' is consistent, then application of default rules cannot lead to inconsistency. Here we notice another problem with considering just the set of basic facts:

*Example 14.* Consider the following default theory: $T = (W, D)$ with prerequisite $W = \{\mathsf{green}, \mathsf{aaaMember}\}$ and rules $D = \delta_1, \delta_2$, where

$$\delta_1 = \frac{\mathsf{green}\colon \neg\mathsf{likesCars}}{\neg\mathsf{likesCars}} \text{ , and}$$

$$\delta_1 = \frac{\mathsf{aaaMember}\colon \mathsf{likesCars}}{\mathsf{likesCars}}$$

Here, the first rule says that by default green people do not like cars, whilst members of the AAA (American Automobile Association) typically do. Clearly, a green AAA member generates the inconsistency $\neg\mathsf{likesCar} \wedge \mathsf{likesCar}$.

Clearly, the application of default rules should not lead to inconsistency even in the presence of conflicting rules. Rather, such rule application should *expand* the set of knowledge. To take care of the problems described in the previous two examples, the key concept in the semantics of default logics was introduced, i.e. the notion of **stable extensions**.

Several alternative but equivalent definitions for this notion have been given in the literature, e.g. operational, argumentation theoretic, through a fixpoint equation, or quasi-inductive (see [5]). We here give Reiter's original 1980 definition based on a fixed-point equation [97], as well as its equivalent formulation through a stage construction. The definition of stable extensions in terms of a fixed-point equation is as follows.

**Definition 15 (Stable Extension, Reiter 1980 [97]).** *For a default theory $\langle W, D\rangle$ and set of formulae $E$ we define $\Gamma(E)$ as the smallest set such that*

1. $W \subseteq \Gamma(E)$,
2. $\Gamma(E)$ *is deductively closed, and*
3. *for all defaults* $\frac{\alpha\colon \beta}{\gamma}$ *with* $\alpha \in \Gamma(E)$ *and* $\neg\beta \notin E$, *it holds that* $\gamma \in \Gamma(E)$.

*A* ***stable extension*** *of $\langle W, D\rangle$ is a set $E$ such that $E = \Gamma(E)$.* ■

An intuitive motivation for this definition is to understand stable extensions as sets of facts that correspond to (maximal) possible views of an agent, which might, however, be mutually incompatible. Note that constructing stable extensions is not a constructive process, but essentially non-deterministic as we have to guess the order in which to apply rules. We give one example:

*Example 16.* Consider again the default theory given in Example 14.
*Stable extension 1:* Apply rule $\delta_1$ first; this blocks the application of rule $\delta_2$. Guess $E = Th(\{\mathsf{green}, \mathsf{aaaMember}, \neg\mathsf{likesCars}\})$ and check that $\Gamma(E) = E$.
*Stable extension 2:* Apply rule $\delta_2$ first; this blocks the application of rule $\delta_1$. Guess $E = Th(\{\mathsf{green}, \mathsf{aaaMember}, \mathsf{likesCars}\})$ and check that $\Gamma(E) = E$. ■

The last example showed that stable extensions need not be unique, the next example shows that stable extensions do not always exist.

*Example 17.* Consider the default theory $\left\langle \varnothing, \frac{:p}{\neg p} \right\rangle$. None of the possible guesses yields a stable extension:

$$\begin{aligned} E = Th(\varnothing) &\implies \Gamma(E) = Th\{\neg p\} \\ E = Th(p) &\implies \Gamma(E) = Th\{\neg p\} \\ E = Th(\neg p) &\implies \Gamma(E) = Th\{\varnothing\} \end{aligned}$$

This shows that minimality is not enough (the third guess is minimal). Note that a stable extension only contains formulae for which there is a proof. ■

A default rule is called **normal** if it is of the form $\frac{\varphi : \psi}{\psi}$. Many default rules are normal, such as closed world defaults, exception defaults, or frame defaults. The following theorem is therefore of importance:

**Theorem 18 (Normal Defaults, Reiter 1980 [97]).** *A default theory with only normal default rules always has stable extensions.* ■

The following characterisation of stable extensions is equivalent to the fixpoint definition given above:

**Theorem 19 (Stage Construction, Reiter 1980 [97]).** *Let $E \subseteq \mathcal{L}$ be a set of formulae and $\langle W, D\rangle$ be a default theory. Furthermore let $E_0 = W$, and*

$$E_{i+1} = Th(E_i) \cup \{c(\delta) \mid \delta \in D, E_i \vdash p(\delta), \neg j(\delta) \cap E = \varnothing\},$$

*where $\neg j(\delta)$ denotes the set of all negated sentences contained in $j(\delta)$. Then $E$ is a* (stable) extension *of $\langle W, D\rangle$ if and only if $E = \bigcup_{i\in\mathbb{N}} E_i$.* ■

We have seen that a default theory $\langle W, D\rangle$ can have none or several stable extensions (cf. [54] for more examples). Given a default theory $\langle W, D\rangle$, to determine whether $\langle W, D\rangle$ has a stable extension is called the **extension existence problem**. We then say a sentence $\psi \in \mathcal{L}$ is **credulously** entailed by $\langle W, D\rangle$ if $\psi$ holds in *some* stable extension of $\langle W, D\rangle$. Moreover, if $\psi$ holds in *every* extension of $\langle W, D\rangle$, then $\psi$ is **sceptically** entailed by $\langle W, D\rangle$.

Default rules with empty justification are called **residues**. We use the notation $\mathcal{L}^{res} = \mathcal{L} \cup \left\{ \frac{\alpha}{\gamma} \mid \alpha, \gamma \in \mathcal{L} \right\}$ for the set of all formulae and residues. Residues can be used to alternatively characterise stable extensions. For a set $D$ of defaults and $E \subseteq \mathcal{L}$ let $RES(D,E) = \left\{ \frac{p(\delta)}{c(\delta)} \mid \delta \in D,\ E \cap \neg j(\delta) = \varnothing \right\}$. Apparently, $RES(D,E)$ is a set of residues. We can then build stable extensions via the following closure operator. For a set $R$ of residues we define $Cl_0(W,R) = W$ and $Cl_{i+1}(W,R) = Th(Cl_i(W,R)) \cup \left\{ \gamma \mid \frac{\alpha}{\gamma} \in R, \alpha \in Th(Cl_i(W,R)) \right\}$. Let $Cl(W,R) = \bigcup_{i=0}^{\infty} Cl_i(W,R)$. Then we obtain for the sets $E_i$ from Theorem 19:

**Proposition 20 (Bonatti, Olivetti [16]).** *Let $\langle W, D\rangle$ be a default theory and let $E \subseteq \mathcal{L}$. Then $E_i = Cl_i(W, RES(D,E))$ for all $i \in \mathbb{N}$. In particular, $E$ is a stable extension of $\langle W, D\rangle$ if and only if $E = Cl(W, RES(D,E))$.* ■

If $D$ only contains residues, then there is an easier way of characterising $Cl$:

**Lemma 21 (Bonatti, Olivetti [16]).** *For $D \subseteq \mathcal{L}^{res} \setminus \mathcal{L}$, $W \subseteq \mathcal{L}$, and for $i \in \mathbb{N}$ let $C_0 = W$ and $C_{i+1} = C_i \cup \left\{ \gamma \mid \frac{\alpha}{\gamma} \in D, \alpha \in Th(C_i) \right\}$. Then $\gamma \in Cl(W,D)$ if and only if there exists $k \in \mathbb{N}$ with $\gamma \in Th(C_k)$.* ■

The semantics and the complexity of default logic have been intensively studied during the last decades (cf. [29] for a survey). In particular, Gottlob [54] has identified and studied two reasoning tasks for propositional default logic: the *credulous* and the *sceptical* reasoning problem (see above), which can be understood as analogues of the classical problems SAT and TAUT. Because of the higher expressivity of default logic, however, credulous and sceptical reasoning become harder than their classical counterparts—they are complete for the second level $\Sigma_2^{\mathsf{p}}$ and $\Pi_2^{\mathsf{p}}$ of the polynomial hierarchy [54]. Indeed, the extension existence problem itself is $\Sigma_2^{\mathsf{p}}$-complete.

In Section 7, we will introduce simple and elegant sequent calculi for credulous and sceptical default reasoning, introduced by Bonatti and Olivetti [16], and use this to study the proof complexity of default logic.

## 4 Interpolation and the Feasible Interpolation Technique

Interpolation is a very interesting and important topic in logic. In this section we first explain Craig's classical interpolation theorem and then discuss interpolation for non-classical logics. After this we continue with feasible interpolation. Feasible interpolation is a general lower bound technique that works for a number of diverse proof systems. In Section 5, we want to use a variant of this method to obtain lower bounds even for Frege systems in modal logics.

### 4.1 Interpolation in Classical and Non-Classical Logic

**The Classical Case.** Feasible interpolation has been successfully used to show lower bounds to the proof size of a number of proof systems like Resolution and Cutting Planes. It originates in the classical interpolation theorem of Craig of which we only need the propositional version.

**Theorem 22 (Craig's Interpolation Theorem [36]).**
*Let $\varphi(\bar{x}, \bar{y})$ and $\psi(\bar{x}, \bar{z})$ be propositional formulae with all variables displayed. Let $\bar{y}$ and $\bar{z}$ be distinct tuples of variables such that $\bar{x}$ are the common variables of $\varphi$ and $\psi$. If*

$$\varphi(\bar{x}, \bar{y}) \to \psi(\bar{x}, \bar{z})$$

*is a tautology, then there exists a propositional formula $\theta(\bar{x})$ using only the common variables of $\varphi$ and $\psi$ such that*

$$\varphi(\bar{x}, \bar{y}) \to \theta(\bar{x}) \quad \textit{and} \quad \theta(\bar{x}) \to \psi(\bar{x}, \bar{z})$$

*are tautologies.*

*Proof.* Consider the Boolean function $\exists\bar{y}\varphi(\bar{x},\bar{y})$. This function interpolates $\varphi(\bar{x},\bar{y})$ and $\psi(\bar{x},\bar{y})$ because

$$\varphi(\bar{x},\bar{y}) \to \exists\bar{y}\varphi(\bar{x},\bar{y})$$

is always a tautology and since $\varphi(\bar{x},\bar{y}) \to \psi(\bar{x},\bar{z})$ is tautological this is also true for

$$(\exists\bar{y}\varphi(\bar{x},\bar{y})) \to \psi(\bar{x},\bar{z}) \ .$$

Every Boolean function can be described by a propositional formula in the same variables. Hence any formula expressing $\exists\bar{y}\varphi(\bar{x},\bar{y})$ is an interpolant of $\varphi(\bar{x},\bar{y}) \to \psi(\bar{x},\bar{z})$. Alternatively we could have taken a formula for $\forall\bar{z}\psi(\bar{x},\bar{z})$. ■

A formula $\varphi(\bar{x},\bar{y})$ is **monotone** in the variables $\bar{x}$ if these variables do not occur in the scope of connectives other than conjunction and disjunction. A formula is called monotone, if it is monotone in all its variables, i.e. there are only conjunctions and disjunctions, but no negations or implications.

In the previous theorem, if $\varphi(\bar{x},\bar{y}) \to \psi(\bar{x},\bar{z})$ is monotone in $\bar{x}$, then there exists a monotone interpolating formula $\theta(\bar{x})$.

**The Non-Classical Case.** The basic definition of Craig interpolation straightforwardly carries over to the non-classical case. However, additional distinctions can be introduced, as for instance requiring the interpolant to use only shared modalities. Whilst several of the more well-known non-classical logics enjoy interpolation, such as **INT**, **K**, **K4**, **T**, and **S4**, a general characterisation or giving criteria for modal logics that have Craig interpolation are rather complex problems. A comprehensive overview of results concerning modal and intuitionistic logics can be found in the monograph [47]. Another point to note is that in the non-classical case, extensions of the language can easily lead to the loss of the interpolation property. For instance, consider the language $M(D)$ which extends the basic modal language with the **difference operator** $D$, where $D\varphi$ is true at a point $x$ if $\varphi$ is true at every point $y \neq x$. It has been shown by ten Cate that full first-order logic is the least expressive extension of $M(D)$ that has interpolation [103], i.e. that there is no decidable language using the difference operator that has interpolation.

In non-classical logics, there is also a distinction between Craig's interpolation property (CIP, formulated as in Theorem 22) and the interpolation property for derivability (IPD, formulated with $\varphi(\bar{x},\bar{y}) \vdash \psi(\bar{x},\bar{z})$ instead of $\varphi(\bar{x},\bar{y}) \to \psi(\bar{x},\bar{z})$ and similarly for the two implications involving the interpolant).

In the following, we will restrict our attention to a more restricted form of interpolation that takes into account the *size* of the interpolant, namely the problem of *feasible interpolation.*

### 4.2 Feasible Interpolation

Craig's interpolation theorem (Theorem 22) only states the existence of an interpolating formula. Mundici [88] was the first to consider the question whether there is even an interpolant that has polynomial size in terms of the formulae $\varphi(\bar{x}, \bar{y})$ and $\psi(\bar{x}, \bar{z})$. His results indicate that this is not likely to be the case (unless $\mathsf{NP} \cap \mathsf{coNP} \subseteq \mathsf{P/poly}$). It was Krajíček's idea [71] to measure the size of the interpolant not only in terms of the initial formulae, but also in terms of a proof of the implication $\varphi(\bar{x}, \bar{y}) \to \psi(\bar{x}, \bar{z})$ in a particular proof system. This leads to the notion of feasible interpolation.

**Definition 23 (Krajíček [73]).** *A proof system $P$ has **feasible interpolation** if there exists a polynomial-time procedure that takes as input an implication $\varphi(\bar{x}, \bar{y}) \to \psi(\bar{x}, \bar{z})$ and a $P$-proof $\pi$ of $\varphi(\bar{x}, \bar{y}) \to \psi(\bar{x}, \bar{z})$ and outputs a Boolean circuit $C(\bar{x})$ such that for every propositional assignment $\bar{a}$ the following holds:*

1. *If $\varphi(\bar{a}, \bar{y})$ is satisfiable, then $C(\bar{a})$ outputs $1$.*
2. *If $\neg\psi(\bar{a}, \bar{z})$ is satisfiable, then $C(\bar{a})$ outputs $0$.* ■

We note that the standard definition of feasible interpolation given in [73] is non-uniform: it only states that there exists a polynomial-size circuit $C$ with the required properties. The uniform version is conceptually better and in fact holds for most proof systems with (non-uniform) feasible interpolation. Under mild requirements satisfied by all proof systems encountered in the wild (namely, that there is a polynomial-time algorithm which given a proof of a formula $\varphi(\bar{x}, \bar{y})$ and an assignment $\bar{a}$ produces a proof of $\varphi(\bar{a}, \bar{y})$), the uniform definition of feasible interpolation (Definition 23) can be considerably simplified: it is equivalent to its special case with empty $\bar{x}$, in which case one does not have to mention any circuits at all.

Feasible interpolation has been shown for Resolution [73], the Cutting Planes system [18, 73, 91] and some algebraic proof systems [93].

If we have feasible interpolation for a proof system, this immediately implies conditional super-polynomial lower bounds to the proof size in the proof system as in the following theorem:

**Theorem 24.** *Let $P$ be a proof system with feasible interpolation. If $\mathsf{NP} \cap \mathsf{coNP} \not\subseteq \mathsf{P/poly}$, then $P$ is not polynomially bounded.* ■

This method uses the following idea: suppose we *know* that a sequence of formulae $\varphi_0^n(\bar{x}, \bar{y}) \to \varphi_1^n(\bar{x}, \bar{z})$ cannot be interpolated by a family of polynomial-size circuits as in Definition 23. Then the formulae $\varphi_0^n \to \varphi_1^n$ do not have polynomial-size proofs in any proof system which has feasible interpolation. Such formulae $\varphi_0^n \to \varphi_1^n$ are easy to construct under suitable assumptions. For instance, the formulae could express that factoring integers is not possible in polynomial time (which implies $\mathsf{NP} \cap \mathsf{coNP} \not\subseteq \mathsf{P/poly}$).

To improve Theorem 24 to an unconditional lower bound, we need super-polynomial circuit lower bounds for suitable functions, and such lower bounds are only known for restricted classes of Boolean circuits (cf. [107]). One such restricted class consists of all *monotone* Boolean circuits which only use gates $\wedge$ and $\vee$. Building on earlier work of Razborov [94], Alon and Boppana [3] were able to show exponential lower bounds to the size of monotone circuits which separate the Clique-Colouring pair. The components of this pair contain graphs which are $k$-colourable or have a clique of size $k+1$, respectively. Clearly, this yields a disjoint $\mathsf{NP}$-pair. The disjointness of the Clique-Colouring pair can be expressed by a sequence of propositional formulae

$$\mathit{Clique}_n^{k+1}(\bar{p}, \bar{r}) \to \neg \mathit{Colour}_n^k(\bar{p}, \bar{s}) \tag{1}$$

where $\mathit{Colour}_n^k(\bar{p}, \bar{s})$ expresses that the graph encoded in the variables $\bar{p}$ is $k$-colourable. Similarly, $\mathit{Clique}_n^{k+1}(\bar{p}, \bar{r})$ expresses that the graph specified by $\bar{p}$ contains a clique of size $k+1$. Alon and Boppana [3] prove a strong lower bound on the monotone circuit complexity of computing the size of the largest clique in a graph. Choosing $k = \sqrt{n}$, Alon and Boppana's theorem yields:

**Theorem 25 (Alon, Boppana [3]).** *For $k = \sqrt{n}$, the Clique-Colour formulae* (1) *require monotone interpolating circuits of size $2^{\Omega(n^{\frac{1}{4}})}$.* ■

For example for Resolution, we have monotone feasible interpolation:

**Theorem 26 (Krajíček [73]).** *Let $\varphi(\bar{x}, \bar{y}) \to \psi(\bar{x}, \bar{z})$ be a tautology such that $\varphi(\bar{x}, \bar{y})$ or $\psi(\bar{x}, \bar{z})$ is monotone in $\bar{x}$. If $\pi$ is a Resolution refutation of $\varphi(\bar{x}, \bar{y}) \wedge \neg\psi(\bar{x}, \bar{z})$, then there exists a polynomial-size interpolating circuit $C$ as in Definition 23 which is monotone.* ■

Combining this monotone interpolation for Resolution with Theorem 25 yields:

**Theorem 27.** *For $k = \sqrt{n}$, the clause sets expressing the negation of the Clique-Colour formulae* (1) *require Resolution refutations of size $2^{n^{\Omega(1)}}$.* ■

Monotone feasible interpolation is also known to hold for other systems as Cutting Planes, but does not hold for Frege systems under reasonable assumptions (factoring integers is not possible in polynomial time [77, 19]).

## 5 Lower Bounds for Modal and Intuitionistic Logics

One of the first topics in proof complexity of non-classical logics was the investigation of the **disjunction property** in intuitionistic logic, stating that if $\varphi \vee \psi$ is an intuitionistic tautology, then either $\varphi$ or $\psi$ already is. Buss, Mints, and Pudlák [27, 28] showed that this disjunction property even holds in the following feasible form:

**Theorem 28 (Buss, Mints, Pudlák [27, 28]).** *Intuitionistic logic has the* ***feasible disjunction property****, i. e., for the standard natural deduction calculus for intuitionistic logic (which is polynomially equivalent to the usual intuitionistic Frege system) there is an algorithm $A$ such that for each proof $\pi$ of a disjunction $\varphi \vee \psi$, the algorithm $A$ outputs a proof of either $\varphi$ or $\psi$ in polynomial time in the size of $\pi$.* ■

Subsequently, Ferrari, Fiorentini, and Fiorino [42] extended this result to further logics. They proved the feasible disjunction property for intuitionistic natural deduction (just like Buss and Mints [27]), natural deduction systems for **S4**, **S4**.**Grz**, and **S4.1**, and Frege systems for **GL** and Fisher Servi's **IK**.

A related property to feasible disjunction is the **feasible interpolation property**. As mentioned in Section 1, feasible interpolation is one of the general approaches to lower bounds in proof complexity. This technique was developed by Krajíček [73] and has been successfully applied to show lower bounds for a number of weak systems as Resolution or Cutting Planes (but unfortunately fails for strong systems as Frege systems and their extensions [77, 19]). For intuitionistic logic, feasible interpolation holds in the following form:

**Theorem 29 (Buss, Pudlák [28]).** *Intuitionistic logic has the* feasible interpolation property*, i. e., from a proof $\pi$ of an intuitionistic tautology*

$$(p_1 \vee \neg p_1) \wedge \cdots \wedge (p_n \vee \neg p_n) \to \varphi_0(\bar{p}, \bar{q}) \vee \varphi_1(\bar{p}, \bar{r})$$

*using distinct sequences of variables $\bar{p}, \bar{q}, \bar{r}$ (such that $\bar{p} = p_1, \dots, p_n$ are the common variables of $\varphi_0$ and $\varphi_1$) we can construct a Boolean circuit $C$ of size $|\pi|^{O(1)}$ such that for each input $\bar{a} \in \{0,1\}^n$, if $C(\bar{a}) = i$, then $\varphi_i(\bar{p}/\bar{a})$ is an intuitionistic tautology (where variables $\bar{p}$ are substituted by $\bar{a}$, and $\bar{q}$ or $\bar{r}$ are still free).* ■

A version of feasible interpolation for some special class of modal formulae was also shown for the modal logic **S4** by Ferrari, Fiorentini, and Fiorino [42]. From this version of feasible interpolation[13] we obtain conditional super-polynomial lower bounds to the proof size in the proof systems as in Theorem 24.

**Theorem 30 (Buss, Pudlák [28], Ferrari, Fiorentini, Fiorino [42]).** *If* $\mathsf{NP} \cap \mathsf{coNP} \not\subseteq \mathsf{P/poly}$*, then neither intuitionistic Frege systems nor Frege systems for* **S4** *are polynomially bounded.* ■

Our aim in the rest of this section is to improve Theorem 30 to an unconditional lower bound. The lower bound for Frege in **K** which we will show now is due to Hrubeš [60]. The proof method is a variant of the feasible interpolation technique discussed in Section 4.2 and yields a lower bound for modal formulae derived from the Clique-Colour tautologies. We will first sketch the proof idea and then give the details.

[13] A terminological note (which we owe to Emil Jeřábek): while it became customary to refer to "feasible interpolation" in the context of intuitionistic proof systems, it may be worth a clarification that this is actually a misnomer. Interpolation means that if $\varphi(\bar{p}, \bar{q}) \to \psi(\bar{p}, \bar{r})$ is provable, where $\bar{p}, \bar{q}, \bar{r}$ are disjoint sequences of variables, then there is a formula $\theta(\bar{p})$ such that $\varphi(\bar{p}, \bar{q}) \to \theta(\bar{p})$ and $\theta(\bar{p}) \to \psi(\bar{p}, \bar{r})$ are also provable. In intuitionistic logic, this is a quite different property from the reformulations using disjunction which comes from classical logic. What is called "feasible interpolation" for intuitionistic logic (such as in Theorem 29) has nothing to do with interpolation, it is essentially a feasible version of Haldén completeness. Similarly, the modal "feasible interpolation" from [42] is a restricted version of the feasible modal disjunction property.

### 5.1 Sketch of the Lower Bound

Hrubeš [59, 60] had the idea to modify the Clique-Colouring formulae (1) in a clever way by introducing the modal operator $\Box$ in appropriate places to obtain

$$\mathit{Clique}_n^{k+1}(\Box\bar{p},\bar{r}) \to \Box(\neg \mathit{Colour}_n^k(\bar{p},\bar{s})) \tag{2}$$

with $k = \sqrt{n}$. For these formulae he was able to show in [60] that

1. the formulae (2) are modal tautologies;
2. if the formulae (2) are provable in $\mathbf{K}$ with $m(n)$ distributivity axioms, then the original formulae (1) can be interpolated by monotone circuits of size $O(m(n)^2)$.

Together these steps yield unconditional lower bounds for modal Frege systems:

**Theorem 31 (Hrubeš [59, 60]).** *The formulae* (2) *are* $\mathbf{K}$*-tautologies. If* $L$ *is a sublogic of* **GL** *or* **S4***, then every Frege proof of the formulae* (2) *in the logic* $L$ *uses* $2^{n^{\Omega(1)}}$ *steps.* ■

The first proof of Theorem 31 in [59] was obtained by a rather involved model-theoretic argument, but his later paper [60] contains the simplified approach sketched above.

### 5.2 Lower Bounds for Intuitionistic Logic

Along the same lines, Hrubeš proved lower bounds for intuitionistic Frege systems. For this he modified the Clique-Colouring formulae to the intuitionistic version

$$\bigwedge_{i=1}^{n}(p_i \lor q_i) \to (\neg \mathit{Colour}_n^k(\bar{p},\bar{s}) \lor \neg \mathit{Clique}_n^{k+1}(\neg\bar{q},\bar{r}) \tag{3}$$

where again $k = \sqrt{n}$.

**Theorem 32 (Hrubeš [58, 60]).** *The formulae* (3) *are intuitionistic tautologies and require intuitionistic Frege proofs with* $2^{n^{\Omega(1)}}$ *steps.* ■

The first proof of Theorem 32 in [58] was given via a translation of intuitionistic logic into modal logic, but again [60] reproves the result via the simplified approach. Theorem 32 also implies an exponential speed-up of classical logic over intuitionistic logic, because the formulae (3) have polynomial-size classical Frege proofs [58]. The lower bounds of Theorems 31 and 32 were extended by Jeřábek [65] to further logics, namely all modal and superintuitionistic logics with infinite branching.

The rest of this section contains the full proof of Theorem 31 for the modal logic $\mathbf{K}$. We follow the paper [60].

### 5.3 The Modal Clique-Colour Tautologies

For a sequence of variables $\bar{p} = p_1, \ldots, p_n$ we denote the sequence $\Box p_1, \ldots, \Box p_n$ by $\Box\bar{p}$. The following proposition provides a general method how to transform propositional tautologies into **K**-tautologies.

**Proposition 33.** *Let $\varphi(\bar{p}, \bar{r})$ and $\psi(\bar{p}, \bar{s})$ be propositional formulae which use common variables $\bar{p}$ and let $\varphi(\bar{p}, \bar{r})$ be monotone in $\bar{p}$. If $\varphi(\bar{p}, \bar{r}) \to \psi(\bar{p}, \bar{s})$ is a propositional tautology, then $\varphi(\Box\bar{p}, \bar{r}) \to \Box\psi(\bar{p}, \bar{s})$ is a* **K***-tautology.*

*Proof.* By the monotone version of Craig's interpolation theorem we obtain from the assumptions a monotone formula $\theta(\bar{p})$ which interpolates $\varphi(\bar{p}, \bar{r})$ and $\psi(\bar{p}, \bar{s})$, i.e.

$$\varphi(\bar{p}, \bar{r}) \to \theta(\bar{p}) \tag{4}$$

and

$$\theta(\bar{p}) \to \psi(\bar{p}, \bar{s}) \tag{5}$$

are propositional tautologies.

Substituting $\bar{p}$ by $\Box\bar{p}$ in (4) we obtain the **K**-tautology

$$\varphi(\Box\bar{p}, \bar{r}) \to \theta(\Box\bar{p}) \ . \tag{6}$$

Because $\theta(\bar{p})$ is monotone, we can prove from (6) inductively

$$\varphi(\Box\bar{p}, \bar{r}) \to \Box\theta(\bar{p}) \tag{7}$$

by using the modal tautologies $\Box A \circ \Box B \to \Box(A \circ B)$ for $\circ = \wedge, \vee$.

We also obtain

| | |
|---|---|
| $\Box(\theta(\bar{p}) \to \psi(\bar{p}, \bar{s}))$ | (from (5) by rule of necessitation) |
| $\Box(\theta(\bar{p}) \to \psi(\bar{p}, \bar{s})) \to (\Box\theta(\bar{p}) \to \Box\psi(\bar{p}, \bar{s}))$ | (axiom of distributivity) |
| $\Box\theta(\bar{p}) \to \Box\psi(\bar{p}, \bar{s})$ | (Modus Ponens) |

From this last formula and (7) we obtain the desired **K**-tautology $\varphi(\Box\bar{p}, \bar{r}) \to \Box\psi(\bar{p}, \bar{s})$. ■

Applying this proposition to the Clique-Colour formulae yields:

**Corollary 34.** *For all $n \geq 2$ and $k < n$ the formulae $\mathit{Clique}_n^{k+1}(\Box\bar{p}, \bar{r}) \to \Box(\neg \mathit{Colour}_n^k(\bar{p}, \bar{s}))$ are* **K***-tautologies.* ■

Thus we have shown step 1 from the sketch of the lower bound in Section 5.1.

### 5.4 Modal Assignments

Step 2 of Section 5.1 requires some preparations and preliminary observations on modal assignments and Horn clauses which we give in this and the following section.

**Definition 35.** *We call $\Box A$ an **immediate modal subformula** of a modal formula $\varphi$ if $\Box A$ appears as a subformula in $\varphi$ which is not in the scope of a modal connective $\Box$.* ■

If $\Box A_1, \dots, \Box A_n$ are the immediate modal subformulae of $\varphi$, then $\varphi$ can be written as

$$\psi(\Box A_1, \dots, \Box A_n, s_1, \dots, s_l)$$

where $\psi$ is a propositional formula and $s_1, \dots, s_l$ are the variables appearing in $\varphi$ outside the scope of a modal connective.

If we view $\Box A_1, \dots, \Box A_n$ as new variables, then we can evaluate $\varphi$ under a truth assignment $\sigma$ to $s_1, \dots, s_l$ and $\Box A_1, \dots, \Box A_n$.

**Definition 36.** *We call such an assignment $\sigma$ **consistent with** $\varphi$ if there exists a modal model $M, w$ such that $M, w \models \varphi$, and $M, w \models \Box A_i$ if and only if $\sigma(\Box A_i) = 1$ for $i = 1, \dots, k$.* ■

### 5.5 A Characteristic Set of Horn Clauses

One of the central ideas of [60] is to extract from a **K**-proof a "characteristic set" that in some sense only captures the applications of the modal rules in the proof. By the **modal rules** we mean the rule $\dfrac{p}{\Box p}$ of necessitation and the modal distributivity axiom $\Box(p \to q) \to (\Box p \to \Box q)$. A **modal step** in the proof is an application of one of the modal rules.

Instead of arguing on the full **K**-proof, the analysis is then carried out on the structurally simpler "characteristic skeleton" of the proof that only takes into account the modal steps. This characteristic set is defined as follows:

**Definition 37.** *Let $\pi$ be a proof in the Frege system for* **K**. *We define a **characteristic set** $\mathsf{C}_\pi$ of clauses for $\pi$:*

- *if the rule $\dfrac{A}{\Box A}$ occurs in $\pi$, then $\mathsf{C}_\pi$ contains the clause $\{\Box A\}$;*
- *if the axiom $\Box C \to (\Box A \to \Box B)$ occurs in $\pi$ where $C = A \to B$, then $\mathsf{C}_\pi$ contains the clause $\{\neg\Box C, \neg\Box A, \Box B\}$.* ■

Note that $\mathsf{C}_\pi$ is a set of Horn clauses which does not contain a negative clause.

In the rest of this section we will explore the connection between the characteristic set and the actual **K**-proof from which it originates. First we need two general lemmas on Horn clauses:

**Lemma 38.** *Let $D$ be a set of Horn clauses not containing a negative clause and let $N$ be a set of negative clauses. If $D \cup N$ is unsatisfiable, then there exists a clause $C \in N$ such that $D \cup \{C\}$ is unsatisfiable.* ■

**Definition 39.** *For a set of variables $V$ and an assignment $\sigma$, let*

$$V_\sigma := \{\{q\} \mid q \in V, \sigma(q) = 1\} \ .$$

■

**Lemma 40.** *Let $D$ be a set of Horn clauses of size $n$ not containing a negative clause. Let $V$ be a set of variables and $p$ be a variable. Then there exists a monotone circuit $C$ in variables $V$ of size $O(n^2)$ such that for any assignment $\sigma$ to $V$, $C$ outputs 1 if and only if*

$$D, V_\sigma, \{\neg p\}$$

*is unsatisfiable.* ■

The proof the two previous lemmas follows from the analysis of the standard satisfiability algorithm for Horn formulae.

The following three lemmas explain the connection between characteristic sets of clauses of **K**-proofs and actual **K**-proofs.

**Lemma 41.** *Let $\pi = A_1, \dots, A_k$ be a proof in the Frege system for* **K**. *Let $\sigma$ be an assignment to the immediate modal subformulae in $\pi$ and all variables in $\pi$ outside the scope of a modal connective $\Box$. If $\sigma$ satisfies $\mathsf{C}_\pi$, then $\sigma$ satisfies all formulae $A_i$ in the proof $\pi$.*

*Proof.* If $\sigma$ satisfies $\mathsf{C}_\pi$, then all conclusions of the modal rule of necessitation and all modal distributivity axioms in $\pi$ are satisfied by $\sigma$. The other formulae in $\pi$ are derived either by propositional axioms or Modus Ponens. Substitution instances of propositional axioms are true under all assignments $\sigma$, and if $\sigma$ satisfies the two prerequisites of an application of Modus Ponens, then $\sigma$ also satisfies the conclusion. ■

**Lemma 42.** *Let $\pi = A_1, \dots, A_n$ be a proof in the Frege system for* **K** *and let $B_1, \dots, B_k, B$ be formulae. If*

$$\mathsf{C}_\pi, \{\Box B_1\}, \dots, \{\Box B_k\}, \{\neg \Box B\}$$

*is not satisfiable, then*

$$\bigwedge_{i=1}^{k} \Box B_i \to \Box B$$

*is a* **K**-*tautology.*

*Proof.* Let $F_\pi$ be the set of distributivity axioms and conclusions of necessitation rules in the proof $\pi$. If $\mathsf{C}_\pi, \{\Box B_1\}, \dots, \{\Box B_k\}, \{\neg \Box B\}$ is not satisfiable, then

$$\left( \bigwedge F_\pi \wedge \bigwedge_{i=1}^{k} \Box B_i \right) \to \Box B$$

is a formula which by the deduction theorem is provable in a propositional Frege system. As all formulae in $F_\pi$ are **K**-tautologies, also

$$\bigwedge_{i=1}^{k} \Box B_i \to \Box B$$

is a **K**-tautology, proving the claim. ■

The next lemma is the key lemma in the chain of arguments leading to the lower bound in **K**. It expresses that the characteristic set of clauses of a **K**-proof $\pi$ is indeed "characteristic" for the proof $\pi$ in the sense that the validity of the proof $\pi$ is transferred to its characteristic set $\mathsf{C}_\pi$ (in the precise meaning stated below).

**Lemma 43.** *Let $\varphi$ and $\Box\psi$ be modal formulae and let $\Box A_1, \dots, \Box A_k$ be the immediate subformulae of $\varphi$. Let $\pi$ be a proof of the formula*

$$\varphi \to \Box\psi$$

*in the Frege system for* **K**. *Let $V = \{\Box A_1, \dots, \Box A_k\}$ and let $\sigma$ be an assignment to $V$ which is consistent with $\varphi$. Then the set of clauses*

$$\mathsf{C}_\pi, V_\sigma, \{\neg\Box\psi\}$$

*is not satisfiable.*

*Proof.* Let $Y_\sigma := \{\{\neg v\} \mid v \in V, \sigma(v) = 0\}$. We claim that

$$\mathsf{D} := \mathsf{C}_\pi, V_\sigma, Y_\sigma, \{\neg\Box\psi\}$$

is not satisfiable. Aiming for a contradiction, we us assume that $\mathsf{D}$ is satisfied by the assignment $\rho$. As $\sigma$ is fully described by $V_\sigma$ and $Y_\sigma$, the assignment $\rho$ extends $\sigma$.

As $\sigma$ is consistent with $\varphi$ there exists a model $M, w$ of $\varphi$ such that $M, w \models \Box A_i$ if and only if $\sigma(\Box A_i) = 1$. Let $\bar{s}$ be the variables in $\pi$ which do not appear in a modal context. For these variables we define an assignment $\rho'$ by setting $\rho'(s) = 1$ if and only if $M, w \models s$.

Let $\sigma' := \rho \cup \rho'$. By Lemma 41 $\sigma'$ satisfies all formulae from the proof $\pi$. Therefore, in particular, $\sigma'(\varphi \to \Box\psi) = 1$.

On the other hand, by the choice of $\sigma$, we have $\sigma(\neg\Box\psi) = 1$ and therefore also $\sigma'(\neg\Box\psi) = 1$. Also $M, w$ is a model of $\varphi$ and $M, w$ is consistent with $\sigma'$, implying $\sigma'(\varphi) = 1$. This yields $\sigma'(\varphi \to \Box\psi) = 0$ which is a contradiction to the previous paragraph.

It remains to show that also

$$\mathsf{C}_\pi, V_\sigma, \{\neg\Box\psi\}$$

is unsatisfiable. The only negative clauses in $\mathsf{D}$ are $\{\neg\Box\psi\}$ and the clauses from $Y_\sigma$. By Lemma 38 we know that there exists a clause $C \in \{\neg\Box\psi\} \cup Y_\sigma$ such that $\mathsf{C}_\pi, V_\sigma, C$ is already unsatisfiable. We have to show that $C$ is not a clause from $Y_\sigma$. Assume on the contrary that $C = \{\neg\Box A_j\}$ for some $j \in [k]$. Then, by Lemma 42, the formula

$$\bigwedge_{\Box A_i \in V_\sigma} \Box A_i \to \Box A_j$$

is a **K**-tautology. But $M, w \models \bigwedge_{\Box A_i \in V_\sigma} \Box A_i$ and $M, w \models \neg\Box A_j$ which is a contradiction. ■

### 5.6 A Version of Monotone Interpolation for K

The following theorem is a version of monotone feasible interpolation for Frege systems for **K**. It is not a full interpolation theorem (and we also cannot expect such a result because presumably we do not have feasible interpolation for classical Frege, cf. Section 4.2), but only holds for a special class of modal formulae.

**Theorem 44.** *Let $\pi$ be a proof of the formula*

$$\varphi \to \Box\psi$$

*in the Frege system for* **K** *which uses $n$ modal steps. Let $\Box A_1, \dots, \Box A_k$ be the immediate modal subformulae of $\varphi$. Then there exists a monotone circuit $C$ of size $O(n^2)$ in $k$ variables such that*

$$\varphi(\Box A_1, \dots, \Box A_k, \bar{s}) \to C(\Box A_1, \dots, \Box A_k) \qquad \textit{and} \qquad C(\Box A_1, \dots, \Box A_k) \to \Box\psi$$

*are* **K***-tautologies.*

*Proof.* The characteristic set $\mathsf{C}_\pi$ has size $\leq 3n$ as $\mathsf{C}_\pi$ contains $n$ clauses and each clause contains at most three literals.

Let $V = \{\Box A_1, \dots, \Box A_k\}$. Let $C$ be the monotone circuit from Lemma 40 of size $O(n^2)$ which outputs 1 if and only if $\mathsf{C}_\pi, V_\sigma, \{\neg\Box\psi\}$ is unsatisfiable. We note that by the previous Lemma, $C$ will always output 1 on assignments $\sigma$ which are consistent with $\varphi$, but we also have to consider other assignments.

We first show that $\varphi(\Box A_1, \dots, \Box A_k, \bar{s}) \to C(\Box A_1, \dots, \Box A_k)$ is a **K**-tautology. Let $M, w$ be a model for $\varphi$ and let $\sigma$ be an assignment to $V$ such that $\sigma(\Box A_i) = 1$ if and only if $M, w \models \Box A_i$. As $\sigma$ is consistent with $\varphi$, the set $\mathsf{C}_\pi, V_\sigma, \{\neg\Box\psi\}$ is unsatisfiable by Lemma 43.

Hence $C$ outputs 1 and therefore $M, w \models C(\Box A_1, \dots, \Box A_k)$.

It remains to show that also $C(\Box A_1, \dots, \Box A_k) \to \Box\psi$ is a **K**-tautology. We choose again a model $M, w$ such that $M, w \models C(\Box A_1, \dots, \Box A_k)$. We choose again an assignment $\sigma$ to $V$ such that $\sigma(\Box A_i) = 1$ if and only if $M, w \models \Box A_i$. By definition of $C$, the set $\mathsf{C}_\pi, V_\sigma, \{\neg\Box\psi\}$ is unsatisfiable. Now we can use Lemma 42 to conclude that

$$\bigwedge_{\Box A_i \in V_\sigma} \Box A_i \to \Box\psi$$

is a **K**-tautology. The model $M, w$ satisfies $\bigwedge_{\Box A_i \in V_\sigma} \Box A_i$, hence it also satisfies $\Box\psi$. ■

As a corollary we obtain:

**Corollary 45.** *Let $\varphi(\Box p_1, \dots, \Box p_k, \bar{s}) \to \Box\psi(\bar{p}, \bar{r})$ be a* **K***-tautology where the formulae $\varphi(p_1, \dots, p_k)$ and $\psi$ do not contain any modal operator. Let $\pi$ be a proof of this formula in the Frege system for* **K** *which uses $n$ modal steps. Then there exists a monotone circuit $C$ of size $O(n^2)$ in variables $\bar{p}$ variables such that*

$$\varphi(p_1, \dots, p_k, \bar{s}) \to C(p_1, \dots, p_k) \qquad \textit{and} \qquad C(p_1, \dots, p_k) \to \psi(\bar{p}, \bar{r})$$

*are propositional tautologies.*

*Proof.* The corollary follows from the previous theorem together with the following fact: if we start with a **K**-tautology $\theta$ and delete in $\theta$ all occurrences of $\Box$, then we obtain a propositional tautology. ■

### 5.7 The Lower Bound

Putting things together we obtain the lower bound for Frege systems in **K** which we already stated in the beginning of this section as Theorem 31:

**Theorem 46 (Hrubeš [59, 60]).** *Every* **K***-Frege proof of the formulae*

$$\mathit{Clique}_n^{\sqrt{n}+1}(\Box\bar{p},\bar{r}) \to \Box(\neg \mathit{Colour}_n^{\sqrt{n}}(\bar{p},\bar{s}))$$

*uses* $2^{n^{\Omega(1)}}$ *steps.*

*Proof.* By Corollary 34 the formulae are **K**-tautologies. By Corollary 45 every **K**-proof with $m$ modal steps yields a monotone circuit of size $O(m^2)$ which interpolates the formulae

$$\mathit{Clique}_n^{\sqrt{n}+1}(\bar{p},\bar{r}) \to (\neg \mathit{Colour}_n^{\sqrt{n}}(\bar{p},\bar{s}))$$

and by Theorem 25 every such interpolating monotone circuit has size $2^{n^{\Omega(1)}}$. ■

Hrubeš' lower bounds (Theorems 31, 32, 46) were extended by Jeřábek [65] to a large class of logics with infinite branching in the underlying Kripke frames.

## 6 Simulations between Non-Classical Proof Systems

So far we have concentrated on proving lower bounds in non-classical logics. A second important topic in proof complexity is the comparison of proof systems via simulations introduced in [34] and [76] (cf. Section 2 for the definitions). While lower bounds show us *absolute* limitations on the strength of proof systems, simulations explain the *relative* strength of proof systems to each other. This is even possible when lower bounds are not yet available as is the case for classical Frege systems.

Indeed, Frege systems and its extensions are one of the most interesting cases with respect to simulations. Frege systems also depend on the choice of the language, i. e., the choice of the propositional connectives. When speaking of the polynomial equivalence of two systems over different propositional languages, it is implicitly understood that the formulae are suitably translated into formulae over the new basis (see [90] for a discussion). In the classical setting, Cook and Reckhow were able to show the equivalence of all Frege systems using different axioms, rules, and propositional connectives [34, 96]. For this equivalence to hold, two things have to be verified:

- First, let $F_1$ and $F_2$ be two Frege systems using the same propositional language. Then the equivalence of $F_1$ and $F_2$ can be shown by deriving every $F_1$-rule in $F_2$ and vice versa.

- Second, if $F_1$ and $F_2$ are Frege systems over distinct propositional languages $L_1$ and $L_2$, respectively, then we have to translate $L_1$-formulae into $L_2$-formulae before we can apply the method from the previous item. To still obtain polynomial size formulae after the translation, Reckhow [96] first rebalances the formulae to logarithmic logical depth. In classical propositional logic this is possible by Spira's theorem.

For non-classical logics the situation is more complicated. Rebalancing the formulae to logarithmic depth is not possible because in modal and intuitionistic logic there are examples of formulae which indeed require linear depth. For this reason, the equivalence of modal or intuitionistic Frege systems using different connectives is still open (cf. [63]).

But even for Frege systems in a fixed language the question is quite intricate because of the presence of *admissible rules.*[14] In general, inference rules

$$R = \frac{\varphi_1 \quad \dots \quad \varphi_k}{\psi}$$

can be classified according to whether they are valid or admissible. The rule $R$ is **valid** in a logic $L$ if $\varphi_1, \dots, \varphi_k \models_L \psi$ where $\models_L$ is the consequence relation of the logic $L$. The rule $R$ is **admissible** in $L$ if for every substitution $\sigma$ the following holds: if $\sigma(\varphi_1), \dots, \sigma(\varphi_k)$ are theorems of $L$, i. e., $\models_L \sigma(\varphi_i)$ holds for $i = 1, \dots, k$, then also $\sigma(\psi)$ is a theorem of $L$, i. e., $\models_L \sigma(\psi)$. In classical logic, every admissible rule is also valid. A property that is also known as **structural completeness**.

As was the case with the interpolation property, the situation with structural completeness in non-classical logic is rather different from the classical case. Here, several important examples of admissible but non-valid rules are known, and the general characterisation of structural completeness in non-classical logics is extremely difficult. We refer the interested reader to the extensive monograph by Rybakov on the subject [100] and here give just one illustrative example:

**Proposition 47.** *The* ($\Box$) *rule*

$$(\Box) \qquad \frac{\Box\varphi}{\varphi}$$

*is valid in* **S4**. *It is admissible, but not valid, in the modal logic* **K**. *It is not admissible in some extensions of* **K**, *for instance in* $\mathbf{K} \oplus \Box\bot$

[14] At this point it should be mentioned that the definition of Frege systems for non-classical logics is a delicate subject. Here we follow the interpretation of Mints and Kojevnikov [86] and Jeřábek [63], where Frege systems are required to be sound and "implicationally" (rather, derivationally) complete, but not necessarily "implicationally" sound. In contrast, a direct adoption of the definition in Section 2.1 would make the systems also implicationally sound (the definition does not even distinguish soundness and completeness), and some authors actually interpret it that way. For implicationally sound Frege systems there is no issue with admissible rules, the easy argument sketched above that all Frege systems in the same language are equivalent works.

*Proof. Validity:* Clearly, because $\Box p \to p$ is an axiom of **S4**, the rule $(\Box)$ is valid in **S4** (i.e. assume a proof for $\Box\varphi$ and apply modus ponens once). Next, because the formula $\Box^n p \to p$ can be refuted in the one point irreflexive frame, $(\Box)$ cannot be valid in **K**.

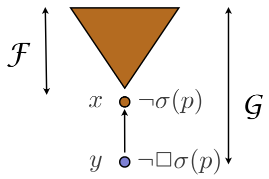


**Fig. 3.** Admissibility of $(\Box)$ in **K**.

*Admissibility in* **K***:* By contraposition, assume $\langle (F,R),\beta,x\rangle \not\models \sigma(p)$ for some frame $\mathcal{F} = (F,R)$ and substitution $\sigma$. Pick some $y \notin F$, and define a new frame $\mathcal{G}$ with worlds $G = F \cup \{y\}$, accessibility relation $S = R \cup \{\langle y,x\rangle\}$, and valuation $\gamma(p) = \beta(p)$ for all $p$—see Fig. 3. It then holds that $\langle (G,S),\gamma,y\rangle \models \neg\Box\sigma(p)$ whilst we still have $\langle (G,S),\gamma,x\rangle \models \neg\sigma(p)$.

*Non-Admissibility in* $\mathbf{K} \oplus \Box\bot$*:* The logic $\mathbf{K} \oplus \Box\bot$ (i.e. the least normal modal logic extending **K** by the axiom $\Box\bot$) is consistent because it is satisfied in the one point irreflexive frame. Now if $(\Box)$ were admissible, it would imply the provability of $\bot$, i.e. inconsistency. It follows, in particular, that a rule admissible in a logic $L$ need not be admissible in its extensions. ■

Admissibility has been thoroughly studied for many non-classical logics. In particular, starting with a question of Friedman [44] it was investigated whether admissibility of a given rule is a decidable property, and this was answered affirmatively for many modal and intuitionistic logics [100]. In fact, for intuitionistic logic and many important modal logics such as **K4** , **GL**, **S4** , and **S4.Grz**, deciding the admissibility of a given rule is coNEXP-complete as shown by Jeřábek [64]. Thus this task is presumably even harder than deciding derivability in these logics which is complete for PSPACE.

Let us come back to the above question of the equivalence of all Frege systems for a non-classical logic. If a Frege system uses non-valid admissible rules, then we might not be able to re-derive the rules in another Frege system. Hence, again Reckhow's proof method from the first item above fails. But of course, admissible rules may help to shorten proofs. Luckily, there is a way out. Building on a characterisation of admissible rules for intuitionistic logic by Ghilardi [50], Iemhoff [61] constructed an explicit set of rules which forms a basis for all admissible intuitionistic rules. Using this basis, Mints and Kojevnikov [86] were able to prove the equivalence of all intuitionistic Frege systems:

**Theorem 48 (Mints, Kojevnikov [86]).** *All intuitionistic Frege systems in the language* $\to, \wedge, \vee, \bot$ *are polynomially equivalent.* ■

Subsequently, Jeřábek [63] generalised these results to an infinite class of modal logics (so-called extensible logics [62]). We single out some of the most important instances in the next theorem:

**Theorem 49 (Jeřábek [63]).** *Let $L$ be one of the modal logics* **K4***,* **GL***,* **S4***, or* **S4.Grz** *and let $B$ be a complete Boolean basis. Then any two Frege systems for $L$ in the language $B \cup \{\Box\}$ are polynomially equivalent.* ∎

We also mention that admissible rules have very recently been studied for many-valued logics by Jeřábek [66, 67].

Another interesting topic is the comparison of Frege systems and their extensions such as extended and substitution Frege systems. **Extended Frege** allows the abbreviation of possibly complex formulae by propositional atoms. **Substitution Frege systems** allow to infer arbitrary substitution instances of a proven formula in one step by the so-called substitution rule. Both these mechanisms might decrease the size of proofs in comparison with Frege, but a separation between these systems is not known for classical propositional logic.

Already in the first paper [34] which introduces these systems, Cook and Reckhow observe that substitution Frege polynomially simulates extended Frege, but conjecture that the former might be strictly stronger than the latter. However, in classical propositional logic both systems are indeed polynomially equivalent as was shown independently by Dowd [40] and Krajíček and Pudlák [76]. While this proof of equivalence fails in non-classical logics, it is still possible to extract some general information from it as in the next result:

**Theorem 50 (Jeřábek [65]).** *For any modal or superintuitionistic logic, extended Frege and tree-like substitution Frege are polynomially equivalent.*[15] ∎

This shows that Cook and Reckhow's intuition on extended vs. substitution Frege was indeed correct and is further confirmed by results of Jeřábek [65] who shows that going from extended to substitution Frege corresponds to a conservative strengthening of the underlying logic by a new modal operator. Building on these characterisations, Jeřábek exhibits examples for logics where the *EF* vs. *SF* question receives different answers:

**Theorem 51 (Jeřábek [65]).**

1. *Extended Frege and substitution Frege are polynomially equivalent for all extensions of the modal logic* **KB***.*
2. *Substitution Frege is exponentially better than extended Frege for the modal logic* **K** *and for intuitionistic logic.* ∎

The precise meaning of the phrase "exponentially better" is that there are sequences of tautologies which have polynomial-size substitution Frege proofs, but require exponential-size proofs in extended Frege. These sequences are again the

[15] In Theorem 50 and the subsequent discussion, it is essential that we only deal with modal logics using a single unary modality. Already for bimodal logics, it is not even clear whether *SF* simulates *EF*.

Clique-Colour tautologies used by Hrubeš [60]. Item 2 of Theorem 51 also holds for all logics with infinite branching for which Jeřábek [65] showed exponential lower bounds.

# 7 Proof Complexity of Default Logic

Besides modal and intuitionistic logics there are many other non-classical logics which are interesting to analyse from a proof complexity perspective. In this section we will have a look at the proof complexity of propositional default logic (cf. Section 3.3 for background on default logic).

Starting with Reiter's work [97], several proof-theoretic methods have been developed for default logic (cf. [45, 84, 79, 98, 4] and [39] for a survey). However, most of these formalisms employ external constraints to model non-monotonic deduction and thus cannot be considered purely axiomatic (cf. [41] for an argument). This was achieved by Bonatti and Olivetti [16] who designed simple and elegant sequent calculi for credulous and sceptical default reasoning. Subsequently, Egly and Tompits [41] extended Bonatti and Olivetti's calculi to first-order default logic and showed a speed-up of these calculi over classical first-order logic, *i.e.*, they construct sequences of first-order formulae which need long classical proofs but have short derivations using default rules.

In what follows we will explain the sequent-style calculi of Bonatti and Olivetti from [16] and accompany this by a proof-theoretic investigation of the calculi. In our exposition we follow the paper [13].

## 7.1 Complexity of the Antisequent and Residual Calculi

Bonatti and Olivetti's calculi for default logic use four main ingredients: usual propositional sequents and rules of $LK$, antisequents to refute formulae, residual rules, and default rules. In this section we will investigate the complexity of the antisequent calculus $AC$ and the residual calculus $RC$.

We start with the definition of Bonatti's *antisequent calculus* $AC$ from [15]. A related refutation calculus for first-order logic was previously developed by Tiomkin [104]. In $AC$ we use *antisequents* $\Gamma \nvdash \Delta$, where $\Gamma, \Delta \subseteq \mathcal{L}$. Intuitively, $\Gamma \nvdash \Delta$ means that $\bigvee \Delta$ does not follow from $\bigwedge \Gamma$. Axioms of $AC$ are all sequents $\Gamma \nvdash \Delta$, where $\Gamma$ and $\Delta$ are disjoint sets of propositional variables. The inference rules of $AC$ are shown in Fig. 4. For this calculus, Bonatti [15] shows:

**Theorem 52 (Bonatti [15]).** *The calculus $AC$ is sound and complete.* ■

Concerning the size of proofs in the antisequent calculus we observe:

**Proposition 53.** *The antisequent calculus $AC$ is polynomially bounded.*

*Proof.* Observe that the calculus contains only unary inference rules, each of which reduces the logical complexity of one of the contained formulae (if perceived bottom-up). Thus each use of an inference rule decrements the size of the formulae by at least one. After a linear number of steps we end up with only

$$\frac{\Gamma \nvdash \Sigma, \alpha}{\Gamma, \neg\alpha \nvdash \Sigma}\ (\neg \nvdash) \qquad \frac{\Gamma, \alpha \nvdash \Sigma}{\Gamma \nvdash \Sigma, \neg\alpha}\ (\nvdash \neg)$$

$$\frac{\Gamma, \alpha, \beta \nvdash \Sigma}{\Gamma, \alpha \wedge \beta \nvdash \Sigma}\ (\wedge \nvdash) \qquad \frac{\Gamma \nvdash \Sigma, \alpha}{\Gamma \nvdash \Sigma, \alpha \wedge \beta}\ (\nvdash \bullet\wedge) \qquad \frac{\Gamma \nvdash \Sigma, \beta}{\Gamma \nvdash \Sigma, \alpha \wedge \beta}\ (\nvdash \wedge\bullet)$$

$$\frac{\Gamma \nvdash \Sigma, \alpha, \beta}{\Gamma \nvdash \Sigma, \alpha \vee \beta}\ (\nvdash \vee) \qquad \frac{\Gamma, \alpha \nvdash \Sigma}{\Gamma, \alpha \vee \beta \nvdash \Sigma}\ (\bullet\vee \nvdash) \qquad \frac{\Gamma, \beta \nvdash \Sigma}{\Gamma, \alpha \vee \beta \nvdash \Sigma}\ (\vee\bullet \nvdash)$$

$$\frac{\Gamma, \alpha \nvdash \Sigma, \beta}{\Gamma \nvdash \Sigma, \alpha \to \beta}\ (\nvdash\to) \qquad \frac{\Gamma \nvdash \Sigma, \alpha}{\Gamma, \alpha \to \beta \nvdash \Sigma}\ (\bullet \to\nvdash) \qquad \frac{\Gamma, \beta \nvdash \Sigma}{\Gamma, \alpha \to \beta \nvdash \Sigma}\ (\to \bullet \nvdash)$$

**Fig. 4.** Inference rules of the antisequent calculus $AC$.

propositional variables which we cannot reduce any further. Each antisequent is of linear size, hence the complete derivation has quadratic size. ■

The above observation is not very astounding, since, to verify $\Gamma \nvdash \Delta$ we could alternatively guess assignments to the propositional variables in $\Gamma$ and $\Delta$ and thereby verify antisequents in NP.

We now turn to the *residual calculus RC* of Bonatti and Olivetti [16]. Its objects are *residual sequents* $\langle W, R\rangle \vdash \Delta$ and *residual antisequents* $\langle W, R\rangle \nvdash \Delta$ where $W, \Delta \subseteq \mathcal{L}$ and $R \subseteq \mathcal{L}^{res}$. The intuitive meaning is that $\Delta$ does (respectively does not) follow from $W$ using the residues $R$. The rules of $RC$ comprise of the inference rules from Fig. 5 together with the rules of $LK$ and $AC$. However, the use of rules from $LK$ and $AC$ is restricted to purely propositional (anti)sequents. For this calculus, Bonatti and Olivetti [16] showed:

$$(\mathbf{Re1})\ \frac{\Gamma \vdash \Delta}{\Gamma, \frac{\alpha}{\gamma} \vdash \Delta} \qquad (\mathbf{Re2})\ \frac{\Gamma \vdash \alpha \qquad \Gamma, \gamma \vdash \Delta}{\Gamma, \frac{\alpha}{\gamma} \vdash \Delta}$$

$$(\mathbf{Re3})\ \frac{\Gamma \nvdash \Delta \qquad \Gamma \nvdash \alpha}{\Gamma, \frac{\alpha}{\gamma} \nvdash \Delta} \qquad (\mathbf{Re4})\ \frac{\Gamma, \gamma \nvdash \Delta}{\Gamma, \frac{\alpha}{\gamma} \nvdash \Delta}$$

**Fig. 5.** Inference rules of the residual calculus $RC$.

**Theorem 54 (Bonatti, Olivetti [16]).** *The residual calculus RC is sound and complete,* i.e., *for all default theories $\langle W, R\rangle$ with $R \subseteq \mathcal{L}^{res}$ and all $\Delta \subseteq \mathcal{L}$,*

1. *$\langle W, R\rangle \vdash \Delta$ is derivable in RC if and only if $\bigvee \Delta \in Cl(W, R)$;*

*2.* $\langle W, R\rangle \nvdash \varDelta$ *is derivable in RC if and only if* $\bigvee \varDelta \notin Cl(W, R)$. ■

To bound the lengths of proofs in this calculus we exploit the property that residues only have to be used at a certain level and are not used to deduce any formulae afterwards (cf. Lemma 21). Using this we prove that the complexity of $RC$ is tightly linked to that of $LK$.

**Lemma 55.** *There exist a polynomial* $p$ *and a constant* $c$ *such that* $s_{RC}(n) \leq p(n) \cdot s_{LK}(cn)$ *and* $t_{RC}(n) \leq p(n) \cdot t_{LK}(cn)$.

*Proof.* The proof consists of two parts. First we will show the bounds stated above for sequents. In the second part we will then show that antisequents even admit polynomial-size proofs in $RC$.

Assume first that we want to derive the sequent $\langle W, R\rangle \vdash \varDelta$, where $W, \varDelta \subseteq \mathcal{L}$ and $R = \{r_1, \ldots, r_k\}$ is a set of residues with $r_i = \frac{\alpha_i}{\gamma_i}$. Let $R' \subseteq R$ be minimal with respect to the size $|R'|$ such that $\langle W, R'\rangle \vdash \varDelta$. We may w.l.o.g. assume that $R' = \{r_1, \ldots, r_{k'}\}$ and $k' \leq k$. Furthermore, by Lemma 21, we may assume that the rules $r_i$ are ordered in the way they are applied when computing the sets $C_i$. In particular, this means that for each $i = 1, \ldots, k'$,

$$W \cup \{\gamma_1, \ldots, \gamma_{i-1}\} \vdash \alpha_i$$

is a true propositional sequent for which we fix an $LK$-proof $\varPi_i$. We augment $\varPi_i$ by $k' - i$ applications of rule (**Re1**) to obtain

$$\langle W \cup \{\gamma_1, \ldots, \gamma_{i-1}\}, \{r_{i+1}, \ldots, r_{k'}\}\rangle \vdash \alpha_i \ \ .$$

Let us call the proof of this sequent $\varPi'_i$.

The proof tree depicted in Fig. 6 for deriving $\langle W, R\rangle \vdash \varDelta$ unfurls as follows. We start with an $LK$-proof for the sequent $W \cup \{\gamma_1, \ldots, \gamma_{k'}\} \vdash \varDelta$ and then apply $k'$-times the rule (**Re2**) in the step

$$\frac{\langle W \cup \{\gamma_1, \ldots, \gamma_{i-1}\}, \{r_{i+1}, \ldots, r_{k'}\}\rangle \vdash \alpha_i \qquad \langle W \cup \{\gamma_1, \ldots, \gamma_i\}, \{r_{i+1}, \ldots, r_{k'}\}\rangle \vdash \varDelta}{\langle W \cup \{\gamma_1, \ldots, \gamma_{i-1}\}, \{r_i, \ldots, r_{k'}\}\rangle \vdash \varDelta}$$

to reach $\langle W, R'\rangle \vdash \varDelta$. To derive the left prerequisite we use the proof $\varPi'_i$. Finally we use $k - k'$ applications of the rule (**Re1**) to get $\langle W, R\rangle \vdash \varDelta$.

Our proof for $\langle W, R\rangle \vdash \varDelta$ uses at most $(k' + 1) \cdot t_{LK}(n) + \frac{k'(k'+1)}{2} + k$ steps, *i.e.*, $t_{RC}(n) \leq \mathcal{O}(n \cdot t_{LK}(n) + n^2)$. Each sequent is of linear size. Hence, $s_{RC}(n) \leq p(n) \cdot s_{LK}(n)$ for some polynomial $p$.

In the second part of the proof we have to show that any true antisequent has an $RC$-proof of polynomial size. We omit the details. ■

Let us remark that while the $RC$-proof of $\langle W, R\rangle \vdash \varDelta$ in Fig. 6 is tree-like, this is not true for our dag-like $RC$-proof of $\langle W, R\rangle \nvdash \varDelta$ constructed in the second part of the proof of Lemma 55.

$$\begin{array}{c} \dfrac{\Pi'_{k'} \qquad \langle W \cup \{\gamma_1, \dots, \gamma_{k'}\}, \varnothing\rangle \vdash \Delta}{\vdots}\,(\mathbf{Re2}) \\ \dfrac{\Pi'_1 \qquad \dfrac{\Pi'_2 \qquad \langle W \cup \{\gamma_1, \gamma_2\}, \{r_3, \dots, r_{k'}\}\rangle \vdash \Delta}{\langle W \cup \{\gamma_1\}, \{r_2, \dots, r_{k'}\}\rangle \vdash \Delta}\,(\mathbf{Re2})}{\dfrac{\langle W, R'\rangle \vdash \Delta}{\vdots}\,(\mathbf{Re1})}\,(\mathbf{Re2}) \\ \langle W, R\rangle \vdash \Delta \end{array}$$

**Fig. 6.** Proof tree for the sequent $\langle W, R\rangle \vdash \Delta$ in the residual calculus.

### 7.2 Proof Complexity of Credulous Default Reasoning

Now we turn to the analysis of Bonatti and Olivetti's calculus for credulous default reasoning. An essential ingredient of the calculus are **provability constraints** which resemble a necessity modality. Provability constraints are of the form $\mathbf{L}\alpha$ or $\neg\mathbf{L}\alpha$ with $\alpha \in \mathcal{L}$. A set $E \subseteq \mathcal{L}$ satisfies a constraint $\mathbf{L}\alpha$ if $\alpha \in Th(E)$. Similarly, $E$ satisfies $\neg\mathbf{L}\alpha$ if $\alpha \notin Th(E)$.

We can now describe the calculus $BO_{cred}$ of Bonatti and Olivetti [16] for credulous default reasoning. A **credulous default sequent** is a 3-tuple $\langle \Sigma, \Gamma, \Delta\rangle$, denoted by $\Sigma; \Gamma \mid\!\sim \Delta$, where $\Gamma = \langle W, D\rangle$ is a default theory, $\Sigma$ is a set of provability constraints and $\Delta$ is a set of propositional sentences. Semantically, the sequent $\Sigma; \Gamma \mid\!\sim \Delta$ is true, if there exists a stable extension $E$ of $\Gamma$ which satisfies all of the constraints in $\Sigma$ and $\bigvee \Delta \in E$. The calculus $BO_{cred}$ uses such sequents and extends $LK$, $AC$, and $RC$ by the inference rules in Fig. 7.

$$(\mathbf{cD1})\ \dfrac{\Gamma \vdash \Delta}{;\ \Gamma \mid\!\sim \Delta} \qquad (\mathbf{cD2})\ \dfrac{\Gamma \vdash \alpha \qquad \Sigma;\ \Gamma \mid\!\sim \Delta}{\mathbf{L}\alpha,\ \Sigma;\ \Gamma \mid\!\sim \Delta} \qquad (\mathbf{cD3})\ \dfrac{\Gamma \nvdash \alpha \qquad \Sigma;\ \Gamma \mid\!\sim \Delta}{\neg\mathbf{L}\alpha,\ \Sigma;\ \Gamma \mid\!\sim \Delta}$$

where $\Gamma \subseteq \mathcal{L}^{res}$ in rules (**cD1**), (**cD2**), and (**cD3**)

$$(\mathbf{cD4})\ \dfrac{\mathbf{L}\neg\beta_i,\ \Sigma;\ \Gamma \mid\!\sim \Delta}{\Sigma;\ \Gamma, \frac{\alpha:\ \beta_1 \dots \beta_n}{\gamma} \mid\!\sim \Delta} \qquad (\mathbf{cD5})\ \dfrac{\neg\mathbf{L}\neg\beta_1 \dots \neg\mathbf{L}\neg\beta_n,\ \Sigma;\ \Gamma, \frac{\alpha}{\gamma} \mid\!\sim \Delta}{\Sigma;\ \Gamma, \frac{\alpha:\ \beta_1 \dots \beta_n}{\gamma} \mid\!\sim \Delta}$$

**Fig. 7.** Inference rules for the credulous default calculus $BO_{cred}$.

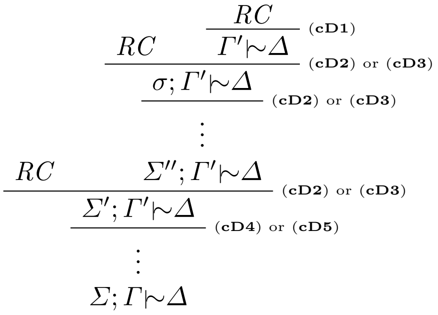
For this calculus Bonatti and Olivetti [16] show the following:

**Theorem 56 (Bonatti, Olivetti [16]).** *$BO_{cred}$ is sound and complete,* i.e., *a credulous default sequent is true if and only if it is derivable in $BO_{cred}$.* ■

We now investigate lengths of proofs in $BO_{cred}$. Our next lemma shows that upper bounds on the proof size of $RC$ can be transferred to $BO_{cred}$.

**Lemma 57.** *For any function $t(n)$, if $RC$ is $t(n)$-bounded, then $BO_{cred}$ is $p(n) \cdot t(n)$-bounded for some polynomial $p$. The same relation holds for the number of steps in $RC$ and $BO_{cred}$.*

*Proof.* Let $\Sigma; \Gamma \mathrel{|\!\sim} \Delta$ be a true credulous default sequent. We will construct a $BO_{cred}$-derivation of $\Sigma; \Gamma \mathrel{|\!\sim} \Delta$ starting from the bottom with the given sequent. Observe that we cannot use any of the rules (**cD1**) through (**cD3**) as long as $\Gamma$ contains proper defaults with nonempty justification. Thus we first have to reduce all defaults to residues plus some set of constraints using (**cD4**) or (**cD5**). As one of these rules has to be applied exactly once for each appearance of some default in $\Gamma$ we end up with $\Sigma'; \Gamma' \mathrel{|\!\sim} \Delta$, where $|\Sigma'|$ is polynomial in $|\Gamma \cup \Sigma|$ and $\Gamma'$ is equal to $\Gamma$ on its propositional part and contains some of the corresponding residues instead of the defaults from $\Gamma$. From this point on we can only use rules (**cD2**) and (**cD3**) until we have eliminated all constraints and then finally apply rule (**cD1**) once. Thus, $BO_{cred}$-proofs look as shown in Fig. 8 where $RC$ indicates



$RC$
(cD1)
$RC$
$\Gamma' \mathrel{|\!\sim} \Delta$
(cD2) or (cD3)
$\sigma; \Gamma' \mathrel{|\!\sim} \Delta$
(cD2) or (cD3)
$RC$
$\Sigma''; \Gamma' \mathrel{|\!\sim} \Delta$
(cD2) or (cD3)
$\Sigma'; \Gamma' \mathrel{|\!\sim} \Delta$
(cD4) or (cD5)
$\Sigma; \Gamma \mathrel{|\!\sim} \Delta$

**Fig. 8.** The structure of the $BO_{cred}$-proof in Lemma 57

a derivation in the residual calculus and $\sigma$ is the remaining constraint from $\Sigma$ after applications of (**cD2**) or (**cD3**). Hence we obtain the bounds on $s_{BO_{cred}}$ and $t_{BO_{cred}}$. ■

Combining Lemmas 55 and 57 we obtain our main result in this section stating a tight connection between the proof complexity of $LK$ and $BO_{cred}$.

**Theorem 58 ([13]).** *The lengths of proofs in the credulous default calculus and in classical Frege systems are polynomially related. The same holds for the number of steps.*

*More precisely, there exist a polynomial $p$ and a constant $c$ such that $s_{LK}(n) \leq s_{BO_{cred}}(n) \leq p(n) \cdot s_{LK}(cn)$ and $t_{LK}(n) \leq t_{BO_{cred}}(n) \leq p(n) \cdot t_{LK}(cn)$.* ■

This means that while the decision complexity of the logic increases, this increase does not manifest in the lengths of proofs. A similar result as Theorem 58 was observed by Jeřábek [65] for tabular modal and superintuitionistic logics which are in $\mathsf{coNP}$. Jeřábek constructs translations of extended Frege proofs in these logics to propositional proofs, thereby obtaining analogous versions of Theorem 58 for extended Frege in these modal and superintuitionistic logics. Thus, the current barrier in classical proof complexity admits natural restatements in terms of non-classical logics.

### 7.3 On the Automatisability of $BO_{cred}$

Practitioners are not only interested in the size of a proof, but face the more complicated problem to actually construct a proof for a given instance. Of course, in the presence of super-polynomial lower bounds to the proof size this cannot be done in polynomial time. Thus, in proof search the best one can hope for is the following notion of automatisability:

**Definition 59 (Bonet, Pitassi, Raz [19]).** *A proof system $P$ for a language $L$ is* ***automatisable*** *if there exists a deterministic procedure that takes as input a string $x$ and outputs a $P$-proof of $x$ in time polynomial in the size of the shortest $P$-proof of $x$ if $x \in L$. If $x \notin L$, then the behaviour of the algorithm is unspecified.* ∎

For practical purposes automatisable systems would be very desirable. Searching for a proof we may not find the shortest one, but we are guaranteed to find one that is only polynomially longer. Unfortunately, for $BO_{cred}$ there are strong limitations towards this goal as our next result shows:

**Theorem 60.** *$BO_{cred}$ is not automatisable unless factoring integers is possible in polynomial time.*

*Proof.* First we observe that automatisability of $BO_{cred}$ implies automatisability of Frege systems. For this let $\varphi$ be a propositional tautology. By assumption, we can construct a $BO_{cred}$-proof of $\varnothing \mid\!\sim \varphi$. This $BO_{cred}$-proof contains an $LK$-proof of $\varnothing \vdash \varphi$ by rule (**cD1**). As $LK$ is polynomially equivalent to Frege systems [72], we can construct from this $LK$-proof a Frege proof of $\varphi$ in polynomial time. By a result of Bonet, Pitassi, and Raz [19], Frege systems are not automatisable unless Blum integers can be factored in polynomial time (a Blum integer is the product of two primes which are both congruent 3 modulo 4). ∎

### 7.4 A General Construction of Proof Systems for Credulous Default Reasoning

In this section we will explain a general method how to construct proof systems for credulous default reasoning. These proof systems arise from the canonical $\Sigma_2^{\mathsf{p}}$ algorithm for credulous default reasoning (Algorithm 1). Algorithm 1 first guesses a generating set $G_{\text{ext}}$ for a potential stable extension and then verifies by the stage construction from Theorem 19 that $G_{\text{ext}}$ indeed generates a stable extension which moreover contains the formula $\varphi$. Algorithm 1 is a $\Sigma_2^{\mathsf{p}}$ procedure, *i.e.*, it can be executed by a nondeterministic polynomial-time Turing machine $M$ with access to a coNP-oracle. The nondeterminism solely lies in line 1 and the oracle queries are made in lines 6 and 11 to the coNP-complete problem of propositional entailment $\text{IMP} = \{\langle \Psi, \varphi\rangle \mid \Psi \subseteq \mathcal{L},\ \varphi \in \mathcal{L},\ \text{and}\ \Psi \models \varphi\}$.

**Algorithm 1** A $\Sigma_2^{\mathsf{p}}$ procedure for credulous default reasoning

```
Require: $\langle W, D\rangle$, $\varphi$
 1: guess $D_0 \subseteq D$ and let $G_{\text{ext}} \leftarrow W \cup \left\{\gamma \mid \frac{\alpha:\beta}{\gamma} \in D_0\right\}$
 2: $G_{\text{new}} \leftarrow W$
 3: repeat
 4:    $G_{\text{old}} \leftarrow G_{\text{new}}$
 5:    for all $\frac{\alpha:\beta}{\gamma} \in D$ do
 6:       if $G_{\text{old}} \models \alpha$ and $G_{\text{ext}} \not\models \neg\beta$ then
 7:          $G_{\text{new}} \leftarrow G_{\text{new}} \cup \{\gamma\}$
 8:       end if
 9:    end for
10: until $G_{\text{new}} = G_{\text{old}}$
11: if $G_{\text{new}} = G_{\text{ext}}$ and $G_{\text{ext}} \models \varphi$ then
12:    return true
13: else
14:    return false
15: end if
```

Algorithm 1 can be converted into a proof system for credulous default reasoning as follows. We fix a propositional proof system $P$ and define a proof system $\mathit{Cred}(P)$ for credulous default reasoning where proofs are of the form

$$\langle W, D, \varphi, \mathit{comp}, q_1, \ldots, q_k, a_1, \ldots, a_k\rangle \quad .$$

Here *comp* is a computation of $M$ on input $\langle W, D, \varphi\rangle$ and $q_1, \ldots, q_k$ are the queries to IMP during this computation. If the IMP-query $q_i = \langle \Psi_i, \varphi_i\rangle$ is answered positively, then $a_i$ is a $P$-proof of $\left(\bigwedge_{\psi\in\Psi_i} \psi\right) \rightarrow \varphi_i$, otherwise $a_i$ is an assignment falsifying this formula. For this proof system we obtain the following bounds:

**Theorem 61.** *Let $P$ be a propositional proof system. Then $\mathit{Cred}(P)$ is a proof system for credulous default reasoning with $s_P(n) \leq s_{\mathit{Cred}(P)}(n) \leq \mathcal{O}(n^2 s_P(n))$.*

*Proof.* The first inequality holds because we can use $\mathit{Cred}(P)$ to prove propositional tautologies $\varphi$ by choosing $W = D = \varnothing$.

For the second inequality, we observe that Algorithm 1 has quadratic running time. In particular, a computation of Algorithm 1 contains at most a quadratic number of queries to IMP. Each of these queries is of linear size because it only consists of formulae from the input. If the query is answered positively, then we have to supply a $P$-proof and there exists such a $P$-proof of size $\leq s_P(n)$. For a negative answer we just include an assignment of linear size. This yields $s_{Cred(P)}(n) \leq \mathcal{O}(n^2 s_P(n))$. ■

Theorem 61 tells us that proving lower bounds for proof systems for credulous default reasoning is more or less the same as proving lower bounds to propositional proof systems. In particular, we get:

**Corollary 62.** *There exists a polynomially bounded proof system for credulous default reasoning if and only if there exists a polynomially bounded propositional proof system.* ■

### 7.5 Lower Bounds for Sceptical Default Reasoning

Bonatti and Olivetti [16] introduce two calculi for sceptical default reasoning. As before, objects are sequents of the form $\Sigma; \Gamma \mathrel{|\!\sim} \Delta$, where $\Sigma$ is a set of constraints, $\Gamma$ is a propositional default theory, and $\Delta$ is a set of propositional formulae. But now, the sequent $\Sigma; \Gamma \mathrel{|\!\sim} \Delta$ is true, if $\bigvee \Delta$ holds in *all* extensions of $\Gamma$ satisfying the constraints in $\Sigma$.

The first calculus $BO_{skep}$ consists of the defining axioms of $LK$ and $AC$, the inference rules of $LK$, $AC$, $RC$, and the rules from Fig. 9. Bonatti and Olivetti show that each true sequent is derivable in $BO_{skep}$, *i.e.*, the calculus is sound and complete. However, they already remark that proofs in $BO_{skep}$ are of exponential size in the number of default rules in the sequent. This is due to the residual rules for they cannot be applied unless all defaults with nonempty justifications have been eliminated using rule (**sD4**).

$$\textbf{(sD1)}\ \frac{\Gamma \vdash \Delta}{\Sigma; \Gamma \mathrel{|\!\sim} \Delta} \qquad \textbf{(sD2)}\ \frac{\Gamma \vdash \alpha}{\neg\mathbf{L}\alpha, \Sigma; \Gamma \mathrel{|\!\sim} \Delta} \qquad \textbf{(sD3)}\ \frac{\Gamma \not\vdash \alpha}{\mathbf{L}\alpha, \Sigma; \Gamma \mathrel{|\!\sim} \Delta}$$

where $\Gamma \subseteq \mathcal{L}^{res}$ in rules (**sD1**), (**sD2**), and (**sD3**)

$$\textbf{(sD4)}\ \frac{\neg\mathbf{L}\neg\beta_1, \ldots, \neg\mathbf{L}\neg\beta_n, \Sigma; \Gamma, \frac{\alpha}{\gamma} \mathrel{|\!\sim} \Delta \qquad \mathbf{L}\neg\beta_1, \Sigma; \Gamma \mathrel{|\!\sim} \Delta \ \ldots\ \mathbf{L}\neg\beta_n, \Sigma; \Gamma \mathrel{|\!\sim} \Delta}{\Sigma; \Gamma, \frac{\alpha:\beta_1\ldots\beta_n}{\gamma} \mathrel{|\!\sim} \Delta}$$

**Fig. 9.** Inference rules for the sceptical default calculus $BO_{skep}$.

To get more concise proofs, Bonatti and Olivetti [16] suggest an enhanced calculus $BO'_{skep}$ where the rules (**sD1**) to (**sD3**) are replaced by rules (**sD1′**) to (**sD3′**) and rule (**sD4**) is kept (see Fig. 10). Bonatti and Olivetti prove soundness and completeness for $BO'_{skep}$. Moreover, they show that $BO'_{skep}$ is exponentially separated from $BO_{skep}$, *i.e.*, there exist sequents $(S_n)_{n\geq 1}$ which require

$$\textbf{(sD1')}\ \frac{\Sigma', \Gamma' \vdash \Delta}{\Sigma; \Gamma \mid\!\sim \Delta} \qquad \textbf{(sD2')}\ \frac{\Sigma; \Gamma \mid\!\sim \alpha}{\neg \mathbf{L}\alpha, \Sigma; \Gamma \mid\!\sim \Delta} \qquad \textbf{(sD3')}\ \frac{\Gamma'' \nvdash \alpha}{\mathbf{L}\alpha, \Sigma; \Gamma \mid\!\sim \Delta}$$

$$\textbf{(sD4)}\ \frac{\neg\mathbf{L}\neg\beta_1, \dots, \neg\mathbf{L}\neg\beta_n, \Sigma; \Gamma, \frac{\alpha}{\gamma} \mid\!\sim \Delta \qquad \mathbf{L}\neg\beta_1, \Sigma; \Gamma \mid\!\sim \Delta \ \dots\ \mathbf{L}\neg\beta_n, \Sigma; \Gamma \mid\!\sim \Delta}{\Sigma; \Gamma, \frac{\alpha:\beta_1 \dots \beta_n}{\gamma} \mid\!\sim \Delta}$$

where $\Sigma' \subseteq \{\alpha \mid \mathbf{L}\alpha \in \Sigma\}$, $\Gamma' \subseteq \Gamma \cap \mathcal{L}^{res}$, and $\Gamma'' = (\Gamma \cap \mathcal{L}) \cup \left\{ \frac{p(\delta)}{c(\delta)} \,\middle|\, \delta \in \Gamma \right\}$.

**Fig. 10.** Inference rules for the enhanced sceptical default calculus $BO'_{skep}$.

exponential-size proofs in $BO_{skep}$ but have linear-size derivations in $BO'_{skep}$. In our next result we will show an exponential lower bound to the proof length (and therefore also to the proof size) in the enhanced sceptical calculus $BO'_{skep}$.

**Theorem 63 ([13]).** *The calculus $BO'_{skep}$ has exponential lower bounds to the lengths of proofs. More precisely, there exist sequents $S_n$ of size $\mathcal{O}(n)$ such that every $BO'_{skep}$-proof of $S_n$ uses $2^{\Omega(n)}$ steps. Therefore, $s_{BO'_{skep}}(n), t_{BO'_{skep}}(n) \in 2^{\Omega(n)}$.*

*Proof. (Sketch)* We construct a sequence $(S_n)_{n\geq 1} = (\Sigma_n; \Gamma_n \mid\!\sim \psi_n)_{n \geq 1}$ such that for some constant $c$, every $BO'_{skep}$-proof of $S_n$ has length at least $2^{\Omega(n)}$. We choose $\Sigma_n = \varnothing$, $\psi_n = x_{2n}$, and $\Gamma_n = \langle \varnothing, D_{2n} \rangle$, where $D_{2n}$ consists of the defaults listed in Fig. 11. The default theory $\Gamma_n$ possesses $2^{n+1}$ stable extensions. Observe that each of these contains $x_{2n}$, but that each pair of stable extensions differs in truth assigned to the propositional variables $x_0, \dots, x_n$. We claim that

$$\frac{:\ x_0}{x_0} \qquad \frac{:\ \neg x_0}{\neg x_0}$$

$$\frac{x_i\ :\ x_{i+1}}{x_{i+1}} \qquad \frac{\neg x_i\ :\ x_{i+1}}{x_{i+1}} \qquad \frac{x_i\ :\ \neg x_{i+1}}{\neg x_{i+1}} \qquad \frac{\neg x_i\ :\ \neg x_{i+1}}{\neg x_{i+1}}$$

$$\frac{x_{n+j}\ :\ x_{n-j-1}}{x_{n+j+1}} \qquad \frac{\neg x_{n+j}\ :\ x_{n-j-1}}{x_{n+j+1}} \qquad \frac{x_{n+j}\ :\ \neg x_{n-j-1}}{\neg x_{n+j+1}}$$

$$\frac{\neg x_{n+j}\ :\ \neg x_{n-j-1}}{\neg x_{n+j+1}}$$

for $i = 0, \dots, n-1$ and $j = 0, \dots, n-2$

$$\frac{x_{2n-1}\ :\ x_0}{x_{2n}} \qquad \frac{\neg x_{2n-1}\ :\ x_0}{x_{2n}} \qquad \frac{x_{2n-1}\ :\ \neg x_0}{x_{2n}} \qquad \frac{\neg x_{2n-1}\ :\ \neg x_0}{x_{2n}}$$

**Fig. 11.** The defaults in $D_{2n}$ in the proof of Theorem 63.

every proof of $S_n$ has exponential length in $n$. More precisely, we show that rule (**sD4**) has to be applied an exponential number of times.

We point out that our argument does not only work against tree-like proofs, but also rules out the possibility of sub-exponential dag-like derivations for $D_{2n} \mid\!\sim x_{2n}$. The lower bound is obtained from the fact that to derive $x_{2n}$, we have to derive $x_i$ and $\neg x_i$ for each $n < i < 2n$, each of which can only be achieved from ancestors with mutually different proof constraints. This, by definition of $BO_{skep}$, leads to mutually disjoint sets of ancestor sequents. ■

## 8 Discussion and Open Problems

Our aim in these notes was to provide an introduction to the fascinating topic of proof complexity of non-classical logics. Proof complexity still offers a wealth of open problems, and this is even more true for the relatively new field of proof complexity of non-classical logics. All results presented here stem from the last decade. Rather than an open problem, an *open field* here is to extend analysis to further non-classical logics: many of these have not yet been investigated at all from a proof-complexity point of view. Instead of listing these logics we conclude with two general open questions which we find interesting.

**Problem I.** So far, research on proof complexity of non-classical logics has concentrated on Frege type systems or their equivalent sequent style formulations. Quite in contrast, many results in classical proof complexity concern systems which are motivated by algebra, geometry, or combinatorics. Can we construct algebraic or geometric proof systems for non-classical logics?

**Problem II.** One important tool in the analysis of classically strong systems such as Frege systems is their correspondence to weak arithmetic theories, known as bounded arithmetic (cf. the monographs [72, 33] or [11] for an introduction). Is there a similar connection between non-classical logics, particularly modal and intuitionistic logics, to first-order theories yielding further insight into lengths of proofs questions? Buss [23–25] and Cook and Urquhart [35] developed intutionistic bounded arithmetic. From this perspective, it seems very interesting to study intuitionistic bounded arithmetic in proof complexity.

## Acknowledgements

We are very grateful to Rosalie Iemhoff and Emil Jeřábek for numerous helpful comments on an earlier version of these notes.

## References

1. Ajtai, Miklós, 'The complexity of the pigeonhole-principle', *Combinatorica*, 14 (1994), 4, 417–433.
2. Alekhnovich, Michael, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson, 'Pseudorandom generators in propositional proof complexity', *SIAM Journal on Computing*, 34 (2004), 1, 67–88.
3. Alon, Noga, and Ravi B. Boppana, 'The monotone circuit complexity of boolean functions', *Combinatorica*, 7 (1987), 1, 1–22.
4. Amati, Gianni, Luigia Carlucci Aiello, Dov M. Gabbay, and Fiora Pirri, 'A proof theoretical approach to default reasoning I: Tableaux for default logic', *Journal of Logic and Computation*, 6 (1996), 2, 205–231.
5. Antoniou, Grigoris, and Kewen Wang, *Handbook of the History of Logic*, vol. 8, chap. Default Logic, North-Holland, 2007, pp. 517–556.
6. Areces, C., H. de Nivelle, and M. de Rijke, 'Resolution in Modal, Description and Hybrid Logic', *Journal of Logic and Computation*, 11 (2001), 5, 717–736.
7. Beame, Paul W., Russel Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák, 'Lower bounds on Hilbert's Nullstellensatz and propositional proofs', *Proc. London Mathematical Society*, 73 (1996), 3, 1–26.
8. Beame, Paul W., Russel Impagliazzo, Jan Krajíček, Toniann Pitassi, Pavel Pudlák, and Alan Woods, 'Exponential lower bounds for the pigeonhole principle', in *Proc. 24th ACM Symposium on Theory of Computing*, 1992, pp. 200–220.
9. Beame, Paul W., Toniann Pitassi, and Russel Impagliazzo, 'Exponential lower bounds for the pigeonhole principle', *Computational Complexity*, 3 (1993), 2, 97–140.
10. Ben-Sasson, Eli, and Avi Wigderson, 'Short proofs are narrow - resolution made simple', *Journal of the ACM*, 48 (2001), 2, 149–169.
11. Beyersdorff, Olaf, 'On the correspondence between arithmetic theories and propositional proof systems – a survey', *Mathematical Logic Quarterly*, 55 (2009), 2, 116–137.
12. Beyersdorff, Olaf, 'Proof complexity of non-classical logics', in *Proc. 7th Conference on Theory and Applications of Models of Computation*, vol. 6108 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin Heidelberg, 2010, pp. 15–27.
13. Beyersdorff, Olaf, Arne Meier, Sebastian Müller, Michael Thomas, and Heribert Vollmer, 'Proof complexity of propositional default logic', *Archive for Mathematical Logic*, 50 (2011), 7, 727–742.
14. Blackburn, Patrick, Maarten de Rijke, and Yde Venema, *Modal Logic*, vol. 53 of *Cambridge Tracts in Theoretical Computer Science*, Cambridge University Press, Cambridge, 2001.
15. Bonatti, P. A., 'A Gentzen system for non-theorems', Technical Report CD/TR 93/52, Christian Doppler Labor für Expertensysteme, 1993.
16. Bonatti, Piero A., and Nicola Olivetti, 'Sequent calculi for propositional nonmonotonic logics', *ACM Transactions on Computational Logic*, 3 (2002), 2, 226–278.
17. Bonet, Maria Luisa, Samuel R. Buss, and Toniann Pitassi, 'Are there hard examples for Frege systems?', in P. Clote, and J. Remmel, (eds.), *Feasible Mathematics II*, Birkhäuser, 1995, pp. 30–56.
18. Bonet, Maria Luisa, Toniann Pitassi, and Ran Raz, 'Lower bounds for cutting planes proofs with small coefficients', *The Journal of Symbolic Logic*, 62 (1997), 3, 708–728.

19. Bonet, Maria Luisa, Toniann Pitassi, and Ran Raz, 'On interpolation and automatization for Frege systems', *SIAM Journal on Computing*, 29 (2000), 6, 1939–1967.
20. Brouwer, Luitzen Egbertus Jan, *Over de Grondslagen der Wiskunde*, Ph.D. thesis, Amsterdam, 1907. Translation: "On the foundation of mathematics" in Brouwer, Collected Works, I, (A. Heyting ed.), 1975, North-Holland, Amsterdam, pp.11–101.
21. Brouwer, Luitzen Egbertus Jan, 'De onbetrouwbaarheid der logische principes', *Tijdschrift voor Wijsbegeerte*, 2 (1908), 152–158. Translation: The unreliability of the logical principles, Ibid. pp. 107–111.
22. Brouwer, Luitzen Egbertus Jan, 'Historical Background, Principles and Methods of Intuitionism', *South African Journal of Science*, (1952), 139–146.
23. Buss, Samuel R., 'The polynomial hierarchy and intuitionistic bounded arithmetic', in *Proc. Structure in Complexity Theory Conference*, 1986, pp. 77–103.
24. Buss, Samuel R., 'On model theory for intuitionstic bounded arithmetic with applications to independence', in S. R. Buss, and P. J. Scott, (eds.), *Feasible Mathematics*, Birkhauser, 1990, pp. 27–47.
25. Buss, Samuel R., 'A note on bootstrapping intuitionistic bounded arithmetic', in P. Aczel, H. Simmons, and S. Wainer, (eds.), *Proof Theory: a selection of papers from the Leeds Theory Programme 1990*, Cambridge University Press, 1992, pp. 142–169.
26. Buss, Samuel R., 'An introduction to proof theory', in Samuel R. Buss, (ed.), *Handbook of Proof Theory*, Elsevier, Amsterdam, 1998, pp. 1–78.
27. Buss, Samuel R., and Grigori Mints, 'The complexity of the disjunction and existential properties in intuitionistic logic', *Annals of Pure and Applied Logic*, 99 (1999), 1–3, 93–104.
28. Buss, Samuel R., and Pavel Pudlák, 'On the computational content of intuitionistic propositional proofs', *Annals of Pure and Applied Logic*, 109 (2001), 1–2, 49–63.
29. Cadoli, Marco, and Marco Schaerf, 'A survey of complexity results for non-monotonic logics', *Journal of Logic Programming*, 17 (1993), 2/3&4, 127–160.
30. Carnap, Rudolf, *Logische Syntax der Sprache*, Kegan Paul, 1934. English translation 1937, *The Logical Syntax of Language.*
31. Chagrov, Alexander, and Michael Zakharyaschev, *Modal Logic*, vol. 35 of *Oxford Logic Guides*, Clarendon Press, Oxford, 1997.
32. Clegg, Matthew, Jeff Edmonds, and Russell Impagliazzo, 'Using the Groebner basis algorithm to find proofs of unsatisfiability', in *Proc. 28th ACM Symposium on Theory of Computing*, 1996, pp. 174–183.
33. Cook, Stephen A., and Phuong Nguyen, *Logical Foundations of Proof Complexity*, Cambridge University Press, 2010.
34. Cook, Stephen A., and Robert A. Reckhow, 'The relative efficiency of propositional proof systems', *The Journal of Symbolic Logic*, 44 (1979), 1, 36–50.
35. Cook, Stephen A., and Alasdair Urquhart, 'Functional interpretations of feasibly constructive arithmetic', *Ann. Pure Appl. Logic*, 63 (1993), 2, 103–200.
36. Craig, William, 'Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory', *The Journal of Symbolic Logic*, 22 (1957), 3, 269–285.
37. Davis, Martin, and Hilary Putnam, 'A computing procedure for quantification theory', *Journal of the ACM*, 7 (1960), 3, 201–215.
38. De Nivelle, H., R. A. Schmidt, and U. Hustadt, 'Resolution-based methods for modal logics', *Logic J. IGPL*, 8 (2000), 265–292.

39. Dix, Jürgen, Ulrich Furbach, and Ilkka Niemelä, 'Nonmonotonic reasoning: Towards efficient calculi and implementations', in *Handbook of Automated Reasoning*, Elsevier and MIT Press, 2001, pp. 1241–1354.
40. Dowd, Martin, 'Model-theoretic aspects of P≠NP', , 1985. Unpublished manuscript.
41. Egly, Uwe, and Hans Tompits, 'Proof-complexity results for nonmonotonic reasoning', *ACM Transactions on Computational Logic*, 2 (2001), 3, 340–387.
42. Ferrari, Mauro, Camillo Fiorentini, and Guido Fiorino, 'On the complexity of the disjunction property in intuitionistic and modal logics', *ACM Transactions on Computational Logic*, 6 (2005), 3, 519–538.
43. Fitting, Melvin, *Modal Proof Theory*, vol. 3 of *Studies in Logic and Practical Reasoning*, chap. Handbook of Modal Logic, Elsevier, 2006, pp. 85–138.
44. Friedman, Harvey, 'One hundred and two problems in mathematical logic', *The Journal of Symbolic Logic*, 40 (1975), 2, 113–129.
45. Gabbay, Dov, 'Theoretical foundations of non-monotonic reasoning in expert systems', in *Logics and Models of Concurrent Systems*, Springer-Verlag, Berlin Heidelberg, 1985, pp. 439–457.
46. Gabbay, Dov, Agnes Kurucz, Frank Wolter, and Michael Zakharyaschev, *Many-Dimensional Modal Logics: Theory and Applications*, no. 148 in Studies in Logic and the Foundations of Mathematics, Elsevier, Amsterdam, 2003.
47. Gabbay, Dov M., and Larisa Maksimova, *Interpolation and Definability: Modal and Intuitionistic Logics*, vol. 46 of *Oxford Logic Guides*, Clarendon Press, Oxford, 2005.
48. Gentzen, Gerhard, 'Untersuchungen über das logische Schließen', *Mathematische Zeitschrift*, 39 (1935), 68–131.
49. Gerhard Brewka, Miroslaw Truszczynski, Victor W. Marek, (ed.) *Nonmonotonic Reasoning. Essays Celebrating its 30th Anniversary*, College Publications, 2011.
50. Ghilardi, Silvio, 'Unification in intuitionistic logic', *The Journal of Symbolic Logic*, 64 (1999), 2, 859–880.
51. Glivenko, V., 'Sur quelques points de la logique de M. Brouwer', *Bulletin de la Classe des Sciences de l'Académie Royale de Belgique*, 15 (1929), 183–188.
52. Gödel, Kurt, 'Eine Interpretation des intuitionistischen Aussagenkalküls', *Ergebnisse eines mathematischen Kolloquiums*, 4 (1933), 34–40.
53. Goldblatt, Robert, 'Mathematical modal logic: A view of its evolution', *Journal of Applied Logic*, 1 (2003), 309–392.
54. Gottlob, Georg, 'Complexity results for nonmonotonic logics', *Journal of Logic and Computation*, 2 (1992), 3, 397–425.
55. Haken, Amin, 'The intractability of resolution', *Theoretical Computer Science*, 39 (1985), 297–308.
56. Heyting, Arend, 'Die formalen Regeln der intuitionistischen Logik', *Sitzungsberichte der Preussischen Akademie der Wissenschaften*, (1930), 42–56.
57. Horrocks, Ian, Oliver Kutz, and Ulrike Sattler, 'The Even More Irresistible $\mathcal{SROIQ}$', in *Proc. of the 10th Int. Conf. on Principles of Knowledge Representation and Reasoning (KR2006)*, AAAI Press, 2006, pp. 57–67.
58. Hrubeš, Pavel, 'A lower bound for intuitionistic logic', *Annals of Pure and Applied Logic*, 146 (2007), 1, 72–90.
59. Hrubeš, Pavel, 'Lower bounds for modal logics', *The Journal of Symbolic Logic*, 72 (2007), 3, 941–958.

60. Hrubeš, Pavel, 'On lengths of proofs in non-classical logics', *Annals of Pure and Applied Logic*, 157 (2009), 2–3, 194–205.
61. Iemhoff, Rosalie, 'On the admissible rules of intuitionistic propositional logic', *The Journal of Symbolic Logic*, 66 (2001), 1, 281–294.
62. Jeřábek, Emil, 'Admissible rules of modal logics', *Journal of Logic and Computation*, 15 (2005), 4, 411–431.
63. Jeřábek, Emil, 'Frege systems for extensible modal logics', *Annals of Pure and Applied Logic*, 142 (2006), 366–379.
64. Jeřábek, Emil, 'Complexity of admissible rules', *Archive for Mathematical Logic*, 46 (2007), 2, 73–92.
65. Jeřábek, Emil, 'Substitution Frege and extended Frege proof systems in non-classical logics', *Annals of Pure and Applied Logic*, 159 (2009), 1–2, 1–48.
66. Jeřábek, Emil, 'Admissible rules of Łukasiewicz logic', *Journal of Logic and Computation*, 20 (2010), 2, 425–447.
67. Jeřábek, Emil, 'Bases of admissible rules of Łukasiewicz logic', *Journal of Logic and Computation*, 20 (2010), 6, 1149–1163.
68. Kazakov, Yevgeny, 'RIQ and SROIQ Are Harder than SHOIQ', in Gerhard Brewka, and Jérôme Lang, (eds.), *KR*, AAAI Press, 2008, pp. 274–284.
69. Kolmogorov, A.N., 'On the principle tertium non datur', *Mathematics of the USSR, Sbornik*, 32 (1925), 646–667. Translation in: From Frege to Gödel: A Source Book in Mathematical Logic 1879–1931 (J. van Heijenoord ed.), Harvard University Press, Cambridge 1967.
70. Kracht, Marcus, *Tools and Techniques in Modal Logic*, no. 142 in Studies in Logic and the Foundations of Mathematics, Elsevier Science Publishers, Amsterdam, 1999.
71. Krajíček, Jan, 'Lower bounds to the size of constant-depth propositional proofs', *The Journal of Symbolic Logic*, 59 (1994), 73–86.
72. Krajíček, Jan, *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, vol. 60 of *Encyclopedia of Mathematics and Its Applications*, Cambridge University Press, Cambridge, 1995.
73. Krajíček, Jan, 'Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic', *The Journal of Symbolic Logic*, 62 (1997), 2, 457–486.
74. Krajíček, Jan, 'Tautologies from pseudo-random generators', *Bulletin of Symbolic Logic*, 7 (2001), 2, 197–212.
75. Krajíček, Jan, 'Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds', *The Journal of Symbolic Logic*, 69 (2004), 1, 265–286.
76. Krajíček, Jan, and Pavel Pudlák, 'Propositional proof systems, the consistency of first order theories and the complexity of computations', *The Journal of Symbolic Logic*, 54 (1989), 3, 1063–1079.
77. Krajíček, Jan, and Pavel Pudlák, 'Some consequences of cryptographical conjectures for $S^1_2$ and $EF$', *Information and Computation*, 140 (1998), 1, 82–94.
78. Krajíček, Jan, Pavel Pudlák, and Alan Woods, 'Exponential lower bounds to the size of bounded depth Frege proofs of the pigeonhole principle', *Random Structures and Algorithms*, 7 (1995), 1, 15–39.
79. Kraus, Sarit, Daniel J. Lehmann, and Menachem Magidor, 'Nonmonotonic reasoning, preferential models and cumulative logics', *Artificial Intelligence*, 44 (1990), 1–2, 167–207.

80. Kripke, Saul, 'Semantical Analysis of Intuitionistic Logic, I', in J. N. Crossley, and M. A. E. Dummett, (eds.), *Formal Systems and Recursive Functions. Proceedings of the 8th Logic Colloquium*, North-Holland, Amsterdam, 1965, pp. 92–130.
81. Kutz, Oliver, Till Mossakowski, and Dominik Lücke, 'Carnap, Goguen, and the Hyperontologies: Logical Pluralism and Heterogeneous Structuring in Ontology Design', *Logica Universalis*, 4 (2010), 2, 255–333. Special Issue on 'Is Logic Universal?'.
82. Ladner, Richard E., 'The computational complexity of provability in systems of modal propositional logic', *SIAM Journal on Computing*, 6 (1977), 3, 467–480.
83. Lewis, Clarence Irving, *A Survey of Symbolic Logic*, University of California Press, Berkeley, 1918.
84. Makinson, David, 'General theory of cumulative inference', in *Proc. 2nd International Workshop on Non-Monotonic Reasoning*, Springer-Verlag, Berlin Heidelberg, 1989, pp. 1–18.
85. Meseguer, José, and Narciso Martí-Oliet, 'From abstract data types to logical frameworks', in *Selected papers from the 10th Workshop on Specification of Abstract Data Types Joint with the 5th COMPASS Workshop on Recent Trends in Data Type Specification*, Springer-Verlag, London, UK, 1995, pp. 48–80.
86. Mints, Grigori, and Arist Kojevnikov, 'Intuitionistic Frege systems are polynomially equivalent', *Journal of Mathematical Sciences*, 134 (2006), 5, 2392–2402.
87. Mossakowski, Till, Răzvan Diaconescu, and Andrzej Tarlecki, 'What is a logic translation?', *Logica Universalis*, 3 (2009), 1, 95–124.
88. Mundici, Daniele, 'Tautologies with a unique Craig interpolant, uniform vs. nonuniform complexity', *Annals of Pure and Applied Logic*, 27 (1984), 265–273.
89. Orlov, I. E., 'The calculus of compatibility of propositions', *Mathematics of the USSR, Sbornik*, 35 (1928), 263–286. (Russian).
90. Pitassi, Toniann, and Rahul Santhanam, 'Effectively polynomial simulations', in *Proc. 1st Innovations in Computer Science*, 2010.
91. Pudlák, Pavel, 'Lower bounds for resolution and cutting planes proofs and monotone computations', *The Journal of Symbolic Logic*, 62 (1997), 3, 981–998.
92. Pudlák, Pavel, 'The lengths of proofs', in Samuel R. Buss, (ed.), *Handbook of Proof Theory*, Elsevier, Amsterdam, 1998, pp. 547–637.
93. Pudlák, Pavel, and Jiri Sgall, 'Algebraic models of computation and interpolation for algebraic proof systems', in P. W. Beame, and S. R. Buss, (eds.), *Proof Complexity and Feasible Arithmetic*, vol. 39 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, American Mathematical Society, 1998, pp. 279–296.
94. Razborov, Alexander A., 'Lower bounds on the monotone complexity of boolean functions', *Doklady Akademii Nauk SSSR*, 282 (1985), 1033–1037. English translation in: Soviet Math. Doklady, 31, pp. 354–357.
95. Razborov, Alexander A., 'Lower bounds for the polynomial calculus', *Computational Complexity*, 7 (1998), 4, 291–324.
96. Reckhow, Robert A., *On the lengths of proofs in the propositional calculus*, Ph.D. thesis, University of Toronto, 1976.
97. Reiter, Raymond, 'A logic for default reasoning', *Artificial Intelligence*, 13 (1980), 81–132.
98. Risch, Vincent, and Camilla Schwind, 'Tableaux-based characterization and theorem proving for default logic', *Journal of Automated Reasoning*, 13 (1994), 2, 223–242.

99. Robinson, John Alan, 'A machine-oriented logic based on the resolution principle', *Journal of the ACM*, 12 (1965), 1, 23–41.

100. Rybakov, Vladimir V., *Admissibility of Logical Inference Rules*, no. 136 in Studies in Logic and the Foundations of Mathematics, Elsevier, Amsterdam, 1997.

101. Segerlind, Nathan, 'The complexity of propositional proofs', *Bulletin of Symbolic Logic*, 13 (2007), 4, 417–481.

102. Tarski, A., and J. C. C. McKinsey, 'Some Theorems about the Sentential Calculi of Lewis and Heyting', *Journal of Symbolic Logic*, 13 (1948), 1–15.

103. ten Cate, B., 'Interpolation for extended modal languages', *The Journal of Symbolic Logic*, 70 (2005), 1, 223–234.

104. Tiomkin, Michael L., 'Proving unprovability', in *Proc. 3rd Annual Symposium on Logic in Computer Science*, 1988, pp. 22–26.

105. Tseitin, G. C., 'On the complexity of derivations in propositional calculus', in A. O. Slisenko, (ed.), *Studies in Mathematics and Mathematical Logic, Part II*, 1968, pp. 115–125.

106. Urquhart, Alasdair, 'The complexity of propositional proofs', *Bulletin of Symbolic Logic*, 1 (1995), 425–467.

107. Vollmer, H., *Introduction to Circuit Complexity – A Uniform Approach*, Texts in Theoretical Computer Science, Springer Verlag, Berlin Heidelberg, 1999.