A simplified lower bound for implicational logic

Emil Jeřábek

Institute of Mathematics, Czech Academy of Sciences

Žitná 25, 115 67 Praha 1, Czech Republic, email: jerabek@math.cas.cz

October 25, 2023

Abstract

We present a streamlined and simplified exponential lower bound on the length of proofs in intuitionistic implicational logic, adapted to Gordeev and Haeusler's dag-like natural deduction.

1 Introduction

Frege proof systems (often called Hilbert-style systems outside proof complexity) are among the simplest and most natural proof systems for classical and nonclassical propositional logics. By results of Reckhow and Cook [30, 6], all classical Frege systems are not only polynomially equivalent to each other, but also to natural deduction systems and to sequent calculi (with cut), which is further testimony to their robustness and fundamental status. Although it is commonly assumed for all classical propositional proof systems that some tautologies require exponentially large proofs, this has been proven so far only for relatively weak proof systems, such as constant-depth Frege, polynomial calculus, and cutting planes (see e.g. [24, 5]). Unrestricted Frege systems are far beyond the reach of current techniques: nothing better is known than a linear lower bound on the number of proof lines and a quadratic bound on the overall proof size [3, 22].

Interestingly, the state of affairs is much better in nonclassical logics: Hrubeš [12, 13, 14] proved exponential lower bounds on the number of lines in Frege proofs for some modal logics and intuitionistic logic, which was generalized by Jeřábek [18] to all transitive modal and superintuitionistic logics with unbounded branching, and by Jalali [16] to substructural logics. Even though the techniques are based on variants of the feasible disjunction property (i.e., given a proof of $\varphi \vee \psi$, we can decide in polynomial time which of φ or ψ is provable), and as such ostensibly require disjunction, Jeřábek [19] showed that the superintuitionistic exponential lower bounds hold for a sequence of purely implicational intuitionistic tautologies.

In a series of papers, Gordeev and Haeusler [8, 9, 10, 11] claim to prove that all intuitionistic implicational tautologies have polynomial-size proofs in a dag-like version of (Gentzen/Prawitz-style) natural deduction, which—if true—would imply NP = PSPACE. These claims are wrong, as they contradict the above-mentioned exponential lower bounds on the length of proofs of implicational tautologies in intuitionistic proof systems. Unfortunately, this fact may not be so obvious to readers unfamiliar with nonclassical proof complexity literature, and in any event, the full proof of the lower bound requires tracking down multiple papers: the Frege lower bound for implicational tautologies in [19] builds on a lower bound for unrestricted intuitionistic tautologies, as proved in either of [13, 14, 18]; these in turn rely on an exponential lower bound on the size of monotone circuits separating the Clique–Colouring disjoint NP pair which—in view of an observation of Tardos [31]—follows from Alon and Boppana [1] (improving a superpolynomial lower bound by Razborov [29]). Finally, one needs a polynomial simulation of natural deduction by Frege systems: this is originally due to Reckhow and Cook [30, 6], but they state it for a sequent-style formulation of natural deduction rather than Prawitz-style, let alone the further variant introduced only recently by Gordeev and Haeusler; while it is clear to a proof complexity practitioner that the argument can be easily adapted to all such variants, this is, strictly speaking, not explicitly proved in any extant literature.

The primary goal of this paper is to give a simple direct proof of an exponential lower bound on the length of proofs of intuitionistic implicational tautologies in Gordeev and Haeusler's dag-like natural deduction. The streamlined argument replaces all proof-theoretic components of the lower bound mentioned above (intuitionistic lower bound, reduction to implicational logic, simulation of natural deduction by Frege), thus it is self-contained except for the combinatorial component (i.e., a monotone circuit lower bound; to simplify our tautologies, we will use a lower bound by Hrubeš and Pudlák [15] instead of Alon–Boppana). It is based on the efficient Kleene slash approach employed in [7, 26, 17, 18]. While we strive to keep the proof of the main result as simple as possible, we also briefly indicate how to generalize it to recover almost the full strength of the lower bound from [19].

The intended audience of the paper is twofold:

- Readers with some general background in logic or computer science, but unfamiliar with proof complexity. For them, the paper gives a simple, yet detailed, exposition of an exponential lower bound on intuitionistic implicational logic so that they cannot be fooled by the fact that Gordeev and Haeusler's claims have been published.
- Researchers in proof complexity—not necessarily interested in Gordeev and Haeusler's claims—for whom the paper brings a new, much shorter proof of the known implicational lower bound, bypassing implicational translation of full intuitionistic logic. We stress that even though the proof system for which it is formulated is not traditional, it is quite natural, and anyway the lower bound also applies to the standard Frege system for implicational intuitionistic logic as the latter obviously embeds in dag-like natural deduction (up to subproofs of Frege axioms, it can be thought of as natural deduction without the $\to$-introduction rule).

Our proof of the main lower bound does not involve any proof system other than dag-like natural deduction itself. However, for the sake of completeness, we include an appendix showing the equivalence of dag-like natural deduction with the standard intuitionistic implicational Frege system up to polynomial increase in proof size, as well as the polynomial equivalence of both systems to their tree-like versions (adapting the original result of Krajíček along the lines of [19]). Thus, dag-like natural deduction does not offer any significant shortening of proofs compared to the conventional tree-like natural deduction. The appendix may be of independent interest as we took some effort to optimize the bounds.

An anonymous source pointed out that since Gordeev and Haeusler's "horizontal compression" only changes the shape of the proof, but does not introduce any new formulas, their claims also contradict other well-known results in proof complexity, namely constant-depth Frege lower bounds such as Beame et al. [2]. For a sketch of the argument, take a sequence of tautologies exponentially hard for constant-depth proofs, such as the pigeonhole principle, and convert it to a sequence of (intuitionistically valid) implicational tautologies φ_n of polynomial size and constant depth (measured, say, using the definition $\mathrm{dp}(\varphi \to \psi) = \max\{1 + \mathrm{dp}(\varphi), \mathrm{dp}(\psi)\}$). Each φ_n has a cut-free sequent proof of polynomial height (and exponential size), which only involves formulas of constant depth by the subformula property, and thus translates to a natural deduction proof of polynomial height using only formulas of constant depth (with polynomially many distinct formulas). Gordeev and Haeusler's claims imply that this can be compressed to a polynomial-size dag-like natural deduction proof using formulas of constant depth. The latter, however, can be converted to a polynomial-size (classical) constant-depth sequent or Frege proof, contradicting the hardness of the tautologies. We will not pursue this connection further in this paper, and leave the details to an interested reader.

The paper is organized as follows. In Section 2 we review the needed prerequisites such as dag-like natural deduction and monotone Boolean circuits. Section 3 is devoted to the proof of the main exponential lower bound; we discuss extensions of the lower bound in Section 4, and we conclude with a few remarks in Section 5. We present the equivalence of dag-like natural deduction to a Frege system in Appendix A, and the equivalence of both systems to their tree-like versions in Appendix B.

2 Preliminaries

The set Form of *implicational formulas* (or just *formulas* if no confusion arises) is the smallest set that includes the set of *propositional variables* (or *atoms*) $\mathrm{Var} = \{p_n : n \in \omega\}$, and such that if φ and ψ are formulas, then $(\varphi \to \psi)$ is a formula. The *size* $|\varphi|$ of a formula φ is the number of occurrences of variables and connectives in φ, i.e., $|p_n| = 1$ and $|(\varphi \to \psi)| = 1 + |\varphi| + |\psi|$. We may omit outer brackets in $\varphi \to \psi$, and we treat $\to$ as a right-associative operator so that, e.g., $\varphi \to \psi \to \chi \to \omega$ stands for $(\varphi \to (\psi \to (\chi \to \omega)))$. (Despite these conventions, we may leave various redundant brackets in place to highlight the formula structure.) We will denote formulas with lower-case Greek letters, and for convenience, we will often use lower-case Latin letters (with indices and/or other decoration) other than p_n for variables. We write $\vec{p}$ for a finite tuple of variables $\langle p_i : i < n \rangle$, especially if n is immaterial; the notation $\varphi(\vec{p})$ indicates that all variables occurring in φ are among $\vec{p}$.

Upper-case Greek letters will usually denote finite sets or sequences of formulas. Our indices generally start from 0; in particular, $\langle \varphi_i : i < n \rangle$, or more concisely $\langle \varphi_i \rangle_{i<n}$, denotes the sequence $\langle \varphi_0, \ldots, \varphi_{n-1} \rangle$ (which is the empty sequence $\langle\rangle$ if $n = 0$). The *length* of a sequence $\Gamma = \langle \varphi_i \rangle_{i<n}$, denoted $|\Gamma|$, is n, and the *size* of Γ, denoted $\|\Gamma\|$, is $\sum_{i<n} |\varphi_i|$. If $\Gamma = \langle \varphi_i \rangle_{i<n}$ is a sequence of

formulas and $\psi \in \mathrm{Form}$, we introduce the abbreviation $\Gamma \to \psi$ for the formula[1]

$$\varphi_{n-1} \to \cdots \to \varphi_1 \to \varphi_0 \to \psi.$$

Formally, $\Gamma \to \psi$ is defined by induction on n: $\langle \varphi_i \rangle_{i<0} \to \psi$ is ψ and $\langle \varphi_i \rangle_{i<n+1} \to \psi$ is $\varphi_n \to \langle \varphi_i \rangle_{i<n} \to \psi$.

A *substitution* is a mapping $\sigma \colon \mathrm{Form} \to \mathrm{Form}$ such that $\sigma(\varphi \to \psi) = (\sigma(\varphi) \to \sigma(\psi))$ for all $\varphi, \psi \in \mathrm{Form}$. If $\Gamma \subseteq \mathrm{Form}$, we write $\sigma(\Gamma) = \{\sigma(\varphi) : \varphi \in \Gamma\}$.

The *intuitionistic implicational logic* $\mathbf{IPC}_{\to}$ is defined by its consequence relation $\vdash \subseteq \mathcal{P}(\mathrm{Form}) \times \mathrm{Form}$: we put $\Gamma \vdash \varphi$ iff φ belongs to the smallest subset of Form that is closed under the rule of modus ponens

$$\varphi, \varphi \to \psi \;/\; \psi,$$

and includes Γ and the logical axioms

$$\varphi \to \psi \to \varphi$$
$$(\varphi \to \psi \to \chi) \to (\varphi \to \psi) \to (\varphi \to \chi)$$

for $\varphi, \psi, \chi \in \mathrm{Form}$. As is conventional, we omit braces around formulas on the left-hand side of $\vdash$, and write commas in place of $\cup$, so that, e.g., $\Gamma, \varphi, \psi \vdash \chi$ stands for $\Gamma \cup \{\varphi, \psi\} \vdash \chi$; we may also coerce finite sequences Γ to sets. We write $\vdash \varphi$ for $\varnothing \vdash \varphi$, in which case we say that φ is an *intuitionistic implicational tautology*, or $\mathbf{IPC}_{\to}$ *tautology* for short.

Lemma 2.1 (deduction theorem) *Let* $\Pi \subseteq \mathrm{Form}$, $\varphi \in \mathrm{Form}$, *and let* Γ *be a finite sequence of formulas. Then*

$$\Pi, \Gamma \vdash \varphi \iff \Pi \vdash \Gamma \to \varphi. \qquad \square$$

A *Kripke model* is a structure $\langle W, \leq, \vDash \rangle$, where $\leq$ is a partial order on W, and $\vDash \subseteq W \times \mathrm{Form}$ satisfies

$$x \vDash \varphi \implies \forall y \geq x \, y \vDash \varphi,$$
$$x \vDash \varphi \to \psi \iff \forall y \geq x \, (y \vDash \varphi \implies y \vDash \psi)$$

for all $x \in W$ and $\varphi, \psi \in \mathrm{Form}$. Unwinding the definitions, we see that for any sequence $\Gamma = \langle \varphi_i \rangle_{i<n}$,

$$x \vDash \Gamma \to \psi \iff \forall y \geq x \, \big((\forall i < n \, y \vDash \varphi_i) \implies y \vDash \psi \big).$$

A formula φ *holds* in $\langle W, \leq, \vDash \rangle$ if $x \vDash \varphi$ for all $x \in W$.

Theorem 2.2 (finite model property) *A formula is an* $\mathbf{IPC}_{\to}$ *tautology if and only if it holds in all finite Kripke models.* $\square$

[1] It might appear more visually pleasing to define it as $\varphi_0 \to \varphi_1 \to \cdots \to \varphi_{n-1} \to \psi$, but the reverse order will be technically more convenient, e.g. in some inductive arguments in Appendix A.

Let us now present Gordeev and Haeusler's dag-like natural deduction calculus $\mathrm{NM}_{\to}$ based on [9]. An $\mathrm{NM}_{\to}$*-proof skeleton* is a finite directed acyclic graph (dag) $\langle V, E\rangle$ with a unique node of out-degree 0, called the *root*, and with all nodes having in-degree at most 2; nodes of in-degree 0, 1, and 2 are called leaves (assumptions), ($\to$I)-nodes, and ($\to$E)-nodes, respectively. If $\langle u, v\rangle \in E$, then u is a *premise*[2] of v. A *thread* is a directed path starting from a leaf; a thread is *maximal* if it ends in the root. An $\mathrm{NM}_{\to}$*-derivation* $\langle V, E, \gamma\rangle$ is an $\mathrm{NM}_{\to}$-proof skeleton $\langle V, E\rangle$ endowed with a vertex labelling $\gamma = \langle \gamma_v : v \in V\rangle$ with $\gamma_v \in \mathrm{Form}$, such that for all $v \in V$:

- if v is an ($\to$I)-node, it is labelled with an implication $\alpha \to \beta$ such that the premise of v is labelled with β;
- if v is an ($\to$E)-node, there are formulas α, β such that v is labelled with β, and the two premises of v are labelled with α and $\alpha \to \beta$, respectively.

A thread with leaf v is *discharged* if it contains an ($\to$I)-node labelled with $\alpha \to \beta$ where $\alpha = \gamma_v$. Let $\varphi \in \mathrm{Form}$ and $\Gamma \subseteq \mathrm{Form}$. An $\mathrm{NM}_{\to}$-derivation is an $\mathrm{NM}_{\to}$*-derivation of* φ *from* Γ if the root is labelled φ and the leaves of all undischarged maximal threads are labelled with elements of Γ. An $\mathrm{NM}_{\to}$*-proof of* φ is an $\mathrm{NM}_{\to}$-derivation of φ from $\varnothing$. The *number of lines* of an $\mathrm{NM}_{\to}$-derivation $\Pi = \langle V, E, \gamma\rangle$ is $|V|$, and the *size* of Π is $\|\Pi\| = \sum_{v\in V} |\gamma_v|$.

It may be difficult to verify the condition on discharging maximal threads directly from the definition. As observed in [9], it can be checked efficiently as follows. Given an $\mathrm{NM}_{\to}$-derivation $\Pi = \langle V, E, \gamma\rangle$, we define for each $v \in V$ a set $A_v \subseteq \{\gamma_u : u \text{ is a leaf}\}$ by well-founded recursion:

$$A_v = \begin{cases} \{\gamma_v\}, & v \text{ is a leaf,} \\ A_u \smallsetminus \{\alpha\}, & v \text{ is an } (\to\mathrm{I})\text{-node with premise } u \text{ and } \gamma_v = \alpha \to \beta, \\ A_{u_0} \cup A_{u_1}, & v \text{ is an } (\to\mathrm{E})\text{-node with premises } u_0 \text{ and } u_1. \end{cases}$$

Note that given Π, we can compute $\langle A_v : v \in V\rangle$ in polynomial time.

Lemma 2.3 ([9]) *An* $\mathrm{NM}_{\to}$*-derivation* $\langle V, E, \gamma\rangle$ *with root* ϱ *is a derivation of* γ_ϱ *from* Γ *if and only if* $A_\varrho \subseteq \Gamma$.

Proof: Show that A_v is the set of labels of undischarged threads ending in v by well-founded induction on v. □

Likewise, we can show the soundness of $\mathrm{NM}_{\to}$-derivations by well-founded induction on v, using the deduction theorem:

Lemma 2.4 *For any* $\mathrm{NM}_{\to}$*-derivation* $\langle V, E, \gamma\rangle$ *and* $v \in V$*,* $A_v \vdash \gamma_v$. □

On the other hand, *tree-like* $\mathrm{NM}_{\to}$ derivations are the same as the implicational fragment of the usual Gentzen–Prawitz natural deduction (see e.g. [27, 25]). This implies the completeness of the calculus, as observed in [9]:

[2] In [9], proofs go upside down so that edges are directed from conclusions to premises; we reversed them to a more natural order. Also, they include an auxiliary repetition rule that we omit for simplicity (it can be eliminated from any $\mathrm{NM}_{\to}$ derivation without increasing its size).

Lemma 2.5 *A formula φ is an* $\mathbf{IPC}_{\to}$ *tautology if and only if it has an* $\mathrm{NM}_{\to}$*-proof.* $\square$

We assume familiarity with classical propositional logic, but briefly, we consider formulas built from propositional variables using the connectives $\{\to, \wedge, \vee, \neg, \top, \bot\}$. An *assignment* to a set of variables X is a function $a\colon X \to \mathbf{2}$, where $\mathbf{2} = \{0, 1\}$. We denote the set of all such assignments as $\mathbf{2}^X$. For any $a \in \mathbf{2}^X$ and a formula φ over variables X, we define the relation $a \vDash \varphi$ (in words, *a satisfies* φ) in the usual way:

$$\begin{aligned} a \vDash p &\iff a(p) = 1, \quad p \in X, \\ a \vDash (\varphi \to \psi) &\iff a \nvDash \varphi \text{ or } a \vDash \psi, \\ a \vDash \neg\varphi &\iff a \nvDash \varphi, \end{aligned}$$

and so on for the other connectives. A formula φ is a *classical tautology* if $a \vDash \varphi$ for all assignments a to the variables of φ.

We also need a bit of circuit complexity. A *monotone circuit* over a set X of *variables* is $C = \langle V, E, g\rangle$ where $\langle V, E\rangle$ is a dag with a unique node ϱ of out-degree 0 (the *root*), endowed with a labelling $g\colon V \to X \cup \{\wedge, \vee\}$ such that nodes v with $g(v) \in X$ have in-degree 0. Nodes $v \in V$ are also called *gates*, and edges $e \in E$ are called *wires*. We may write $C(\vec{p})$ to denote that C is a circuit over a finite tuple of variables $\vec{p}$. The *size* of a circuit $C = \langle V, E, g\rangle$ is $|C| = |E|$ (i.e., the number of wires). By well-founded recursion, any assignment $a\colon X \to \mathbf{2}$ extends to a unique function $\hat{a}\colon V \to \mathbf{2}$, called the *evaluation* of C, such that

$$\hat{a}(v) = \begin{cases} a(g(v)), & g(v) \in X, \\ \inf\{\hat{a}(u) : \langle u, v\rangle \in E\}, & g(v) = \wedge, \\ \sup\{\hat{a}(u) : \langle u, v\rangle \in E\}, & g(v) = \vee, \end{cases}$$

where $\inf\varnothing = 1$, $\sup\varnothing = 0$ (thus $\wedge$- and $\vee$-gates without inputs act as constants $\top$ and $\bot$, respectively). A circuit C with root ϱ *computes* a Boolean function $f\colon \mathbf{2}^X \to \mathbf{2}$ if $f(a) = \hat{a}(\varrho)$ for each $a \in \mathbf{2}^X$. More generally, a *disjoint pair* is $P = \langle P^0, P^1\rangle$ where $P^0, P^1 \subseteq \mathbf{2}^X$ and $P^0 \cap P^1 = \varnothing$; a circuit C *separates* P if $\hat{a}(\varrho) = i$ for each $i \in \mathbf{2}$ and $a \in P^i$. We will write $a \vDash C$ for $\hat{a}(\varrho) = 1$.

Let $\vec{p}$, $\vec{q}$, and $\vec{r}$ be pairwise disjoint tuples of variables, and $\varphi(\vec{p}, \vec{q})$ and $\psi(\vec{p}, \vec{r})$ classical formulas. Then a circuit $C(\vec{p})$ *interpolates* the implication $\varphi \to \psi$ (which must be a classical tautology) if $\varphi(\vec{p}, \vec{q}) \to C(\vec{p})$ and $C(\vec{p}) \to \psi(\vec{p}, \vec{r})$ are classical tautologies (i.e., $a \vDash \varphi \implies a \vDash C$ and $a \vDash C \implies a \vDash \psi$ for all assignments $a \in \mathbf{2}^{\{\vec{p}, \vec{q}, \vec{r}\}}$), or in other words, if C separates the *interpolation pair* $\mathrm{Itp}_{\varphi,\psi} = \langle \mathrm{Itp}^0_\psi, \mathrm{Itp}^1_\varphi\rangle$, where

$$\begin{aligned} \mathrm{Itp}^0_\psi &= \{a \in \mathbf{2}^{\vec{p}} : \exists c \in \mathbf{2}^{\vec{r}}\, \langle a, c\rangle \nvDash \psi\}, \\ \mathrm{Itp}^1_\varphi &= \{a \in \mathbf{2}^{\vec{p}} : \exists b \in \mathbf{2}^{\vec{q}}\, \langle a, b\rangle \vDash \varphi\}. \end{aligned}$$

For any $n \geq 2$, the *Colouring–Cocolouring* disjoint pair $\mathrm{CC}_n = \langle \mathrm{CC}^0_n, \mathrm{CC}^1_n\rangle$ over the set of variables $X_n = \binom{[n]}{2}$ (i.e., the set of unordered pairs of elements of $[n] = \{0, \dots, n-1\}$) is defined by

$$\begin{aligned} \mathrm{CC}^0_n &= \bigl\{E \subseteq X_n : \text{the graph } \langle [n], E\rangle \text{ is } k\text{-colourable}\bigr\}, \\ \mathrm{CC}^1_n &= \bigl\{E \subseteq X_n : \text{the graph } \langle [n], \overline{E}\rangle \text{ is } k\text{-colourable}\bigr\}, \end{aligned}$$

where $\overline{E} = X_n \smallsetminus E$, $k = \lceil \sqrt{n} \rceil - 1$, and we identify $E \subseteq X_n$ with its characteristic function $X_n \to \mathbf{2}$. To see that $\mathrm{CC}_n^0 \cap \mathrm{CC}_n^1 = \varnothing$, observe that if $c_0, c_1 \colon [n] \to [k]$ are k-colourings of $\langle [n], E\rangle$ and $\langle [n], \overline{E}\rangle$, respectively, then $c_0 \times c_1 \colon [n] \to [k] \times [k]$ is an injection, thus $n \le k^2$.

An exponential lower bound on the monotone circuit complexity (and even monotone *real* circuit complexity) of CC_n was proved by Hrubeš and Pudlák [15, Thm. 10], using machinery from Jukna [20]:

Theorem 2.6 *For $n \gg 0$, all monotone circuits separating CC_n have size $2^{\Omega(k^{1/4})} = 2^{\Omega(n^{1/8})}$.* □

Strictly speaking, Hrubeš and Pudlák work with *bounded fan-in* monotone circuits, i.e., such that the in-degree of all gates is at most 2, and they measure size by the number of gates. This makes no difference, as a d-ary $\wedge$- or $\vee$-gate can be simulated by $d-1$ binary gates using $2(d-1)$ wires, thus any monotone circuit with s wires can be transformed to a bounded fan-in monotone circuit with $s' \le 2s$ wires; moreover, a circuit with s' wires has at most $s'+1$ gates (we may associate each node other than the root with an outgoing wire). This mild size increase does not affect the shape of the lower bound in Theorem 2.6.

3 An exponential lower bound

In this section, we will prove our main lower bound, viz. there is an explicit sequence of implicational intuitionistic tautologies that require $\mathrm{NM}_\to$-proofs with exponentially many lines.

Let us start with construction of the $\mathbf{IPC}_\to$ tautologies, which will express the disjointness of CC_n. Intuitionistic tautologies expressing disjointness of the Clique–Colouring pair were first considered by Hrubeš [13]; they were made negation-free in Jeřábek [18], and implicational in Jeřábek [19]. We will further simplify the tautologies from [19] by using a somewhat more direct translation to implicational logic, and by employing the Colouring–Cocolouring pair in place of Clique–Colouring, which leads to more symmetric (and shorter) formulas. Fix $n \ge 2$ and $k = \lceil \sqrt{n} \rceil - 1$. Our tautologies will employ variables p_{ij} and $p'_{i,j}$ $(i < j < n)$, representing the edge relation of a graph $G = \langle [n], E\rangle$ and its complement, and variables q_{il} and r_{il} $(i < n$, $l < k)$, representing a k-colouring of G and of its complement (respectively).

To motivate the formal definition below, we can state in classical propositional logic that $\vec{q}$ define a (possibly multivalued) k-colouring of G by the formula

$$\bigwedge_{i<n} \bigvee_{l<k} q_{il} \wedge \bigwedge_{\substack{i<j<n \\ l<k}} \neg(q_{il} \wedge q_{jl} \wedge p_{ij}),$$

and similarly for the complement, thus the disjointness of CC_n is expressed by the classical tautology

$$\Big(\bigwedge_{i<n} \bigvee_{l<k} q_{il} \to \bigvee_{\substack{i<j<n \\ l<k}} (q_{il} \wedge q_{jl} \wedge p_{ij})\Big) \vee \Big(\bigwedge_{i<n} \bigvee_{l<k} q_{il} \to \bigvee_{\substack{i<j<n \\ l<k}} (r_{il} \wedge r_{jl} \wedge \neg p_{ij})\Big),$$

which can be made negation-free using the $\vec{p}'$ variables:

$$\bigwedge_{i<j<n}(p_{ij}\vee p'_{ij}) \to \Big(\bigwedge_{i<n}\bigvee_{l<k} q_{il} \to \bigvee_{\substack{i<j<n\\ l<k}}(q_{il}\wedge q_{jl}\wedge p_{ij})\Big) \vee \Big(\bigwedge_{i<n}\bigvee_{l<k} r_{il} \to \bigvee_{\substack{i<j<n\\ l<k}}(r_{il}\wedge r_{jl}\wedge p'_{ij})\Big).$$

This turns out to be an intuitionistic tautology as well. In order to convert it to an implicational tautology, we introduce further auxiliary variables u, v, and w: the idea is to rewrite an implication $\psi \to \chi$ as $(\chi \to u) \to (\psi \to u)$, where $\psi \to u$ and $\chi \to u$ can be written using implicational formulas when ψ and χ are monotone formulas. After some manipulation we end up with the following:

Definition 3.1 Let $n \geq 2$ and $k = \lceil\sqrt{n}\rceil - 1$. We define the following implicational formulas in variables p_{ij}, p'_{ij}, q_{il}, r_{il}, u, v, and w, where $i < j < n$ and $l < k$:

$$\begin{aligned}\alpha_n(\vec{p},\vec{q},v) &= \big\langle\langle q_{il}\to v\rangle_{l<k}\to v\big\rangle_{i<n} \to \langle q_{il}\to q_{jl}\to p_{ij}\to v\rangle_{\substack{i<j<n\\ l<k}} \to v,\\ \tau_n(\vec{p},\vec{p}',\vec{q},\vec{r},u,v,w) &= \big\langle (p_{ij}\to u)\to(p'_{ij}\to u)\to u\big\rangle_{i<j<n}\\ &\qquad \to \big(\alpha_n(\vec{p},\vec{q},v)\to u\big)\to\big(\alpha_n(\vec{p}',\vec{r},w)\to u\big)\to u.\end{aligned}$$

(The order in which we enumerate the multiply-indexed sequences such as $\langle\dots\rangle_{i<j<n}$ does not matter.)

Observation 3.2 $|\tau_n| = O(n^2k) = O(n^{5/2})$. □

Lemma 3.3 *The formulas τ_n are intuitionistic implicational tautologies.*

Proof: Assume for contradiction that τ_n does not hold in a finite Kripke model $\langle W,\leq,\vDash\rangle$. This means that there exists $x\in W$ such that $x \vDash (p_{ij}\to u)\to(p'_{ij}\to u)\to u$ for all $i<j<n$, $x\vDash \alpha_n(\vec{p},\vec{q},v)\to u$, $x\vDash\alpha_n(\vec{p}',\vec{r},w)\to u$, but $x\nvDash u$. Replacing x with some $\tilde{x}\geq x$ if necessary, we may assume that x is maximal such that $x\nvDash u$, i.e., $x'\vDash u$ for all $x'>x$.

For each $i<j<n$, $x\vDash(p_{ij}\to u)\to(p'_{ij}\to u)\to u$ implies that $x\nvDash p_{ij}\to u$ or $x\nvDash p'_{ij}\to u$. Since u is true in all $x'>x$, we obtain

$$\forall i<j<n\,(x\vDash p_{ij}\text{ or }x\vDash p'_{ij}). \tag{1}$$

Since $x\vDash\alpha_n(\vec{p},\vec{q},v)\to u$, we have $x\nvDash\alpha_n(\vec{p},\vec{q},v)$, thus there exists $y\geq x$ such that $y\vDash\langle q_{il}\to v\rangle_{l<k}\to v$ for all $i<n$, and $y\vDash q_{il}\to q_{jl}\to p_{ij}\to v$ for all $i<j<n$ and $l<k$, but $y\nvDash v$. As above, we may assume that $y'\vDash v$ for all $y'>y$. Then for every $i<n$, $y\vDash\langle q_{il}\to v\rangle_{l<k}\to v$ implies $y\nvDash q_{il}\to v$ for some $l<k$, whence $y\vDash q_{il}$ by maximality. That is, we can find a colouring function $c\colon[n]\to[k]$ such that $y\vDash q_{i,c(i)}$ for all $i<n$.

If $i<j<n$ are such that $c(i)=c(j)=l$, then $y\vDash q_{il}\to q_{jl}\to p_{ij}\to v$ and $y\nvDash v$ implies $y\nvDash p_{ij}$, and a fortiori $x\nvDash p_{ij}$. This shows that c is a proper k-colouring of the graph $\langle[n],E\rangle$, where $E=\big\{\{i,j\}:x\vDash p_{ij}\big\}$.

Since $x\vDash\alpha_n(\vec{p}',\vec{r},w)\to u$, the same argument gives a k-colouring $c'\colon[n]\to[k]$ of $\langle[n],E'\rangle$, where $E'=\big\{\{i,j\}:x\vDash p'_{ij}\big\}$. But then (1) implies that the function $c\times c'\colon[n]\to[k]\times[k]$ is injective, thus $n\leq k^2<n$, a contradiction. □

The remaining task is to prove a form of monotone feasible interpolation (based on feasible disjunction property) for $\mathrm{NM}_{\to}$, which will imply an exponential lower bound for the τ_n tautologies using Theorem 2.6. There are many ways how to prove the disjunction property of intuitionistic logic and various intuitionistic theories, one of them being *Kleene's slash* [21]. Efficient versions of Kleene's slash were used by Ferrari, Fiorentini, and Fiorino [7] (under the umbrella machinery of "extraction calculi") to prove the feasible disjunction property for the intuitionistic natural deduction system (which was originally proved by Buss and Mints [4] using a form of cut elimination); by Mints and Kojevnikov [26] to prove the polynomial equivalence of intuitionistic Frege systems using admissible rules (with a considerably simplified argument given by Jeřábek [17]); and by Jeřábek [18] to prove an exponential lower bound on intuitionistic Extended Frege proofs. We will adapt the argument from [18] to a purely implicational setting, using a disjunction-free analogue of the disjunction property.

Definition 3.4 If $P \subseteq \mathrm{Form}$, a *$P$-slash* is a unary predicate $|$ on Form such that

$$|(\varphi \to \psi) \iff \big(\|\varphi \implies |\psi\big)$$

for all $\varphi, \psi \in \mathrm{Form}$, where we define the short-hand

$$\|\varphi \iff |\varphi \text{ and } \varphi \in P.$$

If Γ is a set of formulas, we write $\|\Gamma$ if $\|\varphi$ for all $\varphi \in \Gamma$. When we need to consider several slash operators at the same time, we may distinguish them by subscripts, which are carried over to $\|$. We warn the reader that a P-slash is not uniquely determined by P, as we have liberty in defining $|p$ for $p \in \mathrm{Var}$; however, an arbitrary choice of $|$ on Var has a unique extension to a P-slash.

If $\Pi = \langle V, E, \gamma \rangle$ is an $\mathrm{NM}_{\to}$-derivation, a set $P \subseteq \mathrm{Form}$ is *Π-closed* if $A_v \subseteq P \implies \gamma_v \in P$ for all $v \in V$.

Unwinding the definition, we obtain:

Observation 3.5 *If Γ is a finite sequence of formulas, and $\varphi \in \mathrm{Form}$, then*

$$|(\Gamma \to \varphi) \iff \big(\|\Gamma \implies |\varphi\big). \qquad \square$$

We first verify that being Π-closed is enough to ensure the soundness of the slash:

Lemma 3.6 *Let Π be an $\mathrm{NM}_{\to}$-proof of φ, P be a Π-closed set of formulas, and $|$ be a P-slash. Then $\|\varphi$.*

Proof: We prove

$$\|A_v \implies \|\gamma_v \tag{2}$$

by well-founded induction on $v \in V$. This is trivial if v is a leaf. Let v be an $(\to\mathrm{E})$-node with premises u_0, u_1, such that $\gamma_{u_0} = \alpha$, $\gamma_{u_1} = (\alpha \to \beta)$, and $\gamma_v = \beta$, and assume $\|A_v$. Since

$A_{u_i} \subseteq A_v$, the induction hypothesis gives $\|\alpha$ and $\|(\alpha \to \beta)$. Then the definition of $|(\alpha \to \beta)$ ensures $|\beta$, and $A_v \subseteq P$ implies $\beta \in P$ as P is Π-closed, thus $\|\beta$.

Finally, let v be an ($\to$I)-node with premise u such that $\gamma_u = \beta$ and $\gamma_v = (\alpha \to \beta)$, and assume $\|A_v$. Then $A_v \subseteq P$ implies $\gamma_v \in P$ as P is Π-closed, hence it suffices to show $|(\alpha \to \beta)$. Thus, assume $\|\alpha$; since $A_u \subseteq A_v \cup \{\alpha\}$, we have $\|A_u$, thus $\|\beta$ by the induction hypothesis. $\square$

Next, we need to furnish ourselves with Π-closed sets.

Definition 3.7 Let $\Pi = \langle V, E, \gamma \rangle$ be an $\mathrm{NM}_{\to}$-derivation and $P \subseteq \mathrm{Form}$. The Π-*closure of* P, denoted $\mathrm{cl}_\Pi(P)$, is $P_{|V|}$, where we define P_i for each $i \in \omega$ by

$$\begin{aligned} P_0 &= P, \\ P_{i+1} &= P_i \cup \{\gamma_v : v \in V, A_v \subseteq P_i\}. \end{aligned}$$

Lemma 3.8 *Let* Π *be an* $\mathrm{NM}_{\to}$*-derivation and* $P \subseteq \mathrm{Form}$.

(i) *The set* $\mathrm{cl}_\Pi(P) \supseteq P$ *is* Π*-closed.*

(ii) $P \vdash \varphi$ *for all* $\varphi \in \mathrm{cl}_\Pi(P)$.

Proof:

(i): Let $\Pi = \langle V, E, \gamma \rangle$ and $t = |V|$. It is clear from the definition that if $P_i = P_{i+1}$, then P_i is Π-closed, and $P_i = P_j$ for all $j \geq i$. Thus, it suffices to shows that $P_i = P_{i+1}$ for some $i \leq t$. If not, then $P = P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_{t+1}$, thus $|P_i \smallsetminus P| \geq i$ for each $i \leq t+1$ by induction on i; but $P_i \subseteq P \cup \{\gamma_v : v \in V\}$, thus $t \geq |P_{t+1} \smallsetminus P| \geq t+1$, a contradiction.

(ii): We can prove $P \vdash \varphi$ for all $\varphi \in P_i$ by induction on i using Corollary 2.4. $\square$

It will be crucial in what follows that Π-closure is efficiently computable: e.g., it is easy to see that it is computable in polynomial time; but what we will actually need is that it is computable by polynomial-size monotone circuits in the following sense:

Lemma 3.9 *Let* $\Pi = \langle V, E, \gamma \rangle$ *be an* $\mathrm{NM}_{\to}$*-derivation with* $t = |V|$ *lines,* $F = \{\varphi_i : i < n\} \subseteq \mathrm{Form}$ *be such that* $\{\gamma_v : v \in V\} \subseteq F$*, and* $\varphi \in F$.

Then there exists a monotone circuit C *of size* $O(t^3)$ *over variables* $X = \{x_i : i < n\}$ *such that for every assignment* $a \in \mathbf{2}^X$,

$$a \vDash C \iff \varphi \in \mathrm{cl}_\Pi\bigl(\{\varphi_i : a(x_i) = 1\}\bigr).$$

Proof: We may assume $\varphi = \varphi_0$. If $\varphi \notin F_\Pi = \{\gamma_v : v \in V\}$, then $\varphi \in \mathrm{cl}_\Pi(P) \iff \varphi \in P$, which is computable by the trivial circuit $C = x_0$, thus we may assume $\varphi \in F_\Pi$. More generally, we observe that $\mathrm{cl}_\Pi(P) = P \cup \mathrm{cl}_\Pi(P \cap F_\Pi)$, thus we may assume $F = F_\Pi$; in particular, $n \leq t$.

We consider a circuit C with nodes $y_{i,j}$ for $i < n$ and $j \le t$, and $z_{v,j}$ for $v \in V$ and $j < t$, wired such that

$$\begin{aligned} y_{i,0} &\equiv x_i, \\ y_{i,j+1} &\equiv y_{i,j} \vee \bigvee_{\substack{v \in V \\ \gamma_v = \varphi_i}} z_{v,j}, \\ z_{v,j} &\equiv \bigwedge_{\substack{i<n \\ \varphi_i \in A_v}} y_{i,j}. \end{aligned}$$

We define the root of C to be $y_{0,t}$ (and we remove nodes from which $y_{0,t}$ is not reachable to satisfy the formal definition of a circuit). It follows from the definition by induction on j that if $a \in \mathbf{2}^X$ and $P = \{\varphi_i : a(x_i) = 1\}$, then

$$\begin{aligned} \hat{a}(y_{i,j}) = 1 &\iff \varphi_i \in P_j, \\ \hat{a}(z_{v,j}) = 1 &\iff A_v \subseteq P_j, \end{aligned}$$

where $\hat{a}$ is the evaluation of C extending a. Consequently, $\varphi \in \mathrm{cl}_\Pi(P) \iff \overline{a}(y_{0,t}) = 1$.

In order to determine $|C|$, for each $j < t$ there are n wires going from $y_{i,j}$ to $y_{i,j+1}$, t wires (one for each $v \in V$) going from $z_{v,j}$ to $y_{i,j+1}$ where $\gamma_v = \varphi_i$, and $\sum_v |A_v| \le nt$ wires going from $y_{i,j}$ to $z_{v,j}$ such that $\varphi_i \in A_v$. Thus, $|C| \le (n + t + nt)t = O(nt^2) = O(t^3)$, using $n \le t$. □

Pudlák [28] showed that the feasible disjunction property of intuitionistic calculi can serve a similar role as feasible interpolation for classical proof systems, and as such implies conditional lower bounds on the length of intuitionistic proofs. Hrubeš [13] discovered how to modify the set-up to obtain an analogue of feasible *monotone* interpolation (first considered by Krajíček [23]), which yields unconditional exponential lower bounds utilizing monotone circuit lower bounds such as Alon and Boppana [1]. These results naturally rely on the presence of disjunction. Jeřábek [19] obtained a lower bound on implicational intuitionistic logic based using implicational translations of intuitionistic formulas, but here we follow a more direct approach: we introduce a version of feasible monotone interpolation based on a "disjunction-free disjunction property". This is the main new idea of this paper. To help the reader with intuition, we first prove a most simple version of disjunction-free feasible disjunction property[3], although we will not really use this statement later.

Lemma 3.10 *Given an* $\mathrm{NM}_\to$*-proof* Π *of a formula* φ *of the form*

$$(\alpha_0 \to u) \to (\alpha_1 \to u) \to u,$$

where the variable u *does not occur in* α_0 *and* α_1*, we can compute in polynomial time an* $i \in \{0, 1\}$ *such that* $\vdash \alpha_i$.

[3]It is not surprising that $\alpha_0 \vee \alpha_1$ can be expressed by an implicational formula as in Lemma 3.10; what is supposed to be novel here is the way to prove the feasible disjunction property for this formulation without reintroducing disjunctions.

Proof: Put $P = \mathrm{cl}_\Pi(\alpha_0 \to u, \alpha_1 \to u)$, and let $|$ be a P-slash such that $\nmid u$. Since $|\varphi$ by Lemmas 3.6 and 3.8, we have $\nparallel(\alpha_i \to u)$ for some $i < 2$ by Observation 3.5. In view of $(\alpha_i \to u) \in P$, this means $\nmid(\alpha_i \to u)$, thus $\|\alpha_i$. That is, we have verified

$$\alpha_0 \in P \text{ or } \alpha_1 \in P.$$

Given Π, we can compute P in polynomial time, hence we can compute $i < 2$ such that $\alpha_i \in P$. It remains to verify that this implies $\vdash \alpha_i$. Lemma 3.8 gives

$$\alpha_0 \to u, \alpha_1 \to u \vdash \alpha_i.$$

But u does not occur in α_i, hence we may substitute it with $\top$, obtaining $\vdash \alpha_i$. □

We now generalize this argument to a Hrubeš-style feasible monotone interpolation.

Theorem 3.11 *Let $\vec{p} = \langle p_i : i < n\rangle$, $\vec{p}\,' = \langle p'_i : i < n\rangle$, $\vec{q}$, $\vec{r}$, and u be pairwise disjoint tuples of variables, and assume that a formula φ of the form*

$$\big\langle (p_i \to u) \to (p'_i \to u) \to u \big\rangle_{i<n} \to \big(\alpha_0(\vec{p}, \vec{q}) \to u\big) \to \big(\alpha_1(\vec{p}\,', \vec{r}) \to u\big) \to u$$

has an $\mathrm{NM}_\to$-proof with t lines. Then there exists a monotone circuit $C(\vec{p})$ of size $O(t^3)$ that interpolates the classical tautology

$$\neg\alpha_1(\neg\vec{p}, \vec{r}) \to \alpha_0(\vec{p}, \vec{q}),$$

where $\neg\vec{p}$ denotes $\langle \neg p_i : i < n\rangle$.

Proof: Let $\Pi = \langle V, E, \gamma\rangle$ be a proof of φ with s lines. If $I \subseteq [n]$, we write $p_I = \{p_i : i \in I\}$, and similarly for p'_I. We define

$$\begin{aligned} P &= \{(p_i \to u) \to (p'_i \to u) \to u, \alpha_j \to u : i < n, j < 2\},\\ P_{I,J} &= \mathrm{cl}_\Pi(P \cup p_I \cup p'_J) \end{aligned}$$

for each $I, J \subseteq [n]$. Let $|_{I,J}$ be a $P_{I,J}$-slash such that $\nmid_{I,J} u$ and $|_{I,J} x$ for all variables $x \neq u$.

If $i \in I$, then $\|_{I,J} p_i$, thus $\nmid_{I,J}(p_i \to u)$, and $|_{I,J}(p_i \to u) \to (p'_i \to u) \to u$ by Observation 3.5. Likewise if $i \in J$, using $\nmid_{I,J}(p'_i \to u)$. In view of $(p_i \to u) \to (p'_i \to u) \to u \in P_{I,J}$, we obtain

$$I \cup J = [n] \implies \|_{I,J}\big\{(p_i \to u) \to (p'_i \to u) \to u : i < n\big\}.$$

On the other hand, $|_{I,J}\varphi$ by Lemmas 3.6 and 3.8, thus assuming $I \cup J = [n]$, Observation 3.5 implies $\nparallel_{I,J}(\alpha_j \to u)$ for some $j < 2$. Since $\alpha_j \to u$ is in $P_{I,J}$, this means $\nmid_{I,J}(\alpha_j \to u)$, which implies $\|_{I,J}\alpha_j$. That is,

$$I \cup J = [n] \implies \alpha_0 \in P_{I,J} \text{ or } \alpha_1 \in P_{I,J}.$$

Applying this to $J = \overline{I} := [n] \smallsetminus I$, and using the monotonicity of cl_Π, we obtain

$$\forall I \subseteq [n]\ \big(\alpha_0 \in P_{I,[n]} \text{ or } \alpha_1 \in P_{[n],\overline{I}}\big). \tag{3}$$

Put $F = P \cup p_{[n]} \cup p'_{[n]} \cup \{\gamma_v : v \in V\}$. By Lemma 3.9, there is a monotone circuit of size $O(t^3)$ that determines whether $\alpha \in \mathrm{cl}_\Pi(S)$ for a given $S \subseteq F$, using variables corresponding to each $p_i \in F$, which we may identify with p_i itself, variables corresponding to formulas in $P \cup p'_{[n]}$, which we may substitute with $\top$, and variables corresponding to other formulas from F, which we may substitute with $\bot$. We obtain a monotone circuit $C(\vec{p})$ of size $O(t^3)$ such that

$$a \vDash C \iff \alpha \in P_{I(a),[n]} \tag{4}$$

for all assignments a, where $I(a) = \{i < n : a(p_i) = 1\}$.

We claim that C interpolates $\neg\alpha_1(\neg\vec{p}, \vec{r}) \to \alpha_0(\vec{p}, \vec{q})$. Let $a \in \mathbf{2}^{\{\vec{p},\vec{q},\vec{r}\}}$. On the one hand, assume $a \vDash C$; we need to show $a \vDash \alpha_0$. We have $\alpha_0 \in P_{I(a),[n]}$ by (4). Since all formulas in P are implied by u, we have

$$p_{I(a)}, p'_{[n]}, u \vdash \alpha_0(\vec{p}, \vec{q})$$

by Lemma 3.8. But α_0 does not contain the variables p'_i or u, hence we may substitute these with $\top$, obtaining

$$p_{I(a)} \vdash \alpha_0(\vec{p}, \vec{q}).$$

Since $a \vDash p_{I(a)}$, also $a \vDash \alpha_0$.

On the other hand, assume $a \nvDash C$; we will verify $a \vDash \alpha_1(\neg\vec{p}, \vec{r})$. We have $\alpha_0 \notin P_{I(a),[n]}$ by (4), hence $\alpha_1 \in P_{[n],\overline{I(a)}}$ by (3), thus

$$p_{[n]}, p'_{\overline{I(a)}}, u \vdash \alpha_1(\vec{p}', \vec{r})$$

by Lemma 3.8. Substituting $\top$ for $\vec{p}$ and u, we obtain

$$p'_{\overline{I(a)}} \vdash \alpha_1(\vec{p}', \vec{r}).$$

Finally, we can substitute p'_i with $\neg p_i$ for each i, getting

$$\neg p_{\overline{I(a)}} \vdash \alpha_1(\neg\vec{p}, \vec{r})$$

(in intuitionistic or classical logic with $\neg$). Since a satisfies the left-hand side, this implies $a \vDash \alpha_1(\neg\vec{p}, \vec{r})$. $\square$

We are ready to prove the main lower bound by applying Theorem 3.11 to the τ_n tautologies from Definition 3.1; we only need to observe that interpolation of the implication $\neg\alpha_n(\neg\vec{p}, \vec{r}, w) \to \alpha_n(\vec{p}, \vec{q}, v)$ is essentially identical to separation of the CC_n disjoint pair.

Theorem 3.12 *If n is sufficiently large, then every $\mathrm{NM}_\to$-proof of τ_n has at least $2^{\Omega(n^{1/8})}$ lines.*

Consequently, there are infinitely many intuitionistic implicational tautologies φ such that every $\mathrm{NM}_\to$-proof of φ needs to have at least $2^{\Omega(|\varphi|^{1/20})}$ lines.

Proof: It suffices to prove the first part; the second part then follows using Observation 3.2.

If τ_n has an $\mathrm{NM}_\to$-proof with t lines, there is a monotone circuit $C(\vec{p})$ of size $O(t^3)$ that interpolates

$$\neg\alpha_n(\neg\vec{p}, \vec{r}, w) \to \alpha_n(\vec{p}, \vec{q}, v) \tag{5}$$

by Theorem 3.11. We claim that C separates CC_n, which implies $t = 2^{\Omega(n^{1/8})}$ by Theorem 2.6.

Let $E \subseteq \binom{[n]}{2}$, and let e be the corresponding assignment to $\vec{p}$, i.e., for each $i < j < n$,

$$e(p_{ij}) = 1 \iff \{i, j\} \in E.$$

Assume that $\langle [n], E\rangle$ is k-colourable; we need to show $e \nvDash C$. Fix a vertex colouring $c\colon [n] \to [k]$, and extend e to an assignment on $\vec{q}$ and v by $e(v) = 0$ and

$$e(q_{il}) = 1 \iff c(i) = l$$

for each $i < n$ and $l < k$. Then for every $i < n$, $e \nvDash q_{i,c(i)} \to v$, thus $e \vDash \langle q_{il} \to v\rangle_{l<k} \to v$. Likewise, for every $i < j < n$ and $l < k$, $e \vDash q_{il} \to q_{jl} \to p_{ij} \to v$, i.e., $e \nvDash q_{il} \wedge q_{jl} \wedge p_{ij}$: if $c(i) = l = c(j)$, then $\{i, j\} \notin E$ as c is a proper colouring. Thus, $e \nvDash \alpha_n(\vec{p}, \vec{q}, v)$, which implies $e \nvDash C(\vec{p})$ as C interpolates (5).

A symmetrical argument shows that if $\langle [n], \overline{E}\rangle$ is k-colourable, then e extends to an assignment such that $e \nvDash \alpha_n(\neg\vec{p}, \vec{r}, w)$, whence $e \vDash C(\vec{p})$. □

4 Extensions

The goal of the previous section has been to get to the basic lower bound (Theorem 3.12) as directly and as simply as possible. However, if we expend more effort, we can improve the result in various ways—more or less up to the strength of Theorem 4.22 of [19]. We briefly indicate these modifications and their difficulty below, but we omit most details, and keep this section informal, as it is essentially an extended remark. We refer the reader to [18, 19] for missing definitions.

Logics of unbounded branching. We proved the lower bound for a proof system for $\mathbf{IPC}_{\to}$, but it can be generalized to analogous proof systems for some stronger logics, namely implicational fragments of *superintuitionistic (si) logics of unbounded branching.* A si logic L has *branching at most* k if it is complete wrt a class of finite Kripke models such that every node has at most k immediate successors (or if it is included in such a logic); if L does not have branching at most k for any $k \in \omega$, it has *unbounded branching.* We consider $\mathrm{NM}_{\to}$ extended with finitely many axiom schemata as proof systems for such logics. Any implicational logic of unbounded branching is included in $\mathbf{BD}_2$ (the logic of Kripke models of depth 2), which can be axiomatized over $\mathbf{IPC}$ by the schema

$$((\varphi \to ((\psi \to \chi) \to \psi) \to \psi) \to \varphi) \to \varphi \tag{6}$$

(this is an implicational version of the more familiar axiom $\varphi \vee (\varphi \to (\psi \vee \neg\psi))$). It is not a priori clear that the implicational fragment of $\mathbf{BD}_2$ is also axiomatized by (6) over $\mathbf{IPC}_{\to}$, but this can be shown using the criterion in [19, L. 4.11]. Thus, it suffices to prove our lower bound for $\mathrm{NM}_{\to}$ extended with axioms (6). This can be done by a minor modification of the proof of Theorem 3.11: for each instance ω of (6) used in Π, we include ω itself as well as $\varphi \to ((\psi \to \chi) \to \psi) \to \psi$ in P. These formulas are classically valid, hence they will not affect the final argument showing that C interpolates $\neg\alpha_1(\neg\vec{p}, \vec{r}) \to \alpha_0(\vec{p}, \vec{q})$, and their presence in P easily implies $\|_{I,J}\omega$.

Full propositional language. It is straightforward to generalize dag-like natural deduction to the full language $\{\to, \wedge, \vee, \perp\}$ of intuitionistic logic, including a suitable version of Lemma 2.3. The lower bound still holds for this proof system: we can extend Definition 3.4 using the standard Kleene slash conditions

$$\begin{aligned} |(\varphi \wedge \psi) &\iff |\varphi \text{ and } |\psi, \\ |(\varphi \vee \psi) &\iff \|\varphi \text{ or } \|\psi, \end{aligned}$$

and $\nmid\perp$; then we can prove the analogue of Lemma 3.6, and the rest of the argument goes through unchanged.

The only problem is that this generalization interferes with the extension to logics of unbounded branching from the previous paragraph. While positive fragments (i.e., $\{\to, \wedge, \vee\}$) of logics of unbounded branching are still included in $\mathbf{BD}_2$, this is not true for fragments including $\perp$: then we only get that logics of unbounded branching are included in either $\mathbf{BD}_2$ or $\mathbf{KC} + \mathbf{BD}_3$ (see [18, Thm. 6.9]; $\mathbf{KC}$ denotes the logic of weak excluded middle). The proof of the lower bound in the full language works fine for logics included in $\mathbf{BD}_2$ as indicated above, but unfortunately we do not know a direct way of proving it for $\mathbf{KC} + \mathbf{BD}_3$. It seems that in this case we need the reduction to the $\perp$-free fragment as given in [18, L. 6.30] or [19, §4.1].

Frege and Extended Frege. As we already mentioned in the introduction, the result applies to the Frege system for $\mathbf{IPC}_{\to}$, as this is essentially a fragment of $\mathrm{NM}_{\to}$ without the ($\to$I) rule (see Theorem A.5 in the appendix for more details). However, the argument can be adapted to Frege systems directly, using closure under modus ponens (MP) in place of Π-closure. This also works for Frege systems of si logics included in $\mathbf{BD}_2$ in the full propositional language as explained above. Since the lower bound is on the number of lines rather than overall proof size, it also applies to Extended Frege systems.

Separation from Substitution Frege. We have only shown that the τ_n formulas are $\mathbf{IPC}_{\to}$ tautologies, but more constructively, they have polynomial-size (and polynomial-time constructible) proofs in the *Substitution Frege* proof system for $\mathbf{IPC}_{\to}$. This can be demonstrated along the lines of the proof of [19, Thm. 4.22] or [18, L. 6.29]. Thus, for all proof systems subject to the lower bound, we actually obtain an exponential separation from the $\mathbf{IPC}_{\to}$ Substitution Frege system.

Larger bounds. In the first version of this paper, we used tautologies based on the original Clique–Colouring disjoint pair rather than Colouring-Cocolouring. They have larger size, viz. $O(n^2k^2)$, but the monotone circuit lower bound increases even more to $2^{\Omega(k^{1/2})}$ by Alon–Boppana [1]. For $k \approx \sqrt{n}$, this improves the bound in Theorem 3.12 to $2^{\Omega(|\varphi|^{1/12})}$; if we raise k to $\approx (n/\log n)^{2/3}$ (the largest value to which the Alon–Boppana result applies), it improves further to $2^{\Omega(|\varphi|^{1/10}/(\log|\varphi|)^{1/5})}$.

Another possibility to entertain is that the bounds in Theorem 2.6 might be improvable using an ad hoc analysis (perhaps not applicable to real circuits) instead of the general method from Jukna [20] (e.g., note that Jukna's machinery only gives a $2^{\Omega(k^{1/4})}$ lower bound for Clique–Colouring, worse than Alon–Boppana). Say, if we could improve the bound to $2^{\Omega(k^{1/2})} = 2^{\Omega(n^{1/4})}$, the bound in Theorem 3.12 would improve to $2^{\Omega(|\varphi|^{1/10})}$. But this is only a speculation.

5 Conclusion

We have shown how to prove a disjunction-free formulation of feasible disjunction property for implicational intuitionistic logic directly using an efficient version of Kleene's slash, without reintroducing disjunctions into the proof. More generally, we demonstrated an implicational version of Hrubeš-style feasible monotone interpolation, and exploited it to prove exponential lower bounds on the number of lines in dag-like natural deduction $\mathrm{NM}_\to$ for intuitionistic implicational logic (or equivalent familiar systems such as Frege). This provides a simple refutation of Gordeev and Haeusler's claims that all $\mathbf{IPC}_\to$ tautologies have polynomial-size proofs in $\mathrm{NM}_\to$ that should be accessible to a broad logic-aware audience.

Our approach consolidated the proof-theoretic components of the exponential lower bound to a single argument, obviating the need for translation of intuitionistic logic to its implicational fragment, or of dag-like natural deduction to Frege systems. The lower bound is not fully self-contained as we still rely on monotone circuit lower bounds; this combinatorial component of our lower bound has a quite different flavour from the proof-theoretic part and uses quite different techniques, thus it does not look very promising to try to combine them. Fortunately, we believe there is no pressing need for that, as monotone circuit bounds are now a fairly well-understood part of standard literature. The proof of the original Alon–Boppana bound in [1] is neither long nor difficult to follow; likewise, the relevant arguments in [15, 20] are easily accessible.

Acknowledgments

I want to thank Pavel Hrubeš for the suggestion to use tautologies based on the Colouring–Cocolouring principle, and the anonymous referee for improvements in the presentation.

The research was supported by the Czech Academy of Sciences (RVO 67985840) and GA ČR project 23-04825S.

References

[1] Noga Alon and Ravi B. Boppana, *The monotone circuit complexity of Boolean functions*, Combinatorica 7 (1987), no. 1, pp. 1–22.

[2] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, Pavel Pudlák, and Alan Woods, *Exponential lower bounds for the pigeonhole principle*, in: Proceedings of the 24th Annual ACM Symposium on Theory of Computing, 1992, pp. 200–220.

[3] Samuel R. Buss, *Some remarks on lengths of propositional proofs*, Archive for Mathematical Logic 34 (1995), no. 6, pp. 377–394.

[4] 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.

[5] Samuel R. Buss and Jakob Nordström, *Proof complexity and SAT solving*, in: Handbook of Satisfiability (A. Biere, M. Heule, H. van Maaren, and T. Walsh, eds.), Frontiers in Artificial Intelligence and Applications vol. 336, IOS Press, second ed., 2021, ch. 7, pp. 233–350.

[6] Stephen A. Cook and Robert A. Reckhow, *The relative efficiency of propositional proof systems*, Journal of Symbolic Logic 44 (1979), no. 1, pp. 36–50.

[7] Mauro Ferrari, Camillo Fiorentini, and Guido Fiorino, *On the complexity of the disjunction property in intuitionistic and modal logics*, ACM Transactions on Computational Logic 6 (2005), no. 3, pp. 519–538.

[8] Lew Gordeev and Edward Hermann Haeusler, *Proof compression and NP versus PSPACE*, Studia Logica 107 (2019), no. 1, pp. 53–83.

[9] ———, *Proof compression and NP versus PSPACE II*, Bulletin of the Section of Logic 49 (2020), no. 3, pp. 213–230.

[10] ———, *Proof compression and NP versus PSPACE II: Addendum*, Bulletin of the Section of Logic 51 (2022), no. 2, pp. 197–205.

[11] ———, *On proof theory in computer science*, arXiv:2012.04437 [cs.CC], 2020, `https://arxiv.org/abs/2012.04437`.

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

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

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

[15] Pavel Hrubeš and Pavel Pudlák, *Random formulas, monotone circuits, and interpolation*, in: Proceedings of the 58th Annual IEEE Symposium on Foundations of Computer Science, 2017, pp. 121–131.

[16] Raheleh Jalali, *Proof complexity of substructural logics*, Annals of Pure and Applied Logic 172 (2021), no. 7, article no. 102972, 31 pp.

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

[18] ———, *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.

[19] ———, *Proof complexity of intuitionistic implicational formulas*, Annals of Pure and Applied Logic 168 (2017), no. 1, pp. 150–190.

[20] Stasys Jukna, *Boolean function complexity: Advances and frontiers*, Algorithms and Combinatorics vol. 27, Springer, 2012.

[21] Stephen C. Kleene, *Disjunction and existence under implication in elementary intuitionistic formalisms*, Journal of Symbolic Logic 27 (1962), no. 1, pp. 11–18.

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

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

[24] ———, *Proof complexity*, Encyclopedia of Mathematics and its Applications vol. 170, Cambridge University Press, 2019.

[25] Paolo Mancosu, Sergio Galvan, and Richard Zach, *An introduction to proof theory: Normalization, cut-elimination, and consistency proofs*, Oxford University Press, 2021.

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

[27] Dag Prawitz, *Natural deduction: A proof-theoretical study*, Dover Publications, 2006.

[28] Pavel Pudlák, *On the complexity of propositional calculus*, in: Sets and proofs: Invited papers from Logic Colloquium '97 (S. B. Cooper and J. K. Truss, eds.), Cambridge University Press, 1999, pp. 197–218.

[29] Alexander A. Razborov, *Lower bounds on the monotone complexity of some Boolean functions*, Mathematics of the USSR, Doklady 31 (1985), pp. 354–357.

[30] Robert A. Reckhow, *On the lengths of proofs in the propositional calculus*, Ph.D. thesis, Department of Computer Science, University of Toronto, 1976.

[31] Éva Tardos, *The gap between monotone and non-monotone circuit complexity is exponential*, Combinatorica 7 (1987), no. 4, pp. 141–142.

A Equivalence with Frege

Our objective in Section 3 was to prove an exponential lower bound on the size of $\mathrm{NM}_{\to}$-proofs as directly as we could, and in particular, we avoided translation of $\mathrm{NM}_{\to}$ to other proof systems such as Frege. However, no treatment of the proof complexity of $\mathrm{NM}_{\to}$ can be complete without showing that it is, after all, polynomially equivalent to the (intuitionistic implicational) Frege proof system $\mathrm{F}_{\to}$. This is implicit in Reckhow [30] and Cook and Reckhow [6], but they work with a different formulation of natural deduction, and with classical logic, hence it is worthwhile to spell out the reduction adapted to our situation, which is the main goal of this section (Theorems A.5, A.10, and A.16).

Let us mention that even though we formulate the results in this and the next section as only bounds on proof size (and other parameters), they are all constructive in that the relevant proofs can be computed by polynomial-time algorithms.

We start by defining the intuitionistic implicational Frege system $\mathrm{F}_{\to}$.

Definition A.1 A *(sequence-like)* $\mathrm{F}_{\to}$*-derivation* of $\varphi \in \mathrm{Form}$ from $\Gamma \subseteq \mathrm{Form}$ is a finite sequence of formulas $\Pi = \langle \gamma_i : i < t \rangle$ such that $t > 0$, $\gamma_{t-1} = \varphi$, and for each $i < t$: $\gamma_i \in \Gamma$, or γ_i is an instance of one of the logical axioms

$$\text{(A1)} \qquad \alpha \to \beta \to \alpha,$$

$$\text{(A2)} \qquad (\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to (\alpha \to \gamma)$$

for some $\alpha, \beta, \gamma \in \mathrm{Form}$, or γ_i is derived from γ_j and γ_k for some $j, k < i$ by the rule of modus ponens

$$\text{(MP)} \qquad \alpha, \alpha \to \beta \ / \ \beta,$$

i.e., $\gamma_k = (\gamma_j \to \gamma_i)$. The *number of lines* of Π is t, and the *size* of Π is $\|\Pi\| = \sum_{i<t} |\gamma_i|$.

A *dag-like* $\mathrm{F}_{\to}$*-derivation* of φ from Γ is $\Pi = \langle V, E, \gamma \rangle$, where $\langle V, E \rangle$ is a finite dag with a unique node ϱ of out-degree 0 (the *root*), all nodes have in-degree 0 (the *axioms* or *leaves*) or 2 (the (MP)*-nodes*), $\gamma = \langle \gamma_v : v \in V \rangle$ is a labelling of nodes by formulas such that $\gamma_\varrho = \varphi$, all leaves are labelled with elements of Γ or instances of (A1) or (A2), and if v is an (MP)-node with premises v_0 and v_1, then γ_v is derived from γ_{v_0} and γ_{v_1} by (MP). The *number of lines* of Π is $|V|$, and the *size* of Π is $\|\Pi\| = \sum_{v \in V} |\gamma_v|$.

A sequence-like or dag-like $\mathrm{F}_{\to}$*-proof of* φ is a sequence-like or dag-like (resp.) $\mathrm{F}_{\to}$-derivation of φ from $\varnothing$.

The *height* of a dag-like $\mathrm{F}_{\to}$-derivation or $\mathrm{NM}_{\to}$-derivation $\langle V, E, \gamma \rangle$ is the maximal length of a directed path from a leaf to the root. Such a derivation is *tree-like* if the underlying dag $\langle V, E \rangle$ is a tree, i.e., all nodes have out-degree at most 1. Tree-like $\mathrm{F}_{\to}$-derivations and $\mathrm{NM}_{\to}$-derivations are also called $\mathrm{F}^*_{\to}$*-derivations* and $\mathrm{NM}^*_{\to}$*-derivations* (respectively), and likewise for $\mathrm{F}^*_{\to}$-proofs and $\mathrm{NM}^*_{\to}$-proofs.

The *formula size* of a dag-like $\mathrm{F}_{\to}$-derivation or $\mathrm{NM}_{\to}$-derivation $\langle V, E, \gamma \rangle$ is $\max_{v \in V} |\varphi_v|$, and likewise for sequence-like $\mathrm{F}_{\to}$-derivations.

Observe that $\mathrm{NM}^*_{\to}$ is the implicational fragment of the standard natural deduction system. It is well known that sequence-like and dag-like Frege are just different presentations of the same proof system:

Lemma A.2 *A sequence-like (dag-like)* $\mathrm{F}_{\to}$*-derivation of* φ *from* Γ *can be converted to a dag-like (sequence-like, resp.)* $\mathrm{F}_{\to}$*-derivation of* φ *from* Γ *with at most the same size, number of lines, and formula size.*

Proof: Given a sequence-like derivation $\langle \gamma_i : i < t \rangle$ of φ from Γ, put $V = [t]$. Let I be the set of $i < t$ such that γ_i is not an axiom (from Γ, or an instance of (A1) or (A2)); for each $i \in I$, fix $i_0, i_1 < i$ such that γ_i is derived from γ_{i_0} and γ_{i_1} by (MP), and let $E = \{\langle i_j, i \rangle : i \in I, j \in \{0,1\}\}$. Observe that $\langle V, E \rangle$ is acyclic as $E \subseteq {<} \restriction [t]$. Then $\langle V, E, \langle \gamma_i : i < t \rangle \rangle$ is a dag-like $\mathrm{F}_{\to}$-derivation of φ from Γ, possibly after eliminating nodes from which the root $t-1$ is not reachable.

Conversely, let $\langle V, E, \gamma \rangle$ be a dag-like $\mathrm{F}_{\to}$-derivation of φ from Γ, and $t = |V|$. Since $\langle V, E \rangle$ is acyclic, we can find an enumeration $V = \{v_i : i < t\}$ such that $E \subseteq \{\langle v_i, v_j \rangle : i < j\}$ (a "topological ordering" of $\langle V, E \rangle$). The root $\varrho \in V$ is the only node without a successor, hence we must have $\varrho = v_{t-1}$. Then $\langle \gamma_{v_i} : i < t \rangle$ is a sequence-like $\mathrm{F}_{\to}$-derivation of φ from Γ. $\square$

The sequence-like definition is simpler, and is usually taken as the official definition of Frege systems (we follow this usage). Nevertheless, the dag-like definition has other benefits, in particular it allows the introduction of tree-like proofs and the height measure: this cannot be done directly with sequence-like proofs as it depends on the choice of the dag structure, which may not be uniquely determined by the proof sequence alone.

Let us also note basic dependencies between the various proof parameters:

Observation A.3 *An* $\mathrm{NM}_{\to}$*- or (dag-like)* $\mathrm{F}_{\to}$*-derivation with formula size* r *and* t *lines has size at most* rt *and at least* $\max\{r, t\}$*. A derivation with height* h *has less than* 2^{h+1} *lines.*

Proof: The first part is obvious. In a dag with in-degree 2 and root ϱ, there are at most 2^l paths of length l ending in ϱ. Thus, if ϱ is reachable from any node in at most h steps, there are at most $\sum_{l \le h} 2^l = 2^{h+1} - 1$ nodes. $\square$

We mostly consider formula size to be an auxiliary measure that can be used to conveniently bound size as per Observation A.3; it is not that interesting on its own.

A simple, yet very useful, property of Frege and natural deduction systems is that instances of any derivable schema have linear-size proofs. This is convenient for construction of asymptotically short proofs without worrying too much about the choice of basic axioms: we can use *any* valid schematic axioms and rules in a given argument as long as the number of different schemata is kept fixed.

Lemma A.4 *Fix* $\Gamma \subseteq \mathrm{Form}$ *and* $\varphi \in \mathrm{Form}$ *in variables* $\{p_i : i < k\}$ *such that* $\Gamma \vdash \varphi$*. Then for all substitutions* σ*, there are* $\mathrm{F}^*_{\to}$*-derivations and* $\mathrm{NM}^*_{\to}$*-derivations of* $\sigma(\varphi)$ *from* $\sigma(\Gamma)$ *with* $O(1)$ *lines and size* $O(s)$*, where* $s = \sum_{i<k} |\sigma(p_i)|$*. (The constants implied in the* $O(\dots)$ *notation depend on* Γ *and* φ*.) Moreover, we may assume the derivations use each axiom from* $\sigma(\Gamma)$ *only once.*

Proof: Let $\Pi = \langle \gamma_i : i < t \rangle$ be a fixed $\mathrm{F}^*_{\to}$-derivation of φ from Γ such that all variables occurring in Π are among $\{p_i : i < k\}$. Then for any substitution σ, $\langle \sigma(\gamma_i) : i < t \rangle$ is an $\mathrm{F}_{\to}$-derivation of $\sigma(\varphi)$ from $\sigma(\Gamma)$ with t lines and size at most $\|\Pi\|\, s$. The argument for $\mathrm{NM}^*_{\to}$ is completely analogous.

Instead of applying the argument directly to $\Gamma \vdash \varphi$, we may apply it to the $\mathbf{IPC}_{\to}$ tautology $\vdash \Gamma \to \varphi$. This yields tree-like proofs of $\sigma(\Gamma \to \varphi)$ with $O(1)$ lines and size $O(s)$, which we can turn into derivations of $\sigma(\varphi)$ from $\sigma(\Gamma)$ by $|\Gamma|$ applications of (MP)/($\to$E); this ensures that each axiom from $\sigma(\Gamma)$ is used only once. $\square$

The simulation of $\mathrm{F}_{\to}$ by $\mathrm{NM}_{\to}$ is completely straightforward:

Theorem A.5 *If φ has a dag-like $\mathrm{F}_{\to}$-derivation from Γ with t lines, height h, formula size r, and size s, then φ has an $\mathrm{NM}_{\to}$-derivation from Γ with $O(t)$ lines, height $h+O(1)$, formula size $O(r)$, and size $O(s)$. If the original $\mathrm{F}_{\to}$-derivation is tree-like, the $\mathrm{NM}_{\to}$-derivation can also be taken tree-like.*

Proof: Let $\Pi = \langle V, E, \gamma\rangle$ be a dag-like $\mathrm{F}_{\to}$-derivation of φ from Γ. Reinterpreting the (MP)-nodes as ($\to$E)-nodes, Π becomes an $\mathrm{NM}_{\to}$-derivation from Γ plus the instances of (A1) and (A2) that appear in Π. By Lemma A.4, each of the latter can be replaced by a tree-like $\mathrm{NM}_{\to}$-subproof with $O(1)$ lines (thus height $O(1)$) and size linear in the size of the axiom instance, yielding an $\mathrm{NM}_{\to}$-derivation of φ from Γ with the stated parameters. $\square$

For the converse simulation of $\mathrm{NM}_{\to}$ by $\mathrm{F}_{\to}$, we will need proofs of some auxiliary formulas. As proved in [19, L. 2.3], there are short proofs of "structural rules" for $\Gamma \to \varphi$, showing in particular that we can arbitrarily reorder Γ so that we can treat it as a set. We include here optimized proofs of some special cases.

Definition A.6 We extend the $\Gamma \to \varphi$ notation to sequences indexed by finite subsets of integers. If $I \subseteq [m]$ and $\Gamma = \langle \alpha_i : i \in I\rangle = \langle \alpha_i\rangle_{i\in I}$, we define $\Gamma \to \varphi$ by induction on $|I|$: $\langle \alpha_i\rangle_{i\in\varnothing} \to \varphi$ is φ, and if $I \neq \varnothing$, then $\langle \alpha_i\rangle_{i\in I} \to \varphi$ is $\alpha_h \to \langle \alpha_i\rangle_{i\in I\smallsetminus\{h\}} \to \varphi$, where $h = \max I$. (I.e., $\langle \alpha_i\rangle_{i\in I} \to \varphi$ is $\langle \alpha_{i_j}\rangle_{j<n} \to \varphi$, where $\langle i_j : j < n\rangle$ is an increasing enumeration of I.)

If $\Gamma = \langle \alpha_i\rangle_{i\in I}$, we put $\mathrm{dom}(\Gamma) = I$, $|\Gamma| = |I|$, and $\|\Gamma\| = \sum_{i\in I}|\alpha_i|$. We write $\Gamma{\restriction}J = \langle \alpha_i\rangle_{i\in I\cap J}$. If $\Delta = \langle \beta_i\rangle_{i\in J}$, we write $\Gamma \subseteq \Delta$ when $I \subseteq J$ and $\alpha_i = \beta_i$ for all $i \in I$.

First, a general observation that we will keep using to construct proofs of small height:

Lemma A.7 *Given a sequence of formulas $\langle \varphi_i : i \le n\rangle$, $n \ge 1$, there is an $\mathrm{F}^*_{\to}$-derivation of $\varphi_0 \to \varphi_n$ from $\{\varphi_i \to \varphi_{i+1} : i < n\}$ with $O(n)$ lines, height $O(\log n)$, formula size $O(r)$, and size $O(rn)$ that uses each assumption $\varphi_i \to \varphi_{i+1}$ only once, where $r = \max_i|\varphi_i|$.*

Proof: We arrange the implications in a balanced binary tree with n leaves. Formally, we construct for each[4] $k \le \lceil \log n\rceil$ and $i < n$ such that $2^k \mid i$ a derivation Π^k_i of $\varphi_i \to \varphi_{\min\{i+2^k,n\}}$ by induction on k as follows: Π^0_i is the trivial derivation of $\varphi_i \to \varphi_{i+1}$ from itself. Let $k < \lceil \log n\rceil$ and $i < n$ be such that $2^{k+1} \mid i$. If $i + 2^k \ge n$, we put $\Pi^{k+1}_i = \Pi^k_i$; otherwise, we combine Π^k_i and $\Pi^k_{i+2^k}$ to Π^{k+1}_i using an instance of the schematic rule

$$\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \beta,$$

i.e., an $\mathrm{F}^*_{\to}$-derivation of $\varphi_i \to \varphi_{\min\{i+2^{k+1},n\}}$ from $\varphi_i \to \varphi_{i+2^k}$ and $\varphi_{i+2^k} \to \varphi_{\min\{i+2^{k+1},n\}}$ with $O(1)$ lines and size $O(r)$ that uses each assumption only once, which exists by Lemma A.4.

Then $\Pi^{\lceil \log n\rceil}_0$ is the desired derivation of $\varphi_0 \to \varphi_n$. $\square$

[4] In this paper, log denotes base-2 logarithm.

Lemma A.8 *Given sequences of formulas* Γ *and* Δ *such that* $\Delta \subseteq \Gamma$*, and* $\varphi \in \mathrm{Form}$*, there exists an* $\mathrm{F}^*_{\to}$*-proof of*

$$(\Delta \to \varphi) \to (\Gamma \to \varphi) \tag{7}$$

with $O(n)$ *lines, height* $O(\log n)$*, formula size* $O(s)$*, and size* $O(sn)$*, where* $n = \max\{|\Gamma|, 2\}$ *and* $s = \|\Gamma\| + |\varphi|$.

Proof: We may assume $\Gamma = \langle \alpha_i \rangle_{i<n}$ and $\Delta = \langle \alpha_i \rangle_{i \in I}$, $I \subseteq [n]$. For each $i \leq n$, let φ_i denote the formula $(\Delta \restriction [i] \to \varphi) \to (\Gamma \restriction [i] \to \varphi)$. Then $\varphi_i \to \varphi_{i+1}$ is an instance of one of the schemata

$$(\delta \to \gamma) \to (\delta \to \alpha \to \gamma),$$
$$(\delta \to \gamma) \to ((\alpha \to \delta) \to \alpha \to \gamma)$$

with $\delta = (\Delta \restriction [i] \to \varphi)$, $\gamma = (\Gamma \restriction [i] \to \varphi)$, and $\alpha = \alpha_i$, depending on whether $i \in I$. Thus, it has an $\mathrm{F}^*_{\to}$-proof with $O(1)$ lines and size $O(s)$ by Lemma A.4. Using Lemma A.7, we can combine these proofs to a proof of $\varphi_0 \to \varphi_n$ with $O(n)$ lines, height $O(\log n)$, formula size $O(s)$, and size $O(sn)$. Since φ_n is (7), it remains to detach the $\mathbf{IPC}_{\to}$ tautology $\varphi_0 = (\varphi \to \varphi)$, which has a proof with $O(1)$ lines and size $O(|\varphi|)$. □

Lemma A.9 *Given sequences of formulas* Γ*,* Δ*, and* Θ*, and* $\varphi, \psi \in \mathrm{Form}$*, there are* $\mathrm{F}^*_{\to}$*-proofs of*

$$(\Gamma \to \varphi \to \psi) \to (\Gamma \to \varphi) \to (\Gamma \to \psi), \tag{8}$$
$$\Gamma \to (\Gamma \to \varphi) \to \varphi, \tag{9}$$
$$(\Gamma \to \Gamma \to \varphi) \to (\Gamma \to \varphi), \tag{10}$$
$$(\Theta \to \Gamma \to \Delta \to \varphi) \to (\Theta \to \Delta \to \Gamma \to \varphi) \tag{11}$$

with $O(n)$ *lines, height* $O(\log n)$*, formula size* $O(s)$*, and size* $O(sn)$*, where* $n = \max\{|\Gamma| + |\Delta| + |\Theta|, 2\}$ *and* $s = \|\Gamma\| + \|\Delta\| + \|\Theta\| + |\varphi| + |\psi|$.

Proof: We prove (8) using the same strategy as in Lemma A.8: putting

$$\varphi_i = (\Gamma \restriction [i] \to \varphi \to \psi) \to (\Gamma \restriction [i] \to \varphi) \to (\Gamma \restriction [i] \to \psi)$$

for each $i \leq |\Gamma|$, $\varphi_i \to \varphi_{i+1}$ has a proof with $O(1)$ lines and size $O(s)$ as it is an instance of the schema

$$(\beta \to \gamma \to \delta) \to ((\alpha \to \beta) \to (\alpha \to \gamma) \to (\alpha \to \delta)).$$

These proofs combine to a proof of $\varphi_0 \to \varphi_{|\Gamma|}$ with the stated parameters using Lemma A.7. Then $\varphi_{|\Gamma|}$ is (8), and $\varphi_0 = (\varphi \to \psi) \to (\varphi \to \psi)$ has a short proof.

For (9), we put $\varphi_i = ((\Gamma \to \varphi) \to \Gamma \restriction [i] \to \varphi) \to \Gamma \restriction [i] \to (\Gamma \to \varphi) \to \varphi$. Then φ_0 is an instance of $\alpha \to \alpha$, and $\varphi_i \to \varphi_{i+1}$ is an instance of

$$((\alpha \to \beta) \to \delta) \to (\alpha \to \gamma \to \beta) \to \gamma \to \delta$$

(with $\alpha = (\Gamma \to \varphi)$, $\beta = (\Gamma \restriction [i] \to \varphi)$, $\gamma = \gamma_i$, and $\delta = (\Gamma \restriction [i] \to (\Gamma \to \varphi) \to \varphi)$, where $\Gamma = \langle \gamma_i \rangle_{i<|\Gamma|}$). Thus, using Lemmas A.4 and A.7, we obtain an $\mathrm{F}^*_{\to}$-proof of $\varphi_{|\Gamma|}$ with $O(n)$ lines, height $O(\log n)$, formula size $O(s)$, and size $O(sn)$. Detaching the premise $(\Gamma \to \varphi) \to \Gamma \to \varphi$ of $\varphi_{|\Gamma|}$ yields (9).

(10) follows by (MP) from (9) and (8).

(11): We have $(\Gamma \to \Delta \to \varphi) \to (\Delta \to \Gamma \to \Delta \to \Gamma \to \varphi)$ from (7), and $(\Delta \to \Gamma \to \Delta \to \Gamma \to \varphi) \to (\Delta \to \Gamma \to \varphi)$ from (10), thus we obtain (11) when $\Theta = \varnothing$. The general case follows by applying (8). □

Theorem A.10 *If φ has an* $\mathrm{NM}_{\to}$*-derivation from Γ with t lines, height h, and size s, then φ has a dag-like* $\mathrm{F}_{\to}$*-derivation from Γ with $O(t^2)$ lines, height $O(h)$, formula size $O(s)$, and size $O(st^2)$. If the original* $\mathrm{NM}_{\to}$*-derivation is tree-like, the* $\mathrm{F}_{\to}$*-derivation can be taken tree-like as well.*

Proof: Let $\Pi = \langle V, E, \gamma \rangle$ be an $\mathrm{NM}_{\to}$-derivation of φ from Γ. Let $\langle \gamma'_i \rangle_{i<t'}$, $t' \leq t$, be an injective enumeration of the set $\{\gamma_v : v \in V\}$, and for each $v \in V$, let A'_v denote the sequence $\langle \gamma'_i : i < t', \gamma'_i \in A_v \smallsetminus \Gamma \rangle$; notice that $\|A'_v\| \leq s$. We consider the collection of $\mathbf{IPC}_{\to}$ tautologies $\langle A'_v \to \gamma_v : v \in V \rangle$, and complete it to a valid $\mathrm{F}_{\to}$-derivation from Γ using Lemmas A.8 and A.9.

In more detail, for every $v \in V$, we construct an $\mathrm{F}^*_{\to}$-derivation Π_v of $A'_v \to \gamma_v$ from $\{A'_u \to \gamma_u : \langle u, v \rangle \in E\} \cup \Gamma$ with $O(t)$ lines, height $O(\log t)$, and formula size $O(s)$. Moreover, each assumption $A'_u \to \gamma_u$ is used only once, and the path from it to the conclusion has length $O(1)$; both of these properties are obtained by constructing a derivation of $\langle A'_u \to \gamma_u \rangle_{\langle u,v \rangle \in E} \to A'_v \to \gamma_v$ from Γ and applying (MP):

- If v is a leaf, then either $\gamma_v \in \Gamma$ and $A'_v = \varnothing$, in which case we take the trivial derivation of γ_v from itself, or $A'_v = \langle \gamma_v \rangle$, in which case we find an $\mathrm{F}^*_{\to}$-proof of $\gamma_v \to \gamma_v$ with $O(1)$ lines and size $O(s)$ by Lemma A.4.

- If v is an $(\to\mathrm{I})$-node with premise u, we have $\gamma_v = (\alpha \to \beta)$ and $\gamma_u = \beta$ for some α and β, and $A'_v = A'_u \smallsetminus \{\alpha\}$ as a set. If $\alpha \in A'_u$, then $(A'_u \to \beta) \to (A'_v \to \alpha \to \beta)$ is an instance of (11), otherwise it is an instance of (7).

- If v is an $(\to\mathrm{E})$-node with premises u_0 and u_1, then $\gamma_{u_0} = \alpha$, $\gamma_{u_1} = (\alpha \to \beta)$, and $\gamma_v = \beta$ for some α and β. We have $A'_{u_i} \subseteq A'_v$, hence (7) gives $\mathrm{F}^*_{\to}$-proofs of $(A'_{u_0} \to \alpha) \to A'_v \to \alpha$ and $(A'_{u_1} \to \alpha \to \beta) \to A'_v \to \alpha \to \beta$. We infer $(A'_{u_1} \to \alpha \to \beta) \to (A'_{u_0} \to \alpha) \to A'_v \to \beta$ using the instance $(A'_v \to \alpha \to \beta) \to (A'_v \to \alpha) \to A'_v \to \beta$ of (8) and $O(1)$ additional proof lines by Lemma A.4.

Combining these derivations Π_v along the shape of the original derivation Π yields an $\mathrm{F}_{\to}$-derivation (tree-like if Π is tree-like) of φ from Γ with $O(t^2)$ lines, height $O(h + \log t) = O(h)$ (cf. Observation A.3), formula size $O(s)$, and size $O(st^2)$ as promised. □

The bottleneck in the proof of Theorem A.10 is that formulas of the form $\Gamma \to \varphi$ with long Γ are cumbersome to operate as φ is nested deep inside, and when untangling it we need to keep copying large parts of the formula. This could be avoided if we had a conjunction connective: using $\bigwedge \Gamma \to \varphi$ instead, φ sits right at nesting depth 1; if we arrange the big conjunction $\bigwedge \Gamma$ in a balanced binary tree, the individual entries of Γ are also easy to access at nesting depth $O(\log n)$, and wholesale manipulations such as Lemma A.8 can be done using a divide-and-conquer approach that saves size.

We do not have $\wedge$ in implicational logic, as it is not definable in terms of $\to$. However, we may observe that if we fix a formula φ, then formulas α, β of the form $\Phi \to \varphi$ *do* have a definable conjunction operation: α is equivalent to $(\alpha \to \varphi) \to \varphi$, and likewise for β, thus also $\alpha \wedge \beta$ is equivalent to $(\alpha \wedge \beta \to \varphi) \to \varphi$, which can be written as $(\alpha \to \beta \to \varphi) \to \varphi$. This idea was introduced in [19, Prop. 2.6] to prove polynomial simulation of Frege by tree-like Frege for purely implicational logic (cf. Theorem B.3), but here we will use it to improve the bounds in Theorem A.10.

Definition A.11 For any formulas φ, α, and β, we put

$$\begin{aligned} \alpha^{\varphi} &= (\alpha \to \varphi) \to \varphi, \\ \alpha \wedge^{\varphi} \beta &= (\alpha \to \beta \to \varphi) \to \varphi. \end{aligned}$$

For all sequences of formulas $\Gamma = \langle \alpha_i : i \in I \rangle$, $I \subseteq [m]$, we define $\bigwedge^{\varphi}_{i \in I} \alpha_i$, also denoted $\bigwedge^{\varphi} \Gamma$, by induction on m:

$$\bigwedge_{i \in I}^{\varphi} \alpha_i = \begin{cases} \top, & I = \varnothing, \\ \alpha_{i_0}^{\varphi}, & I = \{i_0\}, \\ \bigwedge\limits_{i \in I - 2^k}^{\varphi} \alpha_{2^k + i}, & I \subseteq [2^k, 2^{k+1}), \\ \Big(\bigwedge\limits_{i \in I \cap [2^k]}^{\varphi} \alpha_i \Big) \wedge^{\varphi} \Big(\bigwedge\limits_{i \in I - 2^k}^{\varphi} \alpha_{2^k + i} \Big), & I \subseteq [2^{k+1}], I \cap [2^k] \neq \varnothing \neq I \cap [2^k, 2^{k+1}), \end{cases}$$

where $\top$ is a fixed $\mathbf{IPC}_{\to}$ tautology, $k \geq 0$, and $I - 2^k = \{i : 2^k + i \in I\}$. We write $\bigwedge^{\varphi}_{i<n} \alpha_i$ for $\bigwedge^{\varphi}_{i \in [n]} \alpha_i$.

The idea is that $\bigwedge^{\varphi}_{i<2^k} \alpha_i$ consists of $\wedge^{\varphi}$ arranged in a perfect binary tree of height k, while if $I \subseteq [2^k]$, then $\bigwedge^{\varphi}_{i \in I} \alpha_i$ conforms to the same arrangement except that unused leaves and non-splitting inner nodes are omitted; this ensures that the layouts of $\bigwedge^{\varphi}_{i \in I} \alpha_i$ and $\bigwedge^{\varphi}_{i \in J} \alpha_i$ for any $I, J \subseteq [2^k]$ are compatible, facilitating efficient manipulation of $\bigwedge^{\varphi} \Gamma$ in a divide-and-conquer manner.

Lemma A.12 *The size of $\bigwedge^{\varphi} \Gamma$ is $\|\Gamma\| + O\big(|\varphi|\, n\big)$, where $n = \max\big\{|\Gamma|, 1\big\}$.*

Proof: Observe that the inductive definition introduces $\wedge^{\varphi}$ only when the sequences on both sides are nonempty. Thus, $\bigwedge^{\varphi} \Gamma$ is a binary tree of $\wedge^{\varphi}$ with n leaves where every inner node splits, thus there are $n - 1$ inner nodes. Since α and β occur only once in $\alpha \wedge^{\varphi} \beta$, each node of the tree gives rise to only one subformula of $\bigwedge^{\varphi} \Gamma$; thus, $\bigwedge^{\varphi} \Gamma$ consists of one occurrence of each α_i of total size $\|\Gamma\|$, and $O(1)$ occurrences of φ and $\to$ per each node of the tree of total size $O\big(|\varphi|\, n\big)$. $\square$

The following is a $\bigwedge^{\varphi}$-version of Lemma A.8 that also handles unions of two sequences.

Lemma A.13 *Let $\varphi \in \mathrm{Form}$ and $\Gamma = \langle \alpha_i : i \in I \rangle$ be a sequence of formulas with $|\Gamma| = n \geq 1$ and $I \subseteq [m]$, $m \geq 2$. Let $\Gamma_u = \Gamma \restriction I_u$ for $u = 0, 1, 2$, where $I_u \subseteq I$ are such that $I_2 \subseteq I_0 \cup I_1$. Then there is an $\mathrm{F}^*_{\to}$-proof of*

$$\bigwedge\nolimits^{\varphi}\Gamma_0 \to \bigwedge\nolimits^{\varphi}\Gamma_1 \to \bigwedge\nolimits^{\varphi}\Gamma_2 \tag{12}$$

with $O(n)$ lines, height $O(\log m)$, formula size $O(s + |\varphi|\, n)$, and size $O\big((s + |\varphi|\, n) \log m\big)$, where $s = \|\Gamma\|$.

Proof: We construct the proofs by induction on $\lceil \log m \rceil$. If $m = 2$ or $n = 1$, then (12) has a proof with $O(1)$ lines and size $O(s + |\varphi|)$ by Lemma A.4. If $I \subseteq [2^k, 2^{k+1})$ for some k, we can just apply the induction hypothesis (without changing the proof) to $\Gamma' = \langle \alpha_{2^k+i} : i \in I - 2^k \rangle$ and $\Gamma'_u = \Gamma' \restriction (I_u - 2^k)$, as $\bigwedge^{\varphi}\Gamma_u = \bigwedge^{\varphi}\Gamma'_u$.

Assume that $I \subseteq [2^{k+1}]$ and $I^0, I^1 \neq \varnothing$, where $I^0 = I \cap [2^k]$ and $I^1 = I - 2^k$. For each $u < 3$, put $I^0_u = I_u \cap [2^k]$ and $I^1_u = I_u - 2^k$. Let $\Gamma^0 = \Gamma \restriction I^0$, $\Gamma^1 = \langle \alpha_{2^k+i} : i \in I^1 \rangle$, and $\Gamma^v_u = \Gamma^v \restriction I^v_u$ for each $v < 2$, $u < 3$. There are proofs of

$$\bigwedge\nolimits^{\varphi}\Gamma_u \to \bigwedge\nolimits^{\varphi}\Gamma^v_u, \qquad \bigwedge\nolimits^{\varphi}\Gamma^0_u \to \bigwedge\nolimits^{\varphi}\Gamma^1_u \to \bigwedge\nolimits^{\varphi}\Gamma_u \tag{13}$$

with $O(1)$ lines and size $O(s + |\varphi|\, n)$ using Lemma A.4: if $I^v_u = \varnothing$ for some $v < 2$, then $\bigwedge^{\varphi}\Gamma_u = \bigwedge^{\varphi}\Gamma^{1-v}_u$ and $\bigwedge^{\varphi}\Gamma^v_u = \top$; otherwise, $\bigwedge^{\varphi}\Gamma_u$ is $\big(\bigwedge^{\varphi}\Gamma^0_u\big) \wedge^{\varphi} \big(\bigwedge^{\varphi}\Gamma^1_u\big)$, thus (13) are instances of the valid schemata $(\alpha^0 \to \varphi) \wedge^{\varphi} (\alpha^1 \to \varphi) \to (\alpha^v \to \varphi)$ and $\alpha \to \beta \to \alpha \wedge^{\varphi} \beta$ (observe that each $\bigwedge^{\varphi}\Gamma^v_u$ is of the form $\alpha \to \varphi$ for some formula α).

Using (13), we can construct proofs of

$$\Big(\bigwedge\nolimits^{\varphi}\Gamma^0_0 \to \bigwedge\nolimits^{\varphi}\Gamma^0_1 \to \bigwedge\nolimits^{\varphi}\Gamma^0_2\Big) \to \Big(\bigwedge\nolimits^{\varphi}\Gamma^1_0 \to \bigwedge\nolimits^{\varphi}\Gamma^1_1 \to \bigwedge\nolimits^{\varphi}\Gamma^1_2\Big) \to \Big(\bigwedge\nolimits^{\varphi}\Gamma_0 \to \bigwedge\nolimits^{\varphi}\Gamma_1 \to \bigwedge\nolimits^{\varphi}\Gamma_2\Big) \tag{14}$$

with $O(1)$ lines and size $O(s + |\varphi|\, n)$. The induction hypothesis for Γ^0 and Γ^1 gives us proofs of $\bigwedge^{\varphi}\Gamma^v_0 \to \bigwedge^{\varphi}\Gamma^v_1 \to \bigwedge^{\varphi}\Gamma^v_2$ for $v < 2$, and these together yield (12).

We can imagine the resulting proof as a binary tree of (14) inferences. Since each application of (14) corresponds to splitting I to two nonempty disjoint subsets, each inner node has two children, and the tree has at most n leaves. Thus, the proof has $O(n)$ lines. Each application of (14) also strictly decreases $\lceil \log m \rceil$, hence the height of the proof is $O(\log m)$. The formula size is $O(s + |\varphi|\, n)$ using Lemma A.12.

As for the size of the proof, the root of the tree contributes $O(s + |\varphi|\, n)$. Its two children contribute $O(s_0 + |\varphi|\, n_0)$ and $O(s_1 + |\varphi|\, n_1)$, where $s_0 + s_1 = s$ and $n_0 + n_1 = n$, thus $O(s + |\varphi|\, n)$ together. Continuing the same way, each level of the tree consists of inferences of size $O(s + |\varphi|\, n)$, and there are at most $O(\log m)$ levels, hence the total size is $O\big((s + |\varphi|\, n) \log m\big)$. (More formally, we can prove such a bound by induction on $\lceil \log m \rceil$.) $\square$

We cannot use $\bigwedge^{\varphi} A'_v \to \gamma_v^{\varphi}$ with a fixed formula φ instead of $A'_v \to \gamma_v$ for the simulation of $\mathrm{NM}_{\to}$ by $\mathrm{F}_{\to}$ as in the proof of Theorem A.10, because the ($\to$I)-rule would translate to an unsound inference

$$\bigwedge^{\varphi} A'_v \to \alpha^{\varphi} \to \beta^{\varphi} \vdash \bigwedge^{\varphi} A'_v \to (\alpha \to \beta)^{\varphi}.$$

We will in fact work with $\bigwedge^{\gamma_v} A'_v \to \gamma_v$, but this necessitates that we are able to transform $\bigwedge^{\varphi}\Gamma$ to $\bigwedge^{\psi}\Gamma$ for given φ, ψ:

Lemma A.14 *Let $\varphi, \psi \in \mathrm{Form}$ and $\Gamma = \langle \alpha_i : i \in I \rangle$ be a sequence of formulas with $I \subseteq [m]$, $m \geq 2$. Then there is an $\mathrm{F}^*_{\to}$-proof of*

$$\bigwedge^{\varphi}\Gamma \to \Big(\bigwedge^{\psi}\Gamma\Big)^{\varphi} \tag{15}$$

with $O(n)$ lines, height $O(\log m)$, formula size $O(s + |\varphi|\, n + |\psi|\, n)$, and size $O\big((s + |\varphi|\, n + |\psi|\, n) \log m\big)$, where $n = \max\big\{|\Gamma|, 1\big\}$ and $s = \|\Gamma\|$.

Proof: We construct the proofs by induction on $\lceil \log m \rceil$, similarly to Lemma A.13. If $m = 2$ or $n = 1$, then (15) has a proof with $O(1)$ lines and size $O(s + |\varphi| + |\psi|)$ by Lemma A.4. If $I \subseteq [2^k, 2^{k+1})$ for some k, we can apply the induction hypothesis to $\Gamma' = \langle \alpha_{2^k+i} : i \in I - 2^k \rangle$ without changing the proof. If $I \subseteq [2^{k+1}]$ and $I^0, I^1 \neq \varnothing$, where $I^0 = I \cap [2^k]$ and $I^1 = I - 2^k$, the induction hypothesis applied to $\Gamma^0 = \Gamma \restriction I^0$ and $\Gamma^1 = \langle \alpha_{2^k+i} : i \in I^1 \rangle$ gives proofs of

$$\bigwedge^{\varphi}\Gamma^0 \to \Big(\bigwedge^{\psi}\Gamma^0\Big)^{\varphi}, \qquad \bigwedge^{\varphi}\Gamma^1 \to \Big(\bigwedge^{\psi}\Gamma^1\Big)^{\varphi}.$$

These yield (15) using an instance of the schema

$$(\alpha \to \beta^{\varphi}) \to (\gamma \to \delta^{\varphi}) \to \alpha \wedge^{\varphi} \gamma \to (\beta \wedge^{\psi} \delta)^{\varphi}$$

(we invite the reader to check this is indeed a valid schema).

The resulting proof has the stated size parameters by the same argument as in Lemma A.13. □

Before we get to the improved simulation of $\mathrm{NM}_{\to}$ by $\mathrm{F}_{\to}$, we need to introduce one more size parameter so that we can state the bounds accurately:

Definition A.15 The *inferential size* of a $\mathrm{NM}_{\to}$-derivation or dag-like $\mathrm{F}_{\to}$-derivation $\langle V, E, \gamma \rangle$ is $\sum_{v \in V} s_v$, where $s_v = |\gamma_v| + \sum_{\langle u,v \rangle \in E} |\gamma_u|$.

Clearly, a derivation with t lines and formula size r has inferential size $O(rt)$. A tree-like derivation (or more generally, a derivation where each node has bounded out-degree) of size s has inferential size $O(s)$. We will see later (Lemma B.2) that any dag-like $\mathrm{F}_{\to}$-derivation of size s can be shortened to a derivation with inferential size $O(s)$, but we do not know whether the analogue for $\mathrm{NM}_{\to}$-derivations holds.

Theorem A.16 *If φ has an $\mathrm{NM}_{\to}$-derivation from Γ with t lines, height h, formula size r, and inferential size $\tilde{s}$, then φ has a dag-like $\mathrm{F}_{\to}$-derivation from Γ with $O(t^2)$ lines, height $O(h)$, formula size $O(rt)$, and (inferential) size $O(\tilde{s}t\log t)$. If the original $\mathrm{NM}_{\to}$-derivation is tree-like, the $\mathrm{F}_{\to}$-derivation can be taken tree-like as well.*

Proof: We use the same notation and argument structure as in the proof of Theorem A.10, but we work with the formulas $\delta_v = \bigwedge^{\gamma_v} A'_v \to \gamma_v$ in place of $A'_v \to \gamma_v$. Observe $|\delta_v| = O\bigl(s + |\gamma_v|\,t\bigr) = O(rt)$, where $s = \|\Pi\|$.

For each $v \in V$, we construct an $\mathrm{F}^*_{\to}$-derivation Π_v of $\langle \delta_u \rangle_{\langle u,v\rangle \in E} \to \delta_v$ from Γ with $O(t)$ lines, height $O(\log t)$, formula size $O(s + s_v t) = O(rt)$, and size $O\bigl((s + s_v t)\log t\bigr)$, where $s_v = |\gamma_v| + \sum_{\langle u,v\rangle \in E} |\gamma_u|$:

- The case of v being a leaf is straightforward.

- If v is an ($\to$I)-node with premise u, we have $\gamma_v = (\alpha \to \beta)$ and $\gamma_u = \beta$ for some α and β, and $A'_u \subseteq A'_v \cup \{\alpha\}$ as a set. Lemma A.13 gives a proof of $\bigwedge^{\beta} A'_v \to \alpha^\beta \to \bigwedge^{\beta} A'_u$, which (using $\alpha \to \alpha^\beta$) yields $\delta_u \to \bigwedge^{\beta} A'_v \to \gamma_v$. Combining this with $\bigwedge^{\gamma_v} A'_v \to \bigl(\bigwedge^{\beta} A'_v\bigr)^{\gamma_v}$ from Lemma A.14 gives $\delta_u \to \bigwedge^{\gamma_v} A'_v \to \gamma_v$, i.e., $\delta_u \to \delta_v$.

- If v is an ($\to$E)-node with premises u_0 and u_1, then $\gamma_{u_0} = \alpha$, $\gamma_{u_1} = (\alpha \to \beta)$, and $\gamma_v = \beta$ for some α and β, and $A'_{u_i} \subseteq A'_v$. Using Lemmas A.13 and A.14, we obtain proofs of $\delta_{u_0} \to \bigwedge^{\beta} A'_v \to \alpha^\beta$ and $\delta_{u_1} \to \bigwedge^{\beta} A'_v \to (\alpha \to \beta)^\beta$, which yield $\delta_{u_0} \to \delta_{u_1} \to \bigwedge^{\beta} A'_v \to \beta$ (i.e., $\delta_{u_0} \to \delta_{u_1} \to \delta_v$) using the schema $\alpha^\beta \to (\alpha \to \beta)^\beta \to \beta$.

Combining the Π_v derivations yields an $\mathrm{F}_{\to}$-derivation (tree-like if Π is tree-like) of φ from Γ with $O(t^2)$ lines, height $O(h)$, formula size $O(rt)$, and size $O\bigl(st\log t + \sum_v s_v t \log t\bigr) = O(\tilde{s}t\log t)$.
□

Remark A.17 We can improve the resulting $\mathrm{F}_{\to}$-derivation to a tree-like derivation of height $O(\log t)$ at the expense of a mild size increase: see Theorem B.5.

If we have a real $\wedge$, the $|\gamma_v|$ terms from the size parameters disappear, and we obtain a derivation with formula size $O(s)$ and size $O(st\log t)$ rather than $O(\tilde{s}t\log t)$. It is unclear how to achieve that in the purely implicational setting. One possible improvement is to modify the inductive definition of $\bigwedge^{\varphi}$ so that $\bigwedge^{\varphi}\Gamma = (\Gamma \to \varphi) \to \varphi$ whenever $|\Gamma| \le \ell$, where $\ell \ge 1$ is an extra parameter. Then $\bigwedge^{\varphi}\Gamma$ has size $O\bigl(\|\Gamma\| + |\varphi|\,\frac{n}{\ell}\bigr)$, where $n = \max\bigl\{|\Gamma|, \ell\bigr\}$. The proofs in Lemma A.13 will have formula size $O\bigl(s + |\varphi|\,\frac{n}{\ell}\bigr)$ and size $O\bigl(s(\log m + \ell) + |\varphi|\,\frac{n}{\ell}\log m\bigr)$, and similarly for Lemma A.14. In the context of the proof of Theorem A.16, the optimal choice is $\ell \approx \sqrt{(\tilde{s}/s)\log t}$, which yields an $\mathrm{F}_{\to}$-derivation of φ from Γ with $O(t^2)$ lines, height $O(\log t)$, formula size $O\bigl(s + rt/\ell\bigr)$, and size $O\bigl(st\log t + \sqrt{\tilde{s}st^2\log t}\bigr)$.

Remark A.18 Using similar arguments, we can also prove an efficient version of Lemma 2.1: if φ has an $\mathrm{F}_{\to}$-derivation from $\Gamma = \{\alpha_i : i < n\}$ and Δ with $t \ge n$ lines, height h, formula size r, and size s, then $\bigwedge^{\varphi}\Gamma \to \varphi$ and $\Gamma \to \varphi$ have $\mathrm{F}_{\to}$-derivations from Δ with $O(t)$ lines, height $O(h)$, formula size $O\bigl(r + \|\Gamma\| + |\varphi|\,n\bigr)$, and size $O\bigl(s + (\|\Gamma\| + |\varphi|\,n)t\bigr)$.

B Equivalence of dag-like and tree-like proofs

Our final task is to show that $\mathrm{NM}_{\to}$ and $\mathrm{F}_{\to}$ are polynomially equivalent to their tree-like versions $\mathrm{NM}^*_{\to}$ and $\mathrm{F}^*_{\to}$; more precisely, we will show that an $\mathrm{F}_{\to}$-proof with t lines can be converted to a polynomially larger tree-like proof of height $O(\log t)$ (Theorem B.3), which implies a similar simulation of $\mathrm{NM}_{\to}$ by $\mathrm{NM}^*_{\to}$ (Theorem B.5).

The original argument by Krajíček [22, L. 4.4.8] (stated in the context of classical logic, but intuitionistically valid) relies on conjunctions: given a proof $\langle \gamma_i : i < t\rangle$, we consider the conjunctions $\tau_j = \bigwedge_{i<j} \gamma_i$, construct short tree-like proofs of $\tau_i \to \tau_{i+1}$, and combine them to a proof of τ_t. A purely implicational version of the argument was sketched in [19, Prop. 2.6], using the $\alpha \wedge^{\varphi} \beta$ formulas to emulate conjunctions. We now present the argument in detail, incorporating an extra idea to save proof size: instead of (an implicational emulation of) the long conjunctions $\tau_i \to \tau_{i+1}$, we start with $\tau'_i \to \gamma_i$ where τ'_i only consists of the premises needed to infer γ_i, and we gradually merge these lists of premises in later stages of the proof.

Let us first observe that if we do not care about the exact values of the polynomial bounds, an $O(\log t)$ height bound along with a polynomial formula-size bound is all we need to show, as we will then get tree-like polynomial-size proofs for free:

Lemma B.1 *Let Π be a dag-like $\mathrm{F}_{\to}$-derivation of φ from Γ of height h and formula size r. Then there is a tree-like $\mathrm{F}_{\to}$-derivation Π' of φ from Γ of height h and formula size r, hence with less than 2^{h+1} lines and size $2^{h+1}r$.*

Proof: We can unwind a dag-like derivation $\langle V, E, \gamma\rangle$ with root ϱ to a tree-like derivation $\langle V', E', \gamma'\rangle$ of the same height by taking for V' the set of all paths ending in ϱ, with $\langle p, q\rangle \in E'$ if p initially extends q by one edge, and $\gamma'_p = \gamma_v$ where v is the starting vertex of p. The bounds on the number of lines and size follow from Observation A.3. □

Thus, a reader who is happy with any polynomial may ignore the exact bounds on the number of lines below and concentrate on height bounds, which are easier to verify.

We need one more structural property of $\mathrm{F}_{\to}$-proofs so that we can accurately estimate the resulting proof size. Let us say that an $\mathrm{F}_{\to}$-derivation is *non-redundant* if no formula occurs in it more than once.

Lemma B.2

(i) *Any $\mathrm{F}_{\to}$-derivation of φ from Γ can be made non-redundant by omitting some formulas.*

(ii) *A non-redundant dag-like $\mathrm{F}_{\to}$-derivation of size s has inferential size $O(s)$.*

Proof:

(i): If we omit all but the first occurrence of each formula from a (sequence-like) $\mathrm{F}_{\to}$-derivation, it remains an $\mathrm{F}_{\to}$-derivation.

(ii): Clearly, the total size of axioms (logical or from Γ) is at most s. As for (MP) inferences, the size of an inference $\alpha, \alpha \to \beta \ /\ \beta$ is linear in the size of its second premise $\alpha \to \beta$. In a non-redundant proof, each formula of the form $\alpha \to \beta$ can be used at most once as a second premise of an (MP) inference, because the conclusion of such an inference can only be β, which can only occur once in the derivation. Thus, the total size of (MP) inferences is also $O(s)$. $\Box$

We remark that property (ii) is specific to Frege systems based on (MP) as the only rule of inference; we see no reason it should hold in general. (Another such (MP)-specific property is the last part of Lemma A.4.)

Theorem B.3 *If φ has an $\mathrm{F}_\to$-derivation from Γ with t lines, formula size r, and size s, then it has a tree-like $\mathrm{F}_\to$-derivation from Γ with $O(t\log t)$ lines, height $O(\log t)$, formula size $O(s+|\varphi|\,t)$, and size $O\big((s+|\varphi|\,t)(\log t)^2\big)$.*

Proof: Let $\Pi = \langle \gamma_i : i < t\rangle$ be a derivation of φ from Γ, which we may assume to be non-redundant by Lemma B.2. We fix $E \subseteq {<} \restriction [t]$ that makes $\langle [t], E, \gamma\rangle$ a dag-like derivation by Lemma A.2. For each $j < t$ and $k \le \lceil \log t\rceil$ such that $2^k \mid j$, we put

$$\begin{aligned}
P^k_j &= \big\{ i < j : \exists i' \in [j, j')\, \langle i, i'\rangle \in E \big\},\\
\Gamma^k_j &= \langle \gamma_i : i \in [j, j')\rangle,\\
\Delta^k_j &= \langle \gamma_i : i \in P^k_j\rangle,\\
\tau^k_j &= \textstyle\bigwedge^{\varphi} \Delta^k_j \to \bigwedge^{\varphi}\Gamma^k_j,
\end{aligned}$$

where $j' = \min\{j + 2^k, t\}$. Observe that $|\Gamma^k_j| \le 2^k$, $|\Delta^k_j| = |P^k_j| = O(2^k)$, and $|\tau^k_j| = O\big(\|\Gamma^k_j\| + \|\Delta^k_j\| + |\varphi|\,2^k\big) = O(s_{k,j} + |\varphi|\,2^k)$, where we put $s_i = |\gamma_i| + \sum_{\langle i',i\rangle\in E}|\gamma_{i'}|$ as in Definition A.15, and $s_{k,j} = \sum_{i\in[j,j')} s_i$. Notice that $\sum_i s_i = O(s)$ by Lemma B.2, thus also $\sum_{2^k\mid j} s_{k,j} = O(s)$ for each k.

We construct $\mathrm{F}^*_\to$-derivations Π^k_j of τ^k_j from Γ by induction on k. For $k = 0$, the formula τ^0_j is $\bigwedge^{\varphi}\langle\gamma_i : \langle i, j\rangle \in E\rangle \to \gamma^{\varphi}_j$, which has a derivation from Γ with $O(1)$ lines and size $O(s_j + |\varphi|)$ using Lemma A.4. Assume that Π^k_j have been defined for all $j < t$ such that $2^k \mid j$, and let $j < t$ be such that $2^{k+1} \mid j$. If $j + 2^k \ge t$, we have $\tau^{k+1}_j = \tau^k_j$, thus we can take $\Pi^{k+1}_j = \Pi^k_j$. Otherwise, we combine Π^k_j and $\Pi^k_{j+2^k}$ to Π^{k+1}_j using an $\mathrm{F}^*_\to$-proof of $\tau^k_j \to \tau^k_{j+2^k} \to \tau^{k+1}_j$ with $O(2^k)$ lines, height $O(\log t)$, formula size $O(s_{k+1,j} + |\varphi|\,2^k)$, and size $O\big((s_{k+1,j} + |\varphi|\,2^k)\log t\big)$ that we construct as follows. Observe that Γ^{k+1}_j is the concatenation of Γ^k_j and $\Gamma^k_{j+2^k}$, and $\Delta^k_j \subseteq \Delta^{k+1}_j$, while $\Delta^k_{j+2^k}$ is a concatenation of a subsequence of Δ^{k+1}_j and a subsequence of Γ^k_j. Thus, Lemma A.13 gives us $\mathrm{F}^*_\to$-proofs of

$$\tau^k_j \to \textstyle\bigwedge^{\varphi}\Delta^{k+1}_j \to \bigwedge^{\varphi}\Gamma^k_j,$$

$$\tau^k_{j+2^k} \to \textstyle\bigwedge^{\varphi}\Delta^{k+1}_j \to \bigwedge^{\varphi}\Gamma^k_j \to \bigwedge^{\varphi}\Gamma^k_{j+2^k},$$

$$\textstyle\bigwedge^{\varphi}\Gamma^k_j \to \bigwedge^{\varphi}\Gamma^k_{j+2^k} \to \bigwedge^{\varphi}\Gamma^{k+1}_j.$$

with the stated size parameters. These together imply $\tau^k_j \to \tau^k_{j+2^k} \to \tau^{k+1}_j$.

In the end, $\Pi^{\lceil\log t\rceil}_0$ is a derivation of $\top \to \bigwedge^{\varphi}_{i<t}\gamma_i$ from Γ. This yields $\bigwedge^{\varphi}\langle\gamma_{t-1}\rangle$, i.e., φ^{φ}, using Lemma A.13, and we can infer φ.

It is clear that the whole derivation has height $O(\log t)$ and formula size $O(s + |\varphi|\, t)$. The derivations Π^0_j have together $O(t)$ lines and size $O\bigl(\sum_j (s_j + |\varphi|)\bigr) = O(s + |\varphi|\, t)$. Likewise, for each $k < \lceil \log t \rceil$, there are $t/2^{k+1}$ subproofs of $\tau^k_j \to \tau^k_{j+2^k} \to \tau^{k+1}_j$ with $O(2^k)$ lines each, which together makes $O(t)$ lines of size $O\bigl(\sum_{2^{k+1}|j} (s_{k+1,j} + |\varphi|\, 2^k) \log t\bigr) = O\bigl((s + |\varphi|\, t) \log t\bigr)$. Summing over all $k < \lceil \log t \rceil$, the whole derivation has $O(t \log t)$ lines and size $O\bigl((s + |\varphi|\, t)(\log t)^2\bigr)$. $\square$

Remark B.4 We could avoid the machinery of $\bigwedge^{\varphi}\Gamma$ formulas by defining $\tau^k_j = (\Gamma^k_j \to \varphi) \to (\Delta^k_j \to \varphi)$, and using Lemmas A.8 and A.9 in place of Lemma A.13, yielding an $\mathrm{F}^*_{\to}$-derivation with $O(t \log t)$ lines, height $O(\log t)$, formula size $O(s)$, and size $O(st + |\varphi|\, t \log t)$.

If we have a real $\wedge$, the $|\varphi|$ terms from the size parameters disappear: we obtain a derivation with $O(t \log t)$ lines, height $O(\log t)$, formula size $O(s)$, and size[5] $O\bigl(s(\log t)^2\bigr)$.

Back in the implicational setting, we can alternatively use $\bigwedge^p$ in place of $\bigwedge^{\varphi}$, where p is the right-most variable occurrence in φ, i.e., φ is of the form $\Phi \to p$ for some sequence Φ. This reduces all the $|\varphi|$ terms in the size parameters to $O(1)$: we obtain a derivation of φ^p from Γ with $O(t \log t)$ lines, height $O(\log t)$, formula size $O(s)$, and size $O\bigl(s(\log t)^2\bigr)$. We can construct a proof of $\varphi^p \to \varphi$ using Lemma A.9: two instances of (9) give $\Phi \to (((\Phi \to p) \to p) \to p) \to p$, and (11) yields $(((\Phi \to p) \to p) \to p) \to \Phi \to p$. We obtain an $\mathrm{F}^*_{\to}$-derivation of φ from Γ with $O(t \log t + n)$ lines, height $O\bigl(\log(t + n)\bigr)$, formula size $O(s)$, and size $O\bigl(s(\log t)^2 + |\varphi|\, n\bigr)$, where $n = |\Phi| \le |\varphi|$. Furthermore, if the $\mathbf{IPC}_{\to}$ tautology $\Gamma \to \varphi$ is not a substitution instance of any strictly smaller $\mathbf{IPC}_{\to}$ tautology, then $n = O(t)$ because of [22, L. 4.4.4], which simplifies the bounds to $O(t \log t)$ lines, height $O(\log t)$, formula size $O(s)$, and size $O\bigl(s(\log t)^2 + |\varphi|\, n\bigr)$.

We can also modify the definition of $\bigwedge^{\varphi}$ using an extra parameter ℓ as in Remark A.17. In the context of the proof of Theorem B.3, the optimal choice is $\ell \approx \sqrt{|\varphi|\, t(\log t)/s}$, which yields an $\mathrm{F}^*_{\to}$-derivation of φ from Γ with $O(t \log t)$ lines, height $O(\log t)$, formula size $O\bigl(s + \sqrt{|\varphi|\, st/\log t}\bigr)$, and size $O\bigl(s(\log t)^2 + \sqrt{|\varphi|\, st(\log t)^3}\bigr)$.

Theorems A.10 or A.16, B.3, and A.5 imply a polynomial simulation of $\mathrm{NM}_{\to}$ by $\mathrm{NM}^*_{\to}$, but we can obtain better bounds by taking into account that the building blocks of the proofs constructed in Theorems A.10 and A.16 are already tree-like:

Theorem B.5 *If φ has an $\mathrm{NM}_{\to}$-derivation from Γ with t lines, size s, and inferential size $\tilde{s}$, then it has an $\mathrm{F}^*_{\to}$-derivation and an $\mathrm{NM}^*_{\to}$-derivation from Γ with $O(t^2)$ lines, height $O(\log t)$, formula size $O(st)$, and size $O\bigl(\min\{st^2, \tilde{s}t(\log t)^2\}\bigr)$.*

Proof: In view of Theorem A.5, it suffices to construct an $\mathrm{F}^*_{\to}$-derivation.

We combine the arguments in Theorems A.16 and B.3. Let $\Pi = \langle V, E, \gamma \rangle$ be an $\mathrm{NM}_{\to}$-derivation of φ from Γ. By considering a topological ordering of $\langle V, E \rangle$, we may assume $V = [t]$ and $E \subseteq {<}\restriction[t]$. As in the proof of Theorem A.16, let $\langle \gamma'_i \rangle_{i<t'}$, $t' \le t$, be an injective enumeration of the set $\{\gamma_i : i < t\}$, and for each $i < t$, let A'_i denote the sequence $\langle \gamma'_j : j < t', \gamma'_j \in A_i \smallsetminus \Gamma \rangle$. Put $\delta_i = \bigwedge^{\gamma_i} A'_i \to \gamma_i$; we have $|\delta_i| = O(s + |\gamma_i|\, t)$.

[5] [22, L. 4.4.8] seemingly claims an even better bound $O(s \log t)$, but this is a typo, as the argument only warrants size $O(st \log t)$; cf. `https://www.karlin.mff.cuni.cz/~krajicek/upravy.html`.

Similarly to the proof of Theorem B.3, for all $j < t$ and $k \leq \lceil \log t \rceil$ such that $2^k \mid j$, we put

$$\begin{aligned}
P_j^k &= \bigl\{ i < j : \exists i' \in [j, j')\, \langle i, i' \rangle \in E \bigr\}, \\
\Gamma_j^k &= \langle \delta_i : i \in [j, j') \rangle, \\
\Delta_j^k &= \langle \delta_i : i \in P_j^k \rangle, \\
\tau_j^k &= \bigwedge\nolimits^{\varphi} \Delta_j^k \to \bigwedge\nolimits^{\varphi} \Gamma_j^k,
\end{aligned}$$

where $j' = \min\{j + 2^k, t\}$. We have $|\Gamma_j^k| \leq 2^k$ and $|\Delta_j^k| = |P_j^k| = O(2^k)$, thus $|\tau_j^k| = O\bigl(\|\Gamma_j^k\| + \|\Delta_j^k\| + |\varphi|\, 2^k\bigr) = O(s2^k + s_{k,j}t)$, where $s_{k,j} = \sum_{j \leq i < j'} |\gamma_i| + \sum_{i \in P_j^k} |\gamma_i| \leq s$. Observe $s_{k,j} \leq \sum_{j \leq i < j'} s_{0,i}$, thus for a fixed k, $\sum_j s_{k,j} \leq \sum_{i<t} s_{0,i} = \tilde{s}$. We will now construct $\mathrm{F}^*_{\to}$-derivations Π_j^k of τ_j^k from Γ by induction on k.

As shown in the proof of Theorem A.16, for each $j < t$, there is an $\mathrm{F}^*_{\to}$-derivation of $\Delta_j^0 \to \delta_j$ from Γ with $O(t)$ lines, height $O(\log t)$, formula size $O(s + s_{0,j}t)$, and size $O\bigl((s + s_{0,j}t) \log t\bigr)$. We can infer $\bigwedge^{\varphi} \Delta_j^0 \to \gamma_j^{\varphi}$, which is τ_j^0, using $O(1)$ extra lines of size $O(s + s_{0,j}t)$; we denote the resulting derivation Π_j^0. In total, these derivations have $O(t^2)$ lines, height $O(\log t)$, formula size $O(rt)$ (where r is the formula size of Π) and size $O(\tilde{s}t \log t)$.

Let $k < \lceil \log t \rceil$ and $j < t$ be such that $2^{k+1} \mid j$. If $j + 2^k \geq t$, then $\tau_j^{k+1} = \tau_j^k$, and we put $\Pi_j^{k+1} = \Pi_j^k$. Otherwise, we combine Π_j^k and $\Pi_{j+2^k}^k$ to Π_j^{k+1} using an $\mathrm{F}^*_{\to}$-proof of $\tau_j^k \to \tau_{j+2^k}^k \to \tau_j^{k+1}$ as constructed in the proof of Theorem B.3: it has $O(2^k)$ lines, height $O(\log t)$, formula size $O(s2^k + s_{k+1,j}t) = O(st)$, and size $O\bigl((s2^k + s_{k+1,j}t) \log t\bigr)$; summing this over all j for a fixed k gives $O(t)$ lines of total size $O(\tilde{s}t \log t)$.

Altogether, $\Pi_0^{\lceil \log t \rceil}$ has $O(t^2)$ lines, height $O(\log t)$, formula size $O(st)$, and size $O\bigl(\tilde{s}t(\log t)^2\bigr)$. It is a derivation of $\top \to \bigwedge^{\varphi}_{i<t} \delta_i$ from Γ. Since $\delta_{t-1} = \top \to \varphi$, we can infer φ using Lemma A.13 without asymptotically increasing any of the size parameters.

We can obtain the $O(st^2)$ size bound similarly, using $\delta_i = A_i' \to \gamma_i$ as in the proof of Theorem A.10 in place of Theorem A.16; in this case, we can avoid usage of the $\bigwedge^{\varphi}$ formulas entirely as in Remark B.4. □

We mention that if we have a real $\wedge$, the size bound improves to $O\bigl(st(\log t)^2\bigr)$.