# Weak Systems Have Intractable Theorems

Raheleh Jalali

Utrecht University

Given a proof system, how can we specify the "hardness" of its theorems? One way to tackle this problem is taking the lengths of proofs as the corresponding hardness measure. Following this route, we call a theorem hard when even its shortest proof in the system is "long" in a certain formal sense. Finding hard theorems in proof systems for classical logic has been an open problem for a long time. However, in recent years as significant progress, many super-intuitionistic and modal logics have been shown to have hard theorems. In this talk, we will extend the aforementioned result to also cover a variety of weaker logics in the substructural realm. We show that there are theorems in the usual calculi for substructural logics that are even hard for the intuitionistic systems.

In technical terms, for any proof system **P** at least as strong as Full Lambek calculus, **FL**, and polynomially simulated by the extended Frege system for some infinite branching super-intuitionistic logic, we present an exponential lower bound on the proof lengths. More precisely, we will provide a sequence of **P**-provable formulas $\{A_n\}_{n=1}^{\infty}$ such that the length of the shortest **P**-proof for $A_n$ is exponential in the length of $A_n$. The lower bound also extends to the number of proof-lines (proof-lengths) in any Frege system (extended Frege system) for a logic between $\mathsf{FL}$ and any infinite branching super-intuitionistic logic. Finally, in the classical substructural setting, we will establish an exponential lower bound on the number of proof-lines in any proof system polynomially simulated by the cut-free version of $\mathbf{CFL_{ew}}$.

To be able to present the results formally, we need some ingredients. Let us start with defining substructural logics. For simplicity, we provide hard formulas for $\mathsf{FL_e}$. However, there are also hard theorem for the weaker logic $\mathsf{FL}$ [2]. The language we use is $\{0, 1, \wedge, \vee, *, \rightarrow\}$. Uppercase Greek letters denote multisets of formulas, and lower case Greek letters represent formulas. Consider the following sequent calculus:

$$\varphi \Rightarrow \varphi \qquad \Rightarrow 1 \qquad 0 \Rightarrow$$

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma, 1 \Rightarrow \Delta}\ (1w) \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow 0, \Delta}\ (0w)$$

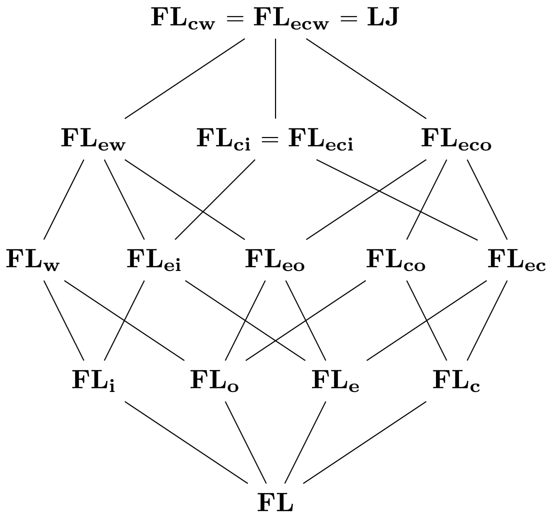
$$\frac{\Gamma, \varphi \Rightarrow \Delta}{\Gamma, \varphi \wedge \psi \Rightarrow \Delta} \qquad \frac{\Gamma, \psi \Rightarrow \Delta}{\Gamma, \varphi \wedge \psi \Rightarrow \Delta} \qquad \frac{\Gamma \Rightarrow \varphi, \Delta \qquad \Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \varphi \wedge \psi, \Delta}$$

$$\frac{\Gamma, \varphi \Rightarrow \Delta \qquad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \varphi \vee \psi \Rightarrow \Delta} \qquad \frac{\Gamma \Rightarrow \varphi, \Delta}{\Gamma \Rightarrow \varphi \vee \psi, \Delta} \qquad \frac{\Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \varphi \vee \psi, \Delta}$$

$$\frac{\Gamma, \varphi, \psi \Rightarrow \Delta}{\Gamma, \varphi * \psi \Rightarrow \Delta} \qquad \frac{\Gamma \Rightarrow \varphi, \Delta \qquad \Sigma \Rightarrow \psi, \Lambda}{\Gamma, \Sigma \Rightarrow \varphi * \psi, \Delta, \Lambda}$$

$$\frac{\Gamma \Rightarrow \varphi, \Delta \qquad \Sigma, \psi \Rightarrow \Lambda}{\Gamma, \Sigma, \varphi \rightarrow \psi \Rightarrow \Delta, \Lambda} \qquad \frac{\Gamma, \varphi \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \varphi \rightarrow \psi, \Delta}$$

$$\frac{\Gamma \Rightarrow \varphi, \Delta \qquad \Sigma, \varphi \Rightarrow \Lambda}{\Gamma, \Sigma \Rightarrow \Delta, \Lambda}\ (cut)$$



The sequent calculus $\mathbf{FL_e}$ is the single-conclusion version of the sequent calculus presented above and $\mathbf{CFL_e}$ is the multi-conclusion version. The structural rules are as usual:

**Weakening rules:**

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma, \varphi \Rightarrow \Delta}\,(i) \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \varphi, \Delta}\,(o)$$

**Contraction rules:**

$$\frac{\Gamma, \varphi, \varphi \Rightarrow \Delta}{\Gamma, \varphi \Rightarrow \Delta}\,(Lc) \qquad \frac{\Gamma \Rightarrow \varphi, \varphi, \Delta}{\Gamma \Rightarrow \varphi, \Delta}\,(Rc)$$

Adding these rules to the sequent calculi defined, result in various substructural calculi. It is worth mentioning that if we consider uppercase Greek letters to be *sequences* of formulas instead of multisets, i.e., the exchange rule is not present, then, we can introduce two implication-like connectives $\backslash$ and $/$, and include their respective rules. This system is called **FL**. The figure on top of this page shows the web of the sequent calculi between the full Lambek calculus **FL** and **LJ**, the usual sequent calculus for the intuitionistic logic $\mathsf{IPC}$. Some other sequent calculi for which our result holds for are listed in Table 1.

Second, let us define Frege systems. They are the most natural calculi for propositional logic. A *(Frege) rule* is an expression of the form $\frac{\varphi_1, \ldots, \varphi_k}{\varphi}$ where $\varphi_1, \ldots, \varphi_k, \varphi$ are propositional formulas. Let $\mathbf{P}$ be a finite set of rules. A $\mathbf{P}$-proof of $\varphi$ from a set of assumptions $X$, denoted by $X \vdash_{\mathbf{P}} \varphi$, is $\varphi_1, \ldots, \varphi_m = \varphi$ such that each $\varphi_i \in X$, or is inferred from some $\varphi_j$, $j < i$, by a substitution instance of rule in $\mathbf{P}$. The formulas $\varphi_i$ are called *lines* of the proof.

A finite set of rules, $\mathbf{P}$, is called a *Frege system* for a logic $\mathsf{L}$ when

(1) $\mathbf{P}$ is strongly sound: if $\varphi_1, \ldots, \varphi_n \vdash_{\mathbf{P}} \varphi$, then $\varphi_1, \ldots, \varphi_n \vdash_{\mathsf{L}} \varphi$,

(2) $\mathbf{P}$ is strongly complete: if $\varphi_1, \ldots, \varphi_n \vdash_{\mathsf{L}} \varphi$, then $\varphi_1, \ldots, \varphi_n \vdash_{\mathbf{P}} \varphi$.

Third, and finally, we give a characterization of superintuitoinistic logics of infinite branching. Consider the following superintuitionistic (si) logics:

$$\mathsf{KC} = \mathsf{IPC} + \neg p \vee \neg\neg p \qquad , \qquad \mathsf{BD_n} = \mathsf{IPC}{+}BD_n$$

Table 1: Some sequent calculi with their definitions.

| Sequent calculus | Definition |
|---|---|
| **RL** | $\mathbf{FL} + (0 \Leftrightarrow 1)$ |
| **CyFL** | $\mathbf{FL} + (\varphi\backslash 0 \Leftrightarrow 0/\varphi)$ |
| **DFL** | $\mathbf{FL} + (\varphi \wedge (\psi \vee \theta) \Leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \theta))$ |
| $\mathbf{P_nFL}$ | $\mathbf{FL} + (\varphi^n \Leftrightarrow \varphi^{n+1})$ |
| **psBL** | $\mathbf{FL_w} + \{(\varphi \wedge \psi \Leftrightarrow \varphi * (\varphi\backslash\psi)), (\varphi \wedge \psi \Leftrightarrow (\psi/\varphi) * \varphi)\}$ |
| **HA** | $\mathbf{FL_w} + (\varphi \Leftrightarrow \varphi^2)$ |
| **DRL** | $\mathbf{RL} + (\varphi \wedge (\psi \vee \theta) \Leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \theta))$ |
| **IRL** | $\mathbf{RL} + (\varphi \Rightarrow 1)$ |
| **CRL** | $\mathbf{RL} + (\varphi * \psi \Leftrightarrow \psi * \varphi)$ |
| **GBH** | $\mathbf{RL} + \{(\varphi \wedge \psi \Leftrightarrow \varphi * (\varphi\backslash\psi)), (\varphi \wedge \psi \Leftrightarrow (\psi/\varphi) * \varphi)\}$ |
| **Br** | $\mathbf{RL} + (\varphi \wedge \psi \Leftrightarrow \varphi * \psi)$ |

where $\mathsf{IPC}$ is the intuitionistic logic and $BD_0 := \bot$ and $BD_{n+1} := p_n \vee (p_n \to BD_n)$. Jeřábek in [3] proved the following interesting theorem that a superintuitionistic logic $\mathsf{L}$ has infinite branching iff $\mathsf{L} \subseteq \mathsf{BD}_2$ or $\mathsf{L} \subseteq \mathsf{KC} + \mathsf{BD}_3$.

Now, let us give a sketch of how to prove the lower bound. In order to do so, we have to provide a sequence of formulas provable in $\mathbf{FL_e}$, such that every proof of them are long. This task requires two steps. The first step, which is the main task, is providing a sequence of $\mathbf{FL_e}$-tautologies. To achieve this goal we change the existing hard intuitionistic tautologies in a suitable way that they become provable in $\mathbf{FL_e}$, but remain hard. The next step, which is the easier part, is proving that these tautologies are hard. To do so, we use the canonical translation of the language of $\mathbf{FL_e}$ to the language of $\mathsf{IPC}$, i.e., sending $\{0, 1, *\}$ to $\{\bot, \top, \wedge\}$, respectively and the other connectives to themselves. It is easy to see that this transformation takes polynomial time.

Let us mention the form of the hard intuitionistic tautologies. The following formulas, $\Theta_{n,k}$, are hard for $\mathsf{IPC}$ and they are negation-free and $\bot$-free. Small Roman letters denote atomic formulas and the formulas $\alpha_n^k$ and $\beta_n^{k+1}$ are monotone, i.e., only consist of atoms, $\wedge$, $\vee$.

$$\Theta_{n,k} := \bigwedge_{i,j}(p_{i,j} \vee q_{i,j}) \to$$

$$[(\bigwedge_{i,l}(s_{i,l} \vee s'_{i,l}) \to \alpha_n^k(\bar{p}, \bar{s}, \bar{s'})) \vee (\bigwedge_{i,l}(r_{i,l} \vee r'_{i,l}) \to \beta_n^{k+1}(\bar{q}, \bar{r}, \bar{r'}))]$$

The result by Hrubeš [1] and Jeřábek [3] is the following theorem:

**Theorem.** The formulas $\Theta_{n,k}$ are $\mathsf{IPC}$-tautologies and require $\mathsf{IPC}$-Frege proofs with $2^{n^{\Omega(1)}}$ lines, for $k = \lfloor\sqrt{n}\rfloor$.

In the following we see the form of the hard $\mathsf{FL_e}$ tautologies:

$$\Theta^*_{n,k} := [\mathop{\ast}\limits_{i,j}((p_{i,j} \wedge 1) \vee (q_{i,j} \wedge 1))] \quad \to$$

$$\Big[(\mathop{\ast}\limits_{i,l}((s_{i,l} \wedge 1) \vee (s'_{i,l} \wedge 1)) \to \alpha_n^k) \ \vee (\mathop{\ast}\limits_{i,l}((r_{i,l} \wedge 1) \vee (r'_{i,l} \wedge 1)) \to \beta_n^{k+1})\Big]$$

Now, we have all the ingredients to formally state our result:

**Theorem.** [2] The formulas $\Theta^*_{n,k}$ are $\mathsf{FL_e}$-tautologies. Moreover, for any substructural logic $\mathsf{L}$ and any superintuitionistic logic of infinite branching $\mathsf{M}$ such that $\mathsf{FL_e} \subseteq \mathsf{L} \subseteq \mathsf{M}$, the formulas $\Theta^*_{n,k}$ require $\mathsf{L}$-Frege proofs with $2^{n^{\Omega(1)}}$ lines, for $k = \lfloor \sqrt{n} \rfloor$.

The concrete application of the theorem follows:

**Corollary.** Let $S \subseteq \{e, c, i, o\}$, and $\mathsf{L}$ be $\mathsf{FL_S}$, or any of the logics of the sequent calculi in Table 1. Then the length of every proof of $\Theta^*_n$ in any (extended) Frege system for $\mathsf{L}$ is exponential in $n$.

Let us end with the following question: what happens in the case of the classical versions of the above substructural logics? They are not included in $\mathsf{IPC}$ and hence our method does not work. However, for their cut-free versions we have the following theorem.

**Theorem.** The length of every proof of $\Theta^*_n$ in the sequent calculi $\mathbf{CFL_e^-}, \mathbf{CFL_{ei}^-}, \mathbf{CFL_{eo}^-}$, and $\mathbf{CFL_{ew}^-}$ is exponential in $n$, where the " $-$ " means without the cut rule.

## References

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

[2] Raheleh Jalali. Proof complexity of substructural logics. *Annals of Pure and Applied Logic*, 172(7):102972, 2021.

[3] 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.