Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 315 (2015) 31–46

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

How Many Times do We Need an Assumption to Prove a Tautology in Minimal Logic? Examples on the Compression Power of Classical Reasoning ⋆

Edward Hermann Haeusler
Departamento de Informática
PUC-Rio
Rio de Janeiro, Brazil

Abstract

In this article we present a class of formulas φ_n, $0 \leq n$, that need at least 2^n assumption occurrences of other formula β_n in any normal proof in Natural Deduction for purely implicational minimal propositional logic ($\mathbf{M}_{\rightarrow}$). In classical implicational logic, each φ_n have normal proofs using at most one assumption occurrence. As a consequence, normal proofs of φ_n have exponential lower bound in $\mathbf{M}_{\rightarrow}$ and linear lower bound in its classical version. In fact, 2^n is the lower-bound for cut-free Sequent proofs too. The existence of this class of formulas have strong influence in designing automatic proof-procedures based in such systems. It is discussed proof-theoretically how tautologies in purely implicational classical logic can be proved by polynomially sized derivations when their minimal counterpart is exponentially sized.

Keywords: Propositional Logic Complexity, Natural Deduction, Minimal propositional logic, Proof Theory

1 Introduction

Providing proofs for propositional tautologies seems to be a hard task. Huge proofs are such that their size is super-polynomial with regard to the size of their conclusions. Knowing that there is a classical propositional logic tautology having only huge proofs is related to know whether $NP = CoNP$ or not [2]. Intuitionistic logic is PSPACE-complete [11] and Richard Statman [17] showed that purely implicational minimal logic ($\mathbf{M}_{\rightarrow}$) is PSPACE-complete too. We showed in [8] that, if a propositional logic has a Natural Deduction (ND) with the sub-formula property then it is in PSPACE. This follows from the fact that $\mathbf{M}_{\rightarrow}$ polynomially encodes any propositional logic that has such ND system. Thus, the existence of huge proofs

⋆ The author is grateful to CAPES and CNPq project PIER for their financial support.
Email:hermann@inf.puc-rio.br

http://dx.doi.org/10.1016/j.entcs.2015.06.004
1571-0661/

for a more general class of propositional logics is related to the existence of huge proofs in $\mathbf{M}_{\rightarrow}$ that amounts to know whether $PSPACE = NP$ or not. The relations between these computational complexity classes and the existence of huge proofs involve arbitrary proof systems, indeed. For example, $NP = PSPACE$ is the case, if and only if, for any $\mathbf{M}_{\rightarrow}$ tautology there is a proof system that produces a polynomially sized proof of this tautology.

A theoretical study of arbitrary proof systems is out of scope of this article. However, studying particular proof systems for key logics, like $\mathbf{M}_{\rightarrow}$ or classical logic, can shed some light on practical aspects of implementing propositional theorem provers from the efficiency and economy of storage point of view. $\mathbf{M}_{\rightarrow}$ carries almost all the proof-theoretical and logical information to produce polynomially bounded proofs in well-behaved [2] propositional logics. Focusing investigations on $\mathbf{M}_{\rightarrow}$ is worth of noticing.

There are many proof systems for $\mathbf{M}_{\rightarrow}$. The most well-known are structural/analytic proof systems. Well-known systems are the Sequent Calculus [4], Natural Deduction [4,14] and Tableaux [1,16] based. These systems, mainly the first and the third kind, are quite good in providing means to produce proofs automatically. The backward chaining procedure, for example, if applied to a Sequent Calculus based proof system provides an automatic way to produce proofs. The problem with these proof procedures is when a decision on which rule to apply has to be made and how to deal with non-provable formulas when it is the case. With respect to this feature of dealing with invalid formulas, the literature on both systems, Sequent Calculus and Tableaux, provides methods that either produce a proof or a counter-model uniformly in a unique proof-procedure. Since CoPSPACE=PSPACE, providing a counter-model in $\mathbf{M}_{\rightarrow}$ is so hard as to provide a proof. The size of the counter-model can be super-polynomial with respect to the formula. It is interesting to investigate how this is related to the size of proofs in $\mathbf{M}_{\rightarrow}$, or at least to have a concrete evidence that huge proofs may be the case. Most well-known huge proofs in the literature are considered inside Classical Logic. They are so in Classical as well as in Minimal logic. Our intention is not only show huge proofs in $\mathbf{M}_{\rightarrow}$. We could use the polynomial translations reported in [17] or [8] to generate a formula of the Pigeon-Hole principle from full Minimal Logic into $\mathbf{M}_{\rightarrow}$. We know, from [9], that this formula has only super-polynomially sized proofs in Resolution, and hence in cut-free Sequent Calculus and normal Natural Deduction. It is hard to detect from these translations why they are huge in $\mathbf{M}_{\rightarrow}$, since there is nothing specific to $\mathbf{M}_{\rightarrow}$. Focusing on $\mathbf{M}_{\rightarrow}$ is promising, since $\mathbf{M}_{\rightarrow}$ has less combinatorial alternatives, less logical constants, less alternative deductive system. The genesis of huge proofs in $\mathbf{M}_{\rightarrow}$ may shed some new light in propositional logic complexity. This is emphasized by the fact that the formulas shown here do not have huge proofs when considered Classical Reasoning. This article has the purpose of showing how the use of Classical Logic can improve the size of proofs obtained by an automatic proof procedure of the kind that is able to generate normal and cut-free derivations.

Developers of theorem provers have to be aware of many aspects of the logic in

[2] With sub-formula property

order to design an efficient system. Any information that can guide the designer is of some help. The number of copies of a formula in a proof can be a “bottleneck” for an efficient implementation. For saving memory an obvious solution would be the use of references instead of copies when representing proofs. The number of references is exponential, but references to formulas are smaller than formulas in most of the cases. This approach points out to the use of graphs (digraphs in fact) for representing proofs. There are a lot of developments done in this direction reported in the literature. Most of them are more semantically than implementation driven. Proof-nets [5] represents an approach that defends the use of graphs as the most adequate representation for proofs. We agree with that and we consider this a practical motivation for taking digraphs instead of trees for representing proofs [15]

It is worth to remark on an important relationship between the size of proofs in Hilbert systems and the size of proofs in Natural Deduction proofs as trees. A Hilbert system is formed by a set of axiom schemata and a set of inference rules. When we have inference rules with more than one premise, proofs may be represented as sequences or as trees. Basically, when dealing with trees a formula can appear more than once in the proof, if it is used more than once in it. When dealing with sequences, formulas are referenced instead of copied. An inference rule is applied by indicating reference to formulas already assumed in the proof. The naive mapping of sequences into trees may point us to an apparent grow on the size (number of formulas occurrences) in the proof. However, by means of a quite ingenuous mechanism, Krajicek[10] proved that, for every proof Π of α, in a Hilbert system for Classical Logic: $size(\Pi_{tree}) \leq poly(size(\Pi_{seq}))$, where $poly$ is a polynomial on one variable. As Natural Deduction can be seem as a Hilbert system with proofs represented as trees, Krajicek polynomial simulation of proofs as trees by proofs as sequences holds for Natural Deduction. The last thing to observed is that the rule of $\rightarrow$-introduction is nothing more than the deduction theorem in Hilbert system. Again, the deduction theorem can be proved in a way that the proof of the conclusion has a size no greater than the proof of the premise. Thus, we can base our discussion on trees in Natural Deduction and carry it to any Hilbert system preserving conclusions modulo polynomial simulation.

In section 4 we introduce the formulas φ_n, $0 \leq n$. In section 5 we show that they have exponentially sized normal proofs in the usual Natural Deduction for $\mathbf{M}_{\rightarrow}$. In the same section we show that this is a lower bound in $\mathbf{M}_{\rightarrow}$. In classical propositional logic, these formulas have linear-sized proofs as it is shown in section 4. Sections 2 and 3 remind us the basics of purely implicational minimal and classical logics, respectively.

All the formal propositional proofs/derivations in this article are presented in Prawitz-style Natural Deduction (ND). The size of these normal proofs/derivations is polynomially simulated by cut-free Sequent Calculus (SC) and/or Tableaux. Thus, the lower bound shown here also applies to them.

2 The purely implicational minimal logic

The (purely) implicational minimal logic $\mathbf{M}_{\rightarrow}$ is the fragment of minimal logic containing only the logical constant $\rightarrow$. Its semantics is the intuitionistic Kripke semantics restricted to $\rightarrow$ only. Given a propositional language $\mathcal{L}$, a $\mathbf{M}_{\rightarrow}$ model is a structure $\langle U, \preceq, \mathcal{V}\rangle$, where U is a non-empty set (worlds), $\preceq$ is a partial order relation on U and $\mathcal{V}$ is a function from U into the power set of $\mathcal{L}$, such that if $i, j \in U$ and $i \preceq j$ then $\mathcal{V}(i) \subseteq \mathcal{V}(j)$. Given a model, the satisfaction relationship $\models$ between worlds, in the model, and formulas is defined as:

- $\langle U, \preceq, \mathcal{V}\rangle \models_i p$, $p \in \mathcal{L}$, iff, $p \in \mathcal{V}(i)$
- $\langle U, \preceq, \mathcal{V}\rangle \models_i \alpha_1 \rightarrow \alpha_2$, iff, for every $j \in U$, such that $i \preceq j$, if $\langle U, \preceq, \mathcal{V}\rangle \models_j \alpha_1$ then $\langle U, \preceq, \mathcal{V}\rangle \models_j \alpha_2$.

Obs: In (full) minimal logic, $\perp$ has no special meaning, so there is no item declaring that $\langle U, \preceq, \mathcal{V}\rangle \not\models_i \perp$. We remind that $\mathbf{M}_{\rightarrow}$ does not have the $\perp$ in its language.

As usual a formula α is valid in a model $\mathcal{M}$, namely $\mathcal{M} \models \alpha$, if and only if, it is satisfiable in every world i of the model, namely $\forall i \in U \mathcal{M} \models_i \alpha$. A formula is a $\mathbf{M}_{\rightarrow}$ tautology, if and only if, it is valid in every model. A formula is satisfiable in $\mathbf{M}_{\rightarrow}$ if it is valid in a model $\mathcal{M}$ of $\mathbf{M}_{\rightarrow}$. The problem of knowing whether a formula is satisfiable or not is trivial in $\mathbf{M}_{\rightarrow}$. Every formula is satisfiable in the model $\langle \{\star\}, \preceq, \mathcal{V}\rangle$, where $\star$ is the only world, and $p \in \mathcal{V}(\star)$, for every p. Thus, SAT is not an interesting problem in $\mathbf{M}_{\rightarrow}$. The same cannot be told about knowing whether a formula is a $\mathbf{M}_{\rightarrow}$ tautology or not.

It is known that Prawitz Natural Deduction system for minimal logic with only the $\rightarrow$-rules ($\rightarrow$-Elim and $\rightarrow$-Intro below) is sound and complete for the $\mathbf{M}_{\rightarrow}$ Kripke semantics. As a consequence of this, Gentzen's LJ system [18] containing only right and left $\rightarrow$-rules is also sound and complete. As it is well-known one of these rules is not invertible[3]. A naive proof-procedure based on backward chaining for $\mathbf{M}_{\rightarrow}$, based only on this usual Gentzen sequent calculus is not possible. In the next section we present and discuss a main aspect of a Natural Deduction system for the purely implicational classical logic.

$$\dfrac{\begin{array}{c}[\alpha] \\ \vdots \\ \beta\end{array}}{\alpha \rightarrow \beta}\rightarrow\text{-Intro} \qquad \dfrac{\alpha \qquad \alpha \rightarrow \beta}{\beta}\rightarrow\text{-Elim}$$

3 Purely implicational classical logic

If we consider only the logical constant $\rightarrow$ we can distinguish the minimal provability from its classical counter-part. Peirce's formula for example, namely $((A \rightarrow B) \rightarrow A) \rightarrow A$, is not provable in minimal logic and it is provable in classical logic. In

[3] A rule is invertible, iff, whenever the premises are valid the conclusion is valid and whenever any premise is invalid the conclusion is also invalid

$$
\begin{prooftree}
\AxiomC{$[A]^a$}
\RightLabel{$\to$-I}
\UnaryInfC{$((A \to B) \to A) \to A$}
\AxiomC{$[(((A \to B) \to A) \to A) \to B]^c$}
\RightLabel{$\to$-E}
\BinaryInfC{B}
\RightLabel{$^a \to$-I}
\UnaryInfC{$A \to B$}
\AxiomC{$[((A \to B) \to A)]^b$}
\RightLabel{$\to$-E}
\BinaryInfC{A}
\RightLabel{$^b \to -I$}
\UnaryInfC{$((A \to B) \to A) \to A$}
\RightLabel{$^c P - rule$}
\UnaryInfC{$((A \to B) \to A) \to A$}
\end{prooftree}
$$

Figure 1. Proof of Peirce's formula using the P-rule in $\mathbf{K}_{\to}$

[12], it is discussed a Natural Deduction system for Purely implicational Classical logic ($\mathbf{K}_{\to}$) with normalization procedure and polynomial translation to $\mathbf{M}_{\to}$ on the basis of a *Glyvenko*-like theorem. In this section we summarize the main results in [12] that have to do with the examples discussed in this article.

The system presented in [12] is strongly based on Peirce's rule. In fact, to prove Peirce's formula it is enough to add the following rule (P-rule) to the Natural Deduction for $\mathbf{M}_{\to}$.

$$
\begin{array}{c}
[\alpha \to \beta] \\
| \\
\dfrac{\alpha}{\alpha}\ P\text{-rule}
\end{array}
$$

Using this rule, it is easy to derive Peirce's formula as it is shown in figure 1.

Since the P-rule is not neither an introduction rule, nor an elimination rule, it is specially considered. Permutation reduction, as Seldin's reduction for the $\perp$-classical rule in Natural Deduction, is taken as the main reduction step in obtaining a normal derivation from any derivation, as described in [12]. There a definition of a normal form, called P-normal form, is provided. This definition, shown below, uses the concept of branch in a derivation. A branch in a derivation Π is a sequence $\delta_0, \ldots, \delta_k$ of formula occurrences in Π, such that, δ_0 is a hypothesis, discharged or not. δ_k is a minor premise of an $\to$-E rule or the conclusion of Π and, for each $i = 0, \ldots, k-1$, δ_i is the major premise of an $\to$-E or the premise of an $\to$-introduction of a rule that has δ_{i+1} as conclusion.

Definition 3.1 A derivation Π in $\mathbf{K}_{\to}$ is in P-normal form, iff, for every branch in Π, there is no formula occurrence that is premise of an elimination rule and conclusion of an introduction rule, besides that, no P-rule conclusion in Π is premise of an $\to$-E or an $\to$-I application rule in this branch.

For example the derivation above of $((A \to B) \to A) \to A$ is a P-normal derivation. The reduction on derivations, called permutation here, shown in figure 2, ensures that any derivation Π of α from Γ in $\mathbf{K}_{\to}$ can be transformed in a derivation Π', of α from Γ, having each application of a P-rule in Π discharging a formula of the form $\beta \to A$, with A atomic. By iterated applications of the reduction in figure 2 we obtain atomic formulas as the right-hand sides of the implications discharged by any P-rule application.

A P-normal derivation/proof where each application of the P-rule discharges formulas of the form $\alpha \to A$, with A atomic, is said to be an atomically expanded

$$\dfrac{\begin{array}{c}[\beta_1 \to (\beta_2 \to \beta_3)]^a \\ \Pi \\ \beta_1\end{array}}{\beta_1}\,a \qquad \text{transforms into} \qquad \dfrac{\begin{array}{c}\dfrac{\dfrac{\dfrac{[\beta_1]^b \qquad [\beta_1 \to \beta_3]^a}{\beta_3}}{\beta_2 \to \beta_3}}{\beta_1 \to (\beta_2 \to \beta_3)}\,b \\ \Pi \\ \beta_1\end{array}}{\beta_1}\,a$$

Figure 2. Reducing the degree of the right-hand side of the discharged formula in a P-rule app

P-normal derivation/proof, also called an AEP-normal derivation/proof. In [12] it is shown the following theorem:

Theorem 3.2 *Every derivation* Π *of* α *from* $\Gamma = \{\gamma_1, \ldots, \gamma_k\}$ *in* $\mathbf{K}_\to$ *can be transformed into an AEP-normal derivation of* α *from* Γ *in* $\mathbf{K}_\to$ *.*

From the form of the branches in an AEP-normal derivation it is drawn the following statement, which is also called a Glyvenko theorem, because of its similarity with the original Glyvenko correspondence between provability in classical and in intuitionistic logic. See [6] and [13] for an updated and detailed presentation.

Theorem 3.3 *Let* α *be a purely implicational formula and* $\{p_1, \ldots, p_k\}$ *the set of propositional variables occurring in* α*. Thus,* $\vdash_{\mathbf{K}_\to} \alpha$*, if and only if,* $\vdash_{\mathbf{M}_\to} (\alpha \to p_1) \to ((\alpha \to p_2) \ldots ((\alpha \to p_n) \to \alpha) \ldots)$*.*

From the proof of the above theorem, in [12], we can conclude that:

Lemma 3.4 *Let* Π *be an AEP-normal proof of* α *in* $\mathbf{K}_\to$ *, such that, the size (number of formula occurrences) of* Π *is* s*, then the normal proof of* $(\alpha \to p_1) \to ((\alpha \to p_2) \ldots ((\alpha \to p_n) \to \alpha) \ldots)$ *in* $\mathbf{M}_\to$ *is bounded by* s^2

The above lemma says that normal proofs in $\mathbf{K}_\to$ are polynomially simulated in $\mathbf{M}_\to$.

Although $\mathbf{K}_\to$ proves Peirce law, it is not a complete classical system. What it lacks has to do with the intuitionistic negation. In order to have a complete system we have to add the intuitionistic absurdity rule [4]. This system we call $\mathbf{KI}_\to$. In this system we can define the negation $\neg\alpha$ as $\alpha \to \bot$.

$$\frac{\bot}{\beta}$$

There is a restricted form of the rule above, whenever we consider β atomic, that is, from $\bot$ infer B, with B atomic. This restriction is not essential. Using the following transformation repeatedly we transform any proof of α in $\mathbf{KI}_\to$ in a proof of α in $\mathbf{KI}_\to$ using the atomic version of ex-falso-sequitur-quolibet, instead of its general version. This reduction to the atomic applications only is due to Prawitz (see [14]).

[4] Also known by ex-falso-sequitur-quodlibet principle

$$\dfrac{\begin{array}{c}\Pi\\ \bot\end{array}}{\beta_1 \to \beta_2} \qquad \text{transforms into} \qquad \dfrac{\dfrac{\begin{array}{c}\Pi\\ \bot\end{array}}{\beta_2}}{\beta_1 \to \beta_2}\,\to\text{-I}$$

The system including the intuitionistic absurdity rule, instead of the general one, is also complete and sound for purely implicational classical logic [5] . The system with atomic intuitionistic absurdity rule is a good help understanding how polynomially simulate $\mathbf{KI}_{\to}$ in $\mathbf{K}_{\to}$. The following proposition is the basis of this polynomial simulation, since it deals with a polynomially bounded translation of formulas. This proposition is a variation on the translation that Ingebrigt Johansson define from intuitionistic logic into minimal logic.

Proposition 3.5 *Let α be a formula in the language $\{\to, \bot\}$, such that $\{p_1, \ldots, p_k\}$ is the set of propositional variables occurring in α. If $r \neq p_i$, for each i, and $\alpha^\star$ is the formula $(r \to p_1) \to ((r \to p_2) \ldots ((r \to p_n) \to \alpha) \ldots)$, then $\vdash_{\mathbf{KI}_{\to}} \alpha$, if and only if, $\vdash_{\mathbf{K}_{\to}} \alpha^\star$.*

The mentioned results imply that the existence of huge proofs in classical logic implies the existence of huge proofs in $\mathbf{M}_{\to}$. This article, by means of material exposed in the next sections, investigates how some these huge, so to say super-polynomially bounded, proofs are and how the use of classical reasoning can cut off in some cases this super-polynomial lower-bound.

4 Needing exponentially many assumptions

In [3] we can find a discussion on the fact that when proving theorems in a logic weaker than classical logic, the need of using an assumption more than once has a strong influence on how complex is the proof procedure and consequently the decision procedure for this logic. There, we can find the formula $((((A \to B) \to A) \to A) \to B) \to B$. Considering the proof systems of ND and CS mentioned in the previous section, this formula needs to use the assumption $((A \to B) \to A) \to A) \to B$ at least twice in order to be proved in $\mathbf{M}_{\to}$. Inspired by this example, we can define a class of formulas with no bounds on the use of assumptions. This shows that limiting the use of assumptions in an automatic proof-procedure for $\mathbf{M}_{\to}$ is not an alternative that ensures completeness. In the sequel we define the class of formulas. Below you find a normal proof of $((((A \to B) \to A) \to A) \to B) \to B$. Note that it cannot be proved with less than the use of 2 assumptions $(((A \to B) \to A) \to A) \to B$.

The following formula combines two instances of the formula mentioned above in order to have a formula that needs 4 times an assumption.

$$((((A \to \xi) \to A) \to A) \to \xi) \to C \tag{1}$$

where $\xi = (((D \to C) \to D) \to D) \to C$.

[5] Of course this system without Peirce's rule is sound and complete for purely implicational intuitionistic logic

In figure 4 we show a normal derivation of this formula 1 above. We can see that it has 4 assumptions of $((A \to \xi) \to A) \to A) \to \xi)$. They are from the two assumption occurrences in the derivation Σ shown in figure 3, that is used twice in the proof in figure 4

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[A]^1}{((A\to\xi)\to A)\to A} \qquad (((A\to\xi)\to A)\to A)\to\xi}{\xi}}{A\to\xi}\,1 \qquad [(A\to\xi)\to A]^2}{A}}{((A\to\xi)\to A)\to A}\,2 \qquad (((A\to\xi)\to A)\to A)\to\xi}{\xi}$$

Figure 3. The derivation Σ that is used in figure 4

We can see how to use this pattern such that if it is repeated n-times we define a formula φ_n, such that, any normal proof of φ_n has to use an assumption at least 2^n times, see section 5. Before we proceed with φ_n definition, we have to show that the need for repeating assumptions is not the case for classical propositional logic.

Consider now that the logic is the purely implicational *classical* logic, $\mathbf{K}_{\to}$, instead of the purely implicational minimal logic. Taking $\mathbf{K}_{\to}$ into account, we provide the proof of the formula 1 with only the use of one assumption, as shown in figure 5. This comes from the fact that $(((D \to C) \to D) \to D)$ is an instance of the implicational form of Peirce's rule, so it is provable. From this proof and $\xi = (((D \to C) \to D) \to D) \to C$ we prove C. ξ itself is provable by means of a proof of the Peirce's formula $((A \to \xi) \to A) \to A)$ and the $(((A \to \xi) \to A) \to A) \to \xi$ discharged to prove the desired formula. The purely implicational classical logic can be also seen in [7] where we can find a detailed presentation of the purely implicational classical logic with some proof-theoretic results in sequent calculus, instead of Natural Deduction, as in [12]. The use of classical logic can, in some cases, for example this case, turn proofs smaller.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[D]^3}{(((D\to C)\to D)\to D)} \qquad \begin{array}{c}[(((A\to\xi)\to A)\to A)\to\xi]^5\\ \Sigma\\ \xi\end{array}}{C}}{D\to C}\,3 \qquad [(D\to C)\to D]^4}{D}}{((D\to C)\to D)\to D}\,4 \qquad \begin{array}{c}[(((A\to\xi)\to A)\to A)\to\xi]^5\\ \Sigma\\ \xi\end{array}}{\dfrac{C}{((((A\to\xi)\to A)\to A)\to\xi)\to C}\,5}$$

Figure 4. Proof of the formula ξ_2 in purely implicational minimal logic

5 No bounds for occurrence assumptions in $\mathbf{M}_{\to}$

In this section we prove that for each n there is a formula φ_n, such that, any normal proof of φ_n has at least 2^n occurrence assumptions of the same formula, that are

$$\cfrac{\cfrac{\begin{matrix}\Pi_{Peirce2}\\((D\to C)\to D)\to D\end{matrix} \qquad \cfrac{\begin{matrix}\Pi_{Peirce1}\\((A\to\xi)\to A)\to A\end{matrix}\qquad [(((A\to\xi)\to A)\to A)\to\xi]^1}{\xi}}{C}}{((((A\to\xi)\to A)\to A)\to\xi)\to C}\;1$$

Figure 5. Proof of the formula ξ_2 in purely implicational *classical* logic

all of them discharged in only one introduction rule. The following proposition 5.4 shows that 2^n is an upper bound by showing the normal proof that uses 2^n assumptions for proving φ_n. Theorem 5.5 shows that there is no normal proof for any of the φ_n, in $\mathbf{M}_{\to}$, with less than 2^n assumptions discharged. In the sequel we define φ_n. As it was already said in section 4, φ_n arises from an iteration process derived from the previous examples.

Definition 5.1 Let $\chi[X,Y] = (((X \to Y) \to X) \to X) \to Y$. Using $\chi[X,Y]$ we define recursively a family of formulas. Consider the propositional letters C and D_i, $i > 0$. Let ξ_i, $i > 0$, be the formula:

$$\xi_1 = \chi[D_1, C] \tag{2}$$

$$\xi_{i+1} = \chi[D_{i+1}, \xi_i] \tag{3}$$

Using this family of formulas we define the formula φ_n, $n > 0$, such that, for any $i \geq 0$:

$$\varphi_{i+1} = \xi_{i+1} \to C$$

We can observe that $\varphi_1 = \xi_1 \to C$ can be proved by using proof Σ (shown in figure 3), replacing ξ by C and A by D_1, and applying an $\to$-introduction as the last rule. The obtained proof has 2 occurrence assumptions of the formula ξ_1. The proof of φ_2 is the proof shown in figure 4, replacing ξ by ξ_1, A by D_2 and D by D_1, resulting in the proof shown below.

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{[D_1]^3}{(((D_1\to C)\to D_1)\to D_1)} \qquad \begin{matrix}[(((D_2\to\xi_1)\to D_2)\\ \to D_2)\to\xi_1]^5\\ \Sigma\\ \xi_1\end{matrix}}{C}}{D_1\to C}\;3 \qquad [(D_1\to C)\to D_1]^4}{D_1}}{((D_1\to C)\to D_1)\to D_1}\;4 \qquad \begin{matrix}[(((D_2\to\xi_1)\to D_2)\\ \to D_2)\to\xi_1]^5\\ \Sigma\\ \xi_1\end{matrix}}{\cfrac{C}{((((D_2\to\xi_1)\to D_2)\to D_2)\to\xi_1)\to C}\;5}$$

The following lemma will be used in the proof of proposition 5.4.

Lemma 5.2 *In the formula ξ_i, $i > 0$, if we simultaneously replace C by ξ_1, and for each $k > 0$, D_k by D_{k+1}, the resulting formula is $\chi[D_{i+1}, \xi_i]$.*

Proof This lemma is proved by induction on i. For ξ_1 we observe that replacing C

by ξ_1 and D_1 by D_2 in ξ_1, the resulting formula is $\chi[D_2, \xi_1]$. Assuming that for $i > 0$, replacing C by ξ_1 and, for each $k = 1, \dots, i$, simultaneously replacing D_i by D_{i+1} in ξ_i, yields $\chi[D_{i+1}, \xi_i]$. Observing that $\xi_{i+1} = \chi[D_{i+1}, \xi_i]$ and by inductive hypothesis, simultaneous replacing C by ξ_1 and D_k by D_{k+1} in ξ_i, $k = 1, i$, yields ξ_{i+1}. As D_{i+1} does not occur in ξ_i, finally replacing D_{i+1} by D_{i+2} in $\xi_{i+1} = \chi[D_{i+1}, \xi_{i+1}]$ yields $\chi[D_{i+2}, \xi_{i+1}]$. This proves the inductive step. □ □

Another observation is that substitutions as the above shown in the lemma, if applied in a derivation Π in $\mathbf{M}_{\to}$, do imply that the resulting tree is a valid derivation too. This fact is justified by observing that the replacements are always on atomic formulas and the rules of $\mathbf{M}_{\to}$ do not have provisos to be unsatisfied as consequence of these replacements. Thus,we have the following fact.

Fact 5.3 *If Π is a derivation of α from $\gamma_1, \dots, \gamma_l$ and a substitution $\mathcal{S}$ (on atomic formulas) is applied to Π then $\mathcal{S}(\Pi)$ is a derivation of $\mathcal{S}(\alpha)$ from $\mathcal{S}(\gamma_1), \dots, \mathcal{S}(\gamma_l)$. Besides that, if Π is normal then $\mathcal{S}(\Pi)$ is normal too.*

Proposition 5.4 *For any $n > 0$, there is a normal proof of φ_n having 2^n occurrences of the same assumptions, that are discharged by the last rule of the proof.*

Proof The proof proceeds by induction. The basis $n = 1$ is the proof Σ shown in figure 3. This proof is inside proof in figure 6 also, occurying as a sub-derivation of $\Pi^\star$. Assuming that φ_i, $i > 0$ has a normal proof Π_{φ_i} having 2^i occurrences of ξ_i discharged by its last inference rule. Thus, we have a normal derivation Π of C from 2^i occurrences of ξ_i, remembering that $\varphi_i = \xi_i \to C$. We argue that if we simultaneously replace C by ξ_1, and for each $k = 1, \dots, i$, replace D_k by D_{k+1}, we will have, by lemma 5.2 and fact 5.3, a normal derivation of ξ_1 from 2^i occurrences of $\chi[D_{i+1}, \xi_i]$. Let us call this derivation $\Pi^\star$. The following derivation (see figure 6) is a derivation of C from $((((D_{i+1} \to \xi_i) \to D_{i+1}) \to D_{i+1}) \to \xi_i) \to C$, i.e., it is a derivation of C from ξ_{i+1}, and hence, by an $\to$-introduction application, we have a normal derivation of φ_{i+1} discharging $2^i + 2^i = 2^{i+1}$ assumptions of the formula ξ_{i+1}. □ □

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[D_1]^3}{(((D_1 \to C) \to D_1) \to D_1)} \quad \begin{matrix}[(((D_{i+1} \to \xi_i) \to D_{i+1}) \\ \to D_{i+1}) \to \xi_i]^5 \\ \Pi^\star \\ \xi_i\end{matrix}}{C}}{D_1 \to C}\,3 \quad [(D_1 \to C) \to D_1]^4}{D_1}}{((D_1 \to C) \to D_1) \to D_1}\,4 \quad \begin{matrix}[(((D_{i+1} \to \xi_i) \to D_{i+1}) \\ \to D_{i+1}) \to \xi_i]^5 \\ \Pi^\star \\ \xi_i\end{matrix}}{C}}{((((D_{i+1} \to \xi_i) \to D_{i+1}) \to D_{i+1}) \to \xi_i) \to C}\,5
$$

Figure 6. Proof of φ_{i+1} in $\mathbf{M}_{\to}$ with 2^{i+1} discharged assumptions of ξ_{i+1}

Theorem 5.5 shows that 2^i is the lower bound for number of assumption occurrences of a sole formula in any normal proof of φ_i in $\mathbf{M}_{\rightarrow}$.

Theorem 5.5 *Any normal proof of φ_i in $\mathbf{M}_{\rightarrow}$ has at least 2^i assumption occurrences of ξ_i.*

Proof We prove that for any i, there is no normal proof of φ_i with less than 2^i assumption occurrences of ξ_i. We first observe that φ_1, i.e., $((((D_1 \rightarrow C) \rightarrow D_1) \rightarrow D_1) \rightarrow C) \rightarrow C$ is not provable with only one occurrence of $\xi_1 = (((D_1 \rightarrow C) \rightarrow D_1) \rightarrow D_1) \rightarrow C)$. If this was the case we would have, from an analysis of the form of the normal proof of C from ξ_1, that $((D_1 \rightarrow C) \rightarrow D_1) \rightarrow D_1$ would be provable in $\mathbf{M}_{\rightarrow}$, and this cannot be the case since this formula is only classically valid. A Kripke model with two worlds such that in the first world neither C nor D_1 holds and in second D_1 holds but not C falsifies $(((D_1 \rightarrow C) \rightarrow D_1) \rightarrow D_1)$. That is, with

$$\mathcal{M} = \langle \{\star_1, \star_2\}, \{\star_1 \preceq \star_1, \star_1 \preceq \star_2, \star_2 \preceq \star_2\}, \{V(\star_1) = \emptyset, V(\star_2) = \{D_1\}\} \rangle$$

then $\mathcal{M} \not\models \alpha_{\star_i}(D_1 \rightarrow C)$, $i = 1, 2$, so, $\mathcal{M} \models \alpha_{\star_i}(D_1 \rightarrow C) \rightarrow D_1$, $i = 1, 2$. Thus, we hava that $\mathcal{M} \not\models \alpha_{\star_1}((D_1 \rightarrow C) \rightarrow D_1) \rightarrow D_1$.

Consider that there are normal proofs of φ_i with less than 2^i assumption occurrences of ξ_i. So there is the least k ($k > 0$), such that, φ_k has a normal proof with less than 2^k assumption occurrences of ξ_k. Let Σ_k be such proof. Since $\varphi_k = \xi_k \rightarrow C$, this proof is as follows. We remember that every open assumption in Σ_k has the form ξ_k.

$$\dfrac{\begin{matrix}[\xi_k]^l \\ \Sigma_k \\ C\end{matrix}}{\xi_k \rightarrow C}\, l$$

Since $\xi_k = \chi[D_k, \xi_{k-1}] = (((D_k \rightarrow \xi_{k-1}) \rightarrow D_k) \rightarrow D_k) \rightarrow \xi_{k-1}$, it has to be major premise of an $\rightarrow$-elim rule. If this is not the case then ξ_k would be a minor premise of a $\rightarrow$-elim rule having a major premise of the form $\xi_k \rightarrow \beta$. This formula on its turn has to be sub-formula of the open assumption of this branch, for the derivation is normal and $\xi_k \rightarrow \beta$ can only be conclusion of an application of an $\rightarrow$-elim rule. Since the only open assumption in Σ_k is ξ_k itself, the case of ξ_k as minor premise is not possible. Thus, as ξ_k is a major premise, Σ_k has the following form, remembering how is ξ_k, showed in the first line of this paragraph.

$$\dfrac{\dfrac{\begin{array}{c}\Sigma' \\ (((D_k \to \xi_{k-1}) \to D_k) \to D_k)\end{array} \qquad [(((D_k \to \xi_{k-1}) \to D_k) \to D_k) \to \xi_{k-1}]^l}{\begin{array}{c}\xi_{k-1} \\ \Sigma_k \\ C\end{array}}}{\xi_k \to C}\, l$$

Note that Σ' is a sub-derivation of Σ_k and it must have ξ_k as open assumption too. It must have an open assumption, for $(((D_k \to \xi_{k-1}) \to D_k) \to D_k)$ is not provable in $\mathbf{M}_{\to}$. As ξ_k is the only possible open formula in Σ_k, then Σ' has ξ_k at least one occurrence of ξ_k open in it. It is very important to note that each occurrence of ξ_k in Σ_k has a companion derivation of the form Σ' with ξ_k open in it. Thus, if we remove every Σ' from Σ_k we end up with the following proof:

$$\dfrac{\begin{array}{c}[\xi_{k-1}]^l \\ \Sigma_{k-1} \\ C\end{array}}{\xi_{k-1} \to C}\, l$$

The proof above is a proof of φ_{k-1} with less than 2^{k-1} assumption occurrences of ξ_{k-1} discharged by the last rule. This is a consequence of the fact that we have removed at least one assumption of ξ_k when removing Σ'. That is we have at least divided the amount of assumption occurrences of ξ_k by two. So, the resulting pruned derivation contradicts the fact that k is the least number holding this property, since it is a derivation of $\xi_{k-1} \to C$ with less than 2^{k-1}. $\square$ $\square$

We have proved that any normal proof of φ_n has at least 2^n assumption occurrences of ξ_n. The size of φ_n ($s(\varphi_n)$) is the length of the string representing it in an alphabet Λ with more than one symbol. Whatever is the size of φ_n, any normal proof of it has at least 2^n occurrences of a formula of size $s(\varphi_n) - 2$, since $s(\xi_n) + 2 = s(\varphi_n)$. Thus, we can affirm that the least size of any normal proof of φ_n is super-polynomially bounded when compared to the size of φ itself. Let Π_n be any normal proof of φ_n, then the ratio $\frac{s(\Pi_n)}{s(\varphi_n)}$ is:

$$\frac{s(\Pi_n)}{s(\varphi_n)} > \frac{s(\xi) \times 2^n}{(s(\xi) + 2)}$$

Let us now consider this fact to estimate the size of a normal proof of φ_n on the basis of the size of n. In order to simplify the evaluation, we consider that the length of a formula is the amount of occurrences of propositional letters in it. The real size is linearly proportional to what we call here as length, since for each propositional there is at most one $\to$ symbol in φ. Parenthesis will be ignored in this evaluation. By the later discussion we can see that $2 \times len(\varphi) \geq s(\varphi)$. The analysis will be accomplished using length (len) to measure the size of strings.

The form of φ_n is $\xi_n \to C$, the length of φ ($len(\varphi)$) is $1+len(\xi_n)$. ξ_n is defined in a recurrent way by $\chi[D_i, \xi_{i-1}]$, with $\xi_1 = ((D_1 \to C) \to D_1) \to D_1$. As $len(\xi_1) = 5$ and $len(\xi_{i+1}) = 2 \times len(\xi_i) + 3$, we can deduce[6] that $len(\xi_n) = 2^{n-1} \times (5+3) - 3$, and hence $len(\varphi_n) = 2^{n-1} \times (5+3) - 2$.

From the previous discussion, we found out that the formulas φ_n are of super-polynomial size on n. In fact, the strings that represent them are huge on n. However, the minimal amount of occurrences of ξ_n in any normal proof of φ_n is not less than 2^n, so we have that:

$$(2^n) \times (2^{n-1} \times (5+3) - 2) < len(\Pi_n)$$

for any normal proof Π_n of φ_n. Finally we have

$$\frac{(2^n) \times (2^{n-1} \times (5+3) - 2)}{(2^{n-1} \times (5+3) - 3)} < \frac{s(\Pi_n)}{s(\varphi_n)}$$

and hence there is $\kappa > 1$, such that $\frac{s(\Pi_n)}{s(\varphi_n)} = \kappa^{s(\varphi_n)}$.

6 Discussing the compression power of Classical Logic

Here we discuss the normal proofs of φ in $\mathbf{K}_{\to}$ and $\mathbf{KI}_{\to}$. We show that any normal proof of φ_n in $\mathbf{KI}_{\to}$ or $\mathbf{K}_{\to}$ is not super-polynomially bounded by the size of φ_n. The main reason for that is the fact that $\chi[D_k, \xi_{k-1}] = (((D_k \to \xi_{k-1}) \to D_k) \to D_k) \to \xi_{k-1}$ has a normal proof of size $k \times \eta \times s(\varphi_k)$, where η is a constant. As a matter of a clear presentation we show in figure 7 the proof in figure 5 adapted, and iterated, to our present discussion.

$$\dfrac{\begin{array}{c}\Pi_{k-1}\\ ((D_{k-1} \to \xi_{k-2}) \to D_{k-1}) \to D_{k-1}\end{array} \qquad \dfrac{\begin{array}{c}\Pi_k\\ ((D_k \to \xi_{k-1}) \to D_k) \to D_k\end{array} \qquad [(((D_k \to \xi_{k-1}) \to D_k) \to D_k) \to \xi_{k-1}]^1}{\xi_{k-1}}}{\xi_{k-2}}$$

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1\\ ((D_1 \to C) \to D_1) \to D_1\end{array} \qquad \begin{array}{c}\vdots\\ \xi_1\end{array}}{C}}{((((D_k \to \xi_{k-1}) \to D_k) \to D_k) \to \xi_{k-1}) \to C}\,1$$

Figure 7. Proof of φ_k in purely $\mathbf{KI}_{\to}$

Remembering that

$$\xi_1 = (((D_1 \to C) \to D_1) \to D_1) \to C$$

and that

$$\xi_{k-1} = (((D_{k-1} \to \xi_{k-2}) \to D_{k-1}) \to D_{k-1}) \to \xi_{k-2}$$

[6] Use your favorite method to solve recurrence equations

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[A]}{B\to A}}{(B\to A)\vee(A\to B)} \qquad [((B\to A)\vee(A\to B))\to B]}{B}}{A\to B}}{(B\to A)\vee(A\to B)} \qquad [((B\to A)\vee(A\to B))\to B]}{B}}{(((B\to A)\vee(A\to B))\to B)\to B}$$

Figure 8. Proof of Dummet's formula needs at least two repeated assumptions

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[A]}{A\vee\neg A} \qquad [(A\vee\neg A)\to\bot]}{\bot}}{\neg A}}{A\vee\neg A} \qquad [(A\vee\neg A)\to\bot]}{\bot}}{((A\vee\neg A)\to\bot)\to\bot}$$

Figure 9. Proof of *Tertium non-datur* formula needs at least two repeated assumptions

The proofs Π_i, $i = 1, k$, have all size $9 \times (s(\xi_i)) + 3)$. This can be checked out by an inspection in the proof in figure 1, making $A = D_i$ and $B = \xi_i$. We can note that $s(\xi_i) \leq s(\xi_k)$, $i = 1, k$, and hence the size of the whole proof is upper bounded by $k \times 9 \times (s(\xi_k)) + 3)$.

In this particular case $\mathbf{K}_{\to}$ saves space in a larger amount than $\mathbf{M}_{\to}$. We could think that this is a very particular situation. In fact this is not the case. Figures 9 and 8 are examples of proofs of classical tautologies that can be used to obtain similar classes of formulas with exponentially many assumptions need in normal proof. This time we have to use the full propositional minimal logic, that is, the minimal logic with the other logical constants $\{\wedge, \vee, \neg, \bot\}$, the same regarding its classical counterpart. Thus, the formulas proved in these figures can be used to provide other examples of the compressing power obtained by the use of Classical reasoning. We will work out this conjecture on a forthcoming article.

We can generalize the situation discussed here. Let α be such that $\nvdash_{\mathbf{M}_{\to}} \alpha$ and there are β and γ, such that, $\alpha \vdash_{\mathbf{M}_{\to}} \beta$ and $\gamma, \beta \vdash_{\mathbf{M}_{\to}} \alpha$. We can conclude that $\vdash_{\mathbf{KI}_{\to}} \alpha$, as shown in the right derivation below. Besides that, in the case that the left derivation has exponentially many assumptions of $\alpha \to \beta$, we conjecture that by a similar reasoning applied in the case of the class of formulas φ_n we can use $\mathbf{KI}_{\to}$ to have a proof of $(\alpha \to \beta) \to \beta$ of polynomial size.

$$\dfrac{\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}[\gamma]\\ \vert\\ \alpha\end{array} \quad [\alpha\to\beta]}{\beta}\\ \vert \\ \beta'\end{array}}{\gamma\to\beta'}\\ \vert\\ \alpha\end{array} \quad [\alpha\to\beta]}{\beta}}{((\alpha\to\beta)\to\beta)} \qquad \dfrac{\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}\dfrac{\dfrac{[\gamma] \quad \dfrac{\dfrac{\begin{array}{c}[\gamma]\\ \vert\\ \alpha\end{array} \quad \neg\alpha}{\bot}}{\neg\gamma}}{\bot}}{\beta}\\ \vert\\ \beta'\end{array}}{\gamma\to\beta'}\\ \vert\\ \alpha\end{array} \quad \neg\alpha}{\bot}}{\alpha}$$

7 Conclusion

Taking into account that $\mathbf{M}_{\to}$ is the hardest and most representative propositional logic to define efficient proof-procedures, we show an example alerting for the fact that allowing unlimited use of assumptions is worth for any complete proof-procedure. This example runs in $\mathbf{M}_{\to}$. We are not aware of a similar one running in classical logic. Classical propositional logic is more efficient than $\mathbf{M}_{\to}$ if such example does not exist. Propositional logic complexity has a lot of conjectures, starting with the relations between the main complexity classes. This article has the sole purpose of providing an example where the exponential grow of proofs has nothing to do with disjunction and combinatorial principles like the Pigeon-Hole [7]. The class of formulas φ_n and other obtained in a similar way from classical tautologies are such examples.

8 Acknowledgments

The author would like to thank prof. Gilles Dowek for hearing and reading the initial ideas presented here and providing very good suggestions. We thank Jefferson dos Santos for the suggestions on improving the text.

References

[1] E.W. Beth. *Semantic Entailment and Formal Derivability*. Mededelingen der Koninklijke Nederlandse Akademie van Wetenschappen: Afd. Letterkunde. Noord-Hollandsche Uitgevers Maatschappij, 1961.

[2] Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, STOC '71, pages 151–158, New York, NY, USA, 1971. ACM. http://doi.acm.org/10.1145/800157.805047.

[3] Gilles Dowek and Ying Jiang. Eigenvariables, bracketing and the decidability of positive minimal predicate logic. *Theoretical Computer Science*, 360(13):193 – 208, 2006. http://www.sciencedirect.com/science/article/pii/S030439750600257X.

[7] The pigeon-hole principle was used to provide a super-polynomial lower bound for Robinson's (propositional) Resolution

[4] G. Gentzen. Untersuchungen ber das logische schlieen i. *Mathematische Zeitschrift*, 39:176–210, 1935. See english version in [?], original version online in http://eudml.org/doc/168546.

[5] Jean-Yves Girard. Proof-nets: The parallel syntax for proof-theory. In P. Agliano and A. Ursini, editors, *Logic and Algebra*. Marcel Dekker, New York, 1996.

[6] V. I. Glivenko. Sur quelques points de la logique de m. brouwer. *Bull. Soc. Math. Belg.*, 15:183–185, 1929.

[7] L. Gordeev. On cut elimination in the presence of peirce rule. *Archiv fr mathematische Logik und Grundlagenforschung*, 26:147–164, 1987.

[8] Edward Hermann Haeusler. Propositional logics complexity and the sub-formula property. *CoRR*, cs/1401.8209v1, 2014. Also proceedings of DCM2014 workshop, Vienna Summer of Logic 2014, Vienna, july/2014, and http://arxiv.org/cs/1401.8209v1.

[9] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39(2–3):297–308, 1985.

[10] Jan Krajıček. Lower bounds to the size of constant-depth propositional proofs. *Journal of Symbolic Logic*, 59(1):73–86, 1994.

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

[12] Luiz Carlos Pereira, Edward Hermann Haeusler, Vaston G. Costa, and Wagner Sanz. A new normalization strategy for the implicational fragment of classical propositional logic. *Studia Logica*, 96(1):95–108, 2010.

[13] Luiz Carlos Pereira, Edward Hermann Haeusler, and Maria da Paz N. de Medeiros. Some results on fragments of propositional logic with classical negation. *O Que Nos Faz Pensar*, 23:105–111, 2008. http://www.oquenosfazpensar.com/adm/uploads/artigo/alguns_resultados_sobre_fragmentos_com_negacao_da_logica_classica/23_Alguns_resultados_sobre_fragmentos.pdf.

[14] D. Prawitz. *Natural deduction: a proof-theoretical study*. PhD thesis, Almqvist & Wiksell, 1965.

[15] Marcela Quispe-Cruz, Edward Hermann Haeusler, and Lew Gordeev. Proof-graphs for minimal implicational logic. In Proceedings 2013 International Workshop on *Developments in Computational Models*, volume 144 of *EPTCS*, pages 16–29, 2014.

[16] R. M. Smullyan. *First–Order Logic*. Springer-Verlag, New York, 1968.

[17] Richard Statman. Intuitionistic propositional logic is polynomial-space complete. *Theoretical Computer Science*, 9(1):67 – 72, 1979.

[18] G. Takeuti. *Proof Theory*. Studies in logic and the foundations of mathematics. North-Holland, 1987.