Proceedings Paper:
Beyersdorff, O (2010) Proof Complexity of Non-classical Logics. In: Kratochvíl, J, Li, A, Fiala, J and Kolman, P, (eds.) Theory and Applications of Models of Computation7th Annual Conference, TAMC 2010, Proceedings. Theory and Applications of Models of Computation, 7th Conference, 07-11 Jun 2010, Prague, Czech Republic. Lecture Notes in Computer Science, 108 (6). Springer , 15 - 27 . ISBN 978-3-642-13561-3

https://doi.org/10.1007/978-3-642-13562-0_3

Proof Complexity of Non-classical Logics

Olaf Beyersdorff

Institute of Computer Science, Humboldt University Berlin, Germany[⋆]
beyersdo@informatik.hu-berlin.de

Abstract. Proof complexity is an interdisciplinary area of research utilizing 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 this paper we give the first survey of this field concentrating on recent developments in proof complexity of non-classical logics.

1 Propositional Proof Complexity

One of the starting points of propositional proof complexity is the seminal paper of Cook and Reckhow [CR79] where they formalized 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 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 NP from coNP (and hence P from 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 [Tse68], 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 formulas describing the pigeonhole principle [Hak85]. In the last two decades these lower bounds were extended to a number of further propositional systems such as the Nullstellensatz system [BIK$^+$96], Cutting Planes [BPR97, Pud97], Polynomial Calculus [CEI96, Raz98], or bounded-depth Frege systems [Ajt94, BIK$^+$92, BPI93, KPW95]. For all these

[⋆] This paper was written while visiting Sapienza University of Rome under support of DFG grant KO 1053/5-2.

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 [Kra97], the size-width trade-off introduced by Ben-Sasson and Wigderson [BSW01], and the use of pseudorandom generators in proof complexity [ABSRW04, Kra01, Kra04].

Despite this enormous success many questions still remain open. In particular Frege systems currently form a strong barrier [BBP95], 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 [Seg07].

Let us mention that the separation of complexity classes is not the only motivation for studying lengths of proofs. In particular for strong systems like Frege and its extensions there is a fruitful connection to bounded arithmetic which adds insight to both subjects (cf. [Kra95]). Further, understanding weak systems as Resolution is vital to applications as the design of efficient SAT solvers (see e. g. [PS10] for a more elaborate argument). Last 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.

2 Why Non-classical Logics?

Besides the vivid research on propositional proof complexity briefly mentioned in the previous section, the last decade has witnessed intense investigation 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. Arguably, for computer science non-classical logics are even more important than classical logic as they are more expressive and often more suitable for concrete applications. It is therefore quite 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.

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 [Lad77], and this was subsequently also established for many other modal and intuitionistic logics.[1] 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

[1] 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 μ-calculus, but I am not aware of any proof complexity research on these, though.

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 [Hru09] and Jeřábek [Jeř09] on non-classical Frege systems (see Sect. 4) 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 [BBP95].

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 Sect. 5). 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.

3 Proof Systems for Modal and Intuitionistic Logics

We start by introducing some of the relevant proof systems for non-classical logic. 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.

Frege systems derive formulas using axioms and rules. In texts on classical logic these systems are usually referred to as Hilbert-style systems, but in proof complexity it has become customary to call them Frege systems [CR79]. A *Frege rule* is a $(k+1)$-tuple $(\varphi_0, \varphi_1, \dots, \varphi_k)$ of formulas such that $\{\varphi_1, \varphi_2, \dots, \varphi_k\} \models \varphi_0$. The standard notation for rules is

$$\frac{\varphi_1 \quad \varphi_2 \quad \cdots \quad \varphi_k}{\varphi_0} \; .$$

A Frege rule with $k = 0$ is called a *Frege axiom.* A formula ψ_0 can be derived from formulas $\psi_1, \dots, \psi_k$ by a Frege rule $(\varphi_0, \varphi_1 \dots, \varphi_k)$ if there exists a substitution σ such that $\sigma(\varphi_i) = \psi_i$ for $i = 0, \dots, k$.

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

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

A *Frege system* is a set $\mathcal{F}$ of Frege rules which is *implicationally complete*, meaning that for all formulas φ and sets of formulas Φ we have $\Phi \models \varphi$ if and only if there exists an $\mathcal{F}$-proof of φ from Φ.

Every text on classical logic uses its own favourite Frege system, but the actual choice of the rules for the system does not matter (see Sect. 5). Typically, these Frege systems use a number of simple axioms like $p \to (q \to p)$ and $(p \to q) \to (p \to (q \to r)) \to (p \to r)$ together with modus ponens

$$\frac{p \quad p \to q}{q}$$

as its only proper rule.

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 $\Box$. 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 a propositional Frege system 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 modal logic K can then simply be defined as the set of all modal formulas 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 $p \to \Box\neg\Box\neg p$, and GL by adding $\Box(\Box p \to p) \to \Box p$. As two last examples, $S4$ is obtained by extending $K4$ by $\Box p \to p$ and $S4Grz$ by extending $S4$ by $\Box(\Box(p \to \Box p) \to p) \to \Box p$. For more information on modal logics we refer to [BdRV01] or the thorough introduction in [Jeř09].

While modal logics extend the classical propositional calculus, *intuitionistic logics* are restrictions thereof. We will not define them precisely, but just mention that intuitionistic logic and its superintuitionistic extensions are again defined via Frege systems with a suitable choice of axioms and modus ponens as their only rule (cf. e. g. [Jeř09] for details).

4 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 φ or ψ already is. Buss, Mints, and Pudlák [BM99, BP01] showed that this disjunction property even holds in the following feasible form:

Theorem 1 (Buss, Mints, Pudlák [BM99, BP01]). *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 π of a disjunction $\varphi \vee \psi$, the algorithm A outputs a proof of either φ or ψ in polynomial time in the size of π.*

Subsequently, Ferrari, Fiorentini, and Fiorino [FFF05] extended this result to Frege systems and to further logics such as the modal logic $S4$.

A related property to feasible disjunction is the *feasible interpolation property.* As mentioned in Sect. 1, feasible interpolation is one of the general approaches to lower bounds in proof complexity. This technique was developed by Krajíček [Kra97] 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 [KP98, BPR00]). For intuitionistic logic, feasible interpolation holds in the following form:

Theorem 2 (Buss, Pudlák [BP01]). *Intuitionistic logic has the* feasible interpolation property*, i. e., from a proof π of an intuitionistic tautology*

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

using distinct sequences of variables $\bar{p}, \bar{q}, \bar{r}$ (such that $\bar{p} = p_1, \ldots, p_n$ are the common variables of φ_0 and φ_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 formulas was also shown for the modal logic $S4$ by Ferrari, Fiorentini, and Fiorino [FFF05]. Once we have feasible interpolation[2] 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 3 (Buss, Pudlák [BP01], Ferrari, Fiorentini, Fiorino [FFF05]). *If $\mathsf{NP} \cap \mathsf{coNP} \not\subseteq \mathsf{P/poly}$, then neither intuitionistic Frege systems nor Frege systems for $S4$ are polynomially bounded.*

This method uses the following idea: suppose we *know* that a sequence of formulas $\varphi_0^n \vee \varphi_1^n$ cannot be interpolated by a family of polynomial-size circuits as in Theorem 2. Then the formulas $\varphi_0^n \vee \varphi_1^n$ do not have polynomial-size proofs in any proof system which has feasible interpolation. Such formulas $\varphi_0^n \vee \varphi_1^n$ are easy to construct under suitable assumptions. For instance, the formulas could express that factoring integers is not possible in polynomial time (which implies $\mathsf{NP} \cap \mathsf{coNP} \not\subseteq \mathsf{P/poly}$).

[2] A terminological note (which I 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 $\varphi(\bar{p}, \bar{q}) \rightarrow \psi(\bar{p}, \bar{r})$ is provable, where $\bar{p}, \bar{q}, \bar{r}$ are disjoint sequences of variables, then there is a formula $\theta(\bar{p})$ such that $\varphi(\bar{p}, \bar{q}) \rightarrow \theta(\bar{p})$ and $\theta(\bar{p}) \rightarrow \psi(\bar{p}, \bar{r})$ are also provable. In intuitionistic logic, this is a quite different property from the reformulations using disjunction which come from classical logic. What is called "feasible interpolation" for intuitionistic logic (such as in Theorem 2) has nothing to do with interpolation, it is essentially a feasible version of Haldén completeness. Similarly, the modal "feasible interpolation" from [FFF05] is a restricted version of the feasible modal disjunction property.

To improve Theorem 3 to an unconditional lower bound, we need superpolynomial circuit lower bounds for suitable functions, and such lower bounds are only known for restricted classes of Boolean circuits (cf. [Vol99]). One such restricted class consists of all *monotone* Boolean circuits. Razborov [Raz85] and Alon and Boppana [AB87] 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 NP-pair. The disjointness of the Clique-Colouring pair can be expressed by a sequence of propositional formulas

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

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 $k+1$.

In order to prove lower bounds for the formulas (1) we need a *monotone feasible interpolation theorem*, i. e., a version of Theorem 2 where the circuits C are monotone. Such a result is known for a number of classical proof systems including Resolution and Cutting Planes, but does not hold for Frege systems under reasonable assumptions (factoring integers is not possible in polynomial time [KP98, BPR00]). Therefore, under the same assumptions we cannot expect a full version of monotone feasible interpolation for modal extensions of the classical Frege system. Note that the above mentioned feasible interpolation theorem of Ferrari et al. [FFF05] also only holds for a restricted class of modal formulas.

Hrubeš [Hru07b, Hru09] had the idea to modify the Clique-Colouring formulas (1) in a clever way by introducing the modal operator $\Box$ in appropriate places to obtain

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

with $k = \sqrt{n}$. For these formulas he was able to show in [Hru09] that

1. the formulas (2) are modal tautologies;
2. if the formulas (2) are provable in K with $m(n)$ distributivity axioms, then the original formulas (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 4 (Hrubeš [Hru07b, Hru09]). *The formulas* (2) *are K-tautologies. If L is a sublogic of GL or $S4$, then every Frege proof of the formulas* (2) *in the logic L uses $2^{n^{\Omega(1)}}$ steps.*

The first proof of Theorem 4 in [Hru07b] was obtained by a rather involved model-theoretic argument, but his later paper [Hru09] contains the simplified approach sketched above.

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

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

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

Theorem 5 (Hrubeš [Hru07a, Hru09]). *The formulas* (3) *are intuitionistic tautologies and require intuitionistic Frege proofs with* $2^{n^{\Omega(1)}}$ *steps.*

The first proof of Theorem 5 in [Hru07a] was given via a translation of intuitionistic logic into modal logic, but again [Hru09] reproves the result via the simplified approach. Theorem 5 also implies an exponential speed-up of classical logic over intuitionistic logic, because the formulas (3) have polynomial-size classical Frege proofs [Hru07a]. The lower bounds of Theorems 4 and 5 were extended by Jeřábek [Jeř09] to further logics, namely all modal and superintuitionistic logics with infinite branching.

5 Simulations between Non-classical Proof Systems

Besides proving lower bounds a second important topic in proof complexity is the comparison of proof systems via simulations introduced in [CR79] and [KP89] (but see also [PS10] for a new notion). Frege systems and its extensions are one of the most interesting cases in this respect. We recall the definition of polynomial simulations from [CR79]: two proof systems P and Q are *polynomially equivalent* if every P-proof can be transformed in polynomial time into a Q-proof of the same formula, and vice versa. 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 formulas are suitably translated into formulas over the new basis (see [PS10] 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 [CR79, Rec76]. 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-formulas into L_2-formulas before we can apply the method from the previous item. To still obtain polynomial size formulas after the translation, Reckhow [Rec76] first rebalances the formulas 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 formulas to logarithmic depth is not possible because in modal and intuitionistic logic there are examples of formulas which indeed require linear depth. For this reason, the equivalence of modal or intuitionistic Frege systems using different connectives is still open (cf. [Jeř06]).

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

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

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 σ 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. But this is not the case in non-classical logic. For instance, in the modal modal logic $K4$ the rule

$$\frac{\Box\varphi}{\varphi}$$

is admissible, but not valid. Admissibility has been thoroughly studied for many non-classical logics. In particular, starting with a question of Friedman [Fri75] it was investigated whether admissibility of a given rule is a decidable property, and this was answered affirmatively for many modal and intuitionistic logics [Ryb97]. In fact, for intuitionistic logic and many important modal logics such as $K4$, GL, $S4$, and $S4Grz$, deciding the admissibility of a given rule is coNEXP-complete as shown by Jeřábek [Jeř07]. 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 characterization of admissible rules for intuitionistic logic by Ghilardi [Ghi99], Iemhoff [Iem01] constructed an explicit set of rules which forms a basis for all admissible intuitionistic rules. Using this basis, Mints and Kojevnikov [MK06] were able to prove the equivalence of all intuitionistic Frege systems:

Theorem 6 (Mints, Kojevnikov [MK06]). *All intuitionistic Frege systems in the language* $\to, \land, \lor, \bot$ *are polynomially equivalent.*

Subsequently, Jeřábek [Jeř06] generalized these results to an infinite class of modal logics (so-called extensible logics [Jeř05]). We single out some of the most important instances in the next theorem:

Theorem 7 (Jeřábek [Jeř06]). *Let L be one of the modal logics $K4$, GL, $S4$, or $S4Grz$ 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 [Jeř10a, Jeř10b].

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 formulas 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 [CR79] 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 [Dow85] and Krajíček and Pudlák [KP89]. 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 8 (Jeřábek [Jeř09]). *For any modal or superintuitionistic logic, extended Frege and tree-like substitution Frege are polynomially equivalent.*

This shows that Cook and Reckhow's intuition on extended vs. substitution Frege was indeed correct and is further confirmed by results of Jeřábek [Jeř09] 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 characterizations, Jeřábek exhibits examples for logics where the *EF* vs. *SF* question receives different answers:

Theorem 9 (Jeřábek [Jeř09]).

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 Clique-Colour tautologies used by Hrubeš [Hru09]. However, Hrubeš' lower bounds were extended by Jeřábek [Jeř09] to a large class of logics with infinite branching in the underlying Kripke frames, and item 2 of Theorem 9 also holds for these logics.

6 Further Logics and Open Problems

Besides modal and intuitionistic logics there are many other non-classical logics which are interesting to analyse from a proof complexity perspective. One example of such logics are non-monotonic logics of which Reiter's *default logic* [Rei80] is one of the most popular. The semantics and the complexity of default logic have been intensively studied during the last decades (cf. [CS93] for a survey).

In particular, Gottlob [Got92] has identified and studied two reasoning tasks for propositional default logic: the *credulous* and the *skeptical* reasoning problem which can be understood as analogues of the classical problems SAT and TAUT. Due to the stronger expressibility of default logic, however, credulous and skeptical reasoning become harder than their classical counterparts—they are complete for the second level Σ_2^{p} and Π_2^{p} of the polynomial hierarchy [Got92].

Elegant sequent calculi were designed for the credulous and skeptical reasoning problems by Bonatti and Olivetti [BO02]. When analysing the proof complexity of these systems it turns out that lower and upper bounds to the proof size in credulous default reasoning and in classical Frege systems are the same up to a polynomial.

Theorem 10 ([BMM$^+$10]). *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.*

This means that while the decision complexity of the logic increases, this increase does not manifest in the lengths of proofs. In contrast, for the skeptical default calculus of Bonatti and Olivetti an exponential lower bound to the number of steps applies [BMM$^+$10].

A similar result as Theorem 10 was observed by Jeřábek [Jeř09] for tabular modal and superintuitionistic logics which are in coNP. Jeřábek constructs translations of extended Frege proofs in these logics to propositional proofs, thereby obtaining analogous versions of Theorem 10 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.

Let us conclude with some open problems. Besides extending research on proof lengths to further logics, we find the following questions interesting:

Problem 1. 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 2. One important tool in the analysis of classically strong systems as Frege systems is their correspondence to weak arithmetic theories, known as bounded arithmetic (cf. [Kra95]). Is there a similar connection between non-classical logics, particularly modal logic, to first-order theories yielding further insight into lengths of proofs questions?

Acknowledgement

I thank Emil Jeřábek for helpful suggestions on an earlier draft of this paper.

References

[AB87] Noga Alon and Ravi B. Boppana. The monotone circuit complexity of boolean functions. *Combinatorica*, 7(1):1–22, 1987.

[ABSRW04] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal on Computing*, 34(1):67–88, 2004.

[Ajt94] Miklós Ajtai. The complexity of the pigeonhole-principle. *Combinatorica*, 14(4):417–433, 1994.

[BBP95] Maria Luisa Bonet, Samuel R. Buss, and Toniann Pitassi. Are there hard examples for Frege systems? In P. Clote and J. Remmel, editors, *Feasible Mathematics II*, pages 30–56. Birkhäuser, 1995.

[BdRV01] Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal Logic*, volume 53 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, Cambridge, 2001.

[BIK$^+$92] Paul W. Beame, 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*, pages 200–220, 1992.

[BIK$^+$96] Paul W. Beame, Russel Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proc. London Mathematical Society*, 73(3):1–26, 1996.

[BM99] Samuel R. Buss and Grigori Mints. The complexity of the disjunction and existential properties in intuitionistic logic. *Annals of Pure and Applied Logic*, 99(1–3):93–104, 1999.

[BMM$^+$10] Olaf Beyersdorff, Arne Meier, Sebastian Müller, Michael Thomas, and Heribert Vollmer. Proof complexity of propositional default logic. In *Proc. 13th International Conference on Theory and Applications of Satisfiability Testing*, Lecture Notes in Computer Science. Springer-Verlag, Berlin Heidelberg, 2010.

[BO02] Piero A. Bonatti and Nicola Olivetti. Sequent calculi for propositional nonmonotonic logics. *ACM Transactions on Computational Logic*, 3(2):226–278, 2002.

[BP01] Samuel R. Buss and Pavel Pudlák. On the computational content of intuitionistic propositional proofs. *Annals of Pure and Applied Logic*, 109(1–2):49–63, 2001.

[BPI93] Paul W. Beame, Toniann Pitassi, and Russel Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3(2):97–140, 1993.

[BPR97] Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. Lower bounds for cutting planes proofs with small coefficients. *The Journal of Symbolic Logic*, 62(3):708–728, 1997.

[BPR00] Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. On interpolation and automatization for Frege systems. *SIAM Journal on Computing*, 29(6):1939–1967, 2000.

[BSW01] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. *Journal of the ACM*, 48(2):149–169, 2001.

[CEI96] Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proc. 28th ACM Symposium on Theory of Computing*, pages 174–183, 1996.

[CR79] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979.

[CS93] Marco Cadoli and Marco Schaerf. A survey of complexity results for nonmonotonic logics. *Journal of Logic Programming*, 17(2/3&4):127–160, 1993.

[Dow85] Martin Dowd. Model-theoretic aspects of P≠NP. Unpublished manuscript, 1985.

[FFF05] Mauro Ferrari, Camillo Fiorentini, and Guido Fiorino. On the complexity of the disjunction property in intuitionistic and modal logics. *ACM Transactions on Computational Logic*, 6(3):519–538, 2005.

[Fri75] Harvey Friedman. One hundred and two problems in mathematical logic. *The Journal of Symbolic Logic*, 40(2):113–129, 1975.

[Ghi99] Silvio Ghilardi. Unification in intuitionistic logic. *The Journal of Symbolic Logic*, 64(2):859–880, 1999.

[Got92] Georg Gottlob. Complexity results for nonmonotonic logics. *Journal of Logic and Computation*, 2(3):397–425, 1992.

[Hak85] Amin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[Hru07a] Pavel Hrubeš. A lower bound for intuitionistic logic. *Annals of Pure and Applied Logic*, 146(1):72–90, 2007.

[Hru07b] Pavel Hrubeš. Lower bounds for modal logics. *The Journal of Symbolic Logic*, 72(3):941–958, 2007.

[Hru09] Pavel Hrubeš. On lengths of proofs in non-classical logics. *Annals of Pure and Applied Logic*, 157(2–3):194–205, 2009.

[Iem01] Rosalie Iemhoff. On the admissible rules of intuitionistic propositional logic. *The Journal of Symbolic Logic*, 66(1):281–294, 2001.

[Jeř05] Emil Jeřábek. Admissible rules of modal logics. *Journal of Logic and Computation*, 15(4):411–431, 2005.

[Jeř06] Emil Jeřábek. Frege systems for extensible modal logics. *Annals of Pure and Applied Logic*, 142:366–379, 2006.

[Jeř07] Emil Jeřábek. Complexity of admissible rules. *Archive for Mathematical Logic*, 46(2):73–92, 2007.

[Jeř09] Emil Jeřábek. Substitution Frege and extended Frege proof systems in non-classical logics. *Annals of Pure and Applied Logic*, 159(1–2):1–48, 2009.

[Jeř10a] Emil Jeřábek. Admissible rules of Łukasiewicz logic. *Journal of Logic and Computation*, 2010. To appear.

[Jeř10b] Emil Jeřábek. Bases of admissible rules of Łukasiewicz logic. *Journal of Logic and Computation*, 2010. To appear.

[KP89] Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54(3):1063–1079, 1989.

[KP98] Jan Krajíček and Pavel Pudlák. Some consequences of cryptographical conjectures for S^1_2 and EF. *Information and Computation*, 140(1):82–94, 1998.

[KPW95] Jan Krajíček, 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(1):15–39, 1995.

[Kra95] Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, volume 60 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, Cambridge, 1995.

[Kra97] Jan Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.

[Kra01] Jan Krajíček. Tautologies from pseudo-random generators. *Bulletin of Symbolic Logic*, 7(2):197–212, 2001.

[Kra04] Jan Krajíček. Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. *The Journal of Symbolic Logic*, 69(1):265–286, 2004.

[Lad77] Richard E. Ladner. The computational complexity of provability in systems of modal propositional logic. *SIAM Journal on Computing*, 6(3):467–480, 1977.

[MK06] Grigori Mints and Arist Kojevnikov. Intuitionistic Frege systems are polynomially equivlalent. *Journal of Mathematical Sciences*, 134(5):2392–2402, 2006.

[PS10] Toniann Pitassi and Rahul Santhanam. Effectively polynomial simulations. In *Proc. 1st Innovations in Computer Science*, 2010.

[Pud97] Pavel Pudlák. Lower bounds for resolution and cutting planes proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, 1997.

[Raz85] Alexander A. Razborov. Lower bounds on the monotone complexity of boolean functions. *Doklady Akademii Nauk SSSR*, 282:1033–1037, 1985. English translation in: Soviet Math. Doklady, 31, pp. 354–357.

[Raz98] Alexander A. Razborov. Lower bounds for the polynomial calculus. *Computational Complexity*, 7(4):291–324, 1998.

[Rec76] Robert A. Reckhow. *On the lengths of proofs in the propositional calculus.* PhD thesis, University of Toronto, 1976.

[Rei80] Raymond Reiter. A logic for default reasoning. *Artificial Intelligence*, 13:81–132, 1980.

[Ryb97] Vladimir V. Rybakov. *Admissibility of logical inference rules*, volume 136 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, 1997.

[Seg07] Nathan Segerlind. The complexity of propositional proofs. *Bulletin of Symbolic Logic*, 13(4):417–481, 2007.

[Tse68] G. C. Tseitin. On the complexity of derivations in propositional calculus. In A. O. Slisenko, editor, *Studies in Mathematics and Mathematical Logic, Part II*, pages 115–125. 1968.

[Vol99] H. Vollmer. *Introduction to Circuit Complexity – A Uniform Approach.* Texts in Theoretical Computer Science. Springer Verlag, Berlin Heidelberg, 1999.