# Proof complexity of intuitionistic implicational formulas

Emil Jeřábek

Institute of Mathematics of the Czech Academy of Sciences
Žitná 25, 115 67 Praha 1, Czech Republic, email: jerabek@math.cas.cz

September 5, 2016

**Abstract**

We study implicational formulas in the context of proof complexity of intuitionistic propositional logic (**IPC**). On the one hand, we give an efficient transformation of tautologies to implicational tautologies that preserves the lengths of intuitionistic extended Frege (*EF*) or substitution Frege (*SF*) proofs up to a polynomial. On the other hand, *EF* proofs in the implicational fragment of **IPC** polynomially simulate full intuitionistic logic for implicational tautologies. The results also apply to other fragments of other superintuitionistic logics under certain conditions.

In particular, the exponential lower bounds on the length of intuitionistic *EF* proofs by Hrubeš [9], generalized to exponential separation between *EF* and *SF* systems in superintuitionistic logics of unbounded branching by Jeřábek [12], can be realized by implicational tautologies.

**Keywords:** proof complexity, intuitionistic logic, implicational fragment

**MSC:** 03F20, 03B55

## 1 Introduction

A major open problem in proof complexity is to show superpolynomial lower bounds on the lengths of proofs in Frege systems for classical propositional logic, or even stronger systems such as extended Frege. It turns out such lower bounds are easier to obtain for some non-classical logics: Hrubeš proved exponential lower bounds on the length of *EF* proofs[1] for certain modal logics and for intuitionistic logic [8, 9, 10]. Jeřábek [12] improved these results to an exponential separation between *EF* and *SF* systems for all superintuitionistic (and transitive modal) logics of unbounded branching. See also [3, 4] for earlier work on the proof complexity of intuitionistic logic, including conditional lower bounds.

Known lower bounds on proof systems for non-classical logics crucially rely on variants of the feasible disjunction property, serving a similar role as feasible interpolation does in weak proof systems for classical logic (cf. [15]). Consequently, the lower bounds are proved for tautologies that involve disjunction in an essential way, and one might get the impression

[1]The results are formulated in [8, 9, 10] as lower bounds on the number of lines in Frege proofs, however, this is essentially the same measure as the length of extended Frege proofs.

that this is unavoidable—perhaps the implicational fragment of **IPC**, or other disjunction-free fragments, behave differently from the full logic.

The purpose of this paper is to show that this dependence on disjunctions is just an artifact of the proofs: the implicational fragment of intuitionistic logic is, after all, essentially equivalent to the full logic with respect to the lengths of proofs. We will demonstrate this by means of two kinds of results: first, *tautologies* can be brought into a form avoiding unwanted connectives (such as disjunction) while preserving their hardness for intuitionistic extended Frege and related systems; second, unwanted connectives can be eliminated from intuitionistic extended Frege *proofs* except for subformulas of the tautology being proved. We include several results of both kinds with varying assumptions.

Elimination results of the first kind are the topic of Section 3. On the one hand, in Theorem 3.6 we present a method that makes tautologies *mostly* implicational with certain disjunctions and $\perp$ left, and preserves (up to a polynomial) the size of $F$, $EF$, and $SF$ proofs in *arbitrary* superintuitionistic logics; in particular, the tautologies with exponential $EF$ lower bounds from [9, 12] can be made purely implicational in this way. On the other hand, in Theorems 3.8 and 3.9 we show how to eliminate *all* disjunctions (and/or $\perp$) from tautologies while preserving the lengths of $EF$ and $SF$ proofs in logics whose proper axioms do not contain disjunctions ($\perp$, respectively).

Elimination results of the second kind come in Section 4. In Theorem 4.3, we show that if the proper axioms of a logic $L$ do not contain disjunction (or $\perp$), we can efficiently eliminate disjunctions ($\perp$, resp.) from $L$-$EF$ proofs, except for those that appear in the final tautology. However, the argument may introduce conjunctions, and we address this in subsequent results: in Corollary 4.15 and Theorem 4.17, we show how to eliminate conjunctions from $EF$-proofs under some conditions on the logic and its axiom system; in Theorem 4.5, we show how to eliminate $\perp$ from proofs without introducing $\wedge$ or other connectives, again under certain conditions on the logic. We also develop a monotone version of the negative translation (Proposition 4.19), which we use in an ad hoc argument that the above-mentioned implicational versions of the tautologies used in [12] to separate $EF$ and $SF$ have short implicational **IPC**-$SF$ proofs (Theorem 4.22).

A few concluding remarks and open problems are mentioned in Section 5.

In order to show the limitations of our methods, the appendices include some negative results that may be of independent interest. Proposition A.5, originally due to Wroński [18], shows that in general, the implicational fragment of a superintuitionistic logic $L = \mathbf{IPC} + \Phi$ with $\Phi$ an implicational axiom may not be axiomatized by $\Phi$ over the implicational fragment of **IPC**, and similarly for other combinations where the target fragment omits conjunction. Appendix B presents certain exponential lower bounds on the size of formulas in fragments of intuitionistic logic, and a linear lower bound on implication nesting depth.

## 2 Preliminaries

We refer to Chagrov and Zakharyaschev [5] and Krajíček [14] for general information on superintuitionistic logics and classical Frege systems and their extensions, respectively. For

Frege and friends in superintuitionistic logics, we will use the notation and basic results from Jeřábek [12]; we include more details below, as we need to generalize the set-up to fragments (e.g., implicational) of si logics, which were not treated in [12].

If $L$ is a language[2], a *proof system for* $L$ is a polynomial-time computable function $P(x)$ whose range is $L$. If $P(x) = y$, the string $x$ is called a $P$*-proof* of $y$. A proof system $P$ *polynomially-simulates* or *p-simulates* a proof system $Q$, denoted $Q \leq_p P$, if there is a poly-time function $f$ such that $Q(x) = P(f(x))$ for all proofs $x$. Proof systems $P$ and $Q$ are *p-equivalent*, written $P \equiv_p Q$, if $P \leq_p Q \leq_p P$.

A *propositional language* is a set $C$ of connectives, each given a finite arity. (That is, formally, a language is a mapping $ar\colon C \to \omega$.) Let $\mathrm{Form}_C$ denote the set of $C$*-formulas*, built from propositional variables $p_i$, $i \in \omega$, using connectives from $C$. We will also denote variables by other lowercase Latin letters for convenience, and we will denote formulas by lowercase Greek letters. We write $\psi \subseteq \varphi$ if $\psi$ is a subformula of $\varphi$. A *substitution* is a mapping of variables to formulas, uniquely extended to a homomorphism $\mathrm{Form}_C \to \mathrm{Form}_C$. A *propositional logic* is a pair $L = \langle C, \vdash_L \rangle$, where $C$ is a propositional language, and $\vdash_L$ is a structural Tarski-style consequence relation: i.e., a relation $\vdash_L \subseteq \mathcal{P}(\mathrm{Form}_C) \times \mathrm{Form}_C$ satisfying

(i) $\varphi \in \Gamma$ implies $\Gamma \vdash_L \varphi$;

(ii) if $\Delta \vdash_L \varphi$, and $\Gamma \vdash_L \psi$ for all $\psi \in \Delta$, then $\Gamma \vdash_L \varphi$;

(iii) $\Gamma \vdash_L \varphi$ implies $\sigma(\Gamma) \vdash_L \sigma(\varphi)$

for all formulas $\varphi$, sets of formulas $\Gamma$, $\Delta$, and substitutions $\sigma$. We will only be interested in *finitary* logics, meaning $\Gamma \vdash_L \varphi$ implies $\Gamma_0 \vdash_L \varphi$ for some finite $\Gamma_0 \subseteq \Gamma$.

If $L$ is a logic in a finite (or computable) language $C$, a *proof system for* $L$ is a proof system (in the sense given above) for the set $\{\varphi : \ \vdash_L \varphi\}$ of $L$*-tautologies*; a *derivation system for* $L$ is a proof system for its finitary consequence relation $\{\langle \varphi_0, \varphi_1, \dots, \varphi_n \rangle : \varphi_1, \dots, \varphi_n \vdash_L \varphi_0\}$.

Let $L = \langle C, \vdash_L \rangle$ be a logic. An *extension* of $L$ is a logic $L' = \langle C', \vdash_{L'} \rangle$ such that $C \subseteq C'$ and $\vdash_L \subseteq \vdash_{L'}$; we will write $L \subseteq L'$. An extension is *simple* if $C = C'$. If $X$ is a set of $C$-formulas, then $L + X$ is the least extension of $L$ such that $\vdash_{L+X} \varphi$ for all $\varphi \in X$. Logics of the form $L + X$ are called *axiomatic extensions* of $L$. For any $C' \subseteq C$, the $C'$*-fragment of* $L$, denoted $L_{C'}$, is the logic $\langle C', \vdash_L \cap (\mathcal{P}(\mathrm{Form}_{C'}) \times \mathrm{Form}_{C'}) \rangle$.

Fix a language $C$. A *Frege rule* is an object of the form

$$\frac{\alpha_1, \dots, \alpha_k}{\alpha_0}, \qquad \text{also written as} \quad \alpha_1, \dots, \alpha_k \mathbin{/} \alpha_0,$$

where $\alpha_0, \dots, \alpha_k$ are formulas. Rules with $k = 0$ can be identified with formulas, and are called *axioms*. If $L$ is a logic, a rule $\alpha_1, \dots, \alpha_k \mathbin{/} \alpha_0$ is $L$*-derivable* if $\alpha_1, \dots, \alpha_k \vdash_L \alpha_0$.

If $R$ is a set of Frege rules, an $R$*-derivation* of $\varphi$ from $\Gamma \subseteq \mathrm{Form}_C$ is a sequence of formulas $\varphi_1, \dots, \varphi_m$, where $\varphi_m = \varphi$, and each $\varphi_i$ is an element of $\Gamma$, or is derived from some of the

[2] In the sense of the theory of computation, i.e., an arbitrary set of strings over a finite alphabet.

formulas $\varphi_1, \dots, \varphi_{i-1}$ by a substitution instance of a rule from $R$. An *$R$-proof* of $\varphi$ is its $R$-derivation from $\Gamma = \varnothing$. If $L$ is a logic such that

$$\Gamma \vdash_L \varphi \quad \text{iff} \quad \varphi \text{ has an } R\text{-derivation from } \Gamma$$

for all $\Gamma \cup \{\varphi\} \subseteq \mathrm{Form}_C$, we say that $R$ is an *axiomatization* of $L$; if $R$ is furthermore finite, we call the $R$-derivation system a *Frege system for $L$*, and denote it *$L$-$F$*. This notation is justified by the next observation:

**Lemma 2.1** *Substitution instances of a fixed $L$-derivable rule have linear-time constructible proofs in any $L$-$F$ system. Consequently, all Frege systems for $L$ are p-equivalent.* □

Notice that our definition is more strict than the one employed in [16, 11], which only requires Frege systems to respect the tautologies of the logic rather than its consequence relation.

The formulas $\varphi_i$ in a Frege derivation $\varphi_1, \dots, \varphi_m$ are called *lines*; thus, the number of lines in the derivation is $m$, whereas its *size* or *length* is its total size when written out as a string in a fixed finite alphabet, i.e., essentially $\sum_i |\varphi_i|$.

The logics we will work with in this paper are extensions of intuitionistic logic (denoted **IPC**) and their fragments. We formulate **IPC** in the language $C_{\mathbf{IPC}} = \{\to, \wedge, \vee, \bot\}$. We define $\neg\varphi = (\varphi \to \bot)$ as an abbreviation. Conversely, $\bot$ is equivalent to $\neg(p \to p)$; since implication will always be present in our fragments, we could equally well formulate all results using $\neg$ instead of $\bot$ as a basic connective, but we feel $\bot$ is more convenient. We can also define $\top$ as $\bot \to \bot$ or $p \to p$, and $(\varphi \leftrightarrow \psi) = (\varphi \to \psi) \wedge (\psi \to \varphi)$. We will call $\{\to\}$-formulas *implicational* (or *purely implicational* for emphasis), $\{\to, \wedge, \vee\}$-formulas *positive*, $\{\wedge, \vee, \bot, \top\}$-formulas *monotone*, and $\{\wedge, \vee\}$-formulas *strict monotone*. (Every monotone formula is equivalent to $\bot$, $\top$, or to a strict monotone formula.)

In order not to get overwhelmed by brackets, we employ the notational conventions that the outermost bracket can be omitted, $\wedge$ and $\vee$ bind more strongly than $\to$, and $\to$ is right-associative, so that e.g.,

$$\varphi_0 \to \cdots \to \varphi_{n-1} \to \psi \wedge \chi = (\varphi_0 \to (\cdots \to (\varphi_{n-1} \to (\psi \wedge \chi)) \cdots)).$$

If $\Gamma = \langle \varphi_i : i < n \rangle$ is a sequence of formulas, we will write

$$\Gamma \to \varphi = \varphi_0 \to \cdots \to \varphi_{n-1} \to \varphi,$$

understood as just $\varphi$ if $n = 0$. Any formula $\varphi$ can be uniquely written in the form $\Gamma \to \xi$, where $\Gamma$ is a sequence of formulas, and $\xi$ is not an implication. We will call $\xi$ the *head* of $\varphi$, and write $H(\varphi) = \xi$.

We can axiomatize **IPC** by the rule of modus ponens

$$\alpha, \alpha \to \beta \;/\; \beta, \tag{1}$$

and the axioms

$$(\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma, \tag{2}$$
$$\alpha \to \beta \to \alpha, \tag{3}$$
$$\alpha \wedge \beta \to \alpha, \tag{4}$$
$$\alpha \wedge \beta \to \beta, \tag{5}$$
$$\alpha \to \beta \to \alpha \wedge \beta, \tag{6}$$
$$\alpha \to \alpha \vee \beta, \tag{7}$$
$$\beta \to \alpha \vee \beta, \tag{8}$$
$$\alpha \vee \beta \to (\alpha \to \gamma) \to (\beta \to \gamma) \to \gamma, \tag{9}$$
$$\bot \to \gamma. \tag{10}$$

The Frege system for **IPC** based on the rules (1)–(10) will be called the *standard* **IPC**-$F$ system.

*Superintuitionistic (si)* logics are axiomatic extensions of **IPC**. The largest consistent si logic is classical logic, which we will denote **CPC**. Only finitely axiomatizable logics have Frege systems, hence unless stated otherwise, we will tacitly assume that all logics mentioned are finitely axiomatizable.

We will rarely need to use Kripke semantics for si logics, as most of our arguments are purely syntactic; we refer the reader to [5, 12].

Apart from si logics themselves, we will be interested in proof systems for fragments $L_C$, where $L$ is a si logic, and $\to\, \in C \subseteq C_{\mathbf{IPC}}$. (We warn the reader that fragments of finitely axiomatized logics are not necessarily finitely axiomatizable, and axiomatic extensions of $\mathbf{IPC}_C$ are not necessarily fragments of si logics.) Notice that if finitely axiomatizable, $L_C$ can be axiomatized by a single formula over $\mathbf{IPC}_C$: in particular, $\mathbf{IPC}_C + \{\varphi_1, \dots, \varphi_k\}$ can be axiomatized by

$$(\varphi_1 \to \dots \to \varphi_k \to p) \to p,$$

where $p$ is a variable not occurring in $\varphi_1, \dots, \varphi_k$. It is well known (see e.g. [7], using a slightly different calculus) that the standard axiom system for **IPC** above has the property of *separation of connectives* for fragments that include implication: $\mathbf{IPC}_C$ is axiomatizable by modus ponens and those axioms among (2)–(10) that only use connectives from $C$. Thus, an $L_C$-$F$ system axiomatized by (1), the $C$-axioms among (2)–(10), and one other $C$-formula (called the *proper axiom* of the given axiom system) will be called a *standard Frege system for $L_C$*.

We mention that si logics split in four types according to which connectives need to appear in their proper axioms. First, no consistent proper extension of **IPC** can be axiomatized by monotone formulas, hence $\to$ is (nearly) always required. On the other hand, conjunction is never needed:

**Lemma 2.2** *Let $C \subseteq \{\to, \vee, \bot\}$. Every $(C \cup \{\wedge\})$-formula is in* **IPC** *equivalent to a conjunction of $C$-formulas.*

*Proof:* By induction on the complexity of the formula, using

$$\Big(\bigwedge_{i<n} \varphi_i\Big) \vee \Big(\bigwedge_{j<m} \psi_j\Big) \leftrightarrow \bigwedge_{\substack{i<n \\ j<m}} (\varphi_i \vee \psi_j), \tag{11}$$

$$\Big(\bigwedge_{i<n} \varphi_i \to \bigwedge_{j<m} \psi_j\Big) \leftrightarrow \bigwedge_{j<m} (\varphi_0 \to \cdots \to \varphi_{n-1} \to \psi_j). \tag{12}$$

□

Thus, the only question is whether axioms of $L$ need to use $\vee$ and/or $\bot$, and this can be characterized semantically (see [5] for a detailed explanation): $L$ can be axiomatized by $\{\to, \vee\}$-formulas (or: by positive formulas) iff the class of $L$-frames is closed under so-called dense subframes (cf. [5, §9.1]); $L$ is axiomatizable by $\{\to, \bot\}$-formulas (or: by $\vee$-free formulas) iff it is a *cofinal-subframe logic* (cf. [5, §11.3]); and $L$ is axiomatizable by $\to$-formulas (or: by positive $\vee$-free formulas) iff it is a *subframe logic* iff it is both positively axiomatizable and cofinal-subframe.

For any Frege system $L$-$F$, we will also consider several associated stronger systems based on the same set of Frege rules. The *extended Frege* system $L$-$EF$ is defined as follows: an $L$-$EF$ derivation of $\varphi$ from a finite set $\Gamma$ is an $L$-$F$ derivation of $\varphi$ from $\Gamma \cup E$, where $E = \{E_1, \dots, E_r\}$ is a list of *extension axioms*: each $E_i$ is a pair of implications[3]

$$q_i \to \psi_i, \qquad \psi_i \to q_i,$$

where the *extension variables* $q_i$ are distinct, and $q_i$ does not occur in $\{\psi_j : j \le i\} \cup \{\varphi\} \cup \Gamma$. Alternatively, the *circuit Frege* system $L$-$CF$ is defined similarly to Frege, except that lines in derivations can be represented by circuits rather than just formulas. In the *substitution Frege* system $L$-$SF$, substitution can be used as a rule of inference along with Frege rules. Unlike the other systems, $L$-$SF$ only makes sense as a proof system, not as a derivation system. If $P$ is any of the sequence-like (dag-like) proof systems we introduced, $P^*$ denotes its tree-like version.

Lemma 2.1 also applies to $L$-$EF$, $L$-$CF$, and $L$-$SF$, but the case of tree-like systems is more complicated (see [12, §3.1]).

Before embarking on the basic properties of these systems, let us mention a technical lemma that allows us to work with chained implications $\Gamma \to \varphi$ with more ease. It is reasonably clear that the formulas below have short **IPC**-$F$ proofs, but it may be less obvious how to derive them shortly in the implicational fragment $\mathbf{IPC}_\to$ without the use of conjunctions.

**Lemma 2.3**

(i) *Given $\Gamma$, $\Delta$, and $\varphi$ such that every formula in $\Gamma$ appears in $\Delta$, we can construct in polynomial time an $\mathbf{IPC}_\to$-$F$ proof of*

$$(\Gamma \to \varphi) \to (\Delta \to \varphi).$$

[3] This formulation of $EF$ is tailored to fragments of si logics. In general, we can reasonably define $EF$ for (finitary, finitely axiomatized) logics that are *finitely equivalential* in the sense of abstract algebraic logic, where the set of equivalence formulas will play the role of $\{x \to y, y \to x\}$ in extension axioms.

(ii) *Given* $\Gamma$, $\varphi$, *and* $\Delta = \langle \psi_i : i < n \rangle$, *we can construct in polynomial time an* $\mathbf{IPC}_{\to}$*-F proof of*

$$(\Delta \to \varphi) \to (\Gamma \to \psi_0) \to \cdots \to (\Gamma \to \psi_{n-1}) \to (\Gamma \to \varphi).$$

*Proof:* Instances of

$$(\psi \to \varphi) \to (\gamma \to \psi) \to (\gamma \to \varphi) \tag{13}$$

have short $\mathbf{IPC}_{\to}$-$F$ proofs by Lemma 2.1. By chaining $|\Gamma|$ of them, we can construct short proofs of

$$(\psi \to \varphi) \to (\Gamma \to \psi) \to (\Gamma \to \varphi). \tag{14}$$

(This is in fact the special case of (ii) with $n = 1$.)

(i): It is easy to see that we can derive each such formula as a composition of polynomially many instances of weakening, exchange, and contraction:

$$(\Gamma \to \Pi \to \varphi) \to (\Gamma \to \alpha \to \Pi \to \varphi), \tag{15}$$
$$(\Gamma \to \alpha \to \beta \to \Pi \to \varphi) \to (\Gamma \to \beta \to \alpha \to \Pi \to \varphi), \tag{16}$$
$$(\Gamma \to \alpha \to \alpha \to \Pi \to \varphi) \to (\Gamma \to \alpha \to \Pi \to \varphi), \tag{17}$$

it thus suffices to prove (15)–(17). By replacing $\varphi$ with $\Pi \to \varphi$, we can assume $\Pi = \varnothing$; using (14), we can also assume $\Gamma = \varnothing$. Then (15)–(17) are instances of constant-size $\mathbf{IPC}_{\to}$ tautologies, hence they have short $\mathbf{IPC}_{\to}$-$F$ proofs by Lemma 2.1.

(ii): By induction on $n$. For $n = 0$, (ii) reduces to $\varphi \to \Gamma \to \varphi$, which is an instance of (i). For the induction step, let $\Delta = \langle \psi_0, \dots, \psi_n \rangle$, and put $\Delta' = \langle \psi_1, \dots, \psi_n \rangle$, and

$$\xi = (\Gamma \to \psi_1) \to \cdots \to (\Gamma \to \psi_n) \to \Gamma \to \varphi.$$

By the induction hypothesis, we have an $\mathbf{IPC}_{\to}$-$F$ proof of

$$(\Delta' \to \varphi) \to \xi.$$

Using (13), we infer

$$(\psi_0 \to \Delta' \to \varphi) \to (\psi_0 \to \xi),$$

and using (14), we obtain

$$(\psi_0 \to \Delta' \to \varphi) \to (\Gamma \to \psi_0) \to \Gamma \to \xi,$$

that is,

$$(\Delta \to \varphi) \to (\Gamma \to \psi_0) \to \Gamma \to (\Gamma \to \psi_1) \to \cdots \to (\Gamma \to \psi_n) \to \Gamma \to \varphi.$$

We conclude

$$(\Delta \to \varphi) \to (\Gamma \to \psi_0) \to (\Gamma \to \psi_1) \to \cdots \to (\Gamma \to \psi_n) \to \Gamma \to \varphi$$

using (i). □

As a consequence of (i), we can extend the notation $\Gamma \to \varphi$ to *sets* $\Gamma$ instead of sequences, as the ordering of the formulas does not make a significant difference. A particular special case of (ii) is when $\vdash \Delta \to \varphi$; for example, we can construct in poly-time $\mathbf{IPC}_{\to}$-$F$ proofs of

$$(\Gamma \to \varphi) \to (\Gamma \to \varphi \to \psi) \to \Gamma \to \psi.$$

Until the end of this section, let $L$ be an si logic, and $C \subseteq C_{\mathbf{IPC}}$ a set of connectives such that $\to \in C$. Armed with Lemma 2.3, we can prove the *feasible deduction theorem* (cf. [12, Prop. 3.6]) using the standard argument by induction on the length of the derivation:

**Proposition 2.4** *Let $P$ denote $L_C$-F, $L_C$-CF, or $L_C$-EF. Given a $P$-derivation of a formula $\varphi$ from a set $\Gamma$, we can construct in polynomial time a $P$-proof of $\Gamma \to \varphi$.* □

Now we turn to the relations between our proof systems. First, $L$-*CF* and $L$-*EF* are more-or-less just different presentations of the same system; moreover, the *size* of $L$-*EF* or $L$-*CF* proofs is (up to a polynomial) essentially the same measure as the number of *lines* in $L$-*F* proofs. These properties are well known for $L = \mathbf{CPC}$, and noted to hold for si logics in [12, Prop. 3.2–3]; we observe that the argument applies to fragments $L_C$ just the same. In order to state it properly, let $s_P(\varphi)$ denote the minimal size of a $P$-proof of a formula $\varphi$, and $k_P(\varphi)$ the minimal number of lines in a $P$-proof of $\varphi$ (for proof systems $P$ where the concept of lines makes sense).

**Proposition 2.5** *$L_C$-EF and $L_C$-CF are p-equivalent. Moreover, for any $L_C$-tautology $\varphi$, we have*

$$k_{L_C\text{-}EF}(\varphi) \le k_{L_C\text{-}F}(\varphi) = k_{L_C\text{-}CF}(\varphi) = O(k_{L_C\text{-}EF}(\varphi)),$$

*and*

$$s_{L_C\text{-}EF}(\varphi) = O(k_{L_C\text{-}F}(\varphi) + |\varphi|^2).$$ □

The next result is again well known for **CPC**, and noted to hold for si logics in [12, Prop. 3.11]. Even with Lemma 2.3 and Proposition 2.4 at hand, it is not immediately obvious that it also applies to fragments, since the standard argument from [14, L. 4.4.8] relies on a tree of conjunctions. We can make it work with the help of the following trick: in intuitionistic logic, propositions expressed by formulas of the form $\Gamma \to \alpha$ for a fixed $\alpha$ form a Boolean algebra, with the induced $\to$ operation, and $\alpha$ serving the role of $\bot$; cf. (22). In particular, they carry a well-behaved conjunction operation

$$(\Gamma \to \alpha) \wedge^{\alpha} (\Delta \to \alpha) = \big((\Gamma \to \alpha) \to (\Delta \to \alpha) \to \alpha\big) \to \alpha.$$

This can be employed to emulate the original Krajíček's argument. We leave the details to the reader.

**Proposition 2.6** *Let $P$ be $L_C$-F, $L_C$-EF, or $L_C$-CF. Given a $P$-proof of a formula $\varphi$ with $m$ lines, we can construct in polynomial time a $P$-proof of $\varphi$ of height $O(\log m)$. Consequently, $P \equiv_p P^*$.* □

Another consequence of Proposition 2.6 is that all tree-like Frege (*EF*, *CF*, resp.) systems for $L_C$ are equivalent. This is no longer true for tree-like *SF* systems: as explained in [12, §3.1], $L_C$-$SF^*$ systems are sensitive to the choice of basic rules[4]. For simplicity, we state the next result for *standard* axiom systems, but it holds more generally under the assumption that (1) has a tree-like Frege derivation in which the premise $\alpha$ is used only once. Then, using Lemma 2.3 and Propositions 2.4 and 2.6, we can generalize [12, Thm. 3.12] to fragments as follows:

**Proposition 2.7** *A standard $L_C$-$SF^*$ system is p-equivalent to $L_C$-$EF$.* □

This leaves us with only three potentially different proof systems for $L_C$ out of those mentioned above (ignoring non-standard $L_C$-$SF^*$ systems): $L_C\text{-}F \leq_p L_C\text{-}EF \leq_p L_C\text{-}SF$. Whether **CPC**-*EF* has superpolynomial speed-up over **CPC**-*F* is a notorious open problem, and it is unresolved for **IPC** or other si logics or their fragments as well. Whether *EF* and *SF* are equivalent depends on the logic: in particular, **CPC**-$EF \equiv_p$ **CPC**-*SF*, whereas **IPC**-*SF* has exponential speed-up over **IPC**-*EF*. These questions are extensively studied in [12], while generalization of the speed-up to fragments is one of the goals of the present paper, so we will get back to it later.

## 3 Elimination of connectives from tautologies

As already mentioned in the introduction, motivation for this section comes from lower bounds on intuitionistic proofs:

**Theorem 3.1 (Hrubeš [9])** *There is a sequence $\{\varphi_n : n \in \omega\}$ of intuitionistic tautologies of the form*

$$\bigwedge_{i<m} (p_i \vee p'_i) \to \neg\alpha(\vec{p}, \vec{s}) \vee \neg\beta(\vec{p'}, \vec{r}), \tag{18}$$

*constructible in time $n^{O(1)}$, that require* **IPC**-*EF proofs of size $2^{n^{\Omega(1)}}$.* □

The original clique–colouring tautologies can be modified to yield the following strengthening:

**Theorem 3.2 (Jeřábek [12])** *There is a sequence $\{\varphi_n : n \in \omega\}$ of intuitionistic tautologies of the form*

$$\bigwedge_{i<m} (p_i \vee p'_i) \to \Big(\bigwedge_{j<m} (s_j \vee s'_j) \to \gamma(\vec{p}, \vec{s}, \vec{s'})\Big) \vee \Big(\bigwedge_{k<m} (r_k \vee r'_k) \to \delta(\vec{p'}, \vec{r}, \vec{r'})\Big), \tag{19}$$

*with $\gamma, \delta$ strict monotone, that have* **IPC**-*SF proofs constructible in time $n^{O(1)}$, but require $L$-EF proofs of size $2^{n^{\Omega(1)}}$ for any si logic $L$ of unbounded branching.* □

($L$ has bounded branching if, roughly, there is a finite constant $b$ such that any point in a finite $L$-frame has at most $b$ immediate successors. See [12] for details.)

[4]Thus, the $L_C$-$SF^*$ notation is misleading. We should properly indicate the set of Frege rules.

We would like to modify these tautologies further to make them purely implicational while preserving the bounds on the lengths of their proofs. Rather than dwelling on these specific examples, we would like to have a method applicable more generally to arbitrary tautologies; the ideal result could look as follows:

**False theorem 3.3** *Given a formula $\varphi$, we can construct in polynomial time an implicational formula $\varphi'$ with the following property. If $P$ denotes $L$-$F$, $L$-$EF$, or $L$-$SF$ for a si logic $L$, then $P$-proofs of $\varphi$ and $\varphi'$ can be constructed from each other in polynomial time.*

As we will discuss in more detail below, this is too good to be true: we need to restrict the class of tautologies or the class of logics. Nevertheless, we will seek results in a similar spirit.

We start with a construction that applies to all si logic in a very uniform way, but does not in general produce fully implicational tautologies from arbitrary formulas $\varphi$. The idea is very simple: we introduce extension variables for subformulas of $\varphi$. This cuts the meat of $\varphi$ into small chunks (extension axioms), most of which can be rewritten with implicational formulas. (We stress that extension variables can be used in this way even in Frege. The point is that here the set of extension axioms is a priori polynomially bounded and we can incorporate them in the tautology, whereas an $L$-$EF$ proof may potentially use an unlimited number of extension axioms that cannot be simulated in this way.)

We recall the usual notion of positive and negative occurrences of subformulas of $\varphi$: the occurrence of $\varphi$ in itself is positive, polarity is flipped when passing to the antecedent of an implication, and it is preserved by other connectives.

**Proposition 3.4** *Given a formula $\varphi$, we can construct in polynomial time a formula $\overline{\varphi}$ of the form*

$$(p_0 \to \bot) \to (p_1 \to q_1 \vee r_1) \to \cdots \to (p_m \to q_m \vee r_m) \to \varphi_{\to},$$

*where $\varphi_{\to}$ is purely implicational, $m$ is the number of disjunctions with negative occurrences in $\varphi$, and the $p_0 \to \bot$ term is omitted if $\varphi$ has no negative occurrences of $\bot$, with the following properties.*

(i) *There are a poly-time constructible substitution $\sigma$, and a poly-time constructible* **IPC**-*F proof of $\sigma(\overline{\varphi}) \to \varphi$.*

(ii) *There is a poly-time constructible* **IPC**-*F proof of $\varphi \to \overline{\varphi}$.*

*In particular, if $L$ is a si logic, and $P$ is $L$-$F$, $L$-$EF$, or $L$-$SF$, then $P$-proofs of $\varphi$ and $\overline{\varphi}$ are poly-time constructible from each other.*

*Proof:* We introduce a variable $p_\psi$ for each subformula $\psi \subseteq \varphi$, where the original variables $p_i$ are identified with $p_{p_i}$. We define a set of formulas $\Xi$, consisting of the following formulas for each nonvariable $\psi \subseteq \varphi$, depending on whether $\psi$ occurs positively or negatively in $\varphi$:

| $\psi$ | positive | negative |
| --- | --- | --- |
| $\bot$ | | $p_\psi \to \bot$ |
| $\psi_0 \to \psi_1$ | $(p_{\psi_0} \to p_{\psi_1}) \to p_\psi$ | $p_\psi \to p_{\psi_0} \to p_{\psi_1}$ |
| $\psi_0 \wedge \psi_1$ | $p_{\psi_0} \to p_{\psi_1} \to p_\psi$ | $p_\psi \to p_{\psi_0}$ |
| | | $p_\psi \to p_{\psi_1}$ |
| $\psi_0 \vee \psi_1$ | $p_{\psi_0} \to p_\psi$ | $p_\psi \to p_{\psi_0} \vee p_{\psi_1}$ |
| | $p_{\psi_1} \to p_\psi$ | |

Enumerate $\Xi = \{\xi_0, \dots, \xi_r\}$ so that the formulas involving $\bot$ or $\vee$ come first, and define $\overline{\varphi}$ as

$$\xi_0 \to \cdots \to \xi_r \to p_\varphi.$$

(i): Put $\sigma(p_\psi) = \psi$. Then the formulas from $\sigma(\Xi)$ are instances of constant-size tautologies, hence they have linear-size proofs, using which it is easy to construct a proof of $\sigma(\overline{\varphi}) \to \sigma(p_\varphi)$.

(ii): Let $\pi$ consist of $\Xi$ followed by formulas

$$\psi \to p_\psi \tag{20}$$

for positively occurring $\psi \subseteq \varphi$, and

$$p_\psi \to \psi \tag{21}$$

for negatively occurring $\psi \subseteq \varphi$, ordered bottom-up. We can easily complete $\pi$ to a valid derivation of $\varphi \to p_\varphi$ from assumptions $\Xi$: for example, let $\psi = \psi_0 \to \psi_1$ have positive occurrence in $\varphi$. Then $\psi \to p_\psi$ has linear-size derivation from the formulas

$$(p_{\psi_0} \to p_{\psi_1}) \to p_\psi$$
$$p_{\psi_0} \to \psi_0$$
$$\psi_1 \to p_{\psi_1}$$

that appear earlier in $\pi$.

Using the feasible deduction theorem (and possibly Lemma 2.3 to reorder the formulas), we can turn $\pi$ into a proof of $\varphi \to \Xi \to p_\varphi$, which is $\varphi \to \overline{\varphi}$. □

This is not yet the end of the story. Let us see where Proposition 3.4 gets us with respect to the original goal. We did not eliminate $\bot$ embedded in $\alpha, \beta$ in (18), but this is not a problem, as a $\bot$-free version of these tautologies is already provided by (19). Elimination of $\vee$ is more interesting. Most crucially, the main disjunctions on the right-hand sides of (18), (19) occur positively, and therefore *are* eliminated by Proposition 3.4. The same applies to $\vee$ embedded in $\gamma, \delta$ of (19). There might be some disjunctions coming from $\alpha, \beta$ left in (18), however we can ignore these as we can apply classical reasoning inside negations. The remaining disjunctions in (18) and (19) occur in the context $\bigwedge_i (p_i \vee p'_i) \to \cdots$, and we will get rid of them by exploiting the intuitionistic equivalences

$$\left.\begin{aligned}
(\varphi \vee \psi \to \chi) &\leftrightarrow (\varphi \to \chi) \wedge (\psi \to \chi), \\
(\varphi \wedge \psi \to \chi) &\leftrightarrow (\varphi \to \psi \to \chi), \\
(\varphi \to \chi) &\leftrightarrow (((\varphi \to \chi) \to \chi) \to \chi).
\end{aligned}\right\} \tag{22}$$

We now formalize these considerations.

**Definition 3.5** An occurrence of $\psi \vee \chi$ in a formula $\varphi$ is *inessential* if

(i) it is positive, or

(ii) it is in the scope of a negation (i.e., inside a subformula of $\varphi$ of the form $\alpha \to \bot$), or

(iii) there is an implication $\alpha \to \beta \subseteq \varphi$ such that the given occurrence of $\psi \vee \chi$ is inside $\alpha$, and not inside any subformula of $\alpha$ that is an implication. In other words, the only connectives on the path from $\psi \vee \chi$ to $\alpha$ in the formula tree are $\vee$ and $\wedge$.

All other occurrences of disjunctions in $\varphi$ are *essential*.

**Theorem 3.6** *Proposition 3.4 holds with $m$ being the number of essential occurrences of disjunctions in $\varphi$.*

*Proof:* For any subformula $\alpha \to \bot$ of $\varphi$, we may replace $\alpha$ with a canonically chosen classically equivalent formula using $\to, \bot$ as the only connectives, hence we may assume without loss of generality that no disjunctions occur inside negations.

We modify the construction from the proof of Proposition 3.4 as follows. Consider any positively occurring implication $\gamma \subseteq \varphi$, and write it as

$$\mu(\alpha_0, \dots, \alpha_{r-1}) \to \beta,$$

where $\mu(x_0, \dots, x_{r-1})$ is a strict monotone formula, and each $\alpha_i$ is a variable, a constant, or an implication. We omit the variables $p_{\nu(\vec{\alpha})}$ for non-variable subformulas $\nu \subseteq \mu$ along with the associated formulas in $\Xi$, and introduce instead variables $q^\gamma_\nu$ for $\nu \subseteq \mu$ with intended meaning $\nu(\vec{\alpha}) \to \beta$, where $q^\gamma_\mu$ is identified with $p_\gamma$. We will write just $q_\nu$ to simplify the notation.

We include in $\Xi$ the following formulas for each $\nu \subseteq \mu$:

| $\nu$ | formula in $\Xi$ |
|---|---|
| $x_i$ | $(p_{\alpha_i} \to p_\beta) \to q_\nu$ |
| $\nu' \vee \nu''$ | $((q_{\nu'} \to q_{\nu''} \to p_\beta) \to p_\beta) \to q_\nu$ |
| $\nu' \wedge \nu''$ | $((q_{\nu'} \to p_\beta) \to q_{\nu''}) \to q_\nu$ |

(i): We extend $\sigma$ by putting $\sigma(q_\nu) = (\nu(\vec{\alpha}) \to \beta)$. As in the proof of Proposition 3.4, it is enough to construct short **IPC**-$F$ proofs of the new formulas in $\sigma(\Xi)$. This is straightforward:

$$\begin{aligned}(\nu'(\vec{\alpha}) \vee \nu''(\vec{\alpha}) \to \beta) &\leftrightarrow (((\nu'(\vec{\alpha}) \vee \nu''(\vec{\alpha}) \to \beta) \to \beta) \to \beta)\\ &\leftrightarrow (((\nu'(\vec{\alpha}) \to \beta) \wedge (\nu''(\vec{\alpha}) \to \beta) \to \beta) \to \beta)\\ &\leftrightarrow (((\nu'(\vec{\alpha}) \to \beta) \to (\nu''(\vec{\alpha}) \to \beta) \to \beta) \to \beta)\end{aligned}$$

using (22); likewise,

$$\begin{aligned}(\nu'(\vec{\alpha}) \wedge \nu''(\vec{\alpha}) \to \beta) &\leftrightarrow (\nu''(\vec{\alpha}) \to \nu'(\vec{\alpha}) \to \beta)\\ &\leftrightarrow (\nu''(\vec{\alpha}) \to ((\nu'(\vec{\alpha}) \to \beta) \to \beta) \to \beta)\\ &\leftrightarrow (((\nu'(\vec{\alpha}) \to \beta) \to \beta) \to \nu''(\vec{\alpha}) \to \beta).\end{aligned}$$

(ii): We modify the proof $\pi$ considered in Proposition 3.4 by including the formulas

$$(\nu(\vec{\alpha}) \to \beta) \to q_\nu \tag{23}$$

for all $\nu \subseteq \mu$. Notice that the final formula (23) for $\nu = \mu$ is just (20) for $\psi = \gamma$. We complete $\pi$ to a valid derivation as in the proof of Proposition 3.4; we only need to take care of the new formulas (23).

If $\nu = \nu' \vee \nu''$, we can derive

$$\begin{aligned}
(\nu(\vec{\alpha}) \to \beta) &\to (\nu'(\vec{\alpha}) \vee \nu''(\vec{\alpha}) \to p_\beta) && \text{(20) for } \beta \\
&\to (((\nu'(\vec{\alpha}) \to p_\beta) \to (\nu''(\vec{\alpha}) \to p_\beta) \to p_\beta) \to p_\beta) && \text{(22)} \\
&\to ((q_{\nu'} \to q_{\nu''} \to p_\beta) \to p_\beta) && \text{(23) for } \nu', \nu'' \\
&\to q_\nu, && \Xi
\end{aligned}$$

using the fact that $q_{\nu'}$ and $q_{\nu''}$ occur positively in $(q_{\nu'} \to q_{\nu''} \to p_\beta) \to p_\beta$.

The other cases are analogous. □

**Corollary 3.7** *There are implicational formulas $\{\varphi_n : n \in \omega\}$ satisfying Theorem 3.2.*

*Proof:* No essential disjunctions occur in (19). □

(See Theorem 4.22 for a further improvement of Corollary 3.7.)

As we will see, we can strengthen Proposition 3.4 for intuitionistic logic so that the resulting formula is always purely implicational, irrespective of what kind of disjunctions occur in $\varphi$. However, this will require a construction of a different kind that no longer applies to arbitrary si logics $L$. The reason is that the properties of $\overline{\varphi}$ as given by Proposition 3.4 imply that $\overline{\varphi}$ is interderivable with $\varphi$ in the sense that $\mathbf{IPC} + \varphi = \mathbf{IPC} + \overline{\varphi}$. If we can always find a positive (i.e., $\bot$-free) $\overline{\varphi}$ with this property for every $L$-tautology $\varphi$, then $L$ is positively axiomatizable over **IPC**, or equivalently, the class of general $L$-frames is closed under dense subframes. For instance, this fails for $L = \mathbf{KC}$, which has the same positive fragment as **IPC**. Similarly, if we can always find a $\vee$-free $\overline{\varphi}$, then $L$ is a cofinal-subframe logic.

This problem comes up even if we do not ask $\overline{\varphi}$ to have the strong properties guaranteed by Proposition 3.4, but merely that it is positive, and preserves proof length in a particular logic $L$ up to a polynomial. If $L \subseteq \mathbf{KC}$, we know from [12, L. 6.30] that $L$-*EF* is polynomially equivalent to **IPC**-*EF* with respect to positive tautologies. Thus, the existence of such a map $\varphi \mapsto \overline{\varphi}$ would imply that $L$-*EF* has essentially the same proof complexity as **IPC**-*EF*, and in particular, that every $L$-tautology has a proof of at most exponential size. However, there are a vast number of logics between **IPC** and **KC**, many of which are outside NEXP, or even undecidable.[5]

So, to make a long story short, we will only show how to eliminate $\bot$ and $\vee$ from tautologies in logics whose proper axioms do not contain the respective connectives, which appears to be the best we can hope for. We start with the simpler case of $\bot$. The idea here is just that the conjunction of all variables is a good enough approximation of $\bot$ vis-à-vis positive formulas.

[5] The undecidable, finitely axiomatized si logics with the disjunction property (which incidentally implies they also have the same $\vee$-free fragment as **IPC**) from [5, Ex. 15.11] are easily seen to be included in **KC**. As for natural examples, the author wonders what is the complexity of the Kreisel–Putnam logic.

**Theorem 3.8** *Given a formula $\varphi$, we can construct in polynomial time a positive formula $\varphi^+$ and a substitution $\sigma$ with the following properties.*

(i) *There is a poly-time constructible* **IPC**-*F proof of $\sigma(\varphi^+) \to \varphi$.*

(ii) *Let $P$ denote L-F, L-EF, or L-SF for a si logic $L$ axiomatizable by positive formulas. Then given a $P$-proof of $\varphi$, we can construct in polynomial time a $P$-proof of $\varphi^+$.*

*Moreover, we can make $\varphi^+$ to have the form*

$$(p_1 \to q_1 \lor r_1) \to \cdots \to (p_m \to q_m \lor r_m) \to \varphi_\to, \tag{24}$$

*where $\varphi_\to$ is purely implicational, and $m$ is the number of essential occurrences of $\lor$ in $\varphi$.*

*Proof:* Write $\varphi = \varphi'(p_0, \dots, p_{n-1}, \bot)$, where $\varphi'$ is positive, and $p_0, \dots, p_{n-1}$ are all variables occurring in $\varphi$. Define $\varphi^+$ as

$$(r \to p_0) \to \cdots \to (r \to p_{n-1}) \to \varphi'(p_0, \dots, p_{n-1}, r), \tag{25}$$

where $r$ is a new variable. (i) is straightforward, using the substitution $\sigma(r) = \bot$.

(ii): We can assume the Frege rules of $P$ consist of positive axioms, modus ponens, and the axiom (10). First, let $P$ be *L-F* or *L-EF*. Let $\pi$ be a $P$-proof of $\varphi$. We may assume that the only variables occurring in $\pi$ are $p_i$ and extension variables, and that none of the extension variables is $r$. We can also assume that the only instances of (10) in $\pi$ are with $\gamma = p_i$: we can derive $\bot \to \gamma$ for an arbitrary $\gamma$ from these by a polynomial-size subproof by induction on the complexity of $\gamma$ (using extension axioms to get $\bot \to q_j$ for extension variables $q_j$).

We replace $\bot$ with $r$ in the proof. Treating the axioms $r \to p_i$ as extra assumptions, we construct a proof of $\varphi^+$ by an application of the feasible deduction theorem.

Now, let $P =$ *L-SF*, and $\pi = \varphi_1, \dots, \varphi_m$ be a $P$-proof of $\varphi_m = \varphi$. We may assume $r$ does not occur in $\pi$. We will complete $\varphi_1^+, \dots, \varphi_m^+$ to a valid $P$-proof, where all the formulas $\varphi_j^+$ use the same $r$, but only variables actually occurring in $\varphi_j$ in the premise of (25).

*L-SF* has a constant finite set of axioms, whose translations have constant-size proofs, which takes care of the case when $\varphi_j$ is an axiom.

If $\varphi_j$ is derived by modus ponens from $\varphi_k$ and $\varphi_l = (\varphi_k \to \varphi_j)$, let $p_0, \dots, p_{n-1}$ be the variables of $\varphi_l$. We can insert extra conjuncts in $\varphi_k^+$ if necessary to obtain

$$\{r \to p_i : i < n\} \to \varphi'_k(\vec{p}, r),$$
$$\{r \to p_i : i < n\} \to \varphi'_k(\vec{p}, r) \to \varphi'_j(\vec{p}, r),$$

from which we derive

$$\{r \to p_i : i < n\} \to \varphi'_j(\vec{p}, r)$$

using Lemma 2.3. We get rid of unwanted conjuncts $r \to p_i$ for $p_i$ not occurring in $\varphi_j$ by substituting $r$ for $p_i$.

Assume that $\varphi_j(p_0, \dots, p_{n-1})$ is derived from $\varphi_k(q_0, \dots, q_{m-1})$ by the substitution rule, so that $\varphi_j = \varphi_k(\alpha_0, \dots, \alpha_{m-1})$ for some formulas $\alpha_i(\vec{p})$, $i < m$. (Here, $\vec{q}$ may well be the same variables as $\vec{p}$; we distinguish them in notation for clarity.) We are given the formula $\varphi_k^+$, which is

$$\{r \to q_l : l < m\} \to \varphi'_k(\vec{q}, r).$$

Applying the substitution rule to $\varphi_k^+$, we derive

$$\{r \to \alpha'_l(\vec{p}, r) : l < m\} \to \underbrace{\varphi'_k(\alpha'_0(\vec{p}, r), \dots, \alpha'_{m-1}(\vec{p}, r), r)}_{\varphi'_j(\vec{p}, r)}.$$

We construct short proofs of

$$\{r \to p_i : i < n\} \to r \to \alpha'_l(\vec{p}, r)$$

for $l < m$ by induction on the complexity of the positive formulas $\alpha'_l(\vec{p}, r)$, and conclude

$$\{r \to p_i : i < n\} \to \varphi'_j(\vec{p}, r),$$

which is $\varphi_j^+$. This finishes the argument for $P = L\text{-}SF$.

Finally, notice that the construction of $\varphi^+$ did not increase the number of essential (or inessential, for that matter) disjunctions, hence if we use $\overline{\varphi^+}$ from Theorem 3.6 instead, it will have the required form (24). $\square$

Elimination of $\vee$ is ostensibly more complicated than elimination of $\bot$, but it can be seen as a generalization of the latter, as $\bot$ is just the empty disjunction. In the proof of Theorem 3.8, we exploited the fact that the algebra of positive formulas in finitely many variables has a least element (and therefore is a Heyting algebra), which we can use to emulate $\bot$. The least element should be the meet of all positive formulas, but this equals the meet of just variables, which makes it definable by a finite formula.

In order to eliminate $\vee$ in a similar way, Diego's theorem [5, §5.4] ensures that the algebra of $\vee$-free formulas in finitely many variables is finite; since it is a $\wedge$-semilattice, it is in fact a complete lattice (and a Heyting algebra). The join operation of this lattice can be used to emulate disjunction. The join of $\psi$ and $\chi$ should be the conjunction of all $\vee$-free formulas implied by $\psi \vee \chi$, which are up to equivalence exactly the formulas of the form

$$(\psi \to \gamma) \to (\chi \to \gamma) \to \gamma.$$

As with $\bot$, it turns out that it is enough to consider just variables (and $\bot$) in place of $\gamma$, resulting in a short conjunction.

We will need to emulate all disjunctions appearing in the proof. Since the replacement for $\psi \vee \chi$ involves many occurrences of $\psi$ and $\chi$, we need to work with circuits to preserve polynomial size. That is, the argument will only give polynomial simulation of *EF* systems, not Frege.

**Theorem 3.9** *Given a formula $\varphi$, we can construct in polynomial time a $\{\to, \bot\}$-formula $\tilde{\varphi}$ (purely implicational if $\varphi$ is positive) and a substitution $\sigma$ with the following properties.*

(i) *There is a poly-time constructible* **IPC**-*F proof of* $\sigma(\tilde{\varphi}) \to \varphi$.

(ii) *Let $P$ denote $L$-EF or $L$-SF for a cofinal-subframe si logic $L$. Given a $P$-proof of $\varphi$, we can construct in polynomial time a $P$-proof of $\tilde{\varphi}$.*

*Proof:* We will first construct a $\vee$-free formula $\tilde{\varphi}$ with these properties.

Let a formula $\varphi(\vec{p})$ be given. For each $\psi \vee \chi \subseteq \varphi$, we introduce a new variable $r_{\psi\vee\chi}$; we denote by $\alpha^*$ the result of replacing all top-most occurrences of disjunctions $\psi \vee \chi$ with $r_{\psi\vee\chi}$. We define

$$\tilde{\varphi} = \Delta_\varphi \to \varphi^*,$$

where the set $\Delta_\varphi$ consists of the formulas

$$\psi^* \to r_{\psi\vee\chi}, \tag{26}$$

$$\chi^* \to r_{\psi\vee\chi}, \tag{27}$$

$$r_{\psi\vee\chi} \to (\psi^* \to v) \to (\chi^* \to v) \to v \tag{28}$$

for $\psi \vee \chi \subseteq \varphi$, and $v \in V_\varphi = \{\vec{p}, \vec{r}, \bot\}$ (where $\vec{r}$ stands for the list $\{r_{\psi\vee\chi} : \psi \vee \chi \subseteq \varphi\}$).

(i): Putting $\sigma(r_{\psi\vee\chi}) = \psi \vee \chi$, we have $\sigma(\alpha^*) = \alpha$ for each $\alpha$, hence $\sigma(\tilde{\varphi}) = \sigma(\Delta_\varphi) \to \varphi$, and the formulas in $\sigma(\Delta_\varphi)$ are instances of constant-size tautologies.

(ii): First, let $P = L\text{-}EF$. We may assume the Frege rules of $P$ are instances of $\vee$-free axioms, modus ponens, and the axioms (7)–(9). Let $\pi$ be a $P$-proof of $\varphi$. We may assume the only variables in $\pi$ are $\vec{p}$ and extension variables. We introduce new variables $r_{\psi\vee\chi}$ for each disjunction appearing in $\pi$, and write $\alpha^*$ for the result of replacing all top-most disjunctions in $\alpha$ with the corresponding variables. Notice that this agrees with the definition of $\alpha^*$ used in the construction of $\tilde{\varphi}$.

We replace each formula $\alpha$ in $\pi$ with $\alpha^*$. At the beginning of the proof, we add the formulas $\Delta_\varphi$ as extra assumptions. We introduce the extension axiom

$$r_{\psi\vee\chi} \leftrightarrow \bigwedge_{v \in V_\varphi} \big((\psi^* \to v) \to (\chi^* \to v) \to v\big) \tag{29}$$

for each $\psi \vee \chi \nsubseteq \varphi$; we place this axiom after extension axioms for all extension variables occurring in $\psi^*, \chi^*$. We stress that $V_\varphi$ does *not* contain variables $r_{\psi\vee\chi}$ for $\psi \vee \chi \nsubseteq \varphi$.

In order to make this a valid derivation, we need to fix occurrences of (7)–(9) in the proof. As for (7) and (8), the formulas

$$\alpha^* \to r_{\alpha\vee\beta}, \qquad \beta^* \to r_{\alpha\vee\beta}$$

are included in $\Delta_\varphi$ for $\alpha \vee \beta \subseteq \varphi$, and easily provable from (29) for other $\alpha \vee \beta$.

As for (9), notice that $\gamma^*$ is $\vee$-free. The formulas

$$r_{\alpha\vee\beta} \to (\alpha^* \to \xi) \to (\beta^* \to \xi) \to \xi \tag{30}$$

are in $\Delta_\varphi$ or derivable from (29) when $\xi \in V_\varphi$. For general $\vee$-free $\xi$ (using only variables occurring in the proof), we construct a derivation of (30) by inner induction on the complexity of $\xi$, and outer induction on the extension variables (old or new) occurring in $\xi$. For the induction hypothesis, if $\circ \in \{\to, \wedge\}$, then

$$r_{\alpha\vee\beta} \to (\alpha^* \to \xi_0) \to (\beta^* \to \xi_0) \to \xi_0,$$
$$r_{\alpha\vee\beta} \to (\alpha^* \to \xi_1) \to (\beta^* \to \xi_1) \to \xi_1 \vdash r_{\alpha\vee\beta} \to (\alpha^* \to \xi_0 \circ \xi_1) \to (\beta^* \to \xi_0 \circ \xi_1) \to \xi_0 \circ \xi_1$$

is an instance of a constant-size derivation. If $\xi$ is an extension variable, we derive (30) for its definition by the induction hypothesis, and use the extension axiom.

In the end, we obtain a valid $P$-derivation of $\varphi^*$ from assumptions $\Delta_\varphi$, and we use the feasible deduction theorem to get a proof of $\tilde{\varphi}$.

Now, let $P = L\text{-}SF$, and $\varphi_1, \dots, \varphi_m$ be a $P$-proof of $\varphi$. We consider the sequence $\tilde{\varphi}_1, \dots, \tilde{\varphi}_m$, and make it a valid $P$-proof as follows.

As in the proof of Theorem 3.8, translations of axioms have constant-size proofs.

If $\varphi_j = \varphi_k(\alpha_1, \dots, \alpha_n)$ is inferred from $\varphi_k$ by substitution, we rename variables $r_{\psi\vee\chi}$ in $\tilde{\varphi}_k$ to $r_{\psi(\vec{\alpha})\vee\chi(\vec{\alpha})}$, and substitute $\alpha_1^*, \dots, \alpha_n^*$ to obtain $\Delta' \to \varphi_j^*$, where $\Delta'$ contains some of the formulas of the form

$$\psi^* \to r_{\psi\vee\chi},$$
$$\chi^* \to r_{\psi\vee\chi},$$
$$r_{\psi\vee\chi} \to (\psi^* \to v) \to (\chi^* \to v) \to v$$

for $\psi \vee \chi \subseteq \varphi_j$, and $v \in \{\alpha_1^*, \dots, \alpha_n^*, \vec{r}, \bot\}$. Only the last are a problem; we construct their short derivations from $\Delta_{\varphi_j}$ by induction on the complexity of $\alpha_i^*$ as in the proof of (30). Thus, we obtain a proof of $\Delta_{\varphi_j} \to \varphi_j^*$, i.e., $\tilde{\varphi}_j$.

If $\varphi_j$ is derived from $\varphi_k$ and $\varphi_l = (\varphi_k \to \varphi_j)$ by modus ponens, we insert dummy premises in $\tilde{\varphi}_k$ to obtain $\Delta_{\varphi_l} \to \varphi_k^*$, and infer

$$\Delta_{\varphi_l} \to \varphi_j^*.$$

We need to get rid of the unwanted conjuncts from $\Delta_{\varphi_l} \smallsetminus \Delta_{\varphi_j}$. First, assume $r_{\psi\vee\chi}$ occurs in $\Delta_{\varphi_l}$ for some $\psi \vee \chi \nsubseteq \varphi_j$, and take $\psi \vee \chi$ maximal such. We substitute $r_{\psi\vee\chi}$ with the formula

$$\xi = \bigwedge_{v \in V} \big((\psi^* \to v) \to (\chi^* \to v) \to v\big),$$

where $V$ is the set of $v$ for which (28) occurs in the formula (minus $v = r_{\psi\vee\chi}$ itself, for which the conjunct is redundant). The formulas (26)–(28) associated with $r_{\psi\vee\chi}$ have short proofs after the substitution, and we can delete them. We can also delete the formulas

$$r_{\psi'\vee\chi'} \to (\psi'^* \to \xi) \to (\chi'^* \to \xi) \to \xi$$

for other $r_{\psi'\vee\chi'}$: they have short derivations from the remaining formulas, as $\xi$ is a $\vee$-free formula not containing $r_{\psi\vee\chi}$. After that, there are no traces left of either $r_{\psi\vee\chi}$ or $\xi$.

We continue in this way to eliminate all variables $r_{\psi\vee\chi}$ for $\psi \vee \chi \nsubseteq \varphi_j$. The only unwanted things left are then formulas (28) for $\psi \vee \chi \subseteq \varphi_j$, and $v = p_i$ a variable not occurring in $\varphi_j$. We can e.g. substitute $\bot$ for $p_i$.

This concludes the proof of (ii), but we have so far only constructed a $\vee$-free formula $\tilde{\varphi}$ with the required properties. In order to make it a $\{\to,\bot\}$-formula, it suffices to apply Proposition 3.4. However, we need to be a bit more careful if we want an implicational formula in case $\varphi$ is positive, as the definition of $\tilde{\varphi}$ unconditionally introduced $\bot$.

Fortunately, if $\varphi$ is positive, the formulas (28) with $v = \bot$ are redundant in $\Delta_\varphi$: the remaining formulas imply

$$r_{\psi\vee\chi} \to (\psi^* \to \bot) \to (\chi^* \to \bot) \to v, \qquad v \in \{\vec{p},\vec{r}\}.$$

Since $\chi^*$ is positive, this yields

$$r_{\psi\vee\chi} \to (\psi^* \to \bot) \to (\chi^* \to \bot) \to \chi^*,$$

hence

$$r_{\psi\vee\chi} \to (\psi^* \to \bot) \to (\chi^* \to \bot) \to \bot$$

as needed. □

For **IPC**, and more generally logics axiomatizable by both $\bot$-free and $\vee$-free formulas (i.e., subframe logics), we can apply Theorems 3.8 and 3.9 in a row:

**Corollary 3.10** *Given a formula $\varphi$, we can construct in polynomial time a purely implicational formula $\hat{\varphi}$ and a substitution $\sigma$ with the following properties.*

(i) *There is a poly-time constructible* **IPC**-*F proof of $\sigma(\hat{\varphi}) \to \varphi$.*

(ii) *Let $P$ denote $L$-$EF$ or $L$-$SF$ for a subframe si logic $L$. Given a $P$-proof of $\varphi$, we can construct in polynomial time a $P$-proof of $\hat{\varphi}$.* □

# 4 Elimination of connectives from proofs

So far we were concerned with elimination of connectives from the formula to be proved, but we still allowed proofs to be carried out in the full logic. It is natural to ask if we can also eliminate connectives other than implication from the proofs themselves, and indeed some of the arguments we used earlier can help with that goal, too. The ideal result could be formulated as

**False theorem 4.1** *Let $P$ denote $L$-$F$, $L$-$EF$, or $L$-$SF$ for a si logic $L$, and $\to\, \in C \subseteq C_{\mathbf{IPC}}$. Given a $P$-proof of a $C$-formula $\varphi$, we can construct in polynomial time a $P$-proof of $\varphi$ consisting only of $C$-formulas.*

In this formulation, the result is extremely sensitive to the choice of axioms of $L$: to begin with, there is no way it could hold if we axiomatize $L$ so that none of the axioms is a $C$-formula. Thus, we can only get results of this form for very particular axiom systems.

We could avoid this dependence on axiomatization by shifting perspective: we can view it as a feasible conservativity result, i.e., a form of p-simulation between two different systems. For example, here is such a statement for $EF$:

**False theorem 4.2** *Let $L$ be a si logic, and $\to \in C \subseteq C_{\mathbf{IPC}}$. Given an $L$-EF proof of a $C$-formula $\varphi$, we can construct in polynomial time an $L_C$-EF proof of $\varphi$. That is, $L_C$-EF p-simulates $L$-EF with respect to $C$-formulas.*

Nevertheless, we start with a result in the form of 4.1; in fact, we formulate it in a stronger way, which gives us control over unwanted connectives even if they appear in the tautology being proved. In a pleasant turn of events, we have no real work to do: we just reap what we have grown in the proofs of Theorems 3.8 and 3.9.

For simplicity, we state the result only for extended Frege. The less interesting part (ii) also works for Frege. The statement also holds for substitution Frege after appropriate modifications (*SF* proofs only include the basic form of each axiom once, and if needed, its instances can be derived by means of the substitution rule, thus the restrictions on instances below are not meaningful).

**Theorem 4.3** *Let $L$ be a si logic, and $P$ a standard $L$-EF system. Given a $P$-proof $\pi$ of a formula $\varphi$, we can construct in polynomial time a $P$-proof $\pi'$ of $\varphi$ with the following properties:*

(i) *If the proper axiom of $P$ is $\vee$-free, then the only disjunctions occurring in $\pi'$ are subformulas of $\varphi$, and the only instances of* (9) *in $\pi'$ are with $\gamma$ a subformula of $\varphi$ which is a variable, a disjunction, or $\bot$.*

(ii) *If $\varphi$ and the proper axiom of $P$ are positive, then $\bot$ does not occur in $\pi'$. Otherwise the only instances of* (10) *in $\pi'$ are with $\gamma$ a variable from $\varphi$.*

*Proof:* (i): Let $\tilde{\varphi}$ be the $\vee$-free (and $\bot$-free, if $\varphi$ is) formula from Theorem 3.9, and $\tilde{\pi}$ its $P$-proof constructed there. There are no disjunctions in $\tilde{\pi}$. We apply to $\tilde{\pi}$ the substitution $\sigma(r_{\psi\vee\chi}) = \psi \vee \chi$. Then the only disjunctions in $\sigma(\tilde{\pi})$ are subformulas of $\varphi$, and the proof does not use axioms (7)–(9). The conclusion of the proof is $\sigma(\Delta_\varphi) \to \varphi$, and the formulas in $\sigma(\Delta_\varphi)$ are instances of (7)–(9) of the required form, hence we can include them in the proof, and infer $\varphi$ by modus ponens.

The argument for (ii) is analogous: we take the $\bot$-free proof of the formula $\varphi^+$ constructed in Theorem 3.8. If $\varphi$ contains $\bot$, we substitute $\bot$ for $r$, and eliminate the premises $\bot \to p_i$ by introducing them as axioms. If $\varphi$ is positive, we substitute $\bigwedge_i p_i$ for $r$ instead. This construction does not introduce any new disjunctions or instances of (9), hence if the axioms of $L$ are $\bot$-free and $\vee$-free, we can satisfy (i) and (ii) simultaneously. □

Theorem 4.3 quite satisfactorily eliminates $\vee$ and $\bot$. Unfortunately, not only it does not eliminate $\wedge$, the argument may even introduce new conjunctions into the proof (cf. (29)). We will spend the rest of this section by trying to remedy this defect in several ways.

Let us first note that while every si logic can be axiomatized without the use of $\wedge$ by Lemma 2.2, we cannot simply extend Theorem 4.3 by adding a conjunction clause analogous to (i). Let $\alpha$ be an implicational axiom. Completely disregarding lengths of proofs, Theorem 4.3 implies that the $\vee$-free fragment of the logic $L = \mathbf{IPC} + \alpha$ can be axiomatized by $\alpha$ over the $\vee$-free fragment of $\mathbf{IPC}$, and similarly for $\bot$. As shown in Proposition A.5, similar statements are not true in the absence of $\wedge$: for example, it may happen that $\mathbf{IPC}_\to + \alpha$

is strictly weaker than $L_{\to}$. This does not mean that elimination of connectives from proofs besides the cases in Theorem 4.3 is impossible, but it cannot work so uniformly; we will need to impose extra requirements on the logics involved, and on their axiom sets.

We include the following particular results. Section 4.1 contains an alternative simple transformation for elimination of $\bot$ that does not rely on the presence of other connectives such as $\wedge$, and works even for Frege, but needs peculiar assumptions on the logic. In Section 4.2 we present a method for elimination of $\wedge$ from $\vee$-free proofs for axiom systems that avoid the obstacle from Proposition A.5. To tie a loose end, we give an ad hoc argument that the implicational tautologies from Corollary 3.7 have short $\mathbf{IPC}_{\to}$-$SF$ proofs in Section 4.3.

### 4.1 Light-weight elimination of $\bot$

We are going to present a method for elimination of $\bot$ from intuitionistic proofs. It is less invasive than the one from Theorem 4.3, and in particular, it avoids introducing $\wedge$ (or other connectives, for that matter) into the proof. The translation also applies to other logics, under a certain semantic condition: the class of frames for the logic must be preserved under attachment of a new top element. (Thus, it does not fully supersede Theorem 4.3 (ii).) Interestingly, unlike other simulations in this paper, this one can even be usefully employed to translate proofs from one logic into another; in fact, its variant was introduced in [12, L. 6.30] for that very purpose. Another presentation of this translation, as well as the associated semantic construction in Definition 4.4, was later given by De Jongh and Zhao [13].

**Definition 4.4** If $\mathcal{F} = \langle F, \le\rangle$ is a Kripke frame, let $\mathcal{F}^t = \langle F^t, \le^t\rangle$ denote the frame obtained from $F$ by attaching a new top element $t$; that is, $F^t = F \cup \{t\}$, and $\le^t = \le \cup (F^t \times \{t\})$. We can also apply the construction to general frames $\mathcal{F} = \langle F, \le, A\rangle$: we define $\mathcal{F}^t = \langle F^t, \le^t, A^t\rangle$ with the same $F^t$ and $\le^t$ as before, and $A^t = \{\varnothing\} \cup \bigl\{X \cup \{t\} : X \in A\bigr\}$.

**Theorem 4.5** *Given an* $\mathbf{IPC}$-$F$ *proof* $\pi$ *of a positive formula* $\varphi$*, we can construct in polynomial time an* $\mathbf{IPC}$-$F$ *proof of* $\varphi$ *containing no* $\bot$*, and only those positive connectives that already occur in* $\pi$*.*

*More generally, assume that* $L^1$ *is a si logic complete wrt a class of frames* $\mathcal{K}$*, and* $L^0$ *is a si logic which is valid in* $\mathcal{F}^t$ *for all* $\mathcal{F} \in \mathcal{K}$*. Let* $C \subseteq \{\to, \wedge, \vee\}$*. Given an* $L^0_{C,\bot}$-$F$ *proof of a* $C$*-formula* $\varphi$*, we can construct in polynomial time an* $L^1_C$-$F$ *proof of* $\varphi$*.*

*The same results hold with EF in place of Frege.*

*Proof:* Let $v$ be the classical assignment that makes all variables true. For every $C \cup \{\bot\}$-formula $\varphi$ such that $v(\varphi) = 1$, we define[6] a $C$-formula $\varphi^*$ by induction on the complexity

[6] We leave $\varphi^*$ undefined when $v(\varphi) = 0$. If we needed it for other purposes, the semantically correct way to define it would be $\varphi^* = \bot$, which is however not a positive formula.

of $\varphi$:

$$\begin{aligned}
p^* &= p,\\
(\varphi \wedge \psi)^* &= \varphi^* \wedge \psi^*,\\
(\varphi \vee \psi)^* &= \begin{cases} \varphi^* \vee \psi^*, & v(\varphi) = v(\psi) = 1,\\ \varphi^*, & v(\psi) = 0,\\ \psi^*, & v(\varphi) = 0,\end{cases}\\
(\varphi \to \psi)^* &= \begin{cases} \varphi^* \to \psi^*, & v(\varphi) = v(\psi) = 1,\\ \top, & v(\varphi) = 0.\end{cases}
\end{aligned}$$

Notice that if $\varphi$ contains no $\bot$, then $v$ satisfies all its subformulas, hence $\varphi^* = \varphi$.

If $L^1$ is inconsistent, every $C$-formula has a linear-size $L^1_C$-$F$ proof. Thus, we can assume $L^1$ is consistent, in which case so is $L^0$ (as $\mathcal{K} \neq \varnothing$), hence $L^0 \subseteq \mathbf{CPC}$.

Let $\pi = \langle \varphi_0, \dots, \varphi_m \rangle$ be an $L^0_{C,\bot}$-$F$ proof of a $C$-formula $\varphi_m$. By our assumption, all $\varphi_i$ are classical tautologies, in particular $v(\varphi_i) = 1$, hence we can construct the sequence $\pi^* = \langle \varphi_0^*, \dots, \varphi_m^* \rangle$. Clearly, $\pi^*$ consists of $C$-formulas, and ends with $\varphi_m^* = \varphi_m$. We need to show that it can be completed to a polynomially larger $L^1_C$-$F$ proof.

**Claim 1** *For any $L^0$-tautology $\varphi$, the formula $\varphi^*$ is an $L^1$-tautology.*

*Proof:* It suffices to show that if $\mathcal{F} \in \mathcal{K}$ and $\vDash$ is an admissible valuation in $\mathcal{F}$, then $\mathcal{F} \vDash \varphi^*$. Let $\vDash^t$ be the valuation in $\mathcal{F}^t$ which agrees with $\vDash$ on variables in points of $F$, and makes all variables true in the new top point $t$. It is easy to show by induction on the complexity of a formula $\alpha$ that

$$\begin{aligned}
\mathcal{F}^t, t \vDash \alpha \quad &\text{iff} \quad v(\alpha) = 1,\\
\mathcal{F}^t, x \vDash \alpha \quad &\text{iff} \quad v(\alpha) = 1 \text{ and } \mathcal{F}, x \vDash \alpha^*
\end{aligned}$$

for $x \in F$. Since $\mathcal{F}^t$ is an $L^0$-frame, it follows that $\mathcal{F}, x \vDash \varphi^*$ for all $x \in F$. $\square$ (Claim 1)

Claim 1 shows that instances of axioms in $\pi$ translate to $L^1_C$-derivable formulas, and this could be easily generalized to rules (in particular, modus ponens). However, we also need to establish these translations have polynomial-size proofs. We cannot directly apply Lemma 2.1: our translation does not commute with substitution, thus instances of a fixed axiom do not translate to substitution instances of a single tautology. The claim below shows the next best thing: they are instances of *finitely many* tautologies, and this also applies to proper rules.

**Claim 2** *Let*

$$\varrho = \frac{\alpha_0(p_0, \dots, p_{k-1}), \dots, \alpha_{l-1}(p_0, \dots, p_{k-1})}{\beta(p_0, \dots, p_{k-1})}$$

*be a Frege rule of $L^0_{C,\bot}$-$F$. There is a set of $K \leq 2^k$ rules $\{\varrho_j : j < K\}$ derivable in $L^1_C$ such that for any substitution instance $\sigma(\varrho)$ whose premises are $L^0$-tautologies, the rule $(\sigma(\varrho))^*$ is a substitution instance of some $\varrho_j$.*

*Proof:* Let us consider substitution instances of formulas in variables $p_i$, $i < k$. It is clear from the definition that if we fix the $k$ values $v(\sigma(p_i)) \in \{0, 1\}$, this determines $v(\sigma(\alpha))$ for every formula $\alpha(p_0, \dots, p_{k-1})$. Moreover, in case this makes $v(\sigma(\alpha)) = 1$, the formula $(\sigma(\alpha))^*$ is a substitution instance of a fixed formula: it can be shown by induction on the complexity of $\alpha$ that $(\sigma(\alpha))^* = \sigma^*((\tau_I(\alpha))^*)$, where $\tau_I(p_i) = \bot$ for $i \in I = \{i < k : v(\sigma(p_i)) = 0\}$, and $\sigma^*(p_i) = (\sigma(p_i))^*$ for each $i \notin I$.

Thus, let $K$ be the number of assignments to the variables $\{p_i : i < k\}$ that satisfy $\alpha_0, \dots, \alpha_{l-1}$, and $\{e_j : j < K\}$ be an enumeration of such assignments. Put $I_j = \{i < k : e_j(p_i) = 0\}$, and

$$\varrho_j = \frac{(\tau_{I_j}(\alpha_0))^*, \dots, (\tau_{I_j}(\alpha_{l-1}))^*}{(\tau_{I_j}(\beta))^*}.$$

Since $v(\tau_{I_j}(\alpha_i)) = e_j(\alpha_i) = 1$, and

$$\vdash_{L^1} \big(\tau_{I_j}(\alpha_0) \wedge \cdots \wedge \tau_{I_j}(\alpha_{l-1}) \to \tau_{I_j}(\beta)\big)^*$$

by Claim 1, we have

$$\vdash_{L^1} (\tau_{I_j}(\alpha_0))^* \wedge \cdots \wedge (\tau_{I_j}(\alpha_{l-1})) \to (\tau_{I_j}(\beta))^*,$$

i.e., the rule $\varrho_j$ is valid in $L^1$. On the other hand, assume that $\sigma$ is a substitution such that $L^0$ proves $\sigma(\alpha_0)$, $\dots$, $\sigma(\alpha_{l-1})$. Let $e_j$ be the assignment defined by $e_j(p_i) = v(\sigma(p_i))$. Then the discussion above shows that $(\sigma(\varrho))^* = \sigma^*(\varrho_j)$. □ (Claim 2)

Resuming the proof of Theorem 4.5, Claim 2 shows that all inference steps in $\pi^*$ are instances of a fixed finite set of $L^1_C$-$F$-derivable rules, and as such they can be implemented with linear-size $L^1_C$-$F$-derivations using Lemma 2.1, resulting in a polynomial-size $L^1_C$-$F$ proof of the original formula $\varphi_m$.

This completes the proof of Theorem 4.5 for Frege systems. The argument for *EF* is similar. If we formulate it as circuit Frege, we can use literally the same proof as above. In the original formulation with extension axioms, we define $v$ so that it satisfies all original variables and all extension axioms; the definition of $\varphi^*$ stays unchanged, so that if $q$ is an extension variable with $v(q) = 1$, we put $q^* = q$. In effect, an extension axiom $q \leftrightarrow \alpha$ from $\pi$ disappears in $\pi^*$ if $v(\alpha) = 0$, and transforms into an extension axiom $q \leftrightarrow \alpha^*$ if $v(\alpha) = 1$. The rest of the argument works the same as for Frege. □

**Example 4.6** The conditions of Theorem 4.5 hold for the pair of logics $L^0 = \mathbf{KC}$, $L^1 = \mathbf{IPC}$, or for $L^0 = L^1 = \mathbf{LC}$.

## 4.2 Elimination of $\wedge$

In this section, we explore to what extent we can eliminate conjunctions from proofs by means of the following simple idea: by Lemma 2.2, we can rewrite any formula in a proof as a conjunction of $\wedge$-free formulas, and then we can replace it by the sequence of its conjuncts. There are two principal difficulties with this method:

(i) The construction in Lemma 2.2 substantially changes the shape and structure of the formula. In particular, it does not commute with substitution: if we fix an axiom $\Phi$, then $\wedge$-free translations of substitution instances of $\Phi$ are not themselves substitution instances of a single formula (or a small finite set). This is responsible for the phenomenon in Proposition A.5, but even if we make sure that $\Phi$ does properly axiomatize the relevant $\wedge$-free fragment, it means that there is no a priori reason why translation of instances of $\Phi$ should have poly-size proofs, and we will invest a lot of effort to fix this. It also means that the construction will not work at all for *SF* systems.

(ii) On the face of it, Lemma 2.2 exponentially blows up the sizes of formulas, hence it is no good for polynomial simulations.

Concerning (ii): first, Proposition B.1 exhibits a simple $\{\wedge, \vee\}$-formula that requires exponentially many distinct conjuncts when written as a conjunction of $\wedge$-free formulas. Thus, the method does not stand a chance in the presence of $\vee$, and we will only work with $\vee$-free proofs. (In fact, we will mostly work in the $\{\to, \wedge\}$-fragment, and indicate at the end how to extend the simulation to the $\{\to, \wedge, \bot\}$-fragment.) In particular, our result will only apply to cofinal subframe (i.e., $\{\to, \bot\}$-axiomatized) logics.

Second, Corollary B.10 shows that an $\{\to, \wedge\}$-formula may still require an exponential blow-up when written as a *formula* with conjunctions only at top. Thus, even in this restricted case, our only hope for a polynomial simulation is to work with *circuits*. In particular, the method will only apply to *EF*, not Frege. These constraints put us on the right track:

**Lemma 4.7** *Given an $\{\to, \wedge\}$-circuit $C$ in variables $\{p_i : i < n\}$, we can construct in polynomial time a sequence of $\{\to\}$-circuits $\{C^{p_i} : i < n\}$ such that*

$$\vdash_{\mathbf{IPC}} C \leftrightarrow \bigwedge_{i<n} C^{p_i},$$

*and each $C^{p_i}$ has the form $\Gamma \to p_i$, i.e., $H(C^{p_i}) = p_i$.*

*Proof:* We construct the circuits $D^{p_i}$ for each $i < n$ and each circuit $D$ represented by a node of $C$ by the following induction on depth.

If $D = p_j$ is a variable, we may put $D^{p_j} = p_j$, and $D^{p_i} = p_i \to p_i$ for $i \neq j$.

If $D = D_0 \to D_1$, we can use the equivalence

$$\vdash_{\mathbf{IPC}} D \leftrightarrow \Big(\bigwedge_{i<n} D_0^{p_i} \to \bigwedge_{i<n} D_1^{p_i}\Big) \leftrightarrow \bigwedge_{i<n} (D_0^{p_0} \to \cdots \to D_0^{p_{n-1}} \to D_1^{p_i}).$$

If $D = D_0 \wedge D_1$, we have

$$\vdash_{\mathbf{IPC}} D \leftrightarrow \Big(\bigwedge_{i<n} D_0^{p_i} \wedge \bigwedge_{i<n} D_1^{p_i}\Big) \leftrightarrow \bigwedge_{i<n} (D_0^{p_i} \wedge D_1^{p_i}).$$

Since $D_0^{p_i}$ and $D_1^{p_i}$ are of the form $\Gamma \to p_i$, this means

$$\vdash_{\mathbf{IPC}} D \leftrightarrow \bigwedge_{i<n} \big((D_0^{p_i} \to D_1^{p_i} \to p_i) \to p_i\big)$$

using (22).

It is readily seen that we added at most $O(n^2)$ new gates for each node of $C$, hence the total size of $\bigwedge_i C^{p_i}$ is $O(n^2|C|)$, and it can be computed by a polynomial-time algorithm. $\square$

**Lemma 4.8** *If $C$ is an implicational circuit with head $H(C) = p_h$, there are polynomial-time constructible* **IPC**$_\to$*-CF proofs of the circuits*

$$C^{p_h} \to C, \qquad C \to C^{p_h}, \qquad C^{p_i}$$

*for $i \neq h$.*

*Proof:* By straightforward induction on the construction of the circuit, using Lemma 2.3. For the induction step, let $C = C_0 \to C_1$, in which case

$$C^{p_i} = C_0^{p_0} \to \cdots \to C_0^{p_{n-1}} \to C_1^{p_i}.$$

By the induction hypothesis, we have constructed proofs of all but one of the circuits $C_0^{p_j}$, and of the equivalence of the remaining one with $C_0$. Using Lemma 2.3, we can thus construct proofs of

$$C^{p_i} \rightleftarrows (C_0 \to C_1^{p_i}).$$

For $i \neq h$, we also have a proof of $C_1^{p_i}$, from which we derive $C^{p_i}$. For $i = h$, we have proofs of $C_1^{p_h} \rightleftarrows C_1$, using which we derive $C^{p_h} \rightleftarrows (C_0 \to C_1)$. $\square$

On the level of proofs, we first show that the translation works in the base case of intuitionistic logic, where we need not worry about translations of unforeseen axioms.

**Proposition 4.9** *Given an* **IPC***-EF proof of an implicational formula $\varphi$, we can construct in polynomial time an* **IPC**$_\to$*-EF proof of $\varphi$.*

*Proof:* It will be more convenient to work with the equivalent standard **IPC**-*CF* system. By Theorem 4.3, we may assume the proof only employs the connectives $\to, \wedge$. Thus, let $C_0, \ldots, C_m$ be an **IPC**$_{\to,\wedge}$-*CF* proof of $\varphi = C_m$ in the axiom system given by (1)–(6). Using the transformation from Lemma 4.7, we construct the sequence of implicational circuits

$$C_0^{p_0}, \ldots, C_0^{p_{n-1}}, C_1^{p_0}, \ldots, C_m^{p_0}, \ldots, C_m^{p_{n-1}},$$

and we complete it to an **IPC**$_\to$-*CF* proof as follows.

If $C_i$ is inferred from $C_k = C_l \to C_i$ and $C_l$ by modus ponens, $C_k^{p_j}$ is

$$C_l^{p_0} \to \cdots \to C_l^{p_{n-1}} \to C_i^{p_j}.$$

Thus, we can infer $C_i^{p_j}$ from $C_k^{p_j}$ and $C_l^{p_0}, \ldots, C_l^{p_{n-1}}$ by $n$ applications of modus ponens.

If $C_i$ is an instance of axiom (2), $C_i^{p_j}$ is of the form $\Gamma \to \gamma^{p_j}$, where $\Gamma$ is the set of formulas

$$\left\{\alpha^{p_k}, \alpha^{p_0} \to \cdots \to \alpha^{p_{n-1}} \to \beta^{p_k}, \alpha^{p_0} \to \cdots \to \alpha^{p_{n-1}} \to \beta^{p_0} \to \cdots \to \beta^{p_{n-1}} \to \gamma^{p_k} : k < n\right\}$$

in an appropriate order. Using Lemma 2.3, we can derive

$$\Gamma \to \beta^{p_k}$$

for each $k < n$, and then we derive $\Gamma \to \gamma^{p_j}$ as required.

If $C_i$ is an instance of axiom (4), $C_i^{p_j}$ is of the form

$$\big((\alpha^{p_0} \to \beta^{p_0} \to p_0) \to p_0\big) \to \cdots \to \big((\alpha^{p_{n-1}} \to \beta^{p_{n-1}} \to p_{n-1}) \to p_{n-1}\big) \to \alpha^{p_j}.$$

Using Lemma 2.3, this follows from

$$\big((\alpha^{p_j} \to \beta^{p_j} \to p_j) \to p_j\big) \to \alpha^{p_j},$$

which is an instance of the implicational tautology

$$\big(((x \to z) \to y \to z) \to z\big) \to x \to z$$

as $\alpha^{p_j}$ is of the form $\cdots \to p_j$. Axioms (3), (5), and (6) are treated similarly.

By Lemma 4.8, we can complete the proof by inferring $\varphi$ from the circuit $C_m^{p_h}$. $\square$

Now we would like to generalize Proposition 4.9 to other si logics $L$ axiomatized by implicational formulas. Since our systems are necessarily finitely axiomatized, we may assume $L = \mathbf{IPC} + \Phi$, where $\Phi$ is an implicational formula. In view of Proposition A.5, we need to recognize when $\mathbf{IPC}_{\to} + \Phi = (\mathbf{IPC} + \Phi)_{\to}$, as otherwise we do not stand a chance of eliminating $\wedge$ from $(\mathbf{IPC} + \Phi)$-proofs at all, never mind the length.

**Definition 4.10** For any $n \geq 1$, let $\xi_n$ denote the substitution

$$\xi_n(p_i) = \bigwedge_{j<n} p_{in+j}.$$

Notice that up to associativity of $\wedge$, $\xi_{nm} = \xi_n \circ \xi_m$.

Let $\Phi(p_0, \dots, p_{k-1})$ be an implicational formula with head $H(\Phi) = p_h$, and consider the transformation from Lemma 4.7. As in Lemma 4.8, it is easy to see that the circuits $\big(\xi_n(\Phi)\big)^{p_{in+j}}$ have short $\mathbf{IPC}_{\to}$-$CF$ proofs for $i \neq h$, hence there are short $\mathbf{IPC}_{\to,\wedge}$-$CF$ proofs of

$$\xi_n(\Phi) \leftrightarrow \bigwedge_{j<n} \big(\xi_n(\Phi)\big)^{p_{hn+j}}. \tag{31}$$

Moreover, the circuits $\big(\xi_n(\Phi)\big)^{p_{hn+j}}$ for $j < n$ differ from each other only in inessential ways: specifically, there are short $\mathbf{IPC}_{\to}$-$CF$ proofs of

$$\sigma_{j,j'}\Big(\big(\xi_n(\Phi)\big)^{p_{hn+j}}\Big) \rightleftarrows \big(\xi_n(\Phi)\big)^{p_{hn+j'}}, \tag{32}$$

where $\sigma_{j,j'}$ is the substitution swapping the variables $p_{hn+j}$ and $p_{hn+j'}$. In particular, proofs of $\big(\xi_n(\Phi)\big)^{p_{hn+j}}$ and $\big(\xi_n(\Phi)\big)^{p_{hn+j'}}$ are polynomial-time constructible from each other. In light of this, we put

$$\Phi^{\wedge n} = \big(\xi_n(\Phi)\big)^{p_{hn}},$$

with the understanding that the choice of $j = 0$ here is arbitrary.

**Lemma 4.11** *If $\Phi$ is an implicational formula, the following are equivalent.*

(i) $(\mathbf{IPC} + \Phi)_{\to} = \mathbf{IPC}_{\to} + \Phi$.

(ii) $(\mathbf{IPC}_{\to,\wedge} + \Phi)_{\to} = \mathbf{IPC}_{\to} + \Phi$.

(iii) $\mathbf{IPC}_{\to} + \Phi$ *proves* $\Phi^{\wedge n}$ *for all* $n \in \omega$.

(iv) $\mathbf{IPC}_{\to} + \Phi$ *proves* $\Phi^{\wedge 2}$.

*Proof:*

(i) $\leftrightarrow$ (ii): We already observed that $(\mathbf{IPC} + \Phi)_{\to,\wedge} = \mathbf{IPC}_{\to,\wedge} + \Phi$ as a consequence of Theorem 4.3 (i.e., **IPC** is hereditarily $\{\to, \wedge\}$-conservative over $\mathbf{IPC}_{\to,\wedge}$ in the terminology of Corollary A.3).

(ii) $\leftrightarrow$ (iii): The left-to-right implication follows from (31), as $\xi_n(\Phi)$ is an instance of $\Phi$ qua an axiom of $\mathbf{IPC}_{\to,\wedge} + \Phi$.

On the other hand, assume that an implicational formula $\varphi$ is provable in $\mathbf{IPC}_{\to,\wedge} + \Phi$. This means there are substitutions $\sigma_u$, $u < r$, such that $\mathbf{IPC}_{\to,\wedge}$ proves

$$\bigwedge_{u<r} \sigma_u(\Phi) \to \varphi.$$

Each $\sigma_u(p_i)$ is equivalent to a conjunction of implicational formulas, hence we may assume

$$\sigma_u(p_i) = \bigwedge_{j<n} \psi_{u,i,j}$$

with $\psi_{u,i,j}$ implicational, and $n$ the same for all $u$ and $i$. But then

$$\sigma_u(\Phi) = \tau_u(\xi_n(\Phi)),$$

where $\tau_u(p_{in+j}) = \psi_{u,i,j}$. Using (31), the implicational formula

$$\{\tau_u\big((\xi_n(\Phi))^{p_{hn+j}}\big) : u < r, j < n\} \to \varphi$$

is provable in **IPC**, i.e., in $\mathbf{IPC}_{\to}$. Using (32), each $\big(\xi_n(\Phi)\big)^{p_{hn+j}}$ is provable in $\mathbf{IPC}_{\to} + \Phi^{\wedge n}$, hence so is $\varphi$. By (iii), it is also provable in $\mathbf{IPC}_{\to} + \Phi$.

(iii) $\leftrightarrow$ (iv): The left-to-right implication is trivial. Assume that $\mathbf{IPC}_{\to} + \Phi$ proves $\Phi^{\wedge 2}$, whence there are implicational substitutions $\sigma_u$, $u < r$, such that **IPC** proves

$$\bigwedge_{u<r} \sigma_u(\Phi) \to \Phi^{\wedge 2}.$$

By (31) and (32), **IPC** also proves

$$\bigwedge_{u<r} \sigma_u(\Phi) \to \xi_2(\Phi). \tag{33}$$

Let $n \geq 1$, and apply $\xi_n$ to (33). Since $\xi_n \circ \xi_2 \equiv \xi_{2n}$, we obtain

$$\bigwedge_{u<r} \xi_n\big(\sigma_u(\Phi)\big) \to \xi_{2n}(\Phi).$$

Applying (31) to the implicational formulas $\sigma_u(p_i)$ in place of $\Phi$, we see that each $\xi_n(\sigma_u(p_i))$ is equivalent to a conjunction of $n$ implicational formulas. Thus,

$$\xi_n \circ \sigma_u \equiv \sigma_{n,u} \circ \xi_n$$

for some implicational substitution $\sigma_{u,n}$, and **IPC** proves

$$\bigwedge_{u<r} \sigma_{n,u}\bigl(\xi_n(\Phi)\bigr) \to \xi_{2n}(\Phi).$$

It follows by induction on $n$ that there are implicational substitutions $\tau_{n,u}$, $u < r_n$, such that **IPC** proves

$$\bigwedge_{u<r_n} \tau_{n,u}(\Phi) \to \xi_n(\Phi),$$

hence also the implicational formula

$$\{\tau_{n,u}(\Phi) : u < r_n\} \to \Phi^{\wedge n}.$$

Thus, $\mathbf{IPC}_\to + \Phi$ proves $\Phi^{\wedge n}$. $\square$

**Example 4.12** Gödel–Dummett logic $\mathbf{LC} = \mathbf{IPC} + (p \to q) \lor (q \to p)$ can be axiomatized by the implicational formula

$$\Phi = \bigl((p \to q) \to r\bigr) \to \bigl((q \to p) \to r\bigr) \to r.$$

Up to renaming of variables, $\Phi^{\wedge 2}$ is the formula

$$\begin{aligned}&\bigl((p \to p' \to q) \to (p \to p' \to q') \to r\bigr) \to \bigl((p \to p' \to q) \to (p \to p' \to q') \to r'\bigr) \to\\ &\bigl((q \to q' \to p) \to (q \to q' \to p') \to r\bigr) \to \bigl((q \to q' \to p) \to (q \to q' \to p') \to r'\bigr) \to r.\end{aligned}$$

We may simplify it using the substitution $r' \mapsto r$, as the result

$$\bigl((p \to p' \to q) \to (p \to p' \to q') \to r\bigr) \to \bigl((q \to q' \to p) \to (q \to q' \to p') \to r\bigr) \to r \tag{34}$$

still implies the original formula. We claim that (34) is provable in $\mathbf{IPC}_\to + \Phi$, hence $\mathbf{LC}_\to = \mathbf{IPC}_\to + \Phi$ by Lemma 4.11. This can be shown by formalizing the argument below.

The effect of $\Phi$ is that instead of proving a formula $\varphi$, it suffices to prove $(\alpha \to \beta) \to \varphi$ and $(\beta \to \alpha) \to \varphi$ for a given pair of formulas $\alpha, \beta$; in other words, we may stipulate that $\alpha \to \beta$ or $\beta \to \alpha$ is given as an assumption. By repeating this argument, we see that when proving (34) in $\mathbf{IPC}_\to + \Phi$, we may assume that a (fixed but arbitrary) linear order on the variables $p, p', q, q'$ is given. If the order is such that $\min\{p, p'\} \le \min\{q, q'\}$, then $p \to p' \to q$ and $p \to p' \to q'$ hold, hence the first premise of (34) indeed implies $r$. The other case is symmetric. $\square$

The argument in the proof of Lemma 4.11 shows that for any implicational axiom $\Phi$, the implicational fragment of the logic $\mathbf{IPC} + \Phi$ is axiomatized by

$$\mathbf{IPC}_\to + \{\Phi^{\wedge n} : n \in \omega\}.$$

However, this is an infinite set of axioms, hence it is no good as a basis for a Frege system.

**Question 4.13** *Let $L$ be a si logic axiomatizable over* **IPC** *by an implicational formula (i.e., a finitely axiomatizable subframe si logic). Can it be axiomatized by a formula $\Phi$ satisfying the conditions of Lemma 4.11? In other words, is $L_\to$ finitely axiomatizable?*

**Theorem 4.14** *Let $L$ be a si logic axiomatizable by an implicational formula satisfying the conditions of Lemma 4.11 (in other words, a subframe si logic $L$ such that $L_\to$ is finitely axiomatizable).*

*Given an $L$-EF proof of an implicational formula $\varphi$, we can construct in polynomial time an $L_\to$-EF proof of $\varphi$.*

*Proof:* Write $L = \mathbf{IPC} + \Phi$, where the axiom $\Phi(p_0, \dots, p_{k-1})$ is as in Lemma 4.11.

We proceed in the same way as in the proof of Proposition 4.9, using the same notation. The only difference is that the proof being translated contains substitution instances of the new axiom, say $C_i = \Phi(C_{i,0}, \dots, C_{i,k-1})$. Now, in the bottom-up construction of $C_i^{p_j}$, we first construct implicational circuits $C_{i,l}^{p_j}$ such that $C_{i,l} \equiv \bigwedge_{j<n} C_{i,l}^{p_j}$, and these are then used as black boxes in the construction of $C_i^{p_j}$; thus, the construction proceeds as if $C_{i,l}$ were a conjunction of $n$ new variables, which are substituted with $C_{i,l}^{p_j}$ in the end-result. The upshot is that

$$C_i^{p_j} = \sigma\big(\big(\xi_n(\Phi)\big)^{p_{hn+j}}\big),$$

where $\sigma(p_{ln+u}) = C_{i,l}^{p_u}$, and $H(\Phi) = p_h$. Furthermore, $\big(\xi_n(\Phi)\big)^{p_{hn+j}}$ is essentially a substitution instance of $\Phi^{\wedge n}$ by (32).

Thus, the only thing we need to do to complete the proof is to construct in polynomial time $L_\to$-$CF$ proofs of $\Phi^{\wedge n}$, given $n$ in unary. We will achieve this by analyzing the argument in Lemma 4.11 (iv) $\to$ (iii).

As in (33), let us fix $r \geq 2$, implicational substitutions $\sigma_u$, $u < r$, and an $\mathbf{IPC}_{\to,\wedge}$-$F$-derivation $\pi$ of $\xi_2(\Phi)$ from the set of assumptions $\{\sigma_u(\Phi) : u < r\}$.

We may assume $n = 2^t$ is a power of 2. For each $s \leq t$ and $u < r$, let $\sigma_{2^s,u}$ be the implicational substitution as in Lemma 4.11, so that

$$\xi_{2^s} \circ \sigma_u \equiv \sigma_{2^s,u} \circ \xi_{2^s}. \tag{35}$$

Since $\sigma_{2^s,u}(p_{i2^s+j}) = \big(\xi_{2^s}(\sigma_u(p_i))\big)^{p_{h'2^s+j}}$ where $p_{h'} = H(\sigma_u(p_i))$, we see readily that $\sigma_{2^s,u}$ is given by formulas of size $2^{O(s)}$, and there are $\mathbf{IPC}_{\to,\wedge}$-$F$ proofs of (35) constructible in time $2^{O(s)}$.

By induction on $s \leq t$, we construct $\mathbf{IPC}_{\to,\wedge}$-$CF$-derivations $\pi_s$ of $\xi_{2^s}(\Phi)$ from assumptions that are implicational substitution instances of $\Phi$ as follows.

Let $\pi_0$ be the trivial derivation of $\Phi$ from itself. Assume that $\pi_s$ has already been constructed, we will build $\pi_{s+1}$. We start by taking $\xi_{2^s}(\pi)$, which is a derivation of $\xi_{2^{s+1}}(\Phi)$ from assumptions $\xi_{2^s}(\sigma_u(\Phi))$, $u < r$. Using short proofs of (35), we include subderivations of every $\xi_{2^s}(\sigma_u(\Phi))$ from $\sigma_{2^s,u}(\xi_{2^s}(\Phi))$. Finally, for each $u < r$, we include $\sigma_{2^s,u}(\pi_s)$ as a derivation of $\sigma_{2^s,u}(\xi_{2^s}(\Phi))$.

Since we are working with circuits, we can write $\sigma_{2^s,u}(\pi_s)$ in such a way that it includes only one copy of each substituted variable, hence roughly,

$$|\sigma_{2^s,u}(\pi_s)| = |\pi_s| + \sum_{\substack{i<k \\ j<2^s}} |\sigma_{2^s,u}(p_{i2^s+j})|.$$

Consequently,

$$|\pi_{s+1}| = r|\pi_s| + 2^{O(s)},$$

and this recurrence resolves to

$$|\pi_s| = 2^{O(s)}.$$

For $s = t = \log_2 n$, we obtain an $\mathbf{IPC}_{\to,\wedge}$-$CF$-derivation $\pi_t$ of size $2^{O(t)} = n^{O(1)}$ of $\xi_n(\Phi)$ from implicational substitution instances of $\Phi$, say $\{\tau_v(\Phi) : v < m\}$. It is clear from the recursive description that $\pi_t$ can also be constructed in polynomial time.

Using (31) and the feasible deduction theorem, we can transform $\pi_t$ into an $\mathbf{IPC}_{\to,\wedge}$-$CF$ proof of the implicational circuit

$$\{\tau_v(\Phi) : v < m\} \to \Phi^{\wedge n}.$$

By Proposition 4.9, we can transform it into an $\mathbf{IPC}_{\to}$-$CF$ proof, which we can turn into an $(\mathbf{IPC}_{\to} + \Phi)$-$CF$ proof of $\Phi^{\wedge n}$ by modus ponens. □

We can immediately generalize Theorem 4.14 in the spirit of Theorem 4.3:

**Corollary 4.15** *Let $P$ be a standard $L$-$EF$ system for a si logic $L$ whose proper axiom is an implicational formula satisfying the conditions of Lemma 4.11.*

*Given a $P$-proof $\pi$ of a formula $\varphi$, we can construct in polynomial time a $P$-proof $\pi'$ of $\varphi$ with the following properties:*

(i) *The only conjunctions occurring in $\pi'$ are subformulas of $\varphi$.*

(ii) *The only disjunctions occurring in $\pi'$ are subformulas of $\varphi$, and the only instances of* (9) *in $\pi'$ are with $\gamma$ a subformula of $\varphi$ which is a variable, a disjunction, or $\bot$.*

(iii) *If $\varphi$ is positive, then $\bot$ does not occur in $\pi'$. Otherwise the only instances of* (10) *in $\pi'$ are with $\gamma$ a variable from $\varphi$.*

*Proof:* Let $\hat{\varphi}$ be the implicational formula from Corollary 3.10. We can construct in polynomial time its $L$-$EF$ proof, hence also an $L_{\to}$-$EF$ proof by Theorem 4.14. We apply the substitution $\sigma$ from Corollary 3.10 to this proof. This reintroduces subformulas of $\varphi$, but no other formula fragments, hence the desired restrictions on non-$\to$ connectives in the proof are satisfied. The proof now ends with a formula of the form $\Delta \to \varphi$, where $\Delta$ consists of instances of (4)–(10) satisfying the required conditions; we include them as actual axioms, and derive $\varphi$ by modus ponens. □

The whole construction can be easily adapted to $\{\to,\wedge,\bot\}$-circuits. In Lemmas 4.7 and 4.8 and Proposition 4.9 we handle $\bot$ as if it were an extra variable. If $\Phi$ is a $\{\to,\bot\}$-formula whose head is a variable, Definition 4.10 works unchanged; if $H(\Phi)=\bot$, we have

$$\xi_n(\Phi)\leftrightarrow\big(\xi_n(\Phi)\big)^{\bot}$$

in place of (31), and we duly define $\Phi^{\wedge n}=\big(\xi_n(\Phi)\big)^{\bot}$. (However, when this happens, $\Phi$ is a negated formula, hence $\mathbf{IPC}+\Phi$ is either $\mathbf{IPC}$ or inconsistent; this is not an interesting case.) The same argument as in Lemma 4.11 yields:

**Lemma 4.16** *If $\Phi$ is an $\{\to,\bot\}$-formula, the following are equivalent.*

(i) $(\mathbf{IPC}+\Phi)_{\to,\bot}=\mathbf{IPC}_{\to,\bot}+\Phi$.

(ii) $(\mathbf{IPC}_{\to,\wedge,\bot}+\Phi)_{\to,\bot}=\mathbf{IPC}_{\to,\bot}+\Phi$.

(iii) $\mathbf{IPC}_{\to,\bot}+\Phi$ *proves* $\Phi^{\wedge n}$ *for all* $n\in\omega$.

(iv) $\mathbf{IPC}_{\to,\bot}+\Phi$ *proves* $\Phi^{\wedge 2}$. □

In the end, we obtain the following version of Corollary 4.15.

**Theorem 4.17** *Let $P$ be a standard $L$-EF system for a si logic $L$ whose proper axiom is an $\{\to,\bot\}$-formula satisfying the conditions of Lemma 4.16.*

*Given a $P$-proof $\pi$ of a formula $\varphi$, we can construct in polynomial time a $P$-proof $\pi'$ of $\varphi$ with the following properties:*

(i) *The only conjunctions occurring in $\pi'$ are subformulas of $\varphi$.*

(ii) *The only disjunctions occurring in $\pi'$ are subformulas of $\varphi$, and the only instances of* (9) *in $\pi'$ are with $\gamma$ a subformula of $\varphi$ which is a variable, a disjunction, or $\bot$.*

(iii) *The only instances of* (10) *in $\pi'$ are with $\gamma$ a variable from $\varphi$.* □

## 4.3 Exponential separation

The exponential speed-up of *SF* over *EF* exhibited in Corollary 3.7 applies to **IPC** and many other si logics, but not to their *fragments*, despite the tautologies being purely implicational. We will close this gap by showing that the tautologies have short (poly-time constructible) $\mathbf{IPC}_{\to}$-*SF* proofs. Notice that Theorem 4.3 (or rather its *SF*-version, as mentioned there) provides poly-time constructible $\mathbf{IPC}_{\to,\wedge}$-*SF* proofs of these tautologies. Unfortunately, elimination of $\wedge$ in Section 4.2 does not work for *SF* systems, hence we will have to resort to an ad hoc argument to get it down all the way to $\mathbf{IPC}_{\to}$. Similarly to the proofs of [12, L. 6.26,29], we will start from classical proofs of the tautologies, and judiciously replace bits and pieces to obtain the desired result.

In order to extract $\mathbf{IPC}_{\to}$ proofs out of **CPC** proofs, we will employ an implicational version of the negative (Glivenko) translation. Hopefully, this may be of independent interest, hence the argument is not *completely* ad hoc after all.

**Definition 4.18** The class of *negative* $\{\to, \bot\}$-formulas is the smallest class of formulas such that

- if $\Gamma$ is a (possibly empty) sequence of variables and negative formulas, then $\Gamma \to \bot$ is a negative formula.

Given a negative formula $\varphi$, and a variable $u$, let $\varphi^u$ denote the result of replacing $\bot$ with $u$ in $\varphi$.

**Proposition 4.19** *Given a* **CPC**-*F proof of a negative formula* $\varphi$*, we can construct in polynomial time an* $\mathbf{IPC}_{\to}$-*F proof of* $\varphi^u$.

*Proof:* It will be convenient to formulate classical logic with unbounded fan-in NAND as the only connective; we will write it as $\overline{\Phi}$, where $\Phi$ is a sequence of formulas. It is easy to check that the one-sided sequent[7] calculus with the following rules is a complete proof system for proving *unsatisfiability* of sequences of NAND-formulas, p-equivalent to Frege:

- the usual structural rules of exchange, contraction, and weakening;
- initial sequents $\overline{\Phi}, \Phi$;
- the cut rule
$$\frac{\Gamma, \Phi \qquad \Gamma, \overline{\Phi}}{\Gamma}.$$

Now, if we identify $\overline{\Phi}$ with $\Phi \to \bot$, then NAND-formulas are exactly the variables and negative formulas. If $\Gamma = \langle \varphi_i : i < n \rangle$, let us write $\Gamma^u = \langle \varphi_i^u : i < n \rangle$. Then given a proof $\Gamma_0; \Gamma_1; \dots; \Gamma_n$ of the unsatisfiability of $\Gamma = \Gamma_n$ in the above system, we consider the sequence of formulas
$$\Gamma_0^u \to u; \dots; \Gamma_n^u \to u$$
and make it an $\mathbf{IPC}_{\to}$-*F* proof of $\Gamma^u \to u$: structural rules are handled by Lemma 2.3 (i), initial sequents translate to the tautologies
$$(\Phi^u \to u) \to \Phi^u \to u,$$
and the cut rule translates to
$$\frac{\Gamma^u \to \Phi^u \to u \qquad \Gamma^u \to (\Phi^u \to u) \to u}{\Gamma^u \to u},$$
which has a short derivation by Lemma 2.3 (ii).

Finally, if $\varphi$ is a negative formula, it has the form $\Gamma \to \bot$, where $\Gamma$ consists of negative formulas and variables. A classical Frege proof of $\varphi$ can be transformed into an unsatisfiability proof for the sequent $\Gamma$, which we translate to an $\mathbf{IPC}_{\to}$-*F* proof of the formula $(\Gamma^u \to u) = \varphi^u$ as above. $\square$

[7] Here, the meaning of a sequent $\Gamma = \langle \varphi_0, \dots, \varphi_{n-1} \rangle$ is the *conjunction* $\bigwedge_{i<n} \varphi_i$. Think of it as representing the two-sided sequent $\Gamma \Longrightarrow$ .

**Definition 4.20** Given a monotone formula $\varphi$, we define a negative formula $\sim\varphi$ equivalent to $\neg\varphi$ as follows:

$$
\begin{aligned}
\sim p &= p \to \bot, \\
\sim(\varphi \vee \psi) &= (\sim\varphi \to \sim\psi \to \bot) \to \bot, \\
\sim(\varphi \wedge \psi) &= (\sim\varphi \to \bot) \to (\sim\psi \to \bot) \to \bot, \\
\sim\bot &= \bot \to \bot, \\
\sim\top &= \bot.
\end{aligned}
$$

Using (22), it is easy to see that $(\sim\varphi)^u$ is equivalent in **IPC** to $\varphi \to u$. Thus, it should be obvious that the formulas below have short **IPC**-$F$ proofs. However, this does not give $\mathbf{IPC}_{\to}$-$F$ proofs, as the formulas $\varphi \to u$ are meaningless as such in $\mathbf{IPC}_{\to}$ (in fact, we essentially introduced $\sim\varphi$ and $(\sim\varphi)^u$ to have a stand-in for $\varphi \to u$). Thus, we need to work a little harder.

**Lemma 4.21** *Let $\varphi$ and $\psi$ be monotone formulas. There are polynomial-time constructible $\mathbf{IPC}_{\to}$-$F$ proofs of*

$$\big(((\sim\varphi)^u \to u\big) \to u\big) \rightleftarrows (\sim\varphi)^u, \tag{36}$$

$$\big(\sim(\varphi \vee \psi)\big)^u \to (\sim\varphi)^u, \qquad \big(\sim(\varphi \vee \psi)\big)^u \to (\sim\psi)^u, \tag{37}$$

$$(\sim\varphi)^u \to (\sim\psi)^u \to \big(\sim(\varphi \vee \psi)\big)^u, \tag{38}$$

$$(\sim\varphi)^u \to \big(\sim(\varphi \wedge \psi)\big)^u, \qquad (\sim\psi)^u \to \big(\sim(\varphi \wedge \psi)\big)^u, \tag{39}$$

$$(\sim\varphi)^{v \to u} \rightleftarrows \big(v \to (\sim\varphi)^u\big), \tag{40}$$

$$(v \to u) \to (\sim\varphi)^v \to (\sim\varphi)^u. \tag{41}$$

*Proof:* (36) follows from (22), as $(\sim\varphi)^u$ is of the form $\Gamma \to u$. Then it is straightforward to show (37)–(39).

(40): Clearly, $v \to \big((v \to u) \rightleftarrows u\big)$ gives short proofs of

$$v \to \big((\sim\varphi)^{v \to u} \rightleftarrows (\sim\varphi)^u\big).$$

Then we can derive

$$\big(v \to (\sim\varphi)^u\big) \rightleftarrows \big(v \to (\sim\varphi)^{v \to u}\big) \rightleftarrows (\sim\varphi)^{v \to u},$$

using the fact that $(\sim\varphi)^{v \to u}$ is of the form $\Gamma \to v \to u$.

(41): For any occurrence of a subformula $\psi \subseteq \varphi$, we define a set of formulas $\Gamma_\psi$ by top-to-bottom induction as follows. We put $\Gamma_\varphi = \varnothing$. If $\psi = \psi_L \vee \psi_R$, then $\Gamma_{\psi_L} = \Gamma_{\psi_R} = \Gamma_\psi$. If $\psi = \psi_L \wedge \psi_R$, we put $\Gamma_{\psi_L} = \Gamma_\psi$, and $\Gamma_{\psi_R} = \Gamma_\psi \cup \{\psi_L\}$. Let

$$
\begin{aligned}
\Gamma_\psi^u &= \big\{(\sim\chi)^u \to u : \chi \in \Gamma_\psi\big\}, \\
\psi_*^u &= \Gamma_\psi^u \to (\sim\psi)^u.
\end{aligned}
$$

We will construct proofs of

$$(v \to u) \to \psi_*^v \to \psi_*^u \tag{42}$$

by induction on $\psi \subseteq \varphi$, where we order the subformulas so that the left child of $\psi$ and its subformulas come before the right child and its subformulas, which come before $\psi$. In particular, all formulas in $\Gamma_\psi$ come before $\psi$. Notice that for $\psi = \varphi$, (42) is just (41).

Let $\psi = p$ be a variable. If $\Gamma_\psi$ is empty, (42) is

$$(v \to u) \to (p \to v) \to (p \to u).$$

Otherwise $\Gamma_\psi = \{\chi\} \cup \Gamma_\chi$ for some $\chi$ coming before $\psi$. We have

$$\psi_*^u \rightleftarrows \big(\Gamma_\chi^u \to \big((\sim\chi)^u \to u\big) \to p \to u\big) \rightleftarrows \big(p \to \Gamma_\chi^u \to (\sim\chi)^u\big) \rightleftarrows (p \to \chi_*^u)$$

by (36), hence (42) follows from the induction hypothesis for $\chi$.

If $\psi = \psi_L \wedge \psi_R$, then

$$(\psi_R)_*^u \rightleftarrows \big(\Gamma_\psi^u \to \big((\sim\psi_L)^u \to u\big) \to (\sim\psi_R)^u\big) \rightleftarrows \big(\Gamma_\psi^u \to (\sim\psi)^u\big) \rightleftarrows \psi_*^u,$$

hence the induction hypothesis for $\psi_R$ immediately yields (42) for $\psi$.

If $\psi = \psi_L \vee \psi_R$, we have

$$(\psi_L)_*^u \rightleftarrows \big(\Gamma_\psi^u \to (\sim\psi_L)^u\big), \qquad (\psi_R)_*^u \rightleftarrows \big(\Gamma_\psi^u \to (\sim\psi_R)^u\big).$$

Thus, we can derive

$$\begin{aligned}(v \to u) &\to \big(\Gamma_\psi^v \to (\sim\psi)^v\big) \to \big(\Gamma_\psi^u \to (\sim\psi_L)^u\big)\\ (v \to u) &\to \big(\Gamma_\psi^v \to (\sim\psi)^v\big) \to \big(\Gamma_\psi^u \to (\sim\psi_R)^u\big)\end{aligned}$$

using (37) and the induction hypothesis, whence

$$(v \to u) \to \big(\Gamma_\psi^v \to (\sim\psi)^v\big) \to \big(\Gamma_\psi^u \to (\sim\psi)^u\big)$$

using (38). □

**Theorem 4.22** *There is a sequence of implicational formulas that have polynomial-time constructible* $\mathbf{IPC}_\to$*-SF proofs, but require L-EF proofs of size* $2^{n^{\Omega(1)}}$ *for any si logic L with unbounded branching.*

*Proof:* A somewhat simplified version of the implicational tautologies $\varphi_n$ from Corollary 3.7, translating the tautologies (19) from Theorem 3.2, can be written as

$$\begin{aligned}\Big(\Big(\sim\bigwedge_{i<n}(p_i \vee p_i')\Big)^u \to u\Big) \to \Big(\Big(\sim\bigwedge_{i<n}(s_i \vee s_i')\Big)^v \to u\Big) \to \Big(\Big(\sim\bigwedge_{i<n}(r_i \vee r_i')\Big)^w \to u\Big) \to&\\ \big(\sim\gamma(\vec{p}, \vec{s}, \vec{s'})\big)^v \to \big(\sim\delta(\vec{p'}, \vec{r}, \vec{r'})\big)^w \to u,& \quad (43)\end{aligned}$$

where $\gamma$ and $\delta$ are monotone. Since (19) has short classical Frege proofs, so does

$$\neg\sim\bigwedge_{i<n}(p_i \vee p_i') \to \neg\sim\bigwedge_{i<n}(s_i \vee s_i') \to \neg\sim\bigwedge_{i<n}(r_i \vee r_i') \to \sim\gamma(\vec{p}, \vec{s}, \vec{s'}) \to \sim\delta(\vec{p'}, \vec{r}, \vec{r'}) \to \bot,$$

hence using Proposition 4.19, we can construct short $\mathbf{IPC}_{\to}$-$F$ proofs of

$$\Big(\Big({\sim}\bigwedge_{i<n}(p_i\vee p'_i)\Big)^u\to u\Big)\to\Big(\Big({\sim}\bigwedge_{i<n}(s_i\vee s'_i)\Big)^u\to u\Big)\to\Big(\Big({\sim}\bigwedge_{i<n}(r_i\vee r'_i)\Big)^u\to u\Big)\to \big({\sim}\gamma(\vec p,\vec s,\vec{s'})\big)^u\to\big({\sim}\delta(\vec{p'},\vec r,\vec{r'})\big)^u\to u. \tag{44}$$

Putting

$$\Gamma(\vec p,\vec{p'},\vec r,\vec{r'},u)=\Big\{\Big({\sim}\bigwedge_{i<n}(p_i\vee p'_i)\Big)^u\to u,\Big({\sim}\bigwedge_{i<n}(r_i\vee r'_i)\Big)^u\to u,({\sim}\delta)^u\Big\},$$

we derive

$$\Gamma\to({\sim}\gamma)^v\to\Big(\Big({\sim}\bigwedge_{i<n}(s_i\vee s'_i)\Big)^u\to u\Big)\to(v\to u)\to u$$

using (41). We proceed to prove

$$\Gamma\to({\sim}\gamma)^v\to\Big(\Big({\sim}\bigwedge_{j\le i<n}(s_i\vee s'_i)\Big)^u\to u\Big)\to\Big(\Big({\sim}\bigwedge_{i<j}(s_i\vee s'_i)\Big)^v\to u\Big)\to u \tag{45}$$

by induction on $j\le n$. Assume we have (45) for $j$. Note that $\big({\sim}\bigwedge_{j\le i<n}(s_i\vee s'_i)\big)^u$ is equivalent to

$$\big((s_j\to u)\to(s'_j\to u)\to u\big)\to\Big({\sim}\bigwedge_{j<i<n}(s_i\vee s'_i)\Big)^u.$$

Thus, if we substitute $\top$ for $s_j$, and $s_j\to v$ for $v$, we obtain

$$\Gamma\to\big({\sim}\gamma(s_j/\top)\big)^{s_j\to v}\to\Big(\Big({\sim}\bigwedge_{j<i<n}(s_i\vee s'_i)\Big)^u\to u\Big)\to\Big(\Big({\sim}\bigwedge_{i<j}(s_i\vee s'_i)\Big)^{s_j\to v}\to u\Big)\to u.$$

(It is essential here that neither $s_j$ nor $v$ occur in $\Gamma$.) Using (40) and short proofs of

$$({\sim}\gamma)^v\to s_j\to\big({\sim}\gamma(s_j/\top)\big)^v,$$

we obtain

$$\Gamma\to({\sim}\gamma)^v\to\Big(\Big({\sim}\bigwedge_{j<i<n}(s_i\vee s'_i)\Big)^u\to u\Big)\to\Big[\Big(s_j\to\Big({\sim}\bigwedge_{i<j}(s_i\vee s'_i)\Big)^v\Big)\to u\Big]\to u.$$

A symmetric argument gives the same formula with $s'_j$ in place of $s_j$. Putting $\varphi=\bigwedge_{i<j}(s_i\vee s'_i)$, we have

$$\big(s_j\to({\sim}\varphi)^v\big)\to\big(s'_j\to({\sim}\varphi)^v\big)\to\underbrace{\big(({\sim}\varphi)^v\to v\big)\to\big((s_j\to v)\to(s'_j\to v)\to v\big)\to v}_{\left({\sim}\bigwedge_{i\le j}(s_i\vee s'_i)\right)^v},$$

and using

$$x\to y\to z\vdash((x\to u)\to u)\to((y\to u)\to u)\to(z\to u)\to u,$$

we can derive

$$\Gamma\to({\sim}\gamma)^v\to\Big(\Big({\sim}\bigwedge_{j<i<n}(s_i\vee s'_i)\Big)^u\to u\Big)\to\Big(\Big({\sim}\bigwedge_{i\le j}(s_i\vee s'_i)\Big)^v\to u\Big)\to u,$$

which is (45) for $j+1$.

In the end, $j=n$ gives

$$\Gamma \to (\sim\gamma)^v \to \Big(\Big(\sim \bigwedge_{i<n}(s_i \vee s_i')\Big)^v \to u\Big) \to u.$$

Repeating the same argument with $\delta, w, r_i, r_i'$ in place of $\gamma, v, s_i, s_i'$ yields (43). $\square$

# 5 Conclusion

The diverse results in this paper show that by and large, the proof complexity of common calculi for intuitionistic logic is concentrated on implicational formulas. On the one hand, we do not miss anything substantial by restricting attention to the lengths of proofs of purely implicational tautologies. On the other hand, we may assume intuitionistic proofs to come in a sort of normal form where the bulk of the proof takes place in the implicational fragment of **IPC**, except for a small predetermined set of nonimplicational axioms that essentially reconstruct the nonimplicational subformulas of the tautology being proved. To some extent the same is true of other superintuitionistic logics.

Nevertheless, our work inevitably revealed various rough spots where our methods leave something to be desired, especially in connection with extensions of intuitionistic logic. In particular, our results on elimination of conjunctions from proofs in Section 4.2 may be limited more by the specific method we employ rather than intrinsically:

**Question 5.1** *Can we extend Theorem 4.14 to si logics whose axioms involve disjunctions, under suitable conditions on their axioms?*

**Question 5.2** *Can we extend Theorem 4.14 to* **IPC**-*SF or other substitution Frege systems?*

Recall that we stated another problem as Question 4.13.

For Question 5.2, it is unclear whether we should expect a positive or a negative answer. Indeed, a superpolynomial speedup of **IPC**-*SF* over $\mathbf{IPC}_{\to}$-*SF* would be an exciting result. Likewise, it would be very interesting if we could turn some of the lower bounds in Appendix B into lower bounds on the lengths of proofs.

Let us also mention the following open problems in the area of intuitionistic proof complexity.

**Question 5.3** *Does* **IPC**-*F polynomially simulate* **IPC**-*EF?*

**Question 5.4** *Can we prove an unconditional lower bound on* **IPC**-*SF proofs?*

While neither question is particularly connected to implicational fragments, we note that they would be interesting to resolve even for proper fragments of **IPC**, or another si logic.

**Acknowledgements**

I am indebted to Pavel Hrubeš for suggesting the topic of this paper, and fruitful discussion, in particular drawing my attention to the constructions in Sections 4.1 and 4.2. I also thank the anonymous referee for useful suggestions to improve the paper.

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013) / ERC grant agreement no. 339691. The Institute of Mathematics of the Czech Academy of Sciences is supported by RVO: 67985840.

## References

[1] Willem J. Blok and Don L. Pigozzi, *Algebraizable logics*, Memoirs of the American Mathematical Society 77 (1989), no. 396.

[2] Stanley N. Burris and Hanamantagouda P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics vol. 78, Springer, 1981.

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

[4] Samuel R. Buss and Pavel Pudlák, *On the computational content of intuitionistic propositional proofs*, Annals of Pure and Applied Logic 109 (2001), no. 1–2, pp. 49–64.

[5] Alexander V. Chagrov and Michael Zakharyaschev, *Modal logic*, Oxford Logic Guides vol. 35, Oxford University Press, 1997.

[6] Petr Cintula and George Metcalfe, *Admissible rules in the implication-negation fragment of intuitionistic logic*, Annals of Pure and Applied Logic 162 (2010), no. 2, pp. 162–171.

[7] Alfred Horn, *The separation theorem of intuitionist propositional calculus*, Journal of Symbolic Logic 27 (1962), no. 4, pp. 391–399.

[8] Pavel Hrubeš, *Lower bounds for modal logics*, Journal of Symbolic Logic 72 (2007), no. 3, pp. 941–958.

[9] ———, *A lower bound for intuitionistic logic*, Annals of Pure and Applied Logic 146 (2007), no. 1, pp. 72–90.

[10] ———, *On lengths of proofs in non-classical logics*, Annals of Pure and Applied Logic 157 (2009), no. 2–3, pp. 194–205.

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

[12] ———, *Substitution Frege and extended Frege proof systems in non-classical logics*, Annals of Pure and Applied Logic 159 (2009), no. 1–2, pp. 1–48.

[13] Dick de Jongh and Zhiguang Zhao, *Positive formulas in intuitionistic and minimal logic*, in: 10th International Tbilisi Symposium on Logic, Language, and Computation, TbiLLC 2013 (M. Aher, D. Hole, E. Jeřábek, and C. Kupke, eds.), Lecture Notes in Computer Science vol. 8984, Springer, 2015, pp. 175–189.

[14] Jan Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications vol. 60, Cambridge University Press, 1995.

[15] ———, *Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic*, Journal of Symbolic Logic 62 (1997), no. 2, pp. 457–486.

[16] Grigori Mints and Arist Kojevnikov, *Intuitionistic Frege systems are polynomially equivalent*, Zapiski Nauchnyh Seminarov POMI 316 (2004), pp. 129–146.

[17] Albert Visser, Johan van Benthem, Dick de Jongh, and Gerard R. Renardel de Lavalette, *NNIL, a study in intuitionistic propositional logic*, in: Modal logic and process algebra, a bisimulation perspective (A. Ponse, M. de Rijke, and Y. Venema, eds.), CSLI Lecture Notes vol. 53, CSLI Publications, Stanford, 1995, pp. 289–326.

[18] Andrzej Wroński, *On reducts of intermediate logics*, Bulletin of the Section of Logic 9 (1980), no. 4, pp. 176–179.

# A Axiomatization of fragments

This section makes an exposition of a result on fragments of si logics originally due to Wroński [18], related to elimination of connectives from Section 4.

We are interested in the following question: if $C$ is a set of connectives, is it true that whenever $L$ is a si logic axiomatized over $\mathbf{IPC}$ by a $C$-formula $\Phi$, the $C$-fragment of $L$ is axiomatized by $\Phi$ over $\mathbf{IPC}_C$? In other words, is every axiomatic extension of $\mathbf{IPC}_C$ the $C$-fragment of a si logic? While trivially $\mathbf{IPC}_C + \Phi \subseteq (\mathbf{IPC} + \Phi)_C$, this inclusion may a priori be strict: a proof of a $C$-formula $\varphi$ in $\mathbf{IPC} + \Phi$ may use substitution instances $\sigma(\Phi)$ involving arbitrary connectives, whereas a proof in $\mathbf{IPC}_C + \Phi$ only allows substitutions by $C$-formulas. Let us first properly introduce some terminology.

**Definition A.1** Let $C, C_0, C_1 \subseteq C_{\mathbf{IPC}}$ be such that $\to \in C \subseteq C_0 \cap C_1$. We say that $\mathbf{IPC}_{C_0}$ *is hereditarily $C$-conservative over* $\mathbf{IPC}_{C_1}$ if for all sets of $C$-formulas $X$, the $C$-fragment of $\mathbf{IPC}_{C_0} + X$ is included in $\mathbf{IPC}_{C_1} + X$.

**Observation A.2** *Let $C, C_0, C_1$ be as in Definition A.1. If $C_0 \subseteq C_1$, then* $\mathbf{IPC}_{C_0}$ *is hereditarily $C$-conservative over* $\mathbf{IPC}_{C_1}$.

*Let $C', C'_0, C'_1$ also obey the restrictions from Definition A.1, and $C' \subseteq C$, $C'_0 \subseteq C_0$, and $C_1 \subseteq C'_1$. If* $\mathbf{IPC}_{C_0}$ *is hereditarily $C$-conservative over* $\mathbf{IPC}_{C_1}$*, then* $\mathbf{IPC}_{C'_0}$ *is hereditarily $C'$-conservative over* $\mathbf{IPC}_{C'_1}$*.* $\square$

A partial positive answer is provided by Theorem 4.3, which shows that we do not need substitutions with $\vee$ or $\bot$ if these connectives do not appear in $\Phi$ or $\varphi$:

**Corollary A.3** *If $C, C_0, C_1$ are as in Definition A.1, and $\wedge \in C_1$, then* $\mathbf{IPC}_{C_0}$ *is hereditarily $C$-conservative over* $\mathbf{IPC}_{C_1}$. $\square$

However, these results for $\vee$ and $\perp$ cannot be directly generalized to $\wedge$—in fact, Observation A.2 and Corollary A.3 cannot be improved:

**Theorem A.4 (Wroński [18])** *Let $C, C_0, C_1$ be as in Definition A.1. The following are equivalent:*

(i) $\mathbf{IPC}_{C_0}$ *is hereditarily $C$-conservative over* $\mathbf{IPC}_{C_1}$.

(ii) $\wedge \in C_1$ *or* $C_0 \subseteq C_1$.

(Wroński only explicitly mentions the cases with $C = C_1$, but his argument proves the formulation given here. He also considers fragments without implication, which we are not interested in.)

For completeness, we will prove Theorem A.4 below. In view of Observation A.2 and Corollary A.3, it suffices to show the three non-conservativity results in the next proposition.[8] We assume familiarity with basic universal algebra and algebraic methods in propositional logics, see e.g. [2, 1]. For typographic convenience, we will write $L \vdash \varphi$ instead of $\vdash_L \varphi$.

**Proposition A.5**

(i) $\mathbf{IPC}_{\to,\wedge}$ *is not hereditarily $\to$-conservative over* $\mathbf{IPC}_{\to,\vee,\perp}$.

(ii) $\mathbf{IPC}_{\to,\perp}$ *is not hereditarily $\to$-conservative over* $\mathbf{IPC}_{\to,\vee}$.

(iii) $\mathbf{IPC}_{\to,\vee}$ *is not hereditarily $\to$-conservative over* $\mathbf{IPC}_{\to,\perp}$.

*Proof:* We will work for the moment with the implicational fragment.

$\mathbf{IPC}_{\to}$ is regularly algebraizable wrt the class of $\to$-subreducts of Heyting algebras, which is the variety of BCKW (aka Hilbert) algebras, hence axiomatic extensions of $\mathbf{IPC}_{\to}$ correspond to subvarieties $V \subseteq$ BCKW. By Diego's theorem [5, §5.4], BCKW is locally finite, hence $V$ is generated by its finite subdirectly irreducible (sdi) algebras. Congruences on a BCKW-algebra $\langle A, 1, \to\rangle$ are determined by filters (subsets $F \subseteq A$ such that $1 \in F$, and $a, a \to b \in F$ implies $b \in F$). Every element $a \in A$ generates the principal filter $a{\uparrow}$. It follows that $A$ is sdi iff it has an *opremum*: a largest element strictly below 1.

Let $A$ be a finite sdi BCKW-algebra with opremum $o$. The *characteristic formula of $A$* is the formula

$$\varphi_A = \Xi_A \to p_o$$

in variables $\{p_a : a \in A\}$, where the set of formulas $\Xi_A$ consists of

$$(p_a \to p_b) \to p_{a\to b}, \qquad p_{a\to b} \to (p_a \to p_b)$$

[8] We mention that item (iii) is relevant to [6].

for $a, b \in A$. Clearly, $\varphi_A$ is invalid in $A$ under the valuation $v(p_a) = a$. On the other hand, let $v$ be a valuation in a BCKW-algebra $B$ such that $v(\varphi_A) \neq 1$. The filter generated by $v(\Xi_A)$, which is

$$F = \{b \in B : v(\Xi_A) \to b = 1\},$$

does not contain $v(p_o)$, hence $v$ induces a valuation $v_F$ on the quotient algebra $B/F$ such that $v_F(\Xi_A) = 1$, and $v_F(p_o) < 1$. Then $v_F(p_{a\to b}) = v_F(p_a) \to v_F(p_b)$ by the definition of $\Xi_A$, hence the mapping $f\colon A \to B/F$ defined by $f(a) = v_F(p_a)$ is a homomorphism. Its kernel does not contain the generator $o$ of the least nontrivial congruence on $A$, hence $f$ is in fact an embedding. Thus, we have established that $B \nvDash \varphi_A$ iff $A \in \mathrm{S}(\mathrm{H}(B))$.

With $A$ as above, let $B$ be a sdi algebra in $\mathrm{H}(\mathrm{S}(\mathrm{P}(A)))$. If $B$ is finite, $A \nvDash \varphi_B$, hence $B \in \mathrm{S}(\mathrm{H}(A))$. If $B$ were infinite, let $B'$ be its finite(ly generated) subalgebra including the opremum. Then $B' \in \mathrm{S}(\mathrm{H}(A))$ by the previous argument, which gives a contradiction if we choose $|B'| > |A|$.[9]

Now, assume that $A$ is a finite sdi $\mathbf{IPC}_{C_1}$-algebra, and that $\mathbf{IPC}_{C_0}$ is hereditarily $\to$-conservative over $\mathbf{IPC}_{C_1}$. Let $X$ be the set of $\to$-formulas valid in $A$. We have $\mathbf{IPC}_{C_1} + X \nvdash \varphi_A$ as witnessed by $A$, hence $\mathbf{IPC}_{C_0} + X \nvdash \varphi_A$, which means that there exists an $\mathbf{IPC}_{C_0}$-algebra $B$ such that $B \restriction \to \in H(S(P(A \restriction \to)))$, and $B \nvDash \varphi_A$. We may assume $B$ is sdi. Since $B{\restriction}{\to}$ and $B$ have the same congruences, $B{\restriction}{\to}$ is also sdi. By the above, $B{\restriction}{\to} \in S(H(A{\restriction}{\to}))$; on the other hand, $B \nvDash \varphi_A$ implies $A \restriction \to \in S(H(B \restriction \to))$, and as $A$ is finite, this gives $A \restriction \to \simeq B \restriction \to$. In other words, $A$ itself must be an $\mathbf{IPC}_{C_0}$-algebra to begin with. (Note that $\to$ determines $\leq$, hence also the lattice operations $\wedge, \vee, \bot$. Thus, $A{\restriction}{\to}$ has at most one expansion to an $\mathbf{IPC}_{C_0}$-algebra.)

It remains to find specific counterexamples for the three statements.

(i): Let $B$ be the Heyting algebra with domain $\{1, o, a, b, c, d, \bot\}$, where $\bot < c < b < o < 1$, $\bot < d < a < o$, and $d < b$. Put $A = B \smallsetminus \{d\}$, and note that $A$ is a $\{\to, \vee, \bot\}$-subalgebra of $B$, and it is sdi with opremum $o$. However, $A$ is not an $\mathbf{IPC}_{\to,\wedge}$-algebra, being a non-distributive lattice.

For (ii), let $B$ be the Heyting algebra with domain $\{1, o, a, b, \bot\}$, where $\bot < \{a, b\} < o < 1$, and $A$ be its $\{\to, \vee\}$-subalgebra $B \smallsetminus \{\bot\}$, which is sdi, and has no least element.

For (iii), we can use $B = \{1, o, a, b, m, c, d, \bot\}$, where $\bot < \{c, d\} < m < \{a, b\} < o < 1$, and $A = B \smallsetminus \{m\}$, which is a $\{\to, \bot\}$-subalgebra of $B$, but not an $\mathbf{IPC}_{\to,\vee}$-algebra, as $c$ and $d$ have no join in $A$. $\square$

**Example A.6** To illustrate the abstract nonsense with actual formulas, put

$$\begin{aligned}
\varphi &= && \big((x \to y) \to z\big) \to \big((y \to x) \to z\big) \to z, \\
\psi &= (w \to x) \to (w \to y) \to && \big((x \to y) \to z\big) \to \big((y \to x) \to z\big) \to z.
\end{aligned}$$

Clearly, $\mathbf{IPC}_{\to,\wedge} + \psi$ and $\mathbf{IPC}_{\to,\bot} + \psi$ derive $\varphi$ by substituting $x \wedge y$ or $\bot$ for $w$. However, $\mathbf{IPC}_{\to,\vee} + \psi \nvdash \varphi$, as $\psi$ is valid in the algebra $A$ in the proof of (ii) above, but $\varphi$ is not.

[9] Alternatively, we could show that BCKW is a congruence-distributive variety, and apply Jónsson's lemma for the slightly weaker conclusion $B \in \mathrm{H}(\mathrm{S}(A))$.

Note that $\mathbf{IPC} + \varphi = \mathbf{IPC} + (x \to y) \vee (y \to x)$ is just the Gödel–Dummett logic $\mathbf{LC}$, and one can show $\mathbf{IPC}_{\to,\dots} + \varphi = \mathbf{LC}_{\to,\dots}$; cf. Example 4.12.

# B Complexity of formulas in intuitionistic logic

In this section, we present several lower bounds on formula complexity in intuitionistic fragments. Our main aim is to show that constraints employed in Section 4.2 are necessary. That is, Lemma 2.2 tells us that every formula $\varphi$ can be in $\mathbf{IPC}$ transformed into a conjunction

$$\bigwedge_{i<m} \varphi_i \tag{46}$$

of $\wedge$-free formulas while not introducing any new connectives; for the $\{\to, \wedge\}$ and $\{\to, \wedge, \bot\}$ fragments, this can be done in such a way that $m$ is at most the number of variables (plus 1 for $\bot$), and the circuit size of $\varphi_i$ is polynomial in the circuit size of $\varphi$ (Lemma 4.7). We will show that $m$ needs to be exponentially large for formulas with $\vee$ (Proposition B.1), and that the formula size of $\varphi_i$ may need to be exponentially large even for $\{\to, \wedge\}$-formulas (Proposition B.8 and Corollary B.10). In the course of establishing the latter, we will also prove a linear lower bound on implication nesting depth (Proposition B.3).

We first deal with disjunctions.

**Proposition B.1** *Let $L \subseteq \mathbf{KC}$ be a si logic, and $\varphi$ be a monotone formula. The optimal (in terms of $m$) expression of $\varphi$ as a conjunction*

$$\vdash_L \varphi \leftrightarrow \bigwedge_{i<m} \varphi_i \tag{47}$$

*with $\varphi_i$ $\wedge$-free is the (unique) nonredundant monotone conjunctive normal form of $\varphi$. In particular, the formula*

$$\varphi = \bigvee_{i<n} (p_i \wedge q_i)$$

*of size $O(n)$ cannot be written as a conjunction of less than $2^n$ $\wedge$-free formulas.*

*Proof:* Assume $\varphi$ uses the variables $\{p_i : i < n\}$. Consider the model $\mathcal{M} = \langle \mathcal{P}([n]), \subseteq, \vDash \rangle$, where $[n] = \{0, \dots, n-1\}$, and $I \vDash p_i$ iff $i \in I$. Since any formula defines an up-set, and each cone $I{\uparrow}$ in $\mathcal{M}$ is definable by $\bigwedge_{i \in I} p_i$, every formula is in $\mathcal{M}$ equivalent to a monotone formula.

In fact, we claim that any $\{\to, \vee, \bot\}$-formula $\psi$ is in $\mathcal{M}$ equivalent to $\top$ or to a (possibly empty) disjunction of variables. This follows by induction on the complexity of $\psi$: it is enough to check that

$$\mathcal{M} \vDash \Big( \bigvee_{i \in I} p_i \to \bigvee_{j \in J} p_j \Big) \leftrightarrow \begin{cases} \top & \text{if } I \subseteq J, \\ \bigvee_{j \in J} p_j & \text{otherwise.} \end{cases}$$

To see this, assume $i \in I \smallsetminus J$, and $K \nvDash \bigvee_{j \in J} p_j$, which means $J \cap K = \varnothing$. Then $K' = K \cup \{i\}$ satisfies $K \le K' \vDash \bigvee_I p_i$, and $K' \nvDash \bigvee_J p_j$, as $J \cap K' = \varnothing$. Thus,

$$K \nvDash \bigvee_{i \in I} p_i \to \bigvee_{j \in J} p_j.$$

Now, if (47) holds, then $\varphi$ is in $\mathcal{M}$ equivalent to a monotone formula

$$\varphi^* = \bigwedge_{i<m} \varphi_i^*,$$

where each $\varphi_i^*$ is a disjunction of variables (or $\top$, which can be omitted). However, if $\alpha, \beta$ are monotone formulas, then $\mathcal{M} \vDash \alpha \to \beta$ only when $\alpha \to \beta$ is provable (in **IPC**, $L$, or **CPC**, this is all equivalent): if $v$ is a variable assignment such that $v(\alpha) = 1$ and $v(\beta) = 0$, then $I = \{i : v(p_i) = 1\}$ satisfies $I \vDash \alpha$ and $I \nvDash \beta$. Thus,

$$\vdash \varphi \leftrightarrow \varphi^*,$$

where $\varphi^*$ is a monotone CNF with $m$ clauses. $\square$

**Remark B.2** In **CPC**, any formula is equivalent to a $\{\to, \bot\}$-formula, and any positive formula $\varphi$ can be written as a conjunction of $m$ $\{\to\}$-formulas, where $m$ is the minimal length of a conjunction of variables that implies $\varphi$ (for monotone $\varphi$, this is the length of the shortest conjunction in its monotone DNF): indeed, if $\bigwedge_{i \in I} p_i$ implies $\varphi$, then

$$\varphi \leftrightarrow \bigwedge_{i \in I} (p_i \vee \varphi),$$

and a Boolean function can be expressed by a $\{\to\}$-formula iff it majorizes a variable.

Now we turn to $\{\to, \wedge\}$-formulas. While every $\{\to, \wedge\}$-circuit is equivalent to a polynomially larger conjunction of $\{\to\}$-circuits, we will prove that a $\{\to, \wedge\}$-formula may need exponential size when expressed as a conjunction of $\wedge$-free formulas (46).

First however, it is not hard to see that if $\varphi$ is a $\{\to, \wedge\}$-formula of depth $d$, we can make the size of (46) to be $|\varphi|^{O(d)}$; this is a quasipolynomial bound in the ideal case when $d = O(\log |\varphi|)$. Thus, if we want exponential lower bounds on the size of (46), we should better make sure that $\varphi$ cannot be written by a formula of low depth.

In **CPC**, every formula can be transformed into a polynomially larger formula of logarithmic depth by Spira's lemma. In contrast, we will show that in **IPC**, formulas may require linear depth, even using a rather relaxed measure—we only count the nesting of implications on the left:

$$\begin{aligned}
\mathrm{ld}_\to(p) = \mathrm{ld}_\to(\bot) = \mathrm{ld}_\to(\top) &= 0, \\
\mathrm{ld}_\to(\varphi \wedge \psi) = \mathrm{ld}_\to(\varphi \vee \psi) &= \max\{\mathrm{ld}_\to(\varphi), \mathrm{ld}_\to(\psi)\}, \\
\mathrm{ld}_\to(\varphi \to \psi) &= \max\{\mathrm{ld}_\to(\varphi) + 1, \mathrm{ld}_\to(\psi)\}.
\end{aligned}$$

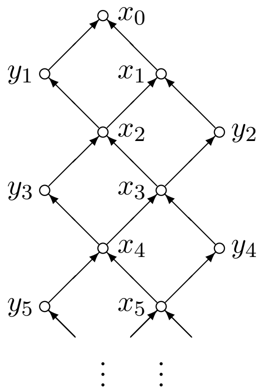



Figure 1: Kripke frame used in Proposition B.3

Let $U_n = \{\varphi : \mathrm{ld}_{\to}(\varphi) \le n\}$; $U_1$-formulas are also called NNIL. These formula classes were studied in [17]. There are only finitely many $U_n$-formulas up to equivalence over a finite set of variables.

If $\mathcal{M} = \langle M, \le, \vDash\rangle$ is a Kripke model for a finite set of variables $V$, and $x, y \in M$, let us write

$$x \to_n y \quad \text{iff} \quad \forall \varphi \in U_n \, (x \vDash \varphi \Rightarrow y \vDash \varphi).$$

Notice that $\to_n$ is transitive, and contains $\le$. Clearly,

$$x \to_0 y \quad \text{iff} \quad \forall p \in V \, (x \vDash p \Rightarrow y \vDash p).$$

By a variant of a characterization from [17], we have $x \to_n y$ if and only if there is a family of relations $\langle \Rightarrow_k : k \le n\rangle$ such that

(i) $x' \Rightarrow_n y$ for some $x' \ge x$;

(ii) $u \Rightarrow_k v$ implies $u \to_0 v$;

(iii) $u \Rightarrow_{k+1} v$ implies $v \Rightarrow_k u$;

(iv) whenever $u \Rightarrow_{k+1} v \le v'$, there is $u'$ such that $u \le u' \Rightarrow_{k+1} v'$.

(The reader should think of $u \Rightarrow_k v$ as an under-approximation of $u \to_k v \to_{k-1} u$.)

Let us define the formula

$$\alpha_n(p_0, \dots, p_n) = (\cdots((p_0 \to p_1) \to p_2) \to \cdots) \to p_n \tag{48}$$

for $n \ge 0$. That is, $\alpha_0 = p_0$, and $\alpha_{n+1} = (\alpha_n \to p_{n+1})$.

**Proposition B.3** *If $L$ is a si logic included in $\mathbf{KC} + \mathbf{BW_2}$, and $n \ge 1$, the implicational $U_n$-formula $\alpha_n$ is not equivalent over $L$ to any $U_{n-1}$-formula.*

*Proof:* We consider the model $\mathcal{M} = \langle M, \leq, \vDash \rangle$, where

$$M = \{x_n : n \geq 0\} \cup \{y_n : n \geq 1\},$$
$$x_n < x_{n-1}, \quad x_{n+1} < y_n < x_{n-1},$$
$$y_1 \vDash p_0,$$
$$x_n, y_n \vDash p_{n+1}.$$

(See Figure 1.) A straightforward induction on $n$ shows

$$u \vDash \alpha_n \quad \text{iff} \quad u \geq y_{n+1},$$

thus the result will follow if we prove $y_{n+1} \to_{n-1} x_{n+1}$ (in fact, also $x_{n+1} \to_n y_{n+1}$). To this end, it is enough to define relations $\Rightarrow_n$ for $n \in \omega$ by

$$\Rightarrow_n = \mathrm{id}_M \cup \{\langle x_m, y_m \rangle : m \geq n+1\} \cup \{\langle y_m, x_m \rangle : m \geq n+2\},$$

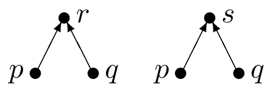
and observe that the conditions (i)–(iv) from the characterization of $\to_n$ are satisfied. $\square$

**Definition B.4** With every $\{\to, \bot\}$-formula $\varphi(\vec{p})$, we associate a rooted tree $T_\varphi$ whose nodes are labelled by variables $p_i$ or by $\bot$ (these will be collectively called *atoms*) using the following inductive definition: if

$$\varphi = \varphi_0 \to \cdots \to \varphi_{n-1} \to v,$$

where $n \geq 0$, and $v$ is an atom (i.e., $v = H(\varphi)$), then $T_\varphi$ has a root labelled by $v$ with children $T_{\varphi_0}, \ldots, T_{\varphi_{n-1}}$.

More generally, we associate each $\wedge$-free formula with a labelled forest $T_\varphi$: if $\varphi$ is an atom, then $T_\varphi$ is the singleton tree labelled $\varphi$; if $\varphi = \psi \vee \chi$, then $T_\varphi$ is the disjoint union of $T_\psi$ and $T_\chi$; if $\varphi = \psi \to \chi$, then $T_\varphi$ is obtained from $T_\chi$ by attaching copies of all trees from $T_\psi$ as children to roots of all trees of $T_\chi$. For example, this is $T_{p\vee q\to r\vee s}$:




A *path* in $T_\varphi$ is a sequence of labels of nodes $x_0, \ldots, x_n \in T_\varphi$, where $x_{i+1}$ is the parent of $x_i$ for each $i < n$, and $x_n$ is a root.

**Lemma B.5** *Let $\mathcal{M}$ be the Kripke model considered in the proof of Proposition B.3. Put $\beta_n = \alpha_n \to p_n$ and $\gamma_n = \alpha_n \wedge p_{n+1}$ for $n \geq 0$; notice that in $\mathcal{M}$, $\beta_0 \equiv \top$, $\beta_1 \equiv \alpha_0 \equiv p_0$, and $\gamma_0 \equiv p_1$.*

*Every $\{\to, \vee\}$-formula is in $\mathcal{M}$ equivalent to an implicational formula, namely $\top$, $p_n$, $\alpha_n$, or $\beta_n$ for some $n \geq 1$. A $\wedge$-free formula is equivalent to an implicational formula as above, or to $\bot$. An arbitrary formula is equivalent either to one of the above mentioned, or to $\gamma_n$ for some $n \geq 1$.*

*If $\varphi$ is a $\{\to, \bot\}$-formula not equivalent to $\top$, then $T_\varphi$ has a path of the following form, depending on the canonical equivalent of $\varphi$:*

| | |
|---|---|
| $p_n,\ n \geq 1$ | $p_n$ |
| $\perp$ | $\perp$ |
| $p_0 \equiv \alpha_0 \equiv \beta_1$ | $p_0 p_1^{2k}$ |
| $\alpha_n,\ n \geq 1$ | $p_0 p_1^{2k_1+1} \dots p_n^{2k_n+1}$ |
| $\beta_n,\ n \geq 2$ | $p_0 p_1^{2k_1+1} \dots p_{n-1}^{2k_{n-1}+1} p_n^{2k_n+2}$ |

*The same also holds for $\wedge$-free formulas $\varphi$ not equivalent to $\top$ or $\beta_n$ for $n \geq 2$.*

*Proof:* Recall that $u \vDash \alpha_n$ iff $u \geq y_{n+1}$. Also, we have $u \vDash \beta_n$ iff $u \geq y_n$ or (for $n > 1$) $u \geq y_{n-1}$; and $u \vDash \gamma_n$ iff $u \geq x_n$.

Let $F = \{\top, p_n, \alpha_n, \beta_n : n \geq 1\}$, and $F^\perp = F \cup \{\perp\}$. In $\mathcal{M}$, every negated formula is equivalent to $\top$ or $\perp$, and for all $n \geq 1$, $\mathcal{M}$ satisfies

$$p_n \to \beta_n, \quad \beta_n \to p_{n+1}, \quad p_n \to \alpha_n, \quad \alpha_n \to \beta_{n+1}. \tag{49}$$

Using this, it is not hard to verify that for any $\psi, \chi \in F^\perp$, $\psi \to \chi$ is equivalent to $\top$ or $\chi$, and $\psi \vee \chi$ is equivalent to $\psi$ or $\chi$, with only the following exceptions, where $n \geq 1$ ($n > 1$ in the cases involving $n - 1$):

$$\left.\begin{aligned} (\alpha_{n-1} \to p_n) \equiv (\beta_n \to p_n) \equiv \alpha_n, \\ (\alpha_n \to p_n) \equiv \beta_n, \\ (\alpha_n \vee p_{n+1}) \equiv (\alpha_n \vee \beta_n) \equiv (\alpha_n \vee \alpha_{n-1}) \equiv \beta_{n+1}. \end{aligned}\right\} \tag{50}$$

This shows that $F$ and $F^\perp$ are closed under $\to$ and $\vee$, hence every $\{\to, \vee\}$-formula is equivalent to a formula from $F$, and every $\{\to, \vee, \perp\}$-formula to a formula from $F^\perp$. A general formula is equivalent to a conjunction of $\wedge$-free formulas; using (49), the only cases where the conjunction of elements of $F^\perp$ is different from one of the conjuncts are $\alpha_n \wedge \beta_n \equiv p_n$, and $\alpha_n \wedge \alpha_{n+1} \equiv \alpha_n \wedge p_{n+1} = \gamma_n$.

Assume $\varphi$ is an $\{\to, \perp\}$-formula not equivalent to $\top$. We can simplify $\varphi$ by repeatedly replacing subformulas $\psi \to \chi$ with $\chi$ when equivalent, yielding a new formula $\varphi'$; this transformation amounts to removing the subtree $T_\psi$ from $T_\varphi$, hence any path in $T_{\varphi'}$ is also a path in $T_\varphi$. Notice that in particular, all subformulas $\psi$ equivalent to $\top$ get deleted. By (50), $\varphi'$ contains no nontrivial formulas equivalent to $p_n$ for $n \geq 1$ or to $\perp$, and the only implications left in $\varphi'$ have variables on the right-hand side, i.e., $T_{\varphi'}$ consists of a single path. It is then easy to check that this path must have the form given in the table.

Now, let $\varphi$ be an $\{\to, \vee, \perp\}$-formula. We simplify it by replacing subformulas $\psi \to \chi$ with $\chi$ when equivalent (as above), and by replacing $\psi \vee \chi$ with $\psi$ or $\chi$ when this does not change $\varphi$ (up to equivalence). Let $\varphi'$ denote the resulting formula. This transformation again amounts to removal of several subtrees from the forest $T_\varphi$, hence every path in $T_{\varphi'}$ is a path in $T_\varphi$. As before, $\varphi'$ contains no nontrivial subformulas equivalent to $p_n$ for $n \geq 1$, or to $\perp$; in particular, if $\varphi'$ itself is equivalent to one of those, it consists of a single symbol.

Assume $\varphi'$ is equivalent to $\alpha_n$; we will show that $T_{\varphi'}$ is a path as given in the table by induction on $|\varphi'|$. By (50), there is no nontrivial way to express $\alpha_1$ or $\alpha_0 = \beta_1$ as a disjunction;

this easily gives the result for $n = 0, 1$ as in the $\{\to, \bot\}$ case. Assume $n \geq 2$. By (50), $\varphi'$ has one of the forms

$$\psi \to p_n,$$
$$(\varphi'' \to p_n) \to p_n,$$
$$\psi \vee \chi \to p_n,$$

where $\psi \equiv \alpha_{n-1}$, $\varphi'' \equiv \alpha_n$, $\chi$ is equivalent to $p_n$, $\beta_{n-1}$, or $\alpha_{n-2}$, and the disjunction may be written in reverse order. In the first two cases, it suffices to apply the induction hypothesis to $\psi$ or $\varphi''$ (resp.). The third case is actually impossible, as we could simplify the formula by deleting the "$\vee \chi$" part. $\square$

**Definition B.6** Let $\varphi$ be a $\wedge$-free formula. An occurrence of a subformula $\psi$ in $\varphi$ is *unnested* if it is not within the left scope of an implication. That is, the set $U(\varphi)$ of unnested occurrences of subformulas of $\varphi$ can be defined inductively by

$$\begin{aligned} U(v) &= \{v\} \qquad \text{if } v \text{ is an atom,} \\ U(\varphi \to \psi) &= \{\varphi \to \psi\} \cup U(\psi), \\ U(\varphi \vee \psi) &= \{\varphi \vee \psi\} \cup U(\varphi) \cup U(\psi). \end{aligned}$$

Notice that atoms in $U(\varphi)$ are exactly the labels of roots of the trees in $T_\varphi$.

**Lemma B.7** *Let $\varphi$ be a $\wedge$-free formula.*

(i) *If $\top \in U(\varphi)$, then $\varphi \equiv \top$.*

(ii) *If $T_\varphi$ has a path $Pv$, where $v$ is an atom, then $v \in U(\varphi)$. If moreover $P$ is nonempty, then $\varphi$ has an unnested subformula of the form $\psi \to \chi$ such that $v \in U(\chi)$, and $T_\psi$ has a path $P$.*

*Proof:* By induction on the complexity of $\varphi$. $\square$

For simplicity, let us define the size of a formula as the number of symbols in Polish notation, that is, the number of occurrences of all variables and connectives, disregarding auxiliary characters (brackets, variable indices).

**Proposition B.8** *If $L$ is a si logic included in $\mathbf{KC} + \mathbf{BW_2}$, then any $\wedge$-free formula $L$-equivalent to*

$$\alpha_n^{\wedge 2} = \alpha_n(p_{0,0} \wedge p_{0,1}, p_{1,0} \wedge p_{1,1}, \ldots, p_{n-1,0} \wedge p_{n-1,1}, p_n)$$

*must have size at least $2^{n+2} - 3$.*

*Proof:* Let $\varphi$ be a $\wedge$-free formula equivalent to $\alpha_n^{\wedge 2}$. For any $f\colon [n] \to \{0, 1\}$, we consider the substitution

$$\sigma_f(p_{i,f(i)}) = p_i,$$
$$\sigma_f(p_{i,1-f(i)}) = \top.$$

Notice that $\sigma_f(\varphi) \equiv \sigma_f(\alpha_n^{\wedge 2}) \equiv \alpha_n$. Let $\varphi_f$ denote the formula $\sigma_f(\varphi)$ with subformulas made true by $\sigma_f$ deleted. By Lemma B.5, $T_{\varphi_f}$ has a path of the form $p_0 p_1^{2k_1+1} \dots p_n^{2k_n+1}$ for some $k_1, \dots, k_n \geq 0$ (depending on $f$). Lifting it back to $T_\varphi$, and using Lemma B.7, we can find a sequence of occurrences of subformulas

$$\varphi = \psi_{f,n,0} \supseteq \varphi_{f,n,0} \supseteq \psi_{f,n,1} \supseteq \dots \supseteq \varphi_{f,n,2k_n} \supseteq \psi_{f,n-1,0} \supseteq \dots \supseteq \varphi_{f,1,2k_1} \supseteq \psi_{f,0,0} \supseteq \varphi_{f,0,0} \tag{51}$$

such that:

(i) $\varphi_{f,i,j} \in U(\psi_{f,i,j})$.

(ii) $\varphi_{f,i+1,j}$ is an implication with premise $\psi_{f,i+1,j+1}$ for $j < 2k_{i+1}$, or $\psi_{f,i,0}$ for $j = 2k_{i+1}$.

(iii) $p_{i,f(i)}$ has an unnested occurrence (denoted $v_{f,i,j}$) in $\varphi_{f,i,j}$. Here, "$p_{n,f(n)}$" stands for $p_n$.

(iv) There are no variables in $U(\psi_{f,i,j})$ other than $p_{0,f(0)}, \dots, p_{n,f(n)}$.

**Claim 1** *Let $f, g\colon [n] \to \{0,1\}$, and $i \leq n$.*

(i) *If $i < n$ and $f(i) \neq g(i)$, then $\varphi_{f,i,0} \nsubseteq \varphi_{g,i,0}$.*

(ii) *$v_{f,i,0} \neq v_{g,i',0}$ unless $i = i'$, and $f$ agrees with $g$ on $\{i, \dots, n-1\}$.*

*Proof:*

(i): Assume that $\varphi_{f,i,0}$ is a suboccurrence of $\varphi_{g,i,0}$. Since each $\psi_{f,i',j'}$ (except $\psi_{f,n,0}$) has an appropriate $\varphi_{f,i'',j''}$ formula as its parent, it follows from (51) that $\varphi_{f,i',j'} \subseteq \varphi_{g,i,0} \subseteq \psi_{f,i',j'}$ for some $i' \geq i$ and $j' \leq 2k_{i'}$. However, since $\varphi_{f,i',j'}$ is unnested in $\psi_{f,i',j'}$, so must be $\varphi_{g,i,0}$, hence $p_{i,g(i)}$ has an unnested occurrence in $\psi_{f,i',j'}$. This contradicts (iv) above.

(ii): Assume $v_{f,i,0} = v_{g,i',0}$. Since $v_{f,i,0}$ is an occurrence of $p_{i,f(i)}$, we must have $i = i'$, and $f(i) = g(i)$. If $f(i'')$ were different from $g(i'')$ for some $i'' > i$, then $\varphi_{f,i'',0}$ and $\varphi_{g,i'',0}$ would be incomparable by the first part of the claim, hence so would be their respective subformulas $v_{f,i,0}$ and $v_{g,i,0}$. □ (Claim 1)

The claim implies that $\{v_{f,i,0} : f\colon [n] \to \{0,1\}, i \leq n\}$ consists of at least $2^n + \dots + 2^0 = 2^{n+1} - 1$ distinct occurrences of variables in $\varphi$, hence the total size of $\varphi$ is at least $2^{n+2} - 3$. □

**Remark B.9** The bound is tight: we can express $\alpha_n^{\wedge 2}$ by an implicational formula of size $2^{n+2} - 3$ using the recurrence

$$\begin{aligned} \alpha_0^{\wedge 2} &= p_0, \\ \alpha_{n+1}^{\wedge 2} &= \alpha_n^{\wedge 2}(p_n/p_{n,0}) \to \alpha_n^{\wedge 2}(p_n/p_{n,1}) \to p_{n+1}. \end{aligned}$$

**Corollary B.10** *If $L$ is a si logic included in $\mathbf{KC} + \mathbf{BW_2}$, and $\varphi$ is a conjunction of $\wedge$-free formulas $L$-equivalent to*

$$\xi_2(\alpha_n) = \alpha_n(p_{0,0} \wedge p_{0,1}, p_{1,0} \wedge p_{1,1}, \dots, p_{n,0} \wedge p_{n,1}),$$

*then $|\varphi| \geq 2^{n+3} - 5$.*

*Proof:* If $\varphi = \bigwedge_{i<m} \varphi_i$, then $\alpha_{n+1}^{\wedge 2}$ is equivalent to the formula $\varphi_0 \to \dots \to \varphi_{m-1} \to p_{n+1}$ of size $|\varphi| + 2$. □

**Example B.11** We may interpret Proposition B.8 as an explicit exponential separation between formula and circuit size in a fragment of intuitionistic logic, and the reader may wonder whether there is such a separation also in the full intuitionistic language. This is indeed true, and essentially well known. One can take for example the Rieger–Nishimura formulas

$$rn_0 = \bot, \qquad rn_1 = p, \qquad rn_2 = \neg p,$$
$$rn_{2n+3} = rn_{2n+1} \vee rn_{2n+2},$$
$$rn_{2n+4} = rn_{2n+2} \to rn_{2n+1}$$

(see [5, Exm. 7.66]). Every intuitionistic formula in one variable $\varphi(p)$ is equivalent to $\top$, or to $rn_k$ for some $k$, and it is not difficult to estimate $k = O(\log|\varphi|)$. On the other hand, $rn_k$ is defined by a circuit of size $O(k)$. Thus, *every intuitionistic formula in one variable can be expressed by an exponentially smaller circuit.* (In a sense, something even stronger holds in classical logic, as every formula in one variable has circuit size $O(1)$. However, the intuitionistic bound is meaningful as unlike **CPC**, there are infinitely many nonequivalent formulas in one variable in **IPC**.)