On the proof complexity of logics of bounded branching

Emil Jeřábek

Institute of Mathematics, Czech Academy of Sciences

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

May 16, 2022

Abstract

We investigate the proof complexity of extended Frege (EF) systems for basic transitive modal logics (**K4**, **S4**, **GL**, ...) augmented with the bounded branching axioms $\mathbf{BB}_k$. First, we study feasibility of the disjunction property and more general extension rules in EF systems for these logics: we show that the corresponding decision problems reduce to total coNP search problems (or equivalently, disjoint NP pairs, in the binary case); more precisely, the decision problem for extension rules is equivalent to a certain special case of interpolation for the classical EF system. Next, we use this characterization to prove superpolynomial (or even exponential, with stronger hypotheses) separations between EF and substitution Frege (SF) systems for all transitive logics contained in $\mathbf{S4.2GrzBB_2}$ or $\mathbf{GL.2BB_2}$ under some assumptions weaker than PSPACE $\neq$ NP. We also prove analogous results for superintuitionistic logics: we characterize the decision complexity of multi-conclusion Visser's rules in EF systems for Gabbay–de Jongh logics $\mathbf{T}_k$, and we show conditional separations between EF and SF for all intermediate logics contained in $\mathbf{T}_2 + \mathbf{KC}$.

Keywords: proof complexity, modal logic, intermediate logic, extended Frege system, disjunction property

MSC (2020): 03F20 (primary) 03B45, 03B55 (secondary)

1 Introduction

The primary focus of proof complexity is on questions about lengths of derivations or refutations in proof systems for classical propositional logic **CPC** (including algebraic proof systems dealing with polynomial equations or inequalities, into which Boolean tautologies can be easily translated). While lower bounds on systems such as resolution exhibit limitations of SAT-solving technology, the original motivation comes from computational complexity, as the fundamental problem NP $\neq$ coNP is equivalent to superpolynomial lower bounds on all proof systems for **CPC**. Despite years of effort, we can currently only prove lower bounds on relatively weak systems such as constant-depth Frege. The unrestricted Frege system (the simplest textbook proof system for **CPC**, also p-equivalent to sequent or natural deduction calculi) is well out of reach.

The situation is rather different in proof complexity of nonclassical propositional logics such as modal logics or intuitionistic logic, where Frege and related systems are the main objects of study. First, unlike the plethora of classical proof systems, there are not many alternatives to variants of Frege systems (or equivalent sequent calculi) in nonclassical logics, though *extended Frege* (EF) systems are perhaps even more natural, or at least more robust: on the one hand, extension axioms formalize the intuitive practice of naming longer formulas so that they can be referred to succinctly in the proof; on the other hand, bounds on the size of EF proofs are essentially equivalent to bounds on the *number of lines* in Frege (or EF) proofs, which is a measure easier to work with than size, and EF systems can be thought of as Frege systems operating with *circuits* instead of formulas, which makes many arguments go through more smoothly.

Crucially, there are a number of nontrivial results on the complexity of Frege and EF systems in various nonclassical logics, in contrast to **CPC**. The underlying theme in many works on the proof complexity of modal or (super)intuitionistic logics is that of *feasibility of the disjunction property* (DP): given a proof of $\Box\varphi_0 \vee \Box\varphi_1$ (or just $\varphi_0 \vee \varphi_1$ in the intuitionistic case), can we efficiently decide which φ_u is provable, or better yet, can we construct its proof?

Buss and Mints [1] proved the feasibility of DP in the natural deduction system for intuitionistic logic (**IPC**); Buss and Pudlák [2] extended this result, and made the important connection that it implies *conditional lower bounds* in a similar way as feasible interpolation does in classical proof systems. Feasibility of DP for some modal proof systems was shown by Ferrari et al. [6]. Mints and Kojevnikov [20] generalized feasible DP in **IPC** to feasibility of *Visser's rules*, and used it to show that all Frege systems for **IPC** are p-equivalent, even if allowed to include inference rules that are not valid, but merely admissible. A similar result was proved for a certain family of transitive modal logics by Jeřábek [12], using feasibility of modal *extension rules* generalizing DP.

A breakthrough was achieved by Hrubeš [8, 9, 10] who proved *unconditional* exponential lower bounds on (effectively) EF proofs in some modal logics and **IPC**, using a modified version of feasible DP as a form of monotone interpolation. Building on his results, Jeřábek [14] proved exponential separation between EF and *substitution Frege* (SF) systems for a class of transitive modal and superintuitionistic logics, while EF and SF systems are equivalent for some other classes of logics (this equivalence was well known for classical EF and SF systems).

More specifically, it was shown in [14] that the proof complexity of modal and superintuitionistic logics is connected to their model-theoretic properties, in particular frame measures such as *width* (maximum size of finite antichains) and *branching* (maximum number of immediate successors): on the one hand, L-SF has exponential speed-up over L-EF for all transitive modal or superintuitionistic logics L of unbounded branching. On the other hand, L-EF and L-SF are p-equivalent (and, in a suitable sense, p-equivalent to **CPC**-EF) for many logics of bounded width: basic logics of bounded width such as $\mathbf{K4BW}_k$, $\mathbf{S4BW}_k$, $\mathbf{GLBW}_k$, and **LC**, all logics of bounded width and depth, and—for a restricted class of tautologies—all cofinal-subframe logics of bounded width. Note that branching is upper bounded by width, hence all logics of bounded width have bounded branching, but the converse is not true—there are logics of branching 2 and unbounded width.

Although these results reveal considerable information about modal EF systems, they do not precisely delimit the boundary between logics for which we have unconditional EF lower bounds and separations from SF, and logics where EF and SF are equivalent and lower bounds on them imply classical EF lower bounds; nor do they establish that such a sharp boundary exists in the first place. Can we say something about the proof complexity of EF for logics of bounded branching and unbounded width? (Cf. [14, Prob. 7.1].)

This is the question we take up in the present paper. We look at basic logics L of bounded branching such as $\mathbf{K4BB}_k$, $\mathbf{S4BB}_k$, and $\mathbf{GLBB}_k$ (more generally, extensible logics as in [12] augmented with the bounded branching axioms $\mathbf{BB}_k$). First, we study the feasibility of DP and extension rules for L-EF: while they are (probably) no longer decidable in polynomial time as was the case for extensible logics, we will show that they are decidable by total coNP search problems (or equivalently, disjoint NP pairs, for two-conclusion rules), which is still much smaller complexity than the trivial PSPACE upper bound. As a consequence, we prove a superpolynomial separation between L-EF and L-SF unless PSPACE = NP = coNP; in fact, this holds not just for the basic logics of bounded branching, but for all logics included in $\mathbf{GLBB_2}$ or $\mathbf{S4GrzBB_2}$. (Note that logics with the DP are PSPACE-hard, hence PSPACE $\neq$ NP implies superpolynomial lower bounds on *all* proof systems for these logics; however, such trivial arguments cannot separate L-EF from L-SF.) The speed-up of L-SF over L-EF can be improved to exponential if we assume PSPACE $\nsubseteq$ NSUBEXP.

We elaborate our basic argument by internalizing parts of it in the EF system itself. In this way, we can characterize the complexity of extension rules for EF systems of basic logics of bounded branching exactly: they are equivalent to certain special cases of *interpolation* for **CPC**-EF. We also extend the argument to cover monotone interpolation in the style of Hrubeš [8, 10]. This leads to separations of L-EF from L-SF under weaker hypotheses than PSPACE $\neq$ NP, but unfortunately we still do not obtain unconditional separations or lower bounds.

We extend the scope of our results in two ways. First, by using positive ($\bot$-free) tautologies, we show (under the same hypotheses) that L-SF has a superpolynomial speed-up over L-EF for a class of logics L that includes all logics contained in $\mathbf{S4.2GrzBB_2}$ or $\mathbf{GL.2BB_2}$. Second, we adapt our results to *superintuitionistic logics*: we characterize the complexity of Visser's rules (which generalize the intuitionistic DP) for EF systems of the Gabbay–de Jongh logics $\mathbf{T}_k$, and we prove a conditional superpolynomial speed-up of L-SF over L-EF for all logics $L \subseteq \mathbf{T}_2 + \mathbf{KC}$.

The paper is organized as follows. In Section 2, we review the necessary background on modal logics, their proof complexity, and extension rules. Section 3 presents an overview of the main results. Section 4 presents the reduction of extension rules for EF systems of our logics to coNP search problems, and the ensuing separation between EF and SF conditional on PSPACE $\neq$ NP. In Section 5 we internalize the argument inside EF, leading to separation under weaker assumptions, and in Section 6 we extend it to Hrubeš-style monotone interpolation, leading to further weakening of the assumptions. The separations between EF and SF are generalized to a larger class of logics using positive tautologies in Section 7, and parallel results for superintuitionistic logics are proved in Section 8. We conclude the paper with a few remarks and open problems in Section 9.

2 Preliminaries

As a general notational convention, we denote the set of natural numbers (including 0) by ω, and unless stated otherwise, our indices and similar integer variables start from 0, so that, e.g., $\{\varphi_i : i < n\}$ means $\{\varphi_0, \dots, \varphi_{n-1}\}$, and $\bigvee_{i<n} \varphi_i$ is $\varphi_0 \vee \dots \vee \varphi_{n-1}$. If $n = 0$, we understand $\bigvee_{i<n} \varphi_i$ as $\bot$, and $\bigwedge_{i<n} \varphi_i$ as $\top$.

2.1 Modal logic

We refer the reader to Chagrov and Zakharyaschev [4] for background on modal logic.

We consider monomodal propositional modal logics in a language using countably infinitely many propositional variables p_i, $i \in \omega$ (often denoted also by other letters such as q, r, … for convenience), a complete set of Boolean connectives (say, $\{\wedge, \vee, \to, \neg, \top, \bot\}$, but for the most part the choice will not matter), and a unary modal connective $\Box$. Let Var denote the set of variables, and Form the set of formulas. We define the abbreviations $\Diamond\varphi = \neg\Box\neg\varphi$, $\boxdot\varphi = \varphi \wedge \Box\varphi$, and $\diamonddot\varphi = \neg\boxdot\neg\varphi$. We will generally denote formulas by lower-case Greek letters φ, ψ, …, or upper-case Latin letters A, B, C, …. If X is a formula or a set of formulas, then $\mathrm{Sub}(X)$ denotes the set of subformulas of (formulas from) X.

A *normal modal logic* is a set of formulas L that contains all classical (Boolean) tautologies and the schema

$$(\mathbf{K}) \qquad \Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi),$$

and it is closed under substitution and the rules of modus ponens and necessitation:

$$(\mathrm{MP}) \qquad \varphi, \varphi \to \psi \,/\, \psi,$$

$$(\mathrm{Nec}) \qquad \varphi \,/\, \Box\varphi.$$

Elements of L are also more explicitly called *L-tautologies*. The *consequence relation* $\vdash_L$ of L is defined such that for any set of formulas $\Gamma \cup \{\varphi\}$, $\Gamma \vdash_L \varphi$ iff φ is in the closure of $L \cup \Gamma$ under (MP) and (Nec). The least normal modal logic is denoted $\mathbf{K}$.

If L is a normal modal logic and X a formula or a set of formulas, let $L \oplus X$ be the least normal modal logic containing $L \cup X$, i.e., the closure of L and substitution instances of X under (MP) and (Nec). A logic is *finitely axiomatizable* if can be written as $\mathbf{K} \oplus \varphi$ for some formula φ (or equivalently, $\mathbf{K} \oplus X$ for a finite set X).

A *transitive modal logic* is a normal modal logic that also includes the schema

$$(\mathbf{4}) \qquad \Box\varphi \to \Box\Box\varphi.$$

The least transitive modal logic is denoted $\mathbf{K4}$. Unless stated otherwise, all logics in this paper are *finitely axiomatizable transitive modal logics*; we will also write $\mathbf{K4} \subseteq L$ as a shorthand for L being a (finitely axiomatizable transitive modal) logic.

A (transitive) *Kripke frame* is a pair $\langle W, < \rangle$ where $<$ is a transitive relation on a set W. (Such notation is not meant to imply that $<$ is irreflexive.) We will write $x \le y$ for $x < y \vee x = y$, $x \sim y$ for $x \le y \wedge y \le x$, and $x \lneqq y$ for $x < y \wedge y \not< x$. Equivalence classes of $\sim$ are called *clusters*, and the quotient partial order $\langle W, \leq\rangle/{\sim}$ is called the *skeleton* of $\langle W, <\rangle$. The cluster of a point x is denoted $\mathrm{cl}(x)$. If $X \subseteq W$, let

$$
\begin{aligned}
X{\downarrow} &= \{y \in W : \exists x \in X\, (y < x)\}, \\
X\underline{\uparrow} &= \{y \in W : \exists x \in X\, (x \leq y)\},
\end{aligned}
$$

and similarly for $X{\uparrow}$, $X\overline{\downarrow}$. A frame $\langle W, <\rangle$ is called *rooted* if $W = \{x\}\underline{\uparrow}$ for some $x \in W$; any such x is called the *root* of W. A point $x \in W$ is called *reflexive* if $x < x$, and *irreflexive* otherwise. As a general notational convention, we will denote irreflexive points and related objects with $\bullet$, and reflexive points with $\circ$.

A *valuation* in a Kripke frame $\langle W, <\rangle$ is a mapping $v\colon \mathrm{Var} \to \mathcal{P}(W)$. A *Kripke model* is $M = \langle W, <, v\rangle$, where $F = \langle W, <\rangle$ is a Kripke frame, and v a valuation in F. The valuation uniquely defines a satisfaction relation for all formulas:

$$
\begin{aligned}
&M, x \vDash p_i && \iff x \in v(p_i), \\
&M, x \vDash c(\varphi_0, \dots, \varphi_{d-1}) && \iff c\big((M, x \vDash \varphi_0), \dots, (M, x \vDash \varphi_{d-1})\big), \quad c \in \{\wedge, \vee, \to, \neg, \top, \bot\}, \\
&M, x \vDash \Box\varphi && \iff \forall y \in W\, (x < y \implies M, y \vDash \varphi).
\end{aligned}
$$

Instead of $M, x \vDash \varphi$, we may write $F, x \vDash \varphi$ or just $x \vDash \varphi$ if the model or frame is understood from the context. We define

$$
\begin{aligned}
M \vDash \varphi &\iff \forall x \in W\; M, x \vDash \varphi, \\
F \vDash \varphi &\iff \forall v\colon \mathrm{Var} \to \mathcal{P}(W)\; \langle W, <, v\rangle \vDash \varphi.
\end{aligned}
$$

A *(general) frame* is $F = \langle W, <, A\rangle$, where $\langle W, <\rangle$ is a Kripke frame, and $A \subseteq \mathcal{P}(W)$ is a Boolean algebra of sets, closed under the operation $X \mapsto \Box X = \{x \in W : \forall y > x\, (y \in X)\}$, or equivalently, under $X \mapsto X{\downarrow}$. An *admissible valuation* in the frame F is a map $v\colon \mathrm{Var} \to A$; the closure conditions on A ensure that the resulting model $\langle W, <, v\rangle$ (which is said to be *based on* F) satisfies $\{x \in W : x \vDash \varphi\} \in A$ for all formulas φ. We put

$$
F \vDash \varphi \iff \forall v\colon \mathrm{Var} \to A\; \langle W, <, v\rangle \vDash \varphi.
$$

If $F \vDash \varphi$, we say that φ is *valid* in F. We will identify a Kripke frame $\langle W, <\rangle$ with the frame $\langle W, <, \mathcal{P}(W)\rangle$. If L is a logic, an *L-frame* is a frame F such that $F \vDash \varphi$ for all $\varphi \in L$, and an *L-model* is a model based on an L-frame. A frame $\langle W, <, A\rangle$ is *refined* if

$$
\begin{aligned}
x < y &\iff \forall X \in A\, (x \in \Box X \implies y \in X), \\
x = y &\iff \forall X \in A\, (x \in \quad X \implies y \in X),
\end{aligned}
$$

for all $x, y \in W$, and a refined frame is *descriptive* if A is compact: every $S \subseteq A$ with the finite intersection property has a nonempty intersection. Kripke frames are refined. Every logic L is complete w.r.t. a class of descriptive frames (whereas some logics are not complete w.r.t. Kripke frames): i.e., if $\nvdash_L \varphi$, there exists a descriptive L-frame F such that $F \nvDash \varphi$. If a frame $F = \langle W, <, A\rangle$ is finite, the atoms of A define a partition of W, and the quotient of F by

logic	axiomatization over **K4**	finite rooted frames
S4	$\Box\varphi \to \varphi$	reflexive
D4	$\Diamond\top$	final clusters reflexive
GL	$\Box(\Box\varphi \to \varphi) \to \Box\varphi$	irreflexive
K4Grz	$\Box\big(\Box(\varphi \to \Box\varphi) \to \varphi\big) \to \Box\varphi$	no proper clusters
K4.1	$\boxdot\Diamond\varphi \to \Diamond\Box\varphi$	no proper final clusters
K4.2	$\Diamond\boxdot\varphi \to \Box\Diamonddot\varphi$	unique final cluster
K4.3	$\Box(\boxdot\varphi \to \psi) \lor \Box(\Box\psi \to \varphi)$	linear (width 1)
K4B	$\varphi \to \Box\Diamond\varphi$	single cluster
S5	**S4** $\oplus$ **K4B**	single reflexive cluster
K4BW$_k$	$\bigvee\limits_{i\le k} \Box\Big(\bigwedge\limits_{j\ne i} \boxdot\varphi_j \to \varphi_i\Big)$	width at most k
K4BD$_k$	(see below)	depth at most k
K4BC$_k$	$\Box\Big[\bigvee\limits_{i\le k} \Box\Big(\bigwedge\limits_{j<i} \varphi_j \to \varphi_i\Big) \to \bigwedge\limits_{i\le k} \varphi_i\Big] \to \Box\varphi_0$	cluster size at most k
K4BB$_k$	(see below)	branching at most k
S4.1.4	$\Box\big(\Box(\varphi \to \Box\varphi) \to \varphi\big) \to (\Box\Diamond\Box\varphi \to \varphi)$	reflexive, no inner proper clusters

Table 1: Some transitive modal logics

the corresponding equivalence relation is a Kripke frame that validates the same formulas as F. For this reason, there is no loss of generality if we reserve the phrase *finite frame* to denote finite Kripke frames. A logic L has the *finite model property* (FMP) if it is complete w.r.t. a class of finite frames.

Several common (or otherwise interesting) transitive modal logics are listed in Table 1, along with frame conditions that characterize them on finite rooted frames. (A cluster is *proper* if it has ≥ 2 elements. It is *final* if it has no successor clusters, otherwise it is *inner*. Other semantic conditions are described below.) Some of the entries are redundant: **K4Grz** $=$ **K4BC$_1$**, **K4.3** $=$ **K4BW$_1$**, **K4B** $=$ **K4BD$_1$**. We will generally form compound names of logics by stacking axiom names on a base logic without $\oplus$ symbols, so that, e.g., **S4.2GrzBB$_2$** $=$ **S4** $\oplus$ **K4.2** $\oplus$ **K4Grz** $\oplus$ **K4BB$_2$**. An exception is **S4.1.4**, which is not a systematic name, but a meaningless numerical label (see Zeman [25]).

If $F = \langle W, <, A\rangle$ is a frame, and $U \subseteq W$ is an upper subset (i.e., $U{\uparrow} = U$), then $\langle U, <_U, A_U\rangle$ is a *generated subframe* of F, where $<_U \,=\, < \cap\, U^2$ and $A_U = \{X \cap U : X \in A\}$. The *disjoint sum* $\sum_{i\in I} F_i$ of a family of frames $F_i = \langle W_i, <_i, A_i\rangle$, $i \in I$, is the frame $\langle W, <, A\rangle$, where W is the disjoint union $\dot{\bigcup}_i W_i$, $< \,=\, \bigcup_i <_i$, and $A = \{X \subseteq W : \forall i \in I\, (X \cap W_i \in A_i)\}$. A *subreduction* from a frame $F = \langle W, <, A\rangle$ to a frame $G = \langle V, \prec, B\rangle$ is a partial mapping f from W onto V such that

(S1) $x < y \implies f(x) \prec f(y)$ for all $x, y \in \mathrm{dom}(f)$,

(S2) $f(x) \prec u \implies \exists y > x\, f(y) = v$ for all $x \in \mathrm{dom}(f)$ and $v \in V$, and

(S3) $f^{-1}[Y] \in A$ for all $Y \in B$ (which implies $\mathrm{dom}(f) \in A$).

If $V \subseteq W$ and $f = \mathrm{id}_V$ (in which case the conditions reduce to $\prec\, = \,< \cap\, V^2$ and $B \subseteq A$), then G is called a *subframe* of F. (Since this implies $V \in A$, generated subframes are *not* necessarily subframes.) A subreduction is called a *p-morphism* (or *reduction*) if it is total, i.e., $\mathrm{dom}(f) = W$.

For any logic L, the class of L-frames is closed under generated subframes, disjoint sums, and p-morphic images; that is, these frame operations preserve the validity of all formulas.

A subframe $\langle V, <, B\rangle$ of $\langle W, <, A\rangle$ is *dense* if $V{\upharpoonleft} \cap V{\downharpoonleft} = V$, i.e., if $x < y < z$ and $x, z \in V$ imply $y \in V$. More generally, a subreduction f from F to G is dense if $\mathrm{dom}(f)$ is a dense subframe of F. Dense subreductions preserve the validity of *positive formulas* (also called *negation-free* or $\perp$*-free*): i.e., formulas built from propositional variables using $\{\Box, \wedge, \vee, \to, \top\}$, disallowing $\neg$ and $\perp$. (In general, a Boolean connective c is positive if $c(1, \dots, 1) = 1$.)

It will be also convenient to have a version of subreductions that is oblivious to reflexivity of points: we define a *weak subreduction* from $F = \langle W, <, A\rangle$ to $G = \langle V, \prec, B\rangle$ to be a partial mapping f from W onto V that satisfies

(S1′) $x < y \implies f(x) \preceq f(y)$ for all $x, y \in \mathrm{dom}(f)$,

(S2′) $f(x) \prec u \implies \exists y \geq x\, f(y) = v$ for all $x \in \mathrm{dom}(f)$ and $v \in V$,

and (S3).

Let $k \geq 1$. A rooted frame $\langle W, <, A\rangle$ has *width* $\leq k$ if it contains no antichain of size $k + 1$, i.e., points $x_0, \dots, x_k \in W$ such that $x_i \nleq x_j$ for $i \neq j$. A logic L has *width* $\leq k$ if it is complete w.r.t. a class of rooted frames of width $\leq k$, or equivalently, if all rooted refined L-frames have width $\leq k$. We say that L has *bounded width* if it has width $\leq k$ for some k, and it has *unbounded width* otherwise.

A frame $\langle W, <, A\rangle$ has *depth* $\leq k$ if it contains no chain of length $k+1$, i.e., $x_0, \dots, x_k \in W$ such that $x_0 \lneqq x_1 \lneqq \cdots \lneqq x_k$. A frame F has *cluster size* $\leq k$ if all clusters of F have at most k elements. Similarly to width, we say a logic L has *depth* (*cluster size*) $\leq k$ if it is complete w.r.t. a class of frames of depth (cluster size, resp.) $\leq k$, or equivalently, if all refined L-frames have depth (cluster size) $\leq k$; L has *bounded depth* (*cluster size*) if it has depth (cluster size) $\leq k$ for some k, and it has *unbounded depth* (*cluster size*) otherwise.

These properties are modally definable: L has width (depth, cluster size) $\leq k$ iff it proves the $\mathbf{BW}_k$ ($\mathbf{BD}_k$, $\mathbf{BC}_k$, resp.) axioms, where $\mathbf{BW}_k$ and $\mathbf{BC}_k$ were given in Table 1, and $\mathbf{BD}_k$ is the schema

$$\varphi_0 \vee \Box(\Box\varphi_0 \to \varphi_1 \vee \Box(\Box\varphi_1 \to \cdots \to \varphi_{k-1} \vee \Box(\Box\varphi_{k-1} \to \perp)\cdots)).$$

A finite frame F has *branching* $\leq k$ if every cluster of F has at most k immediate successor clusters. If L is a logic with FMP, then L has *branching* $\leq k$ if it is complete w.r.t. a class of finite frames of branching $\leq k$, or equivalently, if all finite L-frames have branching $\leq k$.

Again, L has *bounded branching* if it has branching $\leq k$ for some k, and *unbounded branching* otherwise.

It is more complicated to extend the definition of branching to logics without FMP, as the concept of branching does not make good sense for infinite frames: first, a non-leaf point in an infinite frame may have no immediate successors at all, or its immediate successors may not lower bound all its other successors. Second, even in well-behaved frames such as trees where immediate successors have reasonable graph-theoretic properties, a bound on their number does not have the expected modal consequences: for example, it is not difficult to show that an arbitrary finite rooted reflexive frame is a p-morphic image of the infinite complete *binary* tree[1], thus the logic of this tree is just **S4**, which has unbounded branching, even though the tree appears to have branching 2.

These issues are solved by showing that the logic of finite frames of branching $\leq k$ can be axiomatized by a suitable axiom schema, namely

$$(\mathbf{BB}_k) \qquad \Box\Big[\bigvee_{i\leq k}\Box\Big(\boxdot\varphi_i \to \bigvee_{\substack{j\leq k\\ j\neq i}}\boxdot\varphi_j\Big) \to \bigvee_{i\leq k}\boxdot\varphi_i\Big] \to \bigvee_{i\leq k}\Box\bigvee_{\substack{j\leq k\\ j\neq i}}\boxdot\varphi_j$$

(recall that we number indices from 0, hence $i \leq k$ stands for $i = 0, \dots, k$), and then we define a logic L to have branching $\leq k$ iff it includes $\mathbf{K4BB}_k$. Since the $\mathbf{BB}_k$ axioms are a central topic of this paper, and in contrast to the well-known superintuitionistic Gabbay–de Jongh logics, this axiomatization is not commonly found in modal logic literature, we provide more details. (Our $\mathbf{BB}_k$ axioms are mentioned without proof in [14, Rem. 6.11]. The bounded branching logics as such appear in other sources, but they are defined semantically: see e.g. Rybakov [24, p. 331].)

Let Ψ_k denote the *k-prong fork*: the finite frame consisting of a root with k immediate successors. (For definiteness, let Ψ_k be reflexive, but this does not matter.)

Lemma 2.1 *Let $k \geq 1$.*

(i) *A frame F validates $\mathbf{BB}_k$ iff there is no dense weak subreduction from F to Ψ_{k+1}.*

(ii) *A finite frame F has branching $\leq k$ iff there is no dense weak subreduction from F to Ψ_{k+1}.*

(iii) *A formula φ holds in all finite frames of branching $\leq k$ iff it is derivable in $\mathbf{K4BB}_k$.*

Proof: Let us denote the root of Ψ_{k+1} as u, and its leaves as $\{v_i : i \leq k\}$.

(i): Let f be a subreduction from F to Ψ_{k+1}. We endow F with an admissible valuation such that

$$F, x \vDash p_i \iff x \notin \mathrm{dom}(f) \text{ or } f(x) = v_i.$$

Clearly,

$$(1) \qquad f(x) = v_i \implies F, x \vDash \boxdot p_i \wedge \neg \bigvee_{j\neq i} \boxdot p_j,$$

[1]See [4, Thm. 2.21] for the intuitionistic case; the only difference in the modal case is that $f(x_0)$, $f(x_1)$, ... will cycle through the root cluster of $\mathfrak{F}$. One can also modify the argument to apply to all countable rooted **S4**-frames.

hence also

$$f(x)=u \implies F,x\vDash\neg\bigvee_{i\le k}\Box\bigvee_{j\ne i}\boxdot p_j.$$

We claim that

$$f(x)=u \implies F,x\vDash\Box\Big[\bigvee_{i\le k}\Box\Big(\boxdot p_i\to\bigvee_{j\ne i}\boxdot p_j\Big)\to\bigvee_{i\le k}\boxdot p_i\Big],$$

hence $F\nvDash\mathbf{BB}_k$. Indeed, if $f(x)=u$, and $x<y\vDash\neg\bigvee_i\boxdot p_i$, let $z_i\ge y$ be such that $z_i\nvDash p_i$ for each $i\le k$, i.e., $z_i\in\operatorname{dom}(f)$ and $f(z_i)\ne v_i$. Since f is dense, $x<y<z_0$ implies $y\in\operatorname{dom}(f)$. We cannot have $f(y)=v_i$, as $f(y)\le f(z_i)\ne v_i$. Thus, $f(y)=u$. But then y sees points in preimages of all v_i, hence (1) implies

$$F,y\vDash\neg\bigvee_{i\le k}\Box\Big(\boxdot p_i\to\bigvee_{j\ne i}\boxdot p_j\Big).$$

Conversely, assume that $F\nvDash\mathbf{BB}_k$. Fix a model M based on F, and an instance of $\mathbf{BB}_k$ using $\{\varphi_i:i\le k\}$ which is not true in M. Notice that

$$\vdash_{\mathbf{K4}}\Box\Big[\bigvee_{i\le k}\Box\Big(\boxdot\varphi_i\to\bigvee_{j\ne i}\boxdot\varphi_j\Big)\to\bigvee_{i\le k}\boxdot\varphi_i\Big]\to\bigwedge_{i\le k}\Big[\Box\Big(\boxdot\varphi_i\to\bigvee_{j\ne i}\boxdot\varphi_j\Big)\to\Box\bigvee_{j\ne i}\boxdot\varphi_j\Big],$$

hence putting

$$\beta_i=\boxdot\varphi_i\wedge\bigwedge_{j\ne i}\neg\boxdot\varphi_j,\qquad i\le k,$$

$$\alpha=\bigvee_{i\le k}\Box\neg\beta_i\to\bigvee_{i\le k}\boxdot\varphi_i,$$

we have $M\nvDash\Box\alpha\to\bigvee_i\Box\neg\beta_i$. We define a partial (and a priori multi-valued) mapping f from F to Ψ_{k+1} by

$$f(x)=\begin{cases}u & M,x\vDash\Box\alpha\wedge\bigwedge_i\Diamond\beta_i,\\ v_i & M,x\vDash\beta_i,\\ \text{undefined} & \text{otherwise.}\end{cases}$$

We claim that f is a weak dense subreduction. The property (S3) is clear, and for (S2$'$), it suffices to observe that $f(x)=u$ implies $x\vDash\Diamond\beta_i$, hence $f(y_i)=v_i$ for some $y_i>x$. Since there exists x such that $f(x)=u$, this also implies that f is onto.

For (S1$'$), it is clear from the definition that $f(y_i)=v_i$ and $f(y_j)=v_j$ implies $y_i\nleq y_j$ for $i\ne j$. Also, if $f(x)=u$ and $f(y_i)=v_i$, then $y_i\nleq x$: fixing $j\ne i$ (here we use $k\ge1$), we already established that there exists $y_j>x$ such that $f(y_j)=v_j$, hence $y_i\nleq y_j$, and a fortiori $y_i\nleq x$. This also ensures f is single-valued.

It remains to prove that f is dense. Assume $x<y<z$ and $x,z\in\operatorname{dom}(f)$. It is easy to see that $f(x)=f(z)$ implies $f(y)=f(x)$. Otherwise $f(x)=u$ and $f(z)=v_i$ for some $i\le k$. Then $y\vDash\boxdot\alpha$, thus either $f(y)=u$ and we are done, or $y\vDash\bigvee_j\Box\neg\beta_j$, hence (in view of $y\vDash\alpha$)

$y \vDash \boxdot\varphi_{i'}$ for some $i' \leq k$. Since $y < z$, we have $y \vDash \bigwedge_{j \neq i} \neg\boxdot\varphi_j$, hence $i' = i$ and $y \vDash \beta_i$, i.e., $f(y) = v_i$.

(ii): If a point x of F has immediate successors $y_0, \dots, y_k$, each belonging to a different cluster, we can construct a weak dense subreduction from F to Ψ_{k+1} by mapping $\mathrm{cl}(x)$ to u, and each $\mathrm{cl}(y_i)$ to v_i.

On the other hand, if f is such a weak dense subreduction, let x be a $\lnsim$-maximal point of F mapped to u. For each $i \leq k$, there exists $y_i \gnsim x$ such that $f(y_i) = v_i$. Let z_i be an immediate successor of x_i such that $z_i \leq y_i$. Since f is dense, $z_i \in \mathrm{dom}(f)$; by maximality of x, $u \neq f(z_i) \leq f(y_i)$, hence $f(z_i) = v_i$. But then $\{z_i : i \leq k\}$ are pairwise incomparable, i.e., they belong to $k + 1$ different clusters.

(iii): The right-to-left implication follows from (i) and (ii). Conversely, if $\nvdash_{\mathbf{K4BB}_k} \varphi$, let us fix a $\mathbf{K4BB}_k$-frame F such that $F \nvDash \varphi$. Then F validates the axioms $\alpha_{\bullet,k+1}$ and $\alpha_{①,k+1}$ from [15, Def. 4.30]: this follows from (i) and [15, L. 4.31], as any weak morphism to $F_{\bullet,k+1}$ or $F_{①,k+1}$ (as defined there) is a weak dense subreduction to Ψ_{k+1}. By [15, L. 4.35], there exists a finite frame $F_0 \vDash \mathbf{K4} \oplus \alpha_{\bullet,k+1} \oplus \alpha_{①,k+1}$ such that $F_0 \nvDash \varphi$. But then F_0 has branching $\leq k$ by [15, L. 4.34]. (This argument also shows $\mathbf{K4BB}_k = \mathbf{K4} \oplus \alpha_{\bullet,k+1} \oplus \alpha_{①,k+1}$.)

Alternatively, a similar argument can be set up using [14, L. 6.10] (note that the $\mathbf{K4BB}_k$ appearing in the statement of that lemma is *defined* as the logic of all finite frames of branching $\leq k$). $\square$

We remark that our definition of $\mathbf{BB}_k$ does not have the correct semantics for $k = 0$; in order to extend Lemma 2.1 to $k = 0$, we should redefine $\mathbf{K4BB_0}$ as $\mathbf{K4B}$.

We have $\mathbf{K4BB_1} = \mathbf{K4BW_1} = \mathbf{K4.3}$. For $k \geq 2$, all logics of width $\leq k$ also have branching $\leq k$, but there exist logics of branching 2 and unbounded width such as $\mathbf{K4BB_2}$ itself. We have $\mathbf{K4BB_1} \supsetneq \mathbf{K4BB_2} \supsetneq \mathbf{K4BB_3} \supsetneq \dots$, and $\bigcap_k \mathbf{K4BB}_k = \mathbf{K4}$.

We could drop the right-most $\boxdot$ in the definition of $\mathbf{BB}_k$, but for our purposes the definition above will be more convenient to work with. Furthermore, the $\mathbf{BB}_k$ axiom can be simplified to

$$\Box \bigvee_{i \leq k} \boxdot\varphi_i \to \bigvee_{i \leq k} \Box \bigvee_{j \neq i} \varphi_j$$

over $\mathbf{GL}$.

2.2 Proof complexity

An introduction to classical proof complexity can be found in Krajíček [18]; our setup for proof complexity of modal logics is based on Jeřábek [14].

A *Frege rule* consists of all substitution instances of $\alpha_0, \dots, \alpha_{k-1} \;/\; \beta$, where $k \geq 0$, and α_i and β are formulas. A *Frege system* is given by a finite set of Frege rules R. A *Frege R-derivation* of a formula φ from a set of formulas Γ is a sequence of formulas $\varphi_0, \dots, \varphi_m$ such that $\varphi_m = \varphi$, and for each $i \leq m$, $\varphi_i \in \Gamma$, or $\varphi_{j_0}, \dots, \varphi_{j_{k-1}} \;/\; \varphi_i$ is an instance of an R-rule for some $j_0, \dots, j_{k-1} < i$. A *Frege R-proof* of φ is a Frege R-derivation of φ from $\varnothing$. The *length* or *size* of a derivation $\varphi_0, \dots, \varphi_m$ is $\sum_i |\varphi_i|$, and the *number of lines* is $m + 1$. A derivation is *tree-like* if each formula is used at most once as a premise of a Frege rule.

The associated consequence relation $\vdash_R$ is defined such that $\Gamma \vdash_R \varphi$ iff there exists a Frege R-derivation of φ from Γ. If L is a logic, a Frege system using a set of rules R is a *Frege system for L* if $\vdash_R = \vdash_L$. (Note that this disallows the use of proper L-admissible rules as in [20, 12].)

Observation 2.2 *If $\varphi_0, \dots, \varphi_m$ is a Frege R-derivation of size s using variables $\{p_i : i < n\}$, and σ is a substitution, then $\sigma(\varphi_0), \dots, \sigma(\varphi_m)$ is a Frege R-derivation of size $\leq s \sum_{i<n} |\sigma(p_i)|$ with the same number of lines.* □

A proof system P *p-simulates* a proof system Q, written as $Q \leq_p P$, if there exists a poly-time function f such that for any Q-proof π of φ, $f(\pi)$ is a P-proof of φ. The systems P and Q are *p-equivalent*, written as $P \equiv_p Q$, if $P \leq_p Q \leq_p P$. The system P *(weakly) simulates* Q if for any Q-proof π of φ, there exists a P-proof of φ of size polynomial in $|\pi|$. If P does not weakly simulate Q, we also say that Q has *superpolynomial speed-up* over P; more generally, if S is a family of functions $s\colon \omega \to \omega$, then Q has *speed-up* S over P if there exist $s \in S$, an infinite sequence of tautologies $\{\varphi_n : n \in \omega\}$, and for each n, a Q-proof π_n of φ_n such that all P-proofs of φ_n have size at least $s\bigl(|\pi_n|\bigr)$. (For example, for $S = 2^{n^{\Omega(1)}}$, we have *exponential* speed-up.)

Observation 2.2 implies that instances of a fixed Frege rule have linear-size proofs in any Frege system where they are derivable at all, hence:

Corollary 2.3 *For any logics $L \subseteq L'$, all Frege systems for L' p-simulate all Frege systems for L. In particular, all Frege-systems for L are p-equivalent.* □

(We rely here on all our proof systems having the same language. It is well known that in the classical case, Corollary 2.3 holds even if we allow Frege systems using different complete sets of connectives, but the argument fails for modal logics.) In view of Corollary 2.3, we will speak of *the* Frege system for a logic L, and we will denote it L-F. If P is a line-based proof system such as L-F, we denote by P^* the tree-like version of P.

Let us fix an L-F system using a set of rules R. An *extended Frege* derivation of φ from Γ is a sequence $\varphi_0, \dots, \varphi_m = \varphi$ where each φ_i is either from Γ, or derived by a Frege rule, or it is an *extension axiom* of the form $q \leftrightarrow \psi$, where q is a variable (an *extension variable*) that does not occur in φ, Γ, ψ, or φ_j for any $j < i$.

A *substitution Frege* proof of φ is a sequence $\varphi_0, \dots, \varphi_m = \varphi$ such that each φ_i is derived by a Frege rule, or by the *substitution rule*: $\varphi_i = \sigma(\varphi_j)$ for some substitution σ and $j < i$. (SF *derivations* from nonempty sets of premises do not make good sense.)

The extended Frege and substitution Frege systems for L are denoted L-EF and L-SF, respectively. Corollary 2.3 holds for EF systems, SF systems, as well as the circuit-based systems below. It also holds for the tree-like systems L-F*, L-EF*, and L-CF* because of [14, Prop. 3.17], but for L-SF*, we need to assume that (MP) is included among the Frege rules (or at least, that it has a tree-like Frege derivation in which one of the premises is used only once).

For classical logic, EF and SF are p-equivalent. The situation in modal logics is more complicated; the main properties of the two systems are summarized below.

Theorem 2.4 ([14]) *Let $L \supseteq$ **K4**.*

(i) L-F $\equiv_p L$-F* *and* L-EF $\equiv_p L$-EF$^* \equiv_p L$-SF*.

(ii) *If φ has an L-*EF *proof with m lines, it has an L-*F *proof with $O(m)$ lines. If φ has an L-*F *proof with m lines, it has an L-*EF *proof of size $O\big(m + |\varphi|^2\big)$.*

(iii) *If φ has an L-*SF *proof of size s with m lines, it has an L-*F* *proof of size $(s/m)^m < 2^s$ with 2^m lines.*

(iv) *If L has unbounded branching, then L-*SF *has exponential speed-up over L-*EF.

(v) *If L is a logic of bounded width and depth, or L = $\mathbf{K4BW}_k$, $\mathbf{S4BW}_k$, $\mathbf{GLBW}_k$, $\mathbf{K4GrzBW}_k$, or $\mathbf{S4GrzBW}_k$ for some k, then L-*SF $\equiv_p$ L-EF. □

Formulas (both Boolean and modal) can be represented more succinctly by *circuits*: a circuit is a directed acyclic graph (allowing multiple edges) with a unique node of out-degree 0 (the *output* node); each node of the circuit is labelled either with a variable, in which case it has in-degree 0, or with a k-ary connective, in which case it has in-degree k (the incoming edges are ordered). Formulas can be identified with tree-like circuits (i.e., each node other than the output has out-degree 1).

The *circuit Frege system* L-CF (introduced in [11] for **CPC**) is defined essentially the same way as L-F, except that it operates with circuits instead of formulas. There is an additional rule that allows to infer a circuit from another circuit that represents the same formula (this property can be checked in polynomial time, or even in NL); alternatively, this rule may be replaced with several "local" transformation rules that only modify the top part of the circuit.

When used for proving formulas (or deriving formulas from formulas), L-CF is p-equivalent to L-EF. In fact, we can in a sense simulate L-CF by L-EF even for proofs of circuits, but we need to translate them to formulas first.

If φ is a circuit, we interpret $\mathrm{Sub}(\varphi)$ as the set of subcircuits of φ. We fix distinct variables $\{q_\psi : \psi \in \mathrm{Sub}(\varphi)\}$ not occurring in φ, and define

$$\psi^* = \begin{cases} \psi & \psi \text{ is a variable,} \\ c(q_{\psi_0}, \dots, q_{\psi_{k-1}}) & \psi = c(\psi_0, \dots, \psi_{k-1}) \text{ for a connective } c, \end{cases}$$

$$\mathrm{E}_\varphi = \bigwedge_{\psi \in \mathrm{Sub}(\varphi)} \boxdot(q_\psi \leftrightarrow \psi^*).$$

Lemma 2.5 *Let $L \supseteq$ **K4**. Given a modal circuit φ, the following are polynomial-time constructible from each other:*

(i) *An L-*CF *proof of φ.*

(ii) *An L-*CF *proof of* $\mathrm{E}_\varphi \to q_\varphi$.

(iii) *An L-*EF *proof of* $\mathrm{E}_\varphi \to q_\varphi$.

Proof: We can construct **K4**-CF proofs of $\mathrm{E}_\varphi \to \boxdot(q_\psi \leftrightarrow \psi)$ for all $\psi \in \mathrm{Sub}(\varphi)$ by induction on the complexity of ψ, which yields a **K4**-CF proof of $\varphi \to (\mathrm{E}_\varphi \to q_\varphi)$. Conversely, given an L-CF proof of $\mathrm{E}_\varphi \to q_\varphi$, we (simultaneously) substitute ψ for q_ψ in the whole proof, resulting in an L-CF proof of $\bigwedge_\psi \boxdot(\psi \leftrightarrow \psi) \to \varphi$, from which we can infer φ.

(ii) and (iii) are mutually poly-time constructible by [14, Prop. 3.3]. □

In view of Lemma 2.5, EF and CF are essentially identical proof systems. We find it much more convenient to operate with circuits directly rather than by encoding them with extension axioms, hence we will work almost exclusively with CF. We will still formulate lower bounds and similar results for EF as it is the better known of the two systems, but our results on feasibility of the disjunction property will be stated for CF as it makes them more general (i.e., directly applicable to proofs of circuits rather than just formulas).

We would also like to work with circuits directly in SF. Let us define the *substitution circuit Frege* system L-SCF as a version of the L-SF system that operates with circuits in place of formulas, including the L-CF rules. Now, L-SF is p-equivalent to L-SCF just like L-EF is p-equivalent to L-CF:

Lemma 2.6 *Let* $L \supseteq \mathbf{K4}$*. Given a modal circuit* φ*, the following are polynomial-time constructible from each other:*

(i) *An* L-SCF *proof of* φ*.*

(ii) *An* L-SCF *proof of* $\mathrm{E}_\varphi \to q_\varphi$*.*

(iii) *An* L-SF *proof of* $\mathrm{E}_\varphi \to q_\varphi$*.*

Proof: We can construct (i) from (ii) as in the proof of Lemma 2.5, and (iii) is trivially an instance of (ii). Given an L-SCF proof $\varphi_0, \dots, \varphi_m = \varphi$, we consider the sequence of formulas

$$\mathrm{E}_{\varphi_0} \to \boxdot q_{\varphi_0}, \dots, \mathrm{E}_{\varphi_m} \to \boxdot q_{\varphi_m},$$

and complete it to a valid L-SF proof as follows.

If $\varphi_i = \sigma(\varphi_j)$ is derived by substitution from φ_j, $j < i$, we use substitution to rename each q_ψ from E_{φ_j} to the corresponding $q_{\sigma(\psi)}$ from E_{φ_i}, and each original variable p to $q_{\sigma(p)}$. This turns $\mathrm{E}_{\varphi_j} \to \boxdot q_{\varphi_j}$ into $\mathrm{E}'_{\varphi_i} \to \boxdot q_{\varphi_i}$, where E'_{φ_i} is a conjunction of some conjuncts of E_{φ_i} and the tautologies $\boxdot(q_{\sigma(x)} \leftrightarrow q_{\sigma(x)})$. We infer $\mathrm{E}_{\varphi_i} \to \boxdot q_{\varphi_i}$.

If φ_i is derived by an instance of a Frege rule $\alpha_0, \dots, \alpha_{k-1} \,/\, \beta$, say $\varphi_i = \beta(\vec{\chi})$ and $\varphi_{j_u} = \alpha_u(\vec{\chi})$ with $j_u < i$, we first apply the substitution rule on the premises $\mathrm{E}_{\varphi_{j_u}} \to \boxdot q_{\varphi_{j_u}}$ if necessary to rename the extension variables q_ψ so that they are used coherently in all $\mathrm{E}_{\varphi_{j_u}}$ and E_{φ_i}. We unwind the top parts of the circuits to prove $\mathrm{E}_{\varphi_{j_u}} \to \boxdot\big(q_{\varphi_{j_u}} \leftrightarrow \alpha_u(\vec{q}_\chi)\big)$, and derive

$$\mathrm{E}_{\varphi_{j_u}} \to \boxdot \alpha_u(\vec{q}_\chi).$$

We use an instance of the tautology $\bigwedge_{u<k} \boxdot \alpha_u \to \boxdot \beta$ and $\mathrm{E}_{\varphi_i} \to \boxdot(q_{\varphi_i} \leftrightarrow \beta(\vec{q}_\chi))$ to derive

$$\mathrm{E}_{\varphi_i} \wedge \bigwedge_{u<k} \mathrm{E}_{\varphi_{j_u}} \to \boxdot q_{\varphi_i}.$$

Finally, we get rid of the conjuncts $\boxdot(q_\psi \leftrightarrow \psi^*)$ of $\mathrm{E}_{\varphi_{j_u}}$ not present in E_{φ_i} by substituting ψ^* for q_ψ and using the tautology $\boxdot(\psi^* \leftrightarrow \psi^*)$. (We do this in a top-down order, so that q_ψ is not present elsewhere in the formula when it is being substituted for.)

If φ_i represents the same formula as φ_j, $j < i$, we first use substitution to make sure the extension variables $\{q_\psi : \psi \in \mathrm{Sub}(\varphi_i)\}$ from E_{φ_i} are disjoint from the extension variables from E_{φ_j}; let us denote the latter as q'_ψ. Then we prove bottom-up that whenever $\psi \in \mathrm{Sub}(\varphi_i)$ and $\psi' \in \mathrm{Sub}(\varphi_j)$ represent the same formula, we have $\mathrm{E}_{\varphi_j} \land \mathrm{E}_{\varphi_i} \to \boxdot(q_\psi \leftrightarrow q'_{\psi'})$. Using $\mathrm{E}_{\varphi_j} \to \boxdot q'_{\varphi_j}$, we infer $\mathrm{E}_{\varphi_j} \land \mathrm{E}_{\varphi_i} \to \boxdot q_{\varphi_i}$, and we discard E_{φ_j} as in the case of Frege rules. $\Box$

The upshot of Lemmas 2.5 and 2.6 is not just that L-EF $\equiv_p$ L-CF and L-SF $\equiv_p$ L-SCF as proof systems for formulas, but also that a speed-up of L-SCF over L-CF on circuit tautologies implies a speed-up of L-SF over L-EF: if $\{\varphi_n : n \in \omega\}$ is a sequence of circuits that are easy for L-SCF and hard for L-CF, then the formulas $\{\mathrm{E}_{\varphi_n} \to q_{\varphi_n} : n \in \omega\}$ are easy for L-SF and hard for L-EF.

We remark that in a way, the term *formulas* has a double meaning in the paper: formulas-1 are abstract entities that may be L-tautologies, may be true or false in a given model, etc., and they are concretely represented by syntactic objects such as circuits or formulas-2 (= tree-like circuits) that may be operated by proof systems.

Transitive modal logics have a deduction theorem in the form that $\Gamma \vdash_L \varphi$ implies $\vdash_L \bigwedge \boxdot\Gamma \to \varphi$. (Here, if Γ is a sequence of formulas $\varphi_0, \dots, \varphi_{n-1}$, we write $\Box\Gamma$ for $\Box\varphi_0, \dots, \Box\varphi_{n-1}$, and similarly for $\boxdot\Gamma$, $\neg\Gamma$, etc., while $\bigwedge\Gamma$ is $\varphi_0 \land \dots \land \varphi_{n-1}$.) Frege systems and friends without an explicit substitution rule satisfy a *feasible deduction theorem*:

Lemma 2.7 ([14, Prop. 3.6]) *Let $L \supseteq$ **K4**, and P be L-F, L-EF, or L-CF. Given a P-derivation of φ from Γ, we can construct in polynomial time a P-proof of $\bigwedge \boxdot\Gamma \to \varphi$.* $\Box$

We also have feasible substitution of equivalence:

Lemma 2.8 *Given modal circuits φ, ψ, and $\chi(p)$ (with other variables not shown), we can construct in polynomial time* **K4**-CF *proofs of*

$$\boxdot(\varphi \leftrightarrow \psi) \to \bigl(\chi(\varphi) \leftrightarrow \chi(\psi)\bigr).$$

Proof: By induction on χ. $\Box$

Let $\mathbf{2} = \{0, 1\}$. A Boolean function $f\colon \mathbf{2}^n \to \mathbf{2}$ is *monotone* if for all $a, b \in \mathbf{2}^n$, $a \le b$ (i.e., $a_i \le b_i$ for each $i < n$) implies $f(a) \le f(b)$. A *monotone language* is $L \subseteq \mathbf{2}^*$ such that for all $n \in \omega$, the characteristic function of $L_n = L \cap \mathbf{2}^n$ is monotone.

A Boolean formula or circuit is *monotone* if it is built from variables using only the monotone connectives $\{\land, \lor, \top, \bot\}$. More generally, φ is *monotone in variables $\vec{p}$* if it is built using monotone connectives from the variables $\vec{p}$, and from subformulas/subcircuits that do not contain $\vec{p}$. A Boolean formula or circuit is in *negation normal form* if it has the form $\varphi(\vec{p}, \neg\vec{p})$, where φ is monotone (i.e., it is built using monotone connectives from positive and negative literals).

Lemma 2.9 *Given a Boolean circuit $\varphi(p_0, \dots, p_{n-1})$ (possibly using other variables) that is monotone in $\vec{p}$, and Boolean or modal circuits $\vec{\psi}$ and $\vec{\chi}$, there is a polynomial-time constructible* **CPC**-CF *proof or* **K**-CF *proof (as appropriate) of*

$$\bigwedge_{i<n} (\psi_i \to \chi_i) \to \bigl(\varphi(\vec{\psi}) \to \varphi(\vec{\chi})\bigr). \tag{2}$$

Proof: By induction on φ. (Note that (2) is a substitution instance of the Boolean tautology $\bigwedge_i(p_i \to q_i) \to \big(\varphi(\vec{p}) \to \varphi(\vec{q})\big)$, hence even in the modal case, the proof is essentially a **CPC**-CF proof in modal language.) $\Box$

Lemma 2.10 *Given a monotone Boolean circuit $\varphi(\vec{p})$, and (modal) circuits $\vec{\psi}$, there are poly-time constructible* **K**-CF *proofs of*

$$\varphi(\Box\vec{\psi}) \to \Box\varphi(\vec{\psi}).$$

Proof: By induction on the size of φ, using Lemma 2.9, and the tautologies $\Box\psi\wedge\Box\chi \to \Box(\psi\wedge\chi)$ and $\Box\psi \vee \Box\chi \to \Box(\psi \vee \chi)$. $\Box$

Makinson's theorem states that every consistent normal modal logic L is valid in a one-point Kripke frame (irreflexive $\bullet$, or reflexive $\circ$). In other words, L is included in $L(\bullet) = \mathbf{K} \oplus \Box\bot$ or in $L(\circ) = \mathbf{K} \oplus (\varphi \leftrightarrow \Box\varphi)$. In either case, we obtain a poly-time translation of L into **CPC**: if $* \in \{\bullet, \circ\}$, we define a translation of modal formulas φ to Boolean formulas φ^* such that it preserves propositional variables, commutes with Boolean connectives, and

$$(\Box\varphi)^\bullet = \top,$$
$$(\Box\varphi)^\circ = \varphi^\circ.$$

Notice that $\varphi^* = \varphi$ for non-modal formulas φ, and $(\boxdot\varphi)^* \equiv \varphi^*$. Unwinding the definition of satisfaction in one-point frames, we see that

(3) $$\vdash_{L(*)} \varphi \iff \vdash_{\mathbf{CPC}} \varphi^*.$$

Moreover, the translation acts efficiently on proofs:

Lemma 2.11 *Let $* \in \{\bullet, \circ\}$, and $L \subseteq L(*)$ be a normal modal logic. Given an L-*CF *proof of φ, we can construct in polynomial time a* **CPC**-CF *proof of φ^*.*

Proof: We may assume the L-CF system is axiomatized by (MP), (Nec), and axiom schemata. We apply the $-^*$ translation to each line in the proof: modus ponens translates to modus ponens, the translation of (Nec) is trivial, and since $-^*$ commutes with substitution, instances of a fixed axiom schema valid in L translate to instances of a fixed axiom schema, which is valid in **CPC** by (3), and as such has linear-size **CPC**-CF proofs. $\Box$

So far we discussed specific proof systems for a given logic. In general, a (Cook–Reckhow) *proof system* for a logic L is a polynomial-time function P whose image is L. (Here, each string w is considered a P-proof of the L-tautology $P(w)$.) For classical logic, NP $\neq$ coNP implies superpolynomial lower bounds on *all* proof systems because of the coNP-completeness of the set of tautologies.

For the modal logics we are interested in, we will obtain similar automatic lower bounds from PSPACE $\neq$ NP, because they are PSPACE-hard. Ladner [19] proved that **K**, **T**, and **S4** are PSPACE-complete, and that all logics $\mathbf{K} \subseteq L \subseteq \mathbf{S4}$ are PSPACE-hard. It is in fact not difficult to extend Ladner's proof to show the PSPACE-hardness of all normal modal logics with the *disjunction property* (see Section 2.4 for precise definition), but the author is not aware of this argument being published anywhere. (Cf. Lemmas 4.4 and 4.5. The PSPACE-hardness of *superintuitionistic* logics with the DP was proved in Chagrov [3].) The following stronger result was shown in Jeřábek [17]:

Theorem 2.12 *All logics $L \supseteq$ **K4** with the disjunction property are* PSPACE*-hard. More generally, if for every finite binary tree T, there exists a weak subreduction from an L-frame to T, then L is* PSPACE*-hard.* □

Corollary 2.13 *If L is a logic as in Theorem 2.12, then no proof system for L is polynomially bounded unless* PSPACE = NP = coNP. □

The only conditional superpolynomial lower bounds on L-SF we know of follow from Corollary 2.13 (assuming PSPACE $\neq$ NP) and from an SF version of Lemma 2.11 (assuming lower bounds on **CPC**-EF).

2.3 Computational complexity

We assume the reader is familiar with basic notions from complexity theory, in particular the complexity classes P, NP, coNP, and PSPACE, and the notions of polynomial-time reductions, completeness, and hardness.

Recall that a *quantified Boolean formula* (QBF) is a propositional formula that, in addition to the usual Boolean connectives, also allows quantifiers $\exists p$ and $\forall p$ ranging over the set of truth values $\mathbf{2}$. We will generally assume that QBFs are given in prenex normal form, i.e., they consist of a quantifier prefix followed by a quantifier-free formula. A QBF Φ in prenex normal form is in *negation normal form* if its quantifier-free matrix φ is in negation normal form, and it is *monotone in $\vec{p}$* if the $\vec{p}$ variables are not bound in Φ, and φ is monotone in $\vec{p}$.

The validity problem for QBF is a PSPACE-complete language. More uniformly, for any PSPACE-language $L \subseteq \mathbf{2}^*$, there exists a sequence of QBFs $\{\Phi_n(p_0, \dots, p_{n-1}) : n \in \omega\}$ constructible in time $n^{O(1)}$ such that

$$w \in L \iff \Phi_n(w_0, \dots, w_{n-1})$$

for all $w \in \mathbf{2}^n$. If $L \in$ NP ($L \in$ coNP), the Φ_n can be taken existential (universal, respectively).

The computational problems studied in this paper are mostly not YES–NO decision problems, but *search problems*. Here, the search problem S_R associated with a relation $R(x, y)$ is the following computational task: given x, find a y such that $R(x, y)$, if one exists. The class of search problems solvable in polynomial time is denoted FP. A search problem S_R is *total*[2] if $\forall x \, \exists y \, R(x, y)$.

A search problem S_{R_1} is (many-one) *reducible* to S_{R_0}, written as $S_{R_1} \leq S_{R_0}$, if there are poly-time functions f and g such that

$$R_0\bigl(f(x), y\bigr) \implies R_1\bigl(x, g(x, y)\bigr)$$

[2]In practice, we will usually deal with search problems whose input is constrained by syntactic prerequisites, such as "given a proof of φ, …". We can consider them to be total by stipulating that, say, 0 is a valid output if the input does not meet the requirements; this does not change the computational complexity of the problem, as the input condition is checkable in polynomial time.

for all x and y (i.e., f translates instances of S_{R_1} to instances of S_{R_0}, and g translates solutions back). We write $S_{R_0} \equiv S_{R_1}$ if $S_{R_0} \le S_{R_1} \le S_{R_0}$.

This standard notion of search problem reduction is suitable for "open-ended" search problems with many solutions, such as when looking for proofs of some formula. However, we will also encounter search problems with a fixed finite set of possible outcomes that may be better thought of as many-valued decision problems (possibly with non-unique answers). In such cases, it is not appropriate to translate solutions. (Notice that many-one reductions between languages likewise do not allow swapping a language for its complement.)

Thus, we define S_{R_1} to be *strictly reducible* to S_{R_0}, written as $S_{R_1} \le_s S_{R_0}$, if there exists a reduction of S_{R_1} to S_{R_0} with $g(x, y) = y$. Again, we put $S_{R_0} \equiv_s S_{R_1}$ iff $S_{R_0} \le_s S_{R_1} \le_s S_{R_0}$. An even stricter notion of reduction is when f is identity as well, i.e., $R_0 \subseteq R_1$: then we say S_{R_1} is *subsumed* by S_{R_0}.

We will also refer to *nonuniform poly-time* reductions, where the reduction functions are computable in polynomial time using an extra polynomial-size *advice string* that only depends on the length of the input.

We define S_R to be a coNP *search problem*[3] if $R \in \mathrm{coNP}$.

Two-valued search problems are closely related to promise problems, i.e., disjoint pairs. In particular, a *disjoint* NP *pair* is $\langle A_0, A_1\rangle$, where $A_0, A_1 \in \mathrm{NP}$ and $A_0 \cap A_1 = \varnothing$. This represents the following computational task: given $x \in A_0 \cup A_1$, output $i < 2$ such that $x \in A_i$ (if $x \notin A_0 \cup A_1$, any output is valid). A disjoint NP pair $A = \langle A_0, A_1\rangle$ reduces to $B = \langle B_0, B_1\rangle$, written $A \le B$, if there exists a poly-time function f such that

$$x \in A_i \implies f(x) \in B_i, \qquad i = 0, 1.$$

Now, a disjoint NP pair $\langle A_0, A_1\rangle$ represents the same task as the total $\mathbf{2}$-valued coNP search problem S_R, where $R(x, i) \iff x \notin A_{1-i}$. On the other hand, if S_R is a total $\mathbf{2}$-valued coNP search problem, it represents the same task as the disjoint NP pair $\langle A_0, A_1\rangle$, where $A_i = \{x : \neg R(x, 1 - i)\}$. Moreover, if S_R and $S_{R'}$ are total $\mathbf{2}$-valued coNP search problems, and A and A' the corresponding disjoint NP pairs, we have

$$S_R \le_s S_{R'} \iff A \le A',$$

using the same reduction function. For these reasons, we may identify total two-valued coNP search problems with disjoint NP pairs. (More generally, total two-valued search problems may be identified with promise problems.)

2.4 Disjunction properties

A consistent modal logic L has the *disjunction property* (DP) if for all formulas φ_0 and φ_1, L proves $\Box\varphi_0 \vee \Box\varphi_1$ only if it proves φ_0 or φ_1. (We note that it is conceptually more appropriate

[3]Confusingly, NP search problems are those where $R \in \mathrm{P}$. To be consistent with this terminology, we should perhaps call coNP search problems Σ_2^{P} *search problems*. We do not, because we consider the naming of NP search problems somewhat of a misnomer in the first place, and moreover, the idea behind this nomenclature (that Σ_2^{P} search problems seek witnesses for Σ_2^{P} predicates) does not apply to our problems, which have a bounded range, hence the corresponding decision problems are in BH rather than full Σ_2^{P}. (Calling them BH *search problems* would be probably even more confusing.)

to define DP so that for every *finite set* of formulas $\{\varphi_i : i \in I\}$, L proves $\bigvee_{i\in I} \Box\varphi_i$ only if it proves φ_i for some $i \in I$. However, for transitive logics, this more general definition is equivalent to its special cases with $I = \varnothing$, which amounts to the consistency of L, and $|I| = 2$, which is how we introduced DP above. We prefer the definition with $|I| = 2$ as it simplifies the presentation of DP as a computational problem, see below.)

DP is an example of a multi-conclusion admissible rule. In general, a *consecution* is a pair of finite sets of formulas, written as $\Gamma \,/\, \Delta$, and a *multi-conclusion rule*[4] is a set R of consecutions (called the *instances* of R). A rule R is *L-admissible* if for all instances $\Gamma \,/\, \Delta$ of R, if $\vdash_L \varphi$ for all $\varphi \in \Gamma$, then $\vdash_L \psi$ for some $\psi \in \Delta$. We will write rules in a schematic form (analogous to axiom schemata) whenever possible. Thus, L has DP iff the rule $\Box\varphi_0 \vee \Box\varphi_1 \,/\, \varphi_0, \varphi_1$ is admissible, and the finite-set formulation of DP amounts to the admissibility of the rules

$$(\mathrm{DP}_n) \qquad \Box\varphi_0 \vee \cdots \vee \Box\varphi_{n-1} \,/\, \varphi_0, \ldots, \varphi_{n-1}$$

for $n \in \omega$.

Semantically, the disjunction property corresponds to the following closure property on L-frames (see [4, Thm. 15.1]): given two (or finitely many) rooted L-frames F_0 and F_1, there exists a rooted L-frame F that includes disjoint isomorphic copies of F_0 and F_1 as generated subframes. In particular, if for each $i = 0, 1$, W_i is a model based on F_i that refutes φ_i, then $\Box\varphi_0 \vee \Box\varphi_1$ is refuted at the root of F under any valuation that extends that of W_0 and W_1.

The simplest way how to construct a rooted frame that includes given rooted frames $\{F_i : i < n\}$ as generated subframes is to take their disjoint sum $\sum_{i<n} F_i$, and attach to it a new root: we denote the resulting frame $\left(\sum_{i<n} F_i\right)^\bullet$ if the new root is irreflexive, and $\left(\sum_{i<n} F_i\right)^\circ$ if it is reflexive. Many common transitive modal logics with DP are in fact closed under this frame construction; if $* \in \{\bullet, \circ\}$, we say that a logic L is *$*$-extensible* if for every $n \in \omega$ and rooted L-frames $\{F_i : i < n\}$, the frame $\left(\sum_{i<n} F_i\right)^*$ is an L-frame. (We also say that L is *extensible* if it is $\bullet$-extensible unless $L \supseteq \mathbf{S4}$, and $\circ$-extensible unless $L \supseteq \mathbf{GL}$.)

It turns out that $*$-extensible logics do not have just DP, but they admit more general *extension rules*[5]

$$(\mathrm{Ext}^*_{n,m}) \qquad \bigwedge_{j<m} B^*(\chi_j) \to \Box\varphi_0 \vee \cdots \vee \Box\varphi_{n-1} \Big/ \bigwedge_{j<m} \boxdot\chi_j \to \varphi_0, \ldots, \bigwedge_{j<m} \boxdot\chi_j \to \varphi_{n-1}$$

for $n, m \in \omega$, where

$$B^\bullet(\varphi) = \Box\varphi,$$
$$B^\circ(\varphi) = (\varphi \leftrightarrow \Box\varphi).$$

We also put $\mathrm{Ext}^* = \bigcup\{\mathrm{Ext}^*_{n,m} : n, m \in \omega\}$ and $\mathrm{Ext}^*_n = \bigcup\{\mathrm{Ext}^*_{n,m} : m \in \omega\}$.

[4] In structural theory of propositional logics, the term "admissible rule" is usually reserved for *schematic* rules, i.e., rules that consist of all substitutions instances of a single consecution, similarly to Frege rules (see e.g. Rybakov [24]); however, it will be more convenient for our purposes to adopt a more relaxed definition.

[5] By an unfortunate clash of terminology, *extension rule* is also a standard name in proof complexity for the "rule" that warrants postulation of extension axioms in EF proofs. We refrain from this usage to avoid confusion.

For example, the logics **K4**, **S4**, **GL**, **K4Grz**, **K4.1**, **K4BC**$_k$, **S4.1.4**, and their arbitrary combinations, are extensible. The logics **D4**, **D4.1**, **D4Grz**, and **D4BC**$_k$ are $\circ$-extensible, but not $\bullet$-extensible (though they only fail the condition for $n = 0$, hence they admit $\mathrm{Ext}^\bullet_n$ for all $n > 0$, and most results below on $\bullet$-extensible logics can be easily adapted to them).

The following characterization was essentially proved in [12]:

Theorem 2.14 *Let $L \supseteq$ **K4**, and $* \in \{\bullet, \circ\}$. The following are equivalent:*

(i) *L is $*$-extensible.*

(ii) *The rules Ext^* are L-admissible.*

(iii) *L can be axiomatized over **K4** by (substitution instances of) axioms each of which has the form*

$$\Box\beta \wedge \Box(\Box\alpha \to \alpha) \to \Box\alpha \tag{5}$$

if $* = \bullet$, and one of the forms

$$\beta \wedge \Box\alpha \to \alpha \tag{6}$$

or

$$\Box\gamma \wedge \Box(\Box\alpha \to \beta) \wedge \Box(\Box\beta \to \alpha) \wedge \Box(\alpha \vee \beta) \to \Box\alpha \tag{7}$$

if $* = \circ$.

Proof: The equivalence of (i) and (ii) is from [12, Thm. 3.5]. (iii) $\to$ (i): It is straightforward to check that a valuation in $\left(\sum_{i<n} F_i\right)^*$ that makes an axiom of such form true in each F_i also makes it true in the root.

(ii) $\to$ (iii): First, assume $* = \bullet$. Even though [12, Thm. 3.11] is stated only for extensible logics, the argument (using Claim 1) applies directly to $\bullet$-extensible logics, showing they are axiomatizable over **K4** by Zakharyaschev's canonical formulas $\alpha(F, D, \bot)$ (see [4, §9.4] and [12, 3.6–3.10]) where the root of F is reflexive. Considering that $\boxdot$ commutes with $\wedge$, such a canonical formula can be brought to the syntactic form

$$\boxdot\beta \wedge \boxdot(\Box\alpha \to \alpha) \to \alpha \tag{8}$$

for some formulas α and β (in fact, with α being just a variable). Now, for a given α and β, (8) is equiderivable with (5) over **K4**: on the one hand, we can derive (5) from (8) by (Nec) and distributing the boxes; on the other hand, (5) $\to$ (8) is a classical tautology.

If $* = \circ$, then [12, Thm. 3.11] shows that L is axiomatizable by canonical formulas $\alpha(F, D, \bot)$ where the root cluster of F is either proper or irreflexive. In the former case, the canonical formula has the form

$$\boxdot\gamma \wedge \boxdot(\Box\alpha \to \beta) \wedge \boxdot(\Box\beta \to \alpha) \wedge \boxdot(\alpha \vee \beta) \to \alpha,$$

which is equiderivable with (7) similarly to the argument for $* = \bullet$. In the latter case, the canonical formula has the form

$$\beta \wedge \boxdot(\alpha \vee \Box\alpha) \to \alpha,$$

which is equivalent to (6). $\Box$

In contrast to DP, the extension rules are not equivalent to their restrictions with bounded n. For a fixed n, the L-admissibility of $\mathrm{Ext}^\bullet_n$ or Ext°_n is equivalent to the closure of the class of rooted L-frames under taking $\left(\sum_{i<n} F_i\right)^\bullet$ or $\left(\sum_{i<n} F_i\right)^\circ$ (respectively), thus for example, $\mathbf{K4BB}_k$ admits $\mathrm{Ext}^\bullet_n$ and Ext°_n for $n \le k$, but not for any larger n.

On the other hand, since $\wedge$ commutes with $\Box$ and $\boxdot$, $\mathrm{Ext}^\bullet_n$ is (feasibly) equivalent to $\mathrm{Ext}^\bullet_{n,1}$. The reflexive case is more involved, but it was shown in [13] that Ext°_n is equivalent to $\mathrm{Ext}^\circ_{n,2}$, and in fact, to its special case

$$\boxdot(\chi \leftrightarrow \Box\chi) \to \Box\varphi_0 \vee \cdots \vee \Box\varphi_{n-1} \;/\; \boxdot\chi \to \varphi_0, \ldots, \boxdot\chi \to \varphi_{n-1}.$$

However, the reduction as given in [13, L. 3.3] involves formulas of size doubly exponential in m, hence we prefer to state the rules in the more general form above for computational purposes.

The disjunction property gives rise to several computational problems, in particular:

- Given a proof of $\Box\varphi \vee \Box\psi$, decide if φ or ψ is provable.
- Given a proof of $\Box\varphi \vee \Box\psi$, find a proof of φ or of ψ.

More generally, let P be a proof system for a logic L, and R a (polynomial-time recognizable) multi-conclusion L-admissible rule. The *R-decision problem for P*, denoted $\mathrm{Dec}(R, P)$, is the total search problem

- given an instance $\{\varphi_i : i < n\} \;/\; \{\psi_j : j < m\}$ of R, and for each $i < n$, a P-proof of φ_i, find a $j < m$ such that ψ_j is P-provable.

The *R-proof-construction problem for P*, $\mathrm{Cons}(R, P)$, is the total search problem

- given an instance $\{\varphi_i : i < n\} \;/\; \{\psi_j : j < m\}$ of R, and for each $i < n$, a P-proof of φ_i, find a P-proof of some ψ_j.

(Formally, we make $\mathrm{Dec}(R, P)$ and $\mathrm{Cons}(R, P)$ total by allowing the output 0 if the input does not have the stated syntactic form.) We say that P has *feasible* R if $\mathrm{Dec}(R, P) \in \mathrm{FP}$, and *constructive feasible* R if $\mathrm{Cons}(R, P) \in \mathrm{FP}$.

The extension rules Ext^* have the remarkable feature that they are constructively feasible for Frege, EF, and CF systems whenever they are admissible at all. This was proved in [12, Thm. 4.8]. (The result is stated as a p-simulation of Frege systems for extensible logics using additional single-conclusion admissible rules as new rules of inference, but the proof, specifically Claims 2 and 3, applies to multi-conclusion rules as well, and only needs the logic to be $*$-extensible. As is the nature of Frege systems, the original formulation allows for *repeated* applications of the rules, which is something we will not need here.)

Since this is a central tool in this paper, and we will need to adapt the argument later on anyway, we include a self-contained proof.

If R is a rule, and S a set of formulas, let *S-restricted* R be the rule consisting of instances $\Gamma \;/\; \Delta$ of R such that $\Gamma \cup \Delta \subseteq S$.

Theorem 2.15 *Let $* \in \{\bullet, \circ\}$, and $L \supseteq \mathbf{K4}$ be a $*$-extensible logic. Then L-*F *and L-*CF *have constructive feasible* Ext^**, and therefore constructive feasible DP.*

Proof: Assume first $* = \bullet$. By Theorem 2.14 and Corollary 2.3, we may assume L is axiomatized by the usual axioms and rules of **K4**, and substitution instances of axioms

$$\Box\beta_j \to \bigl(\Box(\Box\alpha_j \to \alpha_j) \to \Box\alpha_j\bigr), \qquad j < k,$$

for some k and formulas $\alpha_0, \beta_0, \dots, \alpha_{k-1}, \beta_{k-1}$. Given an L-CF proof $\pi = \langle \theta_0, \dots, \theta_z \rangle$ of

$$\theta_z = \bigwedge_{j<m} \Box\chi_j \to \bigvee_{i<n} \Box\varphi_i,$$

let Π be the closure of $\pi \cup \{\chi_j : j < m\}$ under (MP) and $\mathrm{Sub}(\pi)$-restricted (Nec).

Clearly, all circuits in Π are subcircuits of some θ_i. There are only polynomially many such subcircuits, and then it is easy to see that Π can be computed in polynomial time. Also, Π can be arranged into an L-CF derivation from χ_j, $j < m$, as additional axioms. If π consists of formulas only, then so does Π, i.e., it is an L-F derivation.

Let $v\colon \mathrm{Form} \to \mathbf{2}$ be a Boolean propositional assignment to modal formulas such that $v(p_i)$ is chosen arbitrarily for each variable p_i, and

$$v(\Box\varphi) = 1 \iff \varphi \in \Pi.$$

We claim that

$$v(\theta_i) = 1 \tag{9}$$

for all $i \le z$, which we prove by induction on i. If θ_i is inferred by an axiom or rule of **CPC**, (9) follows from v being a Boolean assignment. If θ_i is an instance of (**K**) or (**4**), then (9) follows from the closure of Π under (MP) or (Nec) (respectively).

Assume that θ_i is

$$\Box\beta'_j \to \bigl(\Box(\Box\alpha'_j \to \alpha'_j) \to \Box\alpha'_j\bigr), \tag{10}$$

where $j < k$, and $\alpha'_j = \sigma(\alpha_j)$, $\beta'_j = \sigma(\beta_j)$ for some substitution σ. If $v(\Box\beta'_j) = 1$ and $v\bigl(\Box(\Box\alpha'_j \to \alpha'_j)\bigr) = 1$, then β'_j and $\Box\alpha'_j \to \alpha'_j$ are in Π. By closure under (Nec), Π also contains $\Box\beta'_j$ and $\Box(\Box\alpha'_j \to \alpha'_j)$, thus in view of $\theta_i \in \Pi$, closure under (MP) gives $\Box\alpha'_j \in \Pi$, hence (using $\Box\alpha'_j \to \alpha'_j \in \Pi$) also $\alpha'_j \in \Pi$. Thus, $v(\Box\alpha'_j) = 1$.

Taking $i = z$ in (9), $v(\Box\chi_j) = 1$ for each j implies $v\bigl(\bigvee_{i<n} \Box\varphi_i\bigr) = 1$, i.e., there exists $i < n$ such that $\varphi_i \in \Pi$. Thus, Π is an L-CF derivation of φ_i from $\{\chi_j : j < m\}$, and we can turn it into an L-CF proof of $\bigwedge_{j<m} \boxdot\chi_j \to \varphi_i$ by Lemma 2.7.

Now, assume $* = \circ$. By Theorem 2.14, we may assume L is axiomatized over **K4** by substitution instances of axioms

$$\beta_j \wedge \Box\alpha_j \to \alpha_j, \qquad j < k, \tag{11}$$

$$\Box\gamma_j \to \Bigl(\Box(\Box\alpha_j \to \beta_j) \to \Bigl(\Box(\Box\beta_j \to \alpha_j) \to \bigl(\Box(\alpha_j \vee \beta_j) \to \Box\alpha_j\bigr)\Bigr)\Bigr), \qquad j < l. \tag{12}$$

Given an L-CF proof $\pi = \langle \theta_0, \dots, \theta_z \rangle$ of

$$\theta_z = \bigwedge_{j<m} (\chi_j \leftrightarrow \Box\chi_j) \to \bigvee_{i<n} \Box\varphi_i,$$

define Π as above. Again, Π is computable in polynomial time, and it is a valid L-CF derivation from axioms χ_j, $j < m$. We define a Boolean assignment v such that

$$v(\Box\varphi) = 1 \iff \varphi \in \Pi \text{ and } v(\varphi) = 1.$$

Again, we prove (9) by induction on $i \leq s$. Axioms and rules of **K4** are handled as before, and (9) holds trivially for instances

$$\beta'_j \wedge \Box\alpha'_j \to \alpha'_j \tag{13}$$

of (11), as $v(\Box\alpha'_j) = 1$ implies $v(\alpha'_j) = 1$ by definition. Assume that θ_i is

$$\Box\gamma'_j \to \big(\Box(\Box\alpha'_j \to \beta'_j) \to \big(\Box(\Box\beta'_j \to \alpha'_j) \to \big(\Box(\alpha'_j \vee \beta'_j) \to \Box\alpha'_j\big)\big)\big), \tag{14}$$

where $j < l$, $\alpha'_j = \sigma(\alpha_j)$, $\beta'_j = \sigma(\beta_j)$, and $\gamma'_j = \sigma(\gamma_j)$ for some substitution σ. If v satisfies the four boxed antecedents of θ_i, the corresponding unboxed circuits are in Π, hence their boxed counterparts as well by closure under (Nec), hence $\Box\alpha'_j \in \Pi$ by closure under (MP). In view of $\Box\alpha'_j \to \beta'_j \in \Pi$, this gives $\beta'_j \in \Pi$, hence $\Box\beta'_j \in \Pi$ by (Nec), hence $\alpha'_j \in \Pi$ using $\Box\beta'_j \to \alpha'_j \in \Pi$. Moreover, $v(\alpha'_j \vee \beta'_j) = 1$. If $v(\alpha'_j) = 1$, then $v(\Box\alpha'_j) = 1$ and we are done. Otherwise, $v(\beta'_j) = 1$, thus (using $\beta'_j \in \Pi$) $v(\Box\beta'_j) = 1$. Since also $v(\Box\beta'_j \to \alpha'_j) = 1$, we obtain $v(\alpha'_j) = 1$ and $v(\Box\alpha'_j) = 1$ again.

Since $\chi_j \in \Pi$, we have $v(\chi_j \leftrightarrow \Box\chi_j) = 1$ for each $j < m$. Thus, $v(\theta_z) = 1$ implies $v\big(\bigvee_{i<n} \Box\varphi_i\big) = 1$, that is, Π is an L-CF derivation of some φ_i from $\{\chi_j : j < m\}$, and we can turn it into an L-CF proof of $\bigwedge_{j<m} \boxdot\chi_j \to \varphi_i$. $\Box$

We stress that this "automatic feasibility" of Ext^* essentially relies on the presence of Ext^*_n for all n. Indeed, the main part of this paper will be a study of the complexity of $\mathrm{Dec}(\mathrm{Ext}^*_k, L\text{-CF})$ for logics L involving the $\mathbf{BB}_k$ axiom.

3 Summary of main results

This is a long paper proving a sequence of theorems some of which gradually improve the previous ones, and it is easy to get lost. For this reason, we provide an overview of the main results, grouping related theorems together, and omitting some of the more complicated details. The results follow two main threads: first, estimates on the complexity of the search problems associated with DP and extension rules for basic logics of bounded branching, and second, conditional superpolynomial speed-ups of L-SF over L-EF under complexity assumptions.

As for the first thread, the following statement summarizes Theorem 4.1, part of Theorem 5.8, and Theorem 8.5:

Theorem 3.1 *Let* $* \in \{\bullet, \circ\}$*,* L_0 *be a* $*$*-extensible logic,* $k \geq t \geq 2$*, and* $L = L_0 \oplus \mathbf{BB}_k$*. Then* $\mathrm{Dec}(\mathrm{Ext}^*_t, L\text{-CF})$*, and therefore* $\mathrm{Dec}(\mathrm{DP}, L\text{-CF})$*, is subsumed by a total* coNP *search problem. More precisely,* $\mathrm{Dec}(\mathrm{Ext}^*_t, L\text{-CF}) \equiv_s \mathrm{Dec}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF})$ *and* $\mathrm{Cons}(\mathrm{Ext}^*_t, L\text{-CF}) \equiv \mathrm{Cons}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF})$*. Likewise,* $\mathrm{Dec}(\mathrm{V}_t, \mathbf{T}_k\text{-CF}) \equiv_s \mathrm{Dec}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF})$*.*

Here, $\mathrm{R}_{k,t}$ is a certain propositional rule introduced in Definition 5.4, whose decision problem reduces to the *interpolation problem* (Lemma 5.5). The superintuitionistic Gabbay–de Jongh logics $\mathbf{T}_k$ and the Visser rules V_t are defined in Section 8.

Another result in this thread is a form of Hrubeš-style monotone interpolation in Theorem 6.1, whose statement is rather technical.

As for the second thread, the following statement summarizes Theorem 4.6, Corollary 5.11, and Theorem 6.3 as generalized in Theorem 7.7 (or rather, Example 7.8), and Theorems 8.12 and 8.15.

Theorem 3.2 *If* $\mathbf{K4} \subseteq L \subseteq \mathbf{S4.2GrzBB_2}$, $\mathbf{K4} \subseteq L \subseteq \mathbf{GL.2BB_2}$, *or* $\mathbf{IPC} \subseteq L \subseteq \mathbf{T}_2 + \mathbf{KC}$, *then* L-SF *has superpolynomial speed-up over* L-EF *unless the following happen:*

- PSPACE = NP = coNP.
- *The disjoint* NP *pair version of* $\mathrm{Dec}(\mathrm{R}_{2,2}, \mathbf{CPC}\text{-CF})$*, and consequently the interpolation* NP *pair for* $\mathbf{CPC}$-EF*, are complete disjoint* PSPACE *pairs under nonuniform poly-time reductions.*
- *For every monotone* PSPACE *language P, there exists a sequence of polynomial-size monotone Boolean circuits $C_n^{\forall}$, $C_n^{\exists}$ in variables $\{p_i : i < n\}$ and $\{s_{l,r} : l < m_n, r < 3\}$ that satisfy certain conditions spelled out in Theorem 6.3 (for modal L) or Theorem 8.15 (for superintuitionistic L).*

4 Disjunction properties for logics of bounded branching

In this section, we will start investigating the complexity of the decision problems for DP and extension rules for basic logics of bounded branching; more precisely, our results will apply to logics of the form $L = L_0 \oplus \mathbf{BB}_k$ where L_0 is a $\bullet$-extensible or $\circ$-extensible logic. We try to apply the same method as in the proof of Theorem 2.15, using Boolean assignments constructed from polynomial-size closures of the given proof under (MP) and some other rules. In order to handle instances of the $\mathbf{BB}_k$ axiom, we need to introduce extra "rules" that are not really sound, hence we will not get a valid proof in the end; nevertheless, the combinatorics of these rules leads to a reduction of the decision problem for Ext_t^* to a certain total coNP search problem (albeit a rather unnatural one). Even though this does not give a polynomial-time algorithm, it still considerably lowers the trivial PSPACE upper bound on the complexity of the problem. As a consequence, we will obtain a superpolynomial speed-up of L-SF over L-EF conditional on PSPACE $\neq$ NP.

Theorem 4.1 *Let* $* \in \{\bullet, \circ\}$, L_0 *be a* $*$*-extensible logic,* $k \geq t \geq 2$*, and* $L = L_0 \oplus \mathbf{BB}_k$*. Then* $\mathrm{Dec}(\mathrm{Ext}_t^*, L\text{-CF})$*, and therefore* $\mathrm{Dec}(\mathrm{DP}, L\text{-CF})$*, is subsumed by a total* coNP *search problem.*

Proof: Let $\pi = \langle \theta_0, \dots, \theta_z \rangle$ be a given L-CF proof of

$$\bigwedge_{v<s} B^*(\chi_v) \to \bigvee_{u<t} \Box\varphi_u, \tag{15}$$

we need to find a $u < t$ such that

$$\vdash_L \bigwedge_{v<s} \boxdot\chi_v \to \varphi_u \tag{16}$$

using a total coNP search problem.

We assume that L_0 is axiomatized as in the proof of Theorem 2.15. Let $\{A_l : l < m\}$ be the list of instances of the $\mathbf{BB}_k$ axiom invoked in π, where

$$A_l = \Box\Big[\bigvee_{i\le k} \Box\Big(\boxdot\psi_{l,i} \to \bigvee_{j\ne i} \boxdot\psi_{l,j}\Big) \to \bigvee_{i\le k} \boxdot\psi_{l,i}\Big] \to \bigvee_{i\le k} \Box \bigvee_{j\ne i} \boxdot\psi_{l,j}, \qquad l < m. \tag{17}$$

Let Ξ_π be a set of auxiliary circuits consisting of

$$\bigvee_{i\le k} \Box \bigvee_{j\ne i} \boxdot\psi_{l,j} \to \bigvee_{i\le k} \Box\Big(\boxdot\psi_{l,i} \to \bigvee_{j\ne i} \boxdot\psi_{l,j}\Big), \qquad l < m, \tag{18}$$

$$\bigvee_{j\ne i} \boxdot\psi_{l,j} \to \Big(\boxdot\psi_{l,i} \to \bigvee_{j\ne i} \boxdot\psi_{l,j}\Big), \qquad l < m,\ i \le k, \tag{19}$$

$$\psi_{l,i'} \to \Box\psi_{l,i'} \to \bigvee_{j\ne i} \boxdot\psi_{l,j}, \qquad l < m,\ i, i' \le k,\ i \ne i'. \tag{20}$$

Clearly, Ξ_π is polynomial-time constructible, and it consists of $\mathbf{K}$-tautologies.

Let us write $[k+1] = \{0, \dots, k\}$. For any $\sigma \in [k+1]^m$, let Π_σ be the closure of

$$\pi \cup \Xi_\pi \cup \{\chi_v : v < s\} \tag{21}$$

under (MP), $\mathrm{Sub}(\pi)$-restricted (Nec), and under the rules

$$\bigvee_{i\le k} \boxdot\psi_{l,i} \Big/ \bigvee_{i\ne r} \boxdot\psi_{l,i}, \qquad l < m, r = \sigma_l. \tag{22}$$

(We stress that we take (22) only literally, we do not consider its substitution instances.) Likewise, let Π^σ denote the closure of (21) under (MP), $\mathrm{Sub}(\pi)$-restricted (Nec), and under the rules (22) for all $l < m$ and $r \ne \sigma_l$. The sets Π_σ and Π^σ are computable in polynomial time given π and σ.

We consider the following coNP-search problem $D(\pi)$: *given an* L-CF *proof* π *of* (15)*, find* $u < t$ *such that* $\forall \tau \in [k+1]^m\, \varphi_u \in \Pi^\tau$ (with a suitable convention if the input does not have the right form). We are going to show that $D(\pi)$ is total, and that it subsumes $\mathrm{Dec}(\mathrm{DP}, L\text{-CF})$.

As in Theorem 2.14, given $\sigma \in [k+1]^m$, we define a Boolean assignment v_σ to modal formulas such that

$$v_\sigma(\Box\varphi) = 1 \iff \begin{cases} \varphi \in \Pi_\sigma, & * = \bullet, \\ \varphi \in \Pi_\sigma \ \&\ v_\sigma(\varphi) = 1, & * = \circ. \end{cases}$$

Claim 4.1.1 *For all* $g \le z$*,* $v_\sigma(\theta_g) = 1$.

Proof: By induction on g. Since Π_σ is closed under (MP) and $\mathrm{Sub}(\pi)$-restricted (Nec), the proof of Theorem 2.14 shows that the claim holds if θ_g was derived by an axiom or rule of L_0. Thus, we only need to prove $v_\sigma(A_l) = 1$ for all $l < m$. Assume that

$$v_\sigma\Big(\Box\Big[\bigvee_{i\le k}\Box\Big(\boxdot\psi_{l,i}\to\bigvee_{j\ne i}\boxdot\psi_{l,j}\Big)\to\bigvee_{i\le k}\boxdot\psi_{l,i}\Big]\Big)=1. \tag{23}$$

Then the following circuits are in Π_σ:

$$\bigvee_{i\le k}\Box\Big(\boxdot\psi_{l,i}\to\bigvee_{j\ne i}\boxdot\psi_{l,j}\Big)\to\bigvee_{i\le k}\boxdot\psi_{l,i} \qquad \text{definition of } v_\sigma, \tag{24}$$

$$\Box\Big[\bigvee_{i\le k}\Box\Big(\boxdot\psi_{l,i}\to\bigvee_{j\ne i}\boxdot\psi_{l,j}\Big)\to\bigvee_{i\le k}\boxdot\psi_{l,i}\Big] \qquad \text{(Nec)}, \tag{25}$$

$$\bigvee_{i\le k}\Box\bigvee_{j\ne i}\boxdot\psi_{l,j} \qquad \text{(MP) with (17)}, \tag{26}$$

$$\bigvee_{i\le k}\Box\Big(\boxdot\psi_{l,i}\to\bigvee_{j\ne i}\boxdot\psi_{l,j}\Big) \qquad \text{(MP) with (18)}, \tag{27}$$

$$\bigvee_{i\le k}\boxdot\psi_{l,i} \qquad \text{(MP) with (24)}, \tag{28}$$

$$\bigvee_{i\ne\sigma_l}\boxdot\psi_{l,i} \qquad \text{by (22)}. \tag{29}$$

If $* = \bullet$, this means

$$v_\sigma\Big(\Box\bigvee_{i\ne\sigma_l}\boxdot\psi_{l,i}\Big)=1$$

and we are done. If $* = \circ$, we need more work. We have

$$v_\sigma\Big(\bigvee_{i\le k}\Box\Big(\boxdot\psi_{l,i}\to\bigvee_{j\ne i}\boxdot\psi_{l,j}\Big)\to\bigvee_{i\le k}\boxdot\psi_{l,i}\Big)=1 \tag{30}$$

from (23). Notice that

$$\boxdot\psi_{l,\sigma_l}\to\bigvee_{i\ne\sigma_l}\boxdot\psi_{l,i}\in\Pi_\sigma \tag{31}$$

by (29) and (19). Thus, if

$$v_\sigma\Big(\boxdot\psi_{l,\sigma_l}\to\bigvee_{i\ne\sigma_l}\boxdot\psi_{l,i}\Big)=1, \tag{32}$$

then $v_\sigma\big(\Box\big(\boxdot\psi_{l,\sigma_l}\to\bigvee_{i\ne\sigma_l}\boxdot\psi_{l,i}\big)\big)=1$, hence $v_\sigma\big(\bigvee_i\boxdot\psi_{l,i}\big)=1$ by (30), and

$$v_\sigma\Big(\bigvee_{i\ne\sigma_l}\boxdot\psi_{l,i}\Big)=v_\sigma\Big(\Box\bigvee_{i\ne\sigma_l}\boxdot\psi_{l,i}\Big)=1$$

using (32) and (29).

On the other hand, if $v_\sigma\big(\boxdot\psi_{l,\sigma_l} \to \bigvee_{i\neq\sigma_l}\boxdot\psi_{l,i}\big) = 0$, then $v_\sigma(\boxdot\psi_{l,\sigma_l}) = 1$. This implies $\psi_{l,\sigma_l} \in \Pi_\sigma$, hence $\Box\psi_{l,\sigma_l} \in \Pi_\sigma$ by closure under (Nec). Using (20), we get $\bigvee_{j\neq i}\boxdot\psi_{l,j} \in \Pi_\sigma$ and

$$v_\sigma\Big(\Box\bigvee_{j\neq i}\boxdot\psi_{l,j}\Big) = 1$$

for any fixed $i \neq \sigma_l$. $\Box$ (Claim 4.1.1)

Since $\chi_v \in \Pi_\sigma$, we have $v_\sigma\big(B^*(\chi_v)\big) = 1$ for all $v < s$. Thus, Claim 4.1.1 for $\theta_z = (15)$ implies $v_\sigma(\Box\varphi_u) = 1$ for some $u < t$, that is,

$$\forall\sigma \in [k+1]^m\ \exists u < t\ \varphi_u \in \Pi_\sigma. \tag{33}$$

If $\sigma, \tau \in [k+1]^m$, let us write $\sigma\#\tau$ if $\sigma_l \neq \tau_l$ for all $l < m$. We claim that

$$\exists u < t\ \forall\tau \in [k+1]^m\ \exists\sigma \in [k+1]^m\ (\sigma\#\tau\ \&\ \varphi_u \in \Pi_\sigma). \tag{34}$$

If not, let us fix for each $u < t$ a counterexample τ^u. Since $t < k+1$, there exists σ such that $\sigma\#\tau^0,\dots,\tau^{t-1}$, say, $\sigma_l = \min\big([k+1]\smallsetminus\{\tau^u_l : u < t\}\big)$ for each $l < m$. But then $\varphi_0,\dots,\varphi_{t-1} \notin \Pi_\sigma$, contradicting (33).

Clearly, $\Pi^\tau \supseteq \Pi_\sigma$ for any $\sigma\#\tau$, thus (34) implies

$$\exists u < t\ \forall\tau \in [k+1]^m\ \varphi_u \in \Pi^\tau,$$

i.e., $D(\pi)$ is total. It remains to verify that a solution to $D(\pi)$ gives a valid solution to $\mathrm{Dec}(\mathrm{Ext}^*_t, L\text{-CF})$, i.e.,

$$\forall\tau \in [k+1]^m\ \varphi_u \in \Pi^\tau \implies \vdash_L \bigwedge_{v<s}\boxdot\chi_v \to \varphi_u. \tag{35}$$

Apart from $\{\chi_v : v < s\}$, the elements of Π^τ are L-tautologies, or they are derived by rules of L (modus ponens, necessitation), or by (22) for $r \neq \tau_l$. Thus, we see by induction on the length of the derivation that

$$\varphi \in \Pi^\tau \implies \vdash_L \bigwedge_{v<s}\boxdot\chi_v \wedge \bigwedge_{l<m}\Big(\bigvee_{i\le k}\boxdot\psi_{l,i} \to \boxdot\psi_{l,\tau_l}\Big) \to \boxdot\varphi.$$

In particular, if $\varphi_u \in \Pi^\tau$ for all $\tau \in [k+1]^m$, then

$$\vdash_L \bigwedge_{v<s}\boxdot\chi_v \wedge \bigvee_{\tau\in[k+1]^m}\bigwedge_{l<m}\Big(\bigvee_{i\le k}\boxdot\psi_{l,i} \to \boxdot\psi_{l,\tau_l}\Big) \to \varphi_u.$$

However,

$$\bigvee_{\tau\in[k+1]^m}\bigwedge_{l<m}\Big(\bigvee_{i\le k}\boxdot\psi_{l,i} \to \boxdot\psi_{l,\tau_l}\Big)$$

is a classical tautology, as it follows from

$$\bigwedge_{l<m}\bigvee_{j\le k}\Big(\bigvee_{i\le k}\boxdot\psi_{l,i} \to \boxdot\psi_{l,j}\Big)$$

by distributivity. Thus, we obtain (35). $\Box$

Our main application of the bounds on the complexity of DP are lower bounds, or more precisely separations between L-EF and L-SF systems. We will make use of the following translation of quantified Boolean formulas to modal circuits.

Definition 4.2 Given a quantified Boolean formula $\Phi(\vec{p})$ in prenex normal form with bound propositional variables $\vec{q}$, we construct a modal circuit $A_\Phi(\vec{p},\vec{q})$ as follows:

$$\begin{aligned} A_\Phi &= \Phi \qquad \text{if } \Phi \text{ is quantifier-free},\\ A_{\forall q\,\Phi} &= \boxdot q \vee \boxdot\neg q \to A_\Phi,\\ A_{\exists q\,\Phi} &= \Box(\boxdot q \to A_\Phi) \vee \Box(\boxdot\neg q \to A_\Phi). \end{aligned}$$

(In order to make a polynomial-size circuit, both disjuncts in the definition of $A_{\exists q\,\Phi}$ use the same copy of A_Φ.) Let $\overline{\Phi}$ denote the prenex normal form of $\neg\Phi$ obtained by dualizing all quantifiers and negating the quantifier-free matrix of Φ.

Lemma 4.3 *Given a Boolean circuit $\varphi(p_0,\dots,p_{n-1})$, there are poly-time constructible* **K**-CF *proofs of*

$$\bigwedge_{i<n}(\Box p_i \vee \Box\neg p_i) \to \Box\varphi \vee \Box\neg\varphi. \tag{36}$$

Proof: By induction on the size of φ, using instances of the tautologies

$$\begin{gathered} \Box\varphi \vee \Box\neg\varphi \to \Box\neg\varphi \vee \Box\neg\neg\varphi,\\ (\Box\varphi \vee \Box\neg\varphi) \wedge (\Box\psi \vee \Box\neg\psi) \to \Box(\varphi\circ\psi) \vee \Box\neg(\varphi\circ\psi) \end{gathered}$$

for $\circ \in \{\wedge,\vee,\to\}$, which have linear-size proofs by Observation 2.2. □

Lemma 4.4 *Given a QBF $\Phi(p_0,\dots,p_{n-1})$, there are poly-time constructible* **K4**-SCF *proofs of*

$$\bigwedge_{i<n}(\Box p_i \vee \Box\neg p_i) \to \Box A_\Phi \vee \Box A_{\overline{\Phi}}. \tag{37}$$

Proof: By induction on the number of quantifiers. The base case is Lemma 4.3. For the induction step, we may assume $\Phi = \exists q\,\Phi_0(q,\vec{p})$ by swapping the roles of Φ and $\overline{\Phi}$ if necessary. By the induction hypothesis, we have a proof of

$$\bigwedge_{i<n}(\Box p_i \vee \Box\neg p_i) \wedge (\Box q \vee \Box\neg q) \to \Box A_{\Phi_0}(q) \vee \Box A_{\overline{\Phi}_0}(q)$$

(not showing other variables). Using the substitution rule twice, we obtain

$$\begin{aligned} \bigwedge_{i<n}(\Box p_i \vee \Box\neg p_i) &\to \big(\Box A_{\Phi_0}(\top) \vee \Box A_{\overline{\Phi}_0}(\top)\big) \wedge \big(\Box A_{\Phi_0}(\bot) \vee \Box A_{\overline{\Phi}_0}(\bot)\big)\\ &\to \big(\Box A_{\Phi_0}(\top) \vee \Box A_{\Phi_0}(\bot)\big) \vee \Box\big(A_{\overline{\Phi}_0}(\top) \wedge A_{\overline{\Phi}_0}(\bot)\big)\\ &\to \big(\Box(\boxdot q \to A_{\Phi_0}) \vee \Box(\boxdot\neg q \to A_{\Phi_0})\big) \vee \Box(\boxdot q \vee \boxdot\neg q \to A_{\overline{\Phi}_0})\\ &\to \Box A_\Phi \vee \Box A_{\overline{\Phi}} \end{aligned}$$

with the help of Lemma 2.8. □

Lemma 4.5 *Let Φ be a QBF in free variables $\vec{p}$, let $\vec{a}$ be a Boolean assignment to $\vec{p}$, and $\vec{p}/\vec{a}$ be the corresponding substitution. If L is a logic with DP, and*

$$\vdash_L A_\Phi(\vec{p}/\vec{a}),$$

then $\Phi(\vec{a})$ is true.

Proof: By induction on the number of quantifiers in Φ. If Φ is quantifier-free, then $A_\Phi(\vec{p}/\vec{a})$ is just $\Phi(\vec{a})$. If $\Phi = \exists q\, \Phi_0(\vec{p}, q)$, and

$$\vdash_L \Box\big(\boxdot q \to A_{\Phi_0}(\vec{p}/\vec{a})\big) \vee \Box\big(\boxdot\neg q \to A_{\Phi_0}(\vec{p}/\vec{a})\big),$$

then by DP,

$$\vdash_L \boxdot q \to A_{\Phi_0}(\vec{p}/\vec{a}) \quad \text{or} \quad \vdash_L \boxdot\neg q \to A_{\Phi_0}(\vec{p}/\vec{a}),$$

hence there exists $b \in \{\bot, \top\}$ such that

$$\vdash_L A_{\Phi_0}(\vec{p}/\vec{a}, q/b).$$

By the induction hypothesis, $\Phi_0(\vec{a}, b)$ is true, hence so is $\Phi(\vec{a})$.

If $\Phi = \forall q\, \Phi_0(\vec{p}, q)$, then $\vdash_L \boxdot q \vee \boxdot\neg q \to A_{\Phi_0}(\vec{p}/\vec{a})$ implies

$$\vdash_L A_{\Phi_0}(\vec{p}/\vec{a}, q/\bot) \wedge A_{\Phi_0}(\vec{p}/\vec{a}, q/\top),$$

hence $\Phi_0(\vec{a}, \bot)$ and $\Phi_0(\vec{a}, \top)$ are true, hence so is $\Phi(\vec{a})$. $\Box$

We come to our basic separation between EF and SF. We use the same tautologies for all logics in question, and while we apply Theorem 4.1 to get the EF lower bounds, the SF upper bounds hold already for the base logic **K4**. This implies a separation for all *sublogics* of logics satisfying the assumptions of Theorem 4.1, which allows us to formulate the result without explicit reference to $*$-extensible logics L_0: the largest $\bullet$-extensible logic is **GL** (being complete w.r.t. finite irreflexive trees), and likewise, the largest $\circ$-extensible logic is **S4Grz**. For the same reason, we only need to refer to the strongest among the $\mathbf{BB}_k$ axioms, viz. $\mathbf{BB_2}$.

Theorem 4.6 *If* $\mathbf{K4} \subseteq L \subseteq \mathbf{S4GrzBB_2}$ *or* $\mathbf{K4} \subseteq L \subseteq \mathbf{GLBB_2}$*, then* L-SF *has superpolynomial speed-up over* L-EF *unless* PSPACE = NP = coNP.

More precisely, if PSPACE $\neq$ NP*, there exists a sequence of formulas that have polynomial-time constructible* **K4**-SF *proofs, but require proofs of superpolynomial size in* $\mathbf{S4GrzBB_2}$-EF *or* $\mathbf{GLBB_2}$-EF.

Proof: We may work with CF and SCF in place of EF and SF (respectively), and then it is enough to construct a sequence of circuits rather than formulas by Lemmas 2.5 and 2.6.

Given a QBF Φ without free variables, the circuits

$$\Box A_\Phi \vee \Box A_{\overline{\Phi}} \tag{38}$$

have polynomial-time constructible **K4**-SCF proofs by Lemma 4.4. Assume for not-quite-a-contradiction that they have L-CF proofs of size $|\Phi|^c$ for some constant c, where w.l.o.g. $L =$

$\mathbf{S4GrzBB_2}$ or $L = \mathbf{GLBB_2}$ using Corollary 2.3. By Theorem 4.1, there are coNP predicates D_0 and D_1 such that

$$\begin{aligned} \pi \text{ is an } L\text{-CF proof of } \Box A_\Phi \vee \Box A_{\overline{\Phi}} &\implies D_0(\Phi,\pi) \vee D_1(\Phi,\pi), \\ D_1(\Phi,\pi) &\implies \vdash_L A_\Phi, \\ D_0(\Phi,\pi) &\implies \vdash_L A_{\overline{\Phi}}. \end{aligned}$$

Since

$$\begin{aligned} \vdash_L A_\Phi &\implies \Phi \text{ is true}, \\ \vdash_L A_{\overline{\Phi}} &\implies \Phi \text{ is false} \end{aligned}$$

by Lemma 4.5, we obtain

$$\begin{aligned} \Phi \text{ is true} &\iff \forall \pi \left(|\pi| \le |\Phi|^c \to D_1(\Phi,\pi) \right) \\ &\iff \exists \pi \left(|\pi| \le |\Phi|^c \mathbin{\&} \neg D_0(\Phi,\pi) \right), \end{aligned}$$

which gives an NP and coNP expression for a PSPACE-complete language. $\Box$

Remark 4.7 We can improve the speed-up to exponential (2^{n^ϵ}) under the stronger hypothesis PSPACE $\nsubseteq$ NSUBEXP.

With some care, we could make sure the formulas had poly-time proofs even in $\mathbf{K}$-SF. (Basically, in Definition 4.2, we need to replace $\boxdot$ with $\Box^d$ (i.e., $\Box \dots \Box$ with d boxes) where d is the number of quantifiers in Φ, and add an extra $\Box$ in front of the definition of $A_{\forall q\,\Phi}$. We also replace $\Box$ with $\Box^{d+1}$ in the premise of (37).)

5 The argument internalized

Theorem 4.1 does not satisfactorily determine the complexity of $\mathrm{Dec}(\mathrm{Ext}_t^*, L\text{-CF})$: the upper bound it gives (total coNP search problem) does not come with a matching lower bound, and in fact, the true complexity of the problem is most probably strictly weaker. The reason for this is that there likely exist no *complete* total coNP search problems (see Pudlák [22] for a detailed discussion of conjectures related to the nonexistence of complete disjoint NP pairs—recall that disjoint NP pairs can be identified with two-valued total coNP search problems).

Thus, unlike classes such as NP, the class of total coNP search problems forms an (upwards directed) preorder of problems of ever growing complexity with no maximum, and any particular total coNP search problem has complexity strictly smaller than the whole class. For this reason, it is desirable to gauge the complexity of $\mathrm{Dec}(\mathrm{Ext}_t^*, L\text{-CF})$ more precisely by reducing it to *specific* natural and/or previously studied total coNP search problems (more informative than the opaque ad hoc problem $D(\pi)$ from the proof of Theorem 4.1), and ideally, to prove it equivalent to such a problem.

In this section, we are going to reduce $\mathrm{Dec}(\mathrm{Ext}_t^*, L\text{-CF})$ to the well known *feasible interpolation* problem for the *classical* extended Frege system, and in fact, we will show that it is equivalent to its special case $\mathrm{Dec}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF})$, where $\mathrm{R}_{k,t}$ is a certain rule introduced in

Definition 5.4. Moreover, the equivalence lifts to the corresponding proof-construction problems. As a consequence, we can improve Theorem 4.6: if, for the logics in question, L-SF has no speed-up over L-EF, then PSPACE collapses not just to NP, but to the interpolation disjoint NP pair for **CPC**-EF (and even to the corresponding problem involving $\mathrm{R}_{2,2}$), albeit with nonuniform advice.

The argument is based on *internalizing* parts of the proof of Theorem 4.1: we express some of the polynomial-time constructions employed in the proof by explicit Boolean circuits, and we derive some of their properties used in the argument by short **CPC**-CF or L-CF proofs. As a bonus, we will obtain additional information on feasibility of some weaker forms of the Ext_t^* rules (see the statement of Theorem 5.8 for details).

From now on, let us fix $k \geq t \geq 2$, $* \in \{\bullet, \circ\}$, a $*$-extensible logic L_0, and $L = L_0 \oplus \mathbf{BB}_k$. Moreover, assume we are given an L-CF proof $\pi = \langle \theta_0, \dots, \theta_z \rangle$ of

$$\bigwedge_{v<s} B^*(\chi_v) \to \bigvee_{u<t} \Box\varphi_u, \tag{39}$$

and let $\{A_l : l < m\}$ and Ξ_π be as in the proof of Theorem 4.1. Put $S = \mathrm{Sub}(\pi \cup \Xi_\pi)$ and $N = |S|$.

We start by describing the sets Π_σ and Π^τ from the proof of Theorem 4.1 with (Boolean) circuits. More generally, if a is any assignment to the propositional variables $\{s_{l,r} : l < m, r \leq k\}$ (which we assume to be distinct from all variables used in π), let $\Pi_a \subseteq S$ be the closure of $\pi \cup \Xi_\pi \cup \{\chi_v : v < s\}$ under (MP), S-restricted (Nec), and the rules (22) for $l < m$ and $r \leq k$ such that $a(s_{l,r}) = 1$. We may stratify it by putting $\Pi_{a,0} = \pi \cup \Xi_\pi \cup \{\vec{\chi}\}$, and inductively defining $\Pi_{a,h+1}$ as $\Pi_{a,h}$ plus conclusions of all the above-mentioned rules whose premises are in $\Pi_{a,h}$. We have $\Pi_{a,N} = \Pi_a$.

In order to describe $\Pi_{a,h}$, we construct monotone Boolean circuits $C_{\varphi,h}(\vec{s})$ for $\varphi \in S$ and $h \leq N+1$ as follows:

$$C_{\varphi,0} = \begin{cases} \top, & \varphi \in \pi \cup \Xi_\pi \cup \{\chi_v : v < s\}, \\ \bot, & \text{otherwise}, \end{cases}$$

$$C_{\varphi,h+1} = C_{\varphi,h} \vee \underbrace{\bigvee\nolimits_{\psi} (C_{\psi,h} \wedge C_{\psi\to\varphi,h})}_{\text{for } \psi \text{ s.t. } \psi\to\varphi \in S} \underbrace{\vee\, C_{\psi,h}}_{\text{if } \varphi = \Box\psi} \vee \underbrace{\bigvee\nolimits_{\psi} (C_{\psi,h} \wedge s_{l,r})}_{\substack{\text{for } \psi = \bigvee_i \boxdot\psi_{l,i} \\ \text{s.t. } \varphi = \bigvee_{i\neq r} \boxdot\psi_{l,i}}}.$$

Finally, we define $C_\varphi = C_{\varphi,N}$. It should be clear from the definition that

$$\begin{aligned} C_{\varphi,h}(a) = 1 &\iff \varphi \in \Pi_{a,h}, \\ C_\varphi(a) = 1 &\iff \varphi \in \Pi_a. \end{aligned}$$

We need to internally verify two basic properties of $\{\varphi : C_\varphi = 1\}$: that it is closed under the above-mentioned rules, and that its elements are provable from appropriate hypotheses. These are formalized by the next two lemmas.

Lemma 5.1 *The following have poly-time constructible* **CPC**-CF *proofs.*

$$C_{\varphi,h} \to C_{\varphi,h'}, \qquad h < h' \le N+1,\ \varphi \in S, \tag{40}$$

$$\bigwedge_{\varphi\in S}(C_{\varphi,h+1} \to C_{\varphi,h}) \to \bigwedge_{\varphi\in S}(C_{\varphi,h+2} \to C_{\varphi,h+1}), \qquad h < N, \tag{41}$$

$$C_{\varphi,N+1} \to C_{\varphi,N}, \qquad \varphi \in S, \tag{42}$$

$$C_\varphi, \qquad \varphi \in \pi \cup \Xi_\pi \cup \{\chi_v : v < s\}, \tag{43}$$

$$C_\varphi \wedge C_{\varphi\to\psi} \to C_\psi, \qquad \varphi \to \psi \in S, \tag{44}$$

$$C_\varphi \to C_{\Box\varphi}, \qquad \Box\varphi \in S, \tag{45}$$

$$s_{l,r} \wedge C_{\bigvee_i \Box\psi_{l,i}} \to C_{\bigvee_{i\ne r}\Box\psi_{l,i}}, \qquad l < m,\ r \le k. \tag{46}$$

Proof: (40) follows by chaining the implications $C_{\varphi,h} \to C_{\varphi,h+1}$, which are immediate consequences of the definition.

(41): For any $\varphi' \in S$, we can prove

$$\bigwedge_{\varphi\in S}(C_{\varphi,h+1} \to C_{\varphi,h}) \to \Big(\bigvee\nolimits_\psi(C_{\psi,h+1} \wedge C_{\psi\to\varphi',h+1}) \to \bigvee\nolimits_\psi(C_{\psi,h} \wedge C_{\psi\to\varphi',h})\Big),$$

and similarly for the other disjuncts in the definition of $C_{\varphi',h+2}$, hence

$$\bigwedge_{\varphi\in S}(C_{\varphi,h+1} \to C_{\varphi,h}) \to (C_{\varphi',h+2} \to C_{\varphi',h+1}).$$

Combining these for all $\varphi' \in S$ gives (41).

(42): In view of (41), it suffices to prove

$$\bigvee_{h\le N}\bigwedge_{\varphi\in S}(C_{\varphi,h+1} \to C_{\varphi,h}). \tag{47}$$

Let $\alpha_{h,\varphi} = C_{\varphi,h+1} \wedge \neg C_{\varphi,h}$. Using (40), we can construct a proof of

$$\bigwedge_{\substack{\varphi\in S\\ h<h'\le N}} \neg(\alpha_{h,\varphi} \wedge \alpha_{h',\varphi}),$$

while obviously

$$\neg\bigvee_{h\le N}\bigwedge_{\varphi\in S}(C_{\varphi,h+1} \to C_{\varphi,h}) \to \bigwedge_{h\le N}\bigvee_{\varphi\in S}\alpha_{h,\varphi}.$$

Thus, (47) follows from an instance of PHP^{N+1}_N, which has short **CPC**-CF proofs [5].

(43) follows from (40), as $C_{\varphi,0} = \top$ by definition.

(44): We derive

$$\begin{aligned} C_{\varphi,N} \wedge C_{\varphi\to\psi,N} &\to C_{\psi,N+1} && \text{definition of } C_{\psi,N+1},\\ &\to C_{\psi,N} && \text{by (42).}\end{aligned}$$

The proofs of (45) and (46) are analogous. $\Box$

Lemma 5.2 *For any $\varphi \in S$ and $h \le N$, there are poly-time constructible L-*CF *proofs of*

$$\bigwedge_{\substack{l<m\\ r\le k}} \Big(s_{l,r} \wedge \boxdot\psi_{l,r} \to \bigvee_{i\ne r} \boxdot\psi_{l,i}\Big) \wedge C_{\varphi,h}(\vec{s}) \wedge \bigwedge_{v<s} \boxdot\chi_v \to \boxdot\varphi. \tag{48}$$

Proof: By induction on h. For $h = 0$, the cases $\varphi = \chi_v$ are trivial, π itself gives a proof of φ (whence $\boxdot\varphi$) for all $\varphi \in \pi$, and it is straightforward to construct short **K**-CF proofs of $\varphi \in \Xi_\pi$.

For $h+1$, we unwind the definition of $C_{\varphi,h+1}$, and use short subproofs of

$$\boxdot\psi \wedge \boxdot(\psi \to \varphi) \to \boxdot\varphi,$$
$$\boxdot\psi \to \boxdot\Box\psi,$$
$$s_{l,r} \wedge \Big(s_{l,r} \wedge \boxdot\psi_{l,r} \to \bigvee_{i\ne r} \boxdot\psi_{l,i}\Big) \wedge \boxdot \bigvee_{i\le k} \boxdot\psi_{l,i} \to \boxdot \bigvee_{i\ne r} \boxdot\psi_{l,i},$$

where the last one employs $\bigvee_{i\ne r} \boxdot\psi_{l,i} \to \Box \bigvee_{i\ne r} \boxdot\psi_{l,i}$. $\Box$

We remark that the same proof shows that if $\alpha(p)$ is a formula such that L proves $\alpha(\top)$, $\alpha(p) \to \alpha(\Box p)$, and $\alpha(p) \wedge \alpha(p \to q) \to \alpha(q)$, then there are poly-time constructible L-CF proofs of

$$\bigwedge_{\substack{l<m\\ r\le k}} \Big[s_{l,r} \wedge \alpha\Big(\bigvee_{i\le k} \boxdot\psi_{l,i}\Big) \to \alpha\Big(\bigvee_{i\ne r} \boxdot\psi_{l,i}\Big)\Big] \wedge C_\varphi(\vec{s}) \wedge \bigwedge_{v<s} \alpha(\chi_v) \to \alpha(\varphi).$$

However, we do not have a use for this more general statement.

The heart of the argument is to show that C_{φ_u} holds for some $u < t$ (under suitable conditions). To this end, we define Boolean circuits $V_\varphi(\vec{s})$ for $\varphi \in S$, representing the Boolean assignments v_σ from the proof of Theorem 4.1: we let V_φ be arbitrary (say, $\top$) if φ is a variable, and we put

$$V_{c(\varphi_0,\dots,\varphi_{d-1})} = c(V_{\varphi_0}, \dots, V_{\varphi_{d-1}}), \qquad c \in \{\wedge, \vee, \to, \neg, \top, \bot\},$$
$$V_{\Box\varphi} = \begin{cases} C_\varphi, & * = \bullet,\\ C_\varphi \wedge V_\varphi, & * = \circ.\end{cases}$$

Lemma 5.3 *There are poly-time constructible* **CPC**-CF *proofs of*

$$\bigwedge_{l<m} \bigvee_{r\le k} s_{l,r} \to V_{\theta_g}, \qquad g \le z, \tag{49}$$

$$\bigwedge_{l<m} \bigvee_{r\le k} s_{l,r} \to \bigvee_{u<t} C_{\varphi_u}. \tag{50}$$

Proof: (49): By induction on g, using the structure of π. If θ_g is derived by (MP) from $\theta_h = \theta_i \to \theta_g$ and θ_i, we have

$$V_{\theta_h} \wedge V_{\theta_i} \to V_{\theta_g}$$

from the definition of V_{θ_h}. Likewise, if θ_g is an instance of an axiom of **CPC**, then V_{θ_g} unwinds to an instance of the same axiom. If $\theta_g = \Box\theta_h$ is derived by (Nec), we have

$$C_{\theta_h} \wedge V_{\theta_h} \to V_{\theta_g}$$

by the definition of V_{θ_g}, while C_{θ_h} is provable by (43). If θ_g is an instance of (**K**), then depending on $*$, V_{θ_g} is one of

$$C_{\varphi\to\psi} \to (C_\varphi \to C_\psi),$$
$$C_{\varphi\to\psi} \wedge (V_\varphi \to V_\psi) \to (C_\varphi \wedge V_\varphi \to C_\psi \wedge V_\psi),$$

which have short proofs using (44). If θ_g is an instance of (**4**), V_{θ_g} is one of

$$C_\varphi \to C_{\Box\varphi},$$
$$C_\varphi \wedge V_\varphi \to C_{\Box\varphi} \wedge C_\varphi \wedge V_\varphi,$$

which follow from (45). This completes the axioms and rules of **K4**.

If $* = \bullet$ and θ_g is (10), V_{θ_g} is

$$C_{\beta'_j} \to (C_{\Box\alpha'_j\to\alpha'_j} \to C_{\alpha'_j}).$$

We can prove

$$\begin{aligned} C_{\beta'_j} \wedge C_{\Box\alpha'_j\to\alpha'_j} &\to C_{\Box\beta'_j} \wedge C_{\Box(\Box\alpha'_j\to\alpha'_j)} && \text{by (45)}, \\ &\to C_{\Box\alpha'_j} && \text{by (43) for } \theta_g, \text{ and (44)}, \\ &\to C_{\alpha'_j} && \text{by (44)}. \end{aligned}$$

If $* = \circ$ and θ_g is (13), V_{θ_g} is the tautology

$$V_{\beta'_j} \wedge C_{\alpha'_j} \wedge V_{\alpha'_j} \to V_{\alpha'_j}.$$

If θ_g is (14), then V_{θ_g} can be proved by formalizing the relevant part of the proof of Theorem 2.15, which we leave to the reader.

The remaining case is $\theta_g = A_l$ for some $l < m$. Let us abbreviate

$$\begin{aligned} \delta_l &= \bigvee_{i\le k} \boxdot\psi_{l,i}, \\ \delta_{l,i} &= \bigvee_{j\ne i} \boxdot\psi_{l,j}, \\ \beta_l &= \bigvee_{i\le k} \Box(\boxdot\psi_{l,i} \to \delta_{l,i}), \end{aligned}$$

so that

$$A_l = \Box(\beta_l \to \delta_l) \to \bigvee_{i\le k} \Box\delta_{l,i}.$$

For any $r \le k$, we prove

$$\begin{aligned} V_{\Box(\beta_l\to\delta_l)} &\to C_{\beta_l\to\delta_l} && \text{by definition}, \\ &\to C_{\Box(\beta_l\to\delta_l)} && \text{by (45)}, \\ &\to C_{\bigvee_i \Box\delta_{l,i}} && \text{by (43) for } A_l, \text{ and (44)}, \\ &\to C_{\beta_l} && \text{by (43) for (18), and (44)}, \\ &\to C_{\delta_l} && \text{by (44)}, \\ &\to (s_{l,r} \to C_{\delta_{l,r}}) && \text{by (46)}. \end{aligned}$$

If $* = \bullet$, this gives

$$\bigvee_{r \leq k} s_{l,r} \wedge V_{\Box(\beta_l \to \delta_l)} \to \bigvee_{r \leq k} V_{\Box \delta_{l,r}},$$

thus (49). If $* = \circ$, we continue with

$$\begin{aligned}
s_{l,r} \wedge V_{\Box(\beta_l \to \delta_l)} &\to C_{\boxdot \psi_{l,r} \to \delta_{l,r}} && \text{by (43) for (19), and (44),} \\
&\to \big((V_{\boxdot \psi_{l,r}} \to V_{\delta_{l,r}}) \to V_{\beta_l}\big) && \text{definition of } V_{\Box(\boxdot \psi_{l,i} \to \delta_{l,i})}, \\
&\to (V_{\beta_l} \to V_{\delta_l}) && \text{definition of } V_{\Box(\beta_l \to \delta_l)}, \\
&\to V_{\boxdot \psi_{l,r}} \vee V_{\delta_{l,r}} && \text{using } V_{\delta_l} \to V_{\boxdot \psi_{l,r}} \vee V_{\delta_{l,r}}, \\
&\to V_{\boxdot \psi_{l,r}} \vee V_{\Box \delta_{l,r}} && \text{definition of } V_{\Box \delta_{l,r}}.
\end{aligned}$$

We also have for any fixed $i \neq r$,

$$\begin{aligned}
V_{\boxdot \psi_{l,r}} &\to C_{\psi_{l,r}} \wedge V_{\delta_{l,i}} && \text{definitions,} \\
&\to C_{\Box \psi_{l,r}} && \text{by (45),} \\
&\to C_{\delta_{l,i}} && \text{by (43) for (20), and (44),} \\
&\to V_{\Box \delta_{l,i}} && \text{definition,}
\end{aligned}$$

thus

$$s_{l,r} \wedge V_{\Box(\beta_l \to \delta_l)} \to \bigvee_{i \leq k} V_{\Box \delta_{l,i}}$$

for all $r \leq k$, which implies (49).

(50): By applying (49) to $\theta_z = (39)$, we obtain

$$\bigwedge_{l<m} \bigvee_{r \leq k} s_{l,r} \wedge \bigwedge_{v<s} V_{B^*(\chi_v)} \to \bigvee_{u<t} V_{\Box \varphi_u}.$$

By definition, $V_{\Box \varphi_u}$ implies C_{φ_u}, and $V_{B^*(\chi_v)}$ is one of the circuits C_{χ_v} or $V_{\chi_v} \leftrightarrow C_{\chi_v} \wedge V_{\chi_v}$ which follow from (43). Thus, we obtain (50). $\Box$

As we already stated, we intend to reduce $\mathrm{Dec}(\mathrm{Ext}_t^*, L\text{-CF})$ to interpolation problems for **CPC**-CF. We formulate feasible interpolation in the following way to fit into our framework of multi-conclusion rules. If P is a classical proof system, the standard interpolation problem for P (introduced by Pudlák [21] as a disjoint NP pair rather than the corresponding search problem) is $\mathrm{Dec}(\mathrm{Itp}_2, P)$ in our notation.

Definition 5.4 For classical logic, the t-ary *interpolation* multi-conclusion rule is

$$(\mathrm{Itp}_t) \qquad \bigvee_{u<t} \varphi_u \Big/ \varphi_0, \dots, \varphi_{t-1},$$

where φ_u, $u < t$, are formulas using pairwise disjoint sets of variables.

For any constants $k \geq t \geq 2$, we introduce the rule

$$(\mathrm{R}_{k,t}) \qquad \frac{\displaystyle\bigwedge_{l<n} \bigvee_{i \leq k} p_{l,i} \to \bigvee_{u<t} \varphi_u}{\displaystyle\bigwedge_{\substack{l<n \\ i<j \leq k}} (p_{l,i} \vee p_{l,j}) \to \varphi_0, \dots, \bigwedge_{\substack{l<n \\ i<j \leq k}} (p_{l,i} \vee p_{l,j}) \to \varphi_{t-1}},$$

where φ_u are monotone formulas or circuits in the (pairwise distinct) variables $p_{l,i}$ ($l < n$, $i \leq k$).

It is well known that Itp_t is admissible in **CPC** (if no φ_u is a tautology, we can combine assignments refuting each φ_u to an assignment refuting $\bigvee_u \varphi_u$, using the disjointness of their sets of variables). It is also easy to see that for proof systems P dealing with circuits such as **CPC**-CF, we may allow φ_u to be circuits without changing the complexity of $\mathrm{Dec}(\mathrm{Itp}_t, P)$, as we can choose disjoint sets of extension variables for each φ_u to express them as formulas.

Lemma 5.5 *For any $k \geq t \geq 2$, the rules $\mathrm{R}_{k,t}$ are admissible in* **CPC**. *Moreover, if $P =$* **CPC**-CF*, then $\mathrm{Dec}(\mathrm{R}_{k,t}, P) \leq_s \mathrm{Dec}(\mathrm{Itp}_t, P)$ and $\mathrm{Cons}(\mathrm{R}_{k,t}, P) \leq \mathrm{Cons}(\mathrm{Itp}_t, P)$.*

Proof: It is enough to prove the latter. Assume we are given a P-proof of

$$\bigwedge_{l<n} \bigvee_{i\leq k} p_{l,i} \to \bigvee_{u<t} \varphi_u(\vec{p}) \tag{51}$$

where the φ_u are monotone. Using t copies $\{p^u_{l,i} : u < t\}$ of each original $p_{l,i}$ variable, it suffices to construct a P-proof of

$$\bigvee_{u<t} \Big(\bigwedge_{l<n} \bigwedge_{i<j\leq k} (p^u_{l,i} \vee p^u_{l,j}) \to \varphi_u(\vec{p}^u) \Big).$$

Since this is clearly implied by $\bigvee_{u<t} \neg \bigwedge_l \bigwedge_{i<j} (p^u_{l,i} \vee p^u_{l,j})$, it is enough to prove

$$\bigwedge_{u<t} \bigwedge_{l<n} \bigwedge_{i<j\leq k} (p^u_{l,i} \vee p^u_{l,j}) \to \bigvee_{u<t} \varphi_u(\vec{p}^u). \tag{52}$$

Now, using n instances of the constant-size tautology

$$\bigwedge_{u<t} \bigwedge_{i<j\leq k} (q^u_i \vee q^u_j) \to \bigvee_{i\leq k} \bigwedge_{u<t} q^u_i$$

(a form of PHP^{k+1}_t), we can construct a proof of

$$\bigwedge_{l<n} \bigwedge_{u<t} \bigwedge_{i<j\leq k} (p^u_{l,i} \vee p^u_{l,j}) \to \bigwedge_{l<n} \bigvee_{i\leq k} \bigwedge_{u<t} p^u_{l,i},$$

hence also

$$\begin{aligned} \bigwedge_{l<n} \bigwedge_{u<t} \bigwedge_{i<j\leq k} (p^u_{l,i} \vee p^u_{l,j}) &\to \bigvee_{u<t} \varphi_u\Big(\ldots, \bigwedge_{v<t} p^v_{l,i}, \ldots\Big) \\ &\to \bigvee_{u<t} \varphi_u(\vec{p}^u) \end{aligned}$$

using a substitution instance of (51) and Lemma 2.9. This establishes (52). □

Remark 5.6 For $P =$ **CPC**-CF (or equivalently, $P =$ **CPC**-EF), the interpolation NP pair is equivalent to the *canonical* pair $\langle SAT^*, REF(P) \rangle$ of Razborov [23] by a folklore argument using the fact that P has polynomial-time constructible proofs of its own reflection principle.

Lemma 5.7 *Under our running assumptions,* $\mathrm{Dec}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF}) \le_s \mathrm{Dec}(\mathrm{Ext}^*_t, L\text{-CF})$ *and* $\mathrm{Cons}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF}) \le \mathrm{Cons}(\mathrm{Ext}^*_t, L\text{-CF})$*.*

Proof: Assume we are given a **CPC**-CF proof of

$$\bigwedge_{l<n} \bigvee_{i\le k} p_{l,i} \to \bigvee_{u<t} \varphi_u, \tag{53}$$

where φ_u are monotone circuits. For each $l < n$ and $i \le k$, put

$$\beta_{l,i} = \boxdot q_{l,i} \to \bigvee_{j\ne i} \boxdot q_{l,j},$$
$$\alpha_l = \bigvee_{i\le k} \Box\beta_{l,i} \to \bigvee_{i\le k} \boxdot q_{l,i}.$$

We can construct for each $l < n$ short L-CF proofs of

$$\begin{aligned}
B^*(\alpha_l) &\to \Box\alpha_l \vee \neg\alpha_l && \text{from definition,}\\
&\to \Box\alpha_l \vee \bigvee_{i\le k} \Box\beta_{l,i}\\
&\to \bigvee_{i\le k} \Box \bigvee_{j\ne i} \boxdot q_{l,j} \vee \bigvee_{i\le k} \Box\beta_{l,i} && \text{by } \mathbf{BB}_k,\\
&\to \bigvee_{i\le k} \Box\beta_{l,i},
\end{aligned}$$

hence of

$$\begin{aligned}
\bigwedge_{l<n} B^*(\alpha_l) &\to \bigwedge_{l<n} \bigvee_{i\le k} \Box\beta_{l,i}\\
&\to \bigvee_{u<t} \varphi_u(\dots, \Box\beta_{l,i}, \dots) && \text{substitution instance of (53),}\\
&\to \bigvee_{u<t} \Box\varphi_u(\dots, \beta_{l,i}, \dots) && \text{Lemma 2.10.}
\end{aligned}$$

This is our reduction to $\mathrm{Dec}(\mathrm{Ext}^*_t, L\text{-CF})$. We need to show that if $u < t$ is such that L proves

$$\bigwedge_{l<n} \boxdot\alpha_l \to \varphi_u(\dots, \beta_{l,i}, \dots), \tag{54}$$

then **CPC** proves

$$\bigwedge_{\substack{l<n\\ i<j\le k}} (p_{l,i} \vee p_{l,j}) \to \varphi_u, \tag{55}$$

and that given an L-CF proof of (54), we can construct a **CPC**-CF proof of (55).

Using short L-CF proofs of

$$\bigvee_{i\le k} \boxdot q_{l,i} \to \boxdot\alpha_l,$$
$$\bigvee_{i\le k} \boxdot q_{l,i} \to \Big(\beta_{l,i} \to \bigvee_{j\ne i} \boxdot q_{l,j}\Big),$$

and Lemma 2.9, (54) yields an L-CF proof of

$$\bigwedge_{l<n} \bigvee_{i\le k} \boxdot q_{l,i} \to \varphi_u\Bigl(\dots, \bigvee_{j\ne i} \boxdot q_{l,j}, \dots\Bigr).$$

By Lemma 2.11, we can construct a **CPC**-CF proof of

$$\bigwedge_{l<n} \bigvee_{i\le k} q_{l,i} \to \varphi_u\Bigl(\dots, \bigvee_{j\ne i} q_{l,j}, \dots\Bigr).$$

We now substitute $\bigwedge_{j\ne i} p_{l,j}$ for $q_{l,i}$ in the proof. Using short proofs of

$$\bigwedge_{i<j\le k} (p_{l,i} \lor p_{l,j}) \to \bigvee_{i\le k} \bigwedge_{j\ne i} p_{l,j},$$

$$\bigvee_{j\ne i} \bigwedge_{r\ne j} p_{l,r} \to p_{l,i},$$

and Lemma 2.9, we obtain a **CPC**-CF proof of (55). $\square$

We can now put everything together.

Theorem 5.8 *Let $* \in \{\bullet, \circ\}$, L_0 be a $*$-extensible logic, $k \ge t \ge 2$, and $L = L_0 \oplus \mathbf{BB}_k$.*

(i) $\mathrm{Dec}(\mathrm{Ext}^*_t, L\text{-CF}) \equiv_s \mathrm{Dec}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF})$, $\mathrm{Cons}(\mathrm{Ext}^*_t, L\text{-CF}) \equiv \mathrm{Cons}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF})$.

(ii) *Given an L-CF proof of*

$$\bigwedge_{v<s} B^*(\chi_v) \to \bigvee_{u<t} \Box\varphi_u \tag{56}$$

using variables $\{p_i : i < n\}$, we can construct in polynomial time an L-CF proof of

$$\bigvee_{u<t} \sigma^u\Bigl(\bigwedge_{v<s} \boxdot\chi_v \to \varphi_u\Bigr), \tag{57}$$

where we choose pairwise distinct variables $\{p^u_i : u < t, i < n\}$, and define σ^u as the substitution such that $\sigma^u(p_i) = p^u_i$ for each $i < n$.

(iii) $\mathrm{Cons}(\mathrm{Ext}^*_1, L\text{-CF}) \in \mathrm{FP}$.

Proof: (i): The right-to-left reductions were given in Lemma 5.7. For the left-to-right directions, assume we are given an L-CF proof of (56) = (39). By Lemma 5.3, we can construct in polynomial time a **CPC**-CF proof of (50). We claim that this gives the desired reduction to $\mathrm{Dec}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF})$: that is, if $u < t$ is such that

$$\bigwedge_{\substack{l<m \\ i<j\le k}} (s_{l,i} \lor s_{l,j}) \to C_{\varphi_u} \tag{58}$$

is a classical tautology, then L proves

$$\bigwedge_{v<s} \boxdot\chi_v \to \varphi_u, \tag{59}$$

and moreover, given a **CPC**-CF proof of (58), we can construct in polynomial time an L-CF proof of (59).

To see this, let σ be the substitution such that $\sigma(s_{l,r}) = \boxdot\psi_{l,r} \to \bigvee_{i\neq r} \boxdot\psi_{l,i}$ for each $l < m$ and $r \leq k$. Applying σ to Lemma 5.2, we can construct in polynomial time an L-CF proof of

$$\sigma(C_{\varphi_u}) \wedge \bigwedge_{v<s} \boxdot\chi_v \to \boxdot\varphi_u. \tag{60}$$

We can also easily construct a proof of the tautology

$$\bigwedge_{\substack{l<m\\ i<j\leq k}} \sigma(s_{l,i} \vee s_{l,j}), \tag{61}$$

hence by applying σ to a proof of (58), we obtain an L-CF proof of $\sigma(C_{\varphi_u})$, which together with (60) yields (59).

(ii): Again, we can construct in polynomial time a **CPC**-CF proof of (50). By the argument in Lemma 5.5, we can construct a **CPC**-CF proof of

$$\bigvee_{u<t}\Big(\bigwedge_{l<m}\bigwedge_{i<j\leq k}(s^u_{l,i} \vee s^u_{l,j}) \to C_{\varphi_u}(\vec{s}^u)\Big).$$

Applying the substitution σ' such that $\sigma'(s^u_{l,r}) = \sigma^u(\sigma(s_{l,r}))$ gives

$$\bigvee_{u<t} \sigma^u(\sigma(C_{\varphi_u})),$$

using short proofs of $\sigma^u(61)$. Using Lemma 5.2 as above, we construct for each $u < t$ an L-CF proof of

$$\sigma^u(\sigma(C_{\varphi_u})) \to \sigma^u\Big(\bigwedge_{v<s} \boxdot\chi_v \to \boxdot\varphi_u\Big).$$

This yields (57).

(iii) follows from (ii), either by noting that the proof above directly works also for $t = 1$, or formally by putting $\varphi_1 = \varphi_0$, applying (ii) with $t = 2$, and substituting p_i back for p^0_i and p^1_i. $\Box$

Remark 5.9 Theorems 4.1 and 5.8 put bounds on the complexity of $\mathrm{Dec}(\mathrm{DP}_t, L\text{-CF})$ for $t \leq k$. The rules DP_t are in fact L-admissible for all t, and we can derive them by iterating DP_2 (or DP_k). Nevertheless, we do not directly get any nontrivial bounds on the complexity of $\mathrm{Dec}(\mathrm{DP}_t, L\text{-CF})$ for $t > k$: in particular, we cannot simply iterate Theorem 5.8, as we will not have an L-CF proof at hand for the second iteration.

We could in principle iterate $\mathrm{Cons}(\mathrm{DP}_2, L\text{-CF})$, but this would only work in the unlikely case that it is polynomially bounded. That is, if **CPC**-EF has constructive feasible interpolation, then $\mathrm{Cons}(\mathrm{DP}_t, L\text{-CF}) \in \mathrm{FP}$ for all t; more generally, if $\mathrm{Cons}(\mathrm{R}_{k,2}, \mathbf{CPC}\text{-CF})$ is polynomially bounded, then $\mathrm{Cons}(\mathrm{DP}_t, L\text{-CF})$ is polynomially bounded for each t, and it is poly-time bounded-query Turing reducible to $\mathrm{Cons}(\mathrm{R}_{k,2}, \mathbf{CPC}\text{-CF})$.

Remark 5.10 It would be very interesting if we could strengthen (57) to

$$\bigvee_{u<t} \boxdot\Big(\bigwedge_{v<s} \boxdot\chi_v \to \varphi_u\Big)$$

(note that if desired, we could reinsert the σ^u's by the form of Theorem 5.8 already proved), or even better, if we could prove that the following single-conclusion version of the Ext^*_t rule is feasible for L-CF:

$$(\mathrm{Ext}^{*,\vee}_t) \qquad \Box\omega \vee \Box\Big(\bigwedge_{v<s} B^*(\chi_v) \to \bigvee_{u<t} \Box\varphi_u\Big) \Big/ \boxdot\omega \vee \bigvee_{u<t} \boxdot\Big(\bigwedge_{v<s} \boxdot\chi_v \to \varphi_u\Big).$$

For one thing, this would imply $\mathrm{Dec}(\mathrm{DP}_t, L\text{-CF}) \equiv_s \mathrm{Dec}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF})$, but the main significance of the $\mathrm{Ext}^{*,\vee}_t$ rules is that they form a *basis* of schematic single-conclusion admissible rules of L (see [15]), hence it would follow that all schematic single-conclusion admissible rules of L are feasible for L-CF. Moreover, if the construction remained polynomial for repeated usage of such rules, we could generalize to the logics $L = L_0 \oplus \mathbf{BB}_k$ (the EF version of) the main result of [12]: all extended Frege systems for L are equivalent, where we relax the definition of Frege and EF systems such that the consequence relation defined by the Frege rules extends $\vdash_L$, and generates the same set of tautologies, but may include non-derivable rules.

Back to earth, Theorem 5.8 allows us to improve Theorem 4.6:

Corollary 5.11 *If* $\mathbf{K4} \subseteq L \subseteq \mathbf{S4GrzBB_2}$ *or* $\mathbf{K4} \subseteq L \subseteq \mathbf{GLBB_2}$*, then* L-SF *has superpolynomial speed-up over* L-EF *unless the disjoint*-NP-*pair version of* $\mathrm{Dec}(\mathrm{R}_{2,2}, \mathbf{CPC}\text{-CF})$*, and consequently the interpolation* NP *pair for* $\mathbf{CPC}$-EF*, are complete disjoint* PSPACE *pairs under nonuniform poly-time reductions.*

Proof: It is enough to prove hardness w.r.t. complementary PSPACE pairs, i.e., PSPACE languages. Any such language $P \subseteq \mathbf{2}^*$ can be defined by a poly-time constructible sequence of QBFs $\Phi_n(p_0, \dots, p_{n-1})$. By Lemma 4.4, there are poly-time constructible $\mathbf{K4}$-SCF proofs of

$$\bigwedge_{i<n} (\Box p_i \vee \Box\neg p_i) \to \Box A_{\Phi_n} \vee \Box A_{\overline{\Phi}_n}.$$

Assume that these circuits have polynomial-size L-CF proofs π_n, where w.l.o.g. $L = \mathbf{GLBB_2}$ or $L = \mathbf{S4GrzBB_2}$. Then the following makes a poly-time reduction of P to $\mathrm{Dec}(\mathrm{DP}_2, L\text{-CF})$ with nonuniform advice π_n: given $\vec{w} \in \mathbf{2}^n$, substitute the bits of $\vec{w}$ for the p_i variables in π_n, and derive $\Box A_{\Phi_n}(\vec{p}/\vec{w}) \vee \Box A_{\overline{\Phi}_n}(\vec{p}/\vec{w})$; pass the resulting proof to $\mathrm{Dec}(\mathrm{DP}_2, L\text{-CF})$ to find which disjunct is provable, which by Lemma 4.5 tells us whether $\vec{w} \in P$. By Theorem 5.8 and Lemma 5.5, $\mathrm{Dec}(\mathrm{DP}_2, L\text{-CF}) \le_s \mathrm{Dec}(\mathrm{R}_{2,2}, \mathbf{CPC}\text{-CF}) \le_s \mathrm{Dec}(\mathrm{Itp}_2, \mathbf{CPC}\text{-EF})$. $\Box$

Remark 5.12 With more care, one can prove the following strengthening of Corollary 5.11 which internalizes circuits computing the reduction to $\mathrm{Dec}(\mathrm{R}_{2,2}, \mathbf{CPC}\text{-CF})$: if L-EF weakly simulates L-SF, then for every language $P \in$ PSPACE, there exist poly-size circuits $\{C^0_n, C^1_n :$

$n \in \omega\}$ in variables $\{p_i : i < n\} \cup \{s_{l,r} : l < m_n, r < 3\}$ that are monotone in $\vec{s}$ such that

$$w \in P \iff \forall \vec{s} \Big(\bigwedge_{l<m_n} \bigwedge_{i<j<3} (s_{l,i} \vee s_{l,j}) \to C_n^1(w, \vec{s}) \Big),$$
$$w \notin P \iff \forall \vec{s} \Big(\bigwedge_{l<m_n} \bigwedge_{i<j<3} (s_{l,i} \vee s_{l,j}) \to C_n^0(w, \vec{s}) \Big),$$

and there are poly-size **CPC**-CF proofs of

$$\bigwedge_{l<m_n} \bigvee_{r<3} s_{l,r} \to C_n^0(\vec{p}, \vec{s}) \vee C_n^1(\vec{p}, \vec{s}).$$

We will prove an even stronger result in the next section.

6 Hrubeš-style monotone interpolation

The original idea of utilizing DP to prove lower bounds on the proof complexity of nonclassical logics comes from Buss and Pudlák [2]: in this setup, feasible DP serves a role analogous to feasible interpolation for classical proof systems, and in accordance with that, it implies *conditional* proof-size lower bounds relying on (unproven) circuit lower bounds. We followed much the same strategy to derive the conditional separations between L-SF and L-EF from bounds on the complexity of $\mathrm{Dec}(\mathrm{DP}, L\text{-EF})$ in Sections 4 and 5.

Hrubeš [8] discovered another setup where DP is replaced by a somewhat different admissible rule (whose feasibility can be proved using similar methods as for DP) which plays a role analogous to *monotone* feasible interpolation for classical proof systems. This enabled him to prove *unconditional* proof-size lower bounds, exploiting known exponential lower bounds on monotone circuit size. (The separations between EF and SF systems for logics of unbounded branching in Jeřábek [14] that make the starting point for this paper also rely on Hrubeš's method.)

This suggests that we should try to adapt our arguments from the previous sections to Hrubeš's setup, with the hope that it might improve our conditional separations between L-SF and L-EF to weaken the required complexity assumptions, or even to make them fully unconditional.

We pursue this idea in the present section to see how far it can get us. We can, indeed, easily adapt our method to Hrubeš's setup, as we will see shortly in Theorem 6.1. Unfortunately, we do not know how to extract unconditional lower bounds from the result; while it does furnish an improvement to our conditional lower bounds, the statement it leads to (Theorem 6.3) is rather complicated, and it is unclear how significant the improvement really is.

Let $L = L_0 \oplus \mathbf{BB}_k$ be as in Section 5. We consider L-tautologies of the form

$$\alpha(\Box\vec{p}, \vec{q}) \to \bigvee_{u<t} \Box\beta_u(\vec{p}, \vec{r}), \tag{62}$$

where the indicated lists of variables $\vec{p}$, $\vec{q}$, and $\vec{r}$ are disjoint, α is a Boolean circuit monotone in the variables $\vec{p}$, and the β_u's are arbitrary modal circuits. (We will actually only use $t = 1$ for the modal lower bounds later on.)

Theorem 6.1 *Given an L-*CF *proof of* (62)*, we can construct in polynomial time monotone Boolean circuits $\{C_u(\vec{p},\vec{s}) : u < t\}$ using extra variables $\{s_{l,i} : l < m,\ i \le k\}$, a* **CPC**-CF *proof of*

$$\alpha(\vec{p},\vec{q}) \wedge \bigwedge_{l<m} \bigvee_{r\le k} s_{l,r} \to \bigvee_{u<t} C_u(\vec{p},\vec{s}), \tag{63}$$

*and for each $u < t$, an L-*CF *proof of*

$$\bigwedge_{\substack{l<m\\ r\le k}} \Big(s_{l,r} \wedge \boxdot\psi_{l,r} \to \bigvee_{i\ne r} \boxdot\psi_{l,i}\Big) \wedge \bigwedge_i (p_i \to \Box p_i) \wedge C_u(\vec{p},\vec{s}) \to \boxdot\beta_u(\vec{p},\vec{r}) \tag{64}$$

for some circuits $\{\psi_{l,i} : l < m,\ i \le k\}$.

Proof: We fix an L-CF proof π of (62), and we modify the argument given in Section 5 as follows. First, the monotone circuits C_φ and $C_{\varphi,h}$ will use both $\vec{s}$ and $\vec{p}$ variables; we change the definition of the base case to

$$C_{\varphi,0} = \begin{cases} \top, & \varphi \in \pi \cup \Xi_\pi, \\ p_i, & \varphi = p_i \text{ for some } i, \\ \bot, & \text{otherwise.} \end{cases}$$

(Since L is consistent, $p_i \notin \pi$.) We define the circuits C_u from the statement of our theorem as C_{β_u}. Lemma 5.1 holds unchanged, except for an obvious adaptation of (43). It is also straightforward to prove an analogue of Lemma 5.2, stating that for any $\varphi \in S$ and $h \le N$, there are poly-time constructible L-CF proofs of

$$\bigwedge_{\substack{l<m\\ r\le k}} \Big(s_{l,r} \wedge \boxdot\psi_{l,r} \to \bigvee_{i\ne r} \boxdot\psi_{l,i}\Big) \wedge \bigwedge_i (p_i \to \Box p_i) \wedge C_{\varphi,h}(\vec{p},\vec{s}) \to \boxdot\varphi.$$

As a special case, this implies (64).

Recall that the definition of V_φ was arbitrary in the case of propositional variables. We now fix it more specifically: we put $V_\varphi = \varphi$ if φ is any of the $\vec{p}$ or $\vec{q}$ variables. Since Lemma 5.3 worked for arbitrary choices of V_φ for propositional variables, the proof of (49) continues to hold unchanged. Taking $g = z$, we obtain a **CPC**-CF proof of

$$\bigwedge_{l<m} \bigvee_{r\le k} s_{l,r} \wedge V_{\alpha(\Box\vec{p},\vec{q})} \to \bigvee_{u<t} V_{\Box\beta_u(\vec{p},\vec{r})}.$$

Now, by definition, $V_{\Box\beta_u}$ implies C_{β_u}, i.e., C_u, and since V commutes with Boolean connectives and preserves $\vec{q}$, we have

$$V_{\alpha(\Box\vec{p},\vec{q})} \equiv \alpha(\dots, V_{\Box p_i}, \dots, \vec{q}).$$

Moreover, $V_{\Box p_i}$ is C_{p_i} or $C_{p_i} \wedge p_i$, and p_i implies C_{p_i} by the definition of $C_{p_i,0}$, hence there are short proofs of $p_i \to V_{\Box p_i}$. By Lemma 2.9, we can thus construct short **CPC**-CF proofs of

$$\alpha(\vec{p},\vec{q}) \to \alpha(\dots, V_{\Box p_i}, \dots, \vec{q}).$$

Putting it all together yields (63). $\Box$

We will apply Theorem 6.1 with $t = 1$. In this case, the circuit C_0 and the stuff around it act as a weird sort of interpolant between $\alpha(\vec{p}, \vec{q})$ and $\beta_0(\vec{p}, \vec{r})$ that does not depend on the $\vec{q}$ or $\vec{r}$ variables. It is thus easy to see that when trying to use it for lower bounds, the optimal choice for β_0 is the circuit $A_{\exists \vec{r}\, \alpha(\vec{p}, \vec{r})}(\vec{p}, \vec{r})$. Since we are interested in separations between CF and SF, let us observe that the resulting tautologies have short SF proofs, at least for formulas in negation normal form.

Lemma 6.2 *Given a monotone Boolean circuit $\alpha(\vec{p}, \vec{p}', \vec{q}, \vec{q}')$, we can construct in polynomial time a* **K4**-SCF *proof of*

$$\alpha(\Box\vec{p}, \Box\neg\vec{p}, \vec{q}, \neg\vec{q}) \to \Box A_{\exists \vec{r}\, \alpha(\vec{p}, \neg\vec{p}, \vec{r}, \neg\vec{r})}(\vec{p}, \vec{r}). \tag{65}$$

Proof: By induction on $n = |\vec{q}|$. If $n = 0$, (65) amounts to $\alpha(\Box\vec{p}, \Box\neg\vec{p}) \to \Box\alpha(\vec{p}, \neg\vec{p})$, which is a substitution instance of Lemma 2.10. Going from n to $n + 1$, we take the q variable that corresponds to the outermost existential quantifier, and reconsider it as part of $\vec{p}$; then the induction hypothesis gives a proof of

$$\alpha(\Box\vec{p}, \Box\neg\vec{p}, \Box q, \Box\neg q, \vec{q}, \neg\vec{q}) \to \Box A(\vec{p}, q, \vec{r}),$$

where we abbreviate $A = A_{\exists \vec{r}\, \alpha(\vec{p}, \neg\vec{p}, q, \neg q, \vec{r}, \neg\vec{r})}$. Substituting $\top$ and $\bot$ for q, we obtain proofs of

$$\begin{aligned}
\alpha(\Box\vec{p}, \Box\neg\vec{p}, \top, \bot, \vec{q}, \neg\vec{q}) &\to \Box A(\vec{p}, \top, \vec{r}) \\
&\to \Box\bigl(\boxdot r \to A(\vec{p}, r, \vec{r})\bigr), \\
\alpha(\Box\vec{p}, \Box\neg\vec{p}, \bot, \top, \vec{q}, \neg\vec{q}) &\to \Box A(\vec{p}, \bot, \vec{r}) \\
&\to \Box\bigl(\boxdot\neg r \to A(\vec{p}, r, \vec{r})\bigr)
\end{aligned}$$

using Lemma 2.8. Since α is Boolean, there is also a short proof of

$$\alpha(\Box\vec{p}, \Box\neg\vec{p}, q, \neg q, \vec{q}, \neg\vec{q}) \to \alpha(\Box\vec{p}, \Box\neg\vec{p}, \top, \bot, \vec{q}, \neg\vec{q}) \lor \alpha(\Box\vec{p}, \Box\neg\vec{p}, \bot, \top, \vec{q}, \neg\vec{q}),$$

hence we obtain

$$\begin{aligned}
\alpha(\Box\vec{p}, \Box\neg\vec{q}, q, \neg q, \vec{q}, \neg\vec{q}) &\to \Box\bigl(\boxdot r \to A(\vec{p}, r, \vec{r})\bigr) \lor \Box\bigl(\boxdot\neg r \to A(\vec{p}, r, \vec{r})\bigr) \\
&\to \Box\bigl[\Box\bigl(\boxdot r \to A(\vec{p}, r, \vec{r})\bigr) \lor \Box\bigl(\boxdot\neg r \to A(\vec{p}, r, \vec{r})\bigr)\bigr],
\end{aligned}$$

where the disjunction inside square brackets is just $A_{\exists r \exists \vec{r}\, \alpha(\vec{p}, \neg\vec{p}, r, \neg r, \vec{r}, \neg\vec{r})}$. $\Box$

We note that as in Remark 4.7, slightly modified variants of the tautologies have even short **K**-SCF proofs.

We come to the final lower bound of this section. The statement of the theorem is somewhat involved as we try to push the argument as far as possible, but the most important component is the first part stating the existence of circuits satisfying (66)–(69). In particular, the gap between (66) and (67) effectively gives a reduction to a certain promise problem (if $w \in P$, then $C^\forall(w, \vec{s})$ holds whenever at least one variable is true in each triple $\{s_{l,0}, s_{l,1}, s_{l,2}\}$, while if $w \notin P$, $C^\forall(w, \vec{s})$ fails under some assignment that makes *two* variables true in each triple), and this does not seem to follow from just PSPACE = NP.

Theorem 6.3 *Let* $\mathbf{K4} \subseteq L \subseteq \mathbf{S4GrzBB_2}$ *or* $\mathbf{K4} \subseteq L \subseteq \mathbf{GLBB_2}$*, and assume that* L-EF *weakly simulates* L-SF*.*

Then for every monotone PSPACE *language* P*, there exists a sequence of polynomial-size monotone Boolean circuits* $\{C_n^\forall, C_n^\exists : n \in \omega\}$ *such that* $C_n^\forall$ *and* $C_n^\exists$ *use variables* $\{p_i : i < n\}$ *and* $\{s_{l,r} : l < m_n, r < 3\}$*, and for every* $w \in \mathbf{2}^n$*, we have*

$$w \in P \iff \forall \vec{s}\Big(\bigwedge_{l<m_n}\bigvee_{r<3} s_{l,r} \to C_n^\forall(w,\vec{s})\Big) \tag{66}$$

$$\iff \forall \vec{s}\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3} (s_{l,i} \vee s_{l,j}) \to C_n^\forall(w,\vec{s})\Big) \tag{67}$$

$$\iff \exists \vec{s}\Big(\bigwedge_{l<m_n}\bigvee_{r<3} s_{l,r} \wedge C_n^\exists(w,\neg\vec{s})\Big) \tag{68}$$

$$\iff \exists \vec{s}\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3} (s_{l,i} \vee s_{l,j}) \wedge C_n^\exists(w,\neg\vec{s})\Big). \tag{69}$$

The circuits

$$\bigwedge_{l<m_n}\bigvee_{r<3} t_{l,r} \wedge C_n^\exists(\vec{p},\neg\vec{t}) \wedge \bigwedge_{l<m_n}\bigvee_{r<3} s_{l,r} \to C_n^\forall(\vec{p},\vec{s}) \tag{70}$$

have poly-size **CPC**-CF *proofs. Moreover, if* $\{\alpha_n(\vec{p},\vec{q}) : n \in \omega\}$ *is a sequence of polynomial-size circuits monotone in* $\vec{p}$ *such that*

$$w \in P \iff \exists \vec{q}\, \alpha_n(w,\vec{q}), \tag{71}$$

we can choose $C_n^\forall$ *in such a way that there are polynomial-size* **CPC**-CF *proofs of*

$$\alpha_n(\vec{p},\vec{q}) \wedge \bigwedge_{l<m_n}\bigvee_{r<3} s_{l,r} \to C_n^\forall(\vec{p},\vec{s}), \tag{72}$$

and if $\{\beta_n(\vec{p},\vec{q}) : n \in \omega\}$ *are polynomial-size circuits monotone in* $\vec{p}$ *such that*

$$w \in P \iff \forall \vec{q}\, \beta_n(w,\vec{q}), \tag{73}$$

we can choose $C_n^\exists$ *such that there are polynomial-size* **CPC**-CF *proofs of*

$$\bigwedge_{l<m_n}\bigvee_{r<3} s_{l,r} \wedge C_n^\exists(\vec{p},\neg\vec{s}) \to \beta_n(\vec{p},\vec{q}). \tag{74}$$

If $P \in$ PSPACE *is not necessarily monotone, the above holds with* $C_n^\forall$ *and* $C_n^\exists$ *monotone in* $\vec{s}$*, and* α_n *and* β_n *arbitrary.*

Proof: Let $P \in$ PSPACE be monotone. By Theorem 4.6, $P \in$ NP, hence there exists a sequence of poly-size formulas $\alpha_n(\vec{p},\vec{q})$ satisfying (71). Since P is monotone, we have

$$w \in P \iff \exists \vec{p}, \vec{q}\,\big(\vec{p} \le w \wedge \alpha_n(\vec{p},\vec{q})\big),$$

hence we can ensure α_n is monotone in $\vec{p}$. Let us fix such a sequence α_n, where we also assume w.l.o.g. that α_n is in negation normal form.

By Lemma 6.2 and the assumption, there are poly-size proofs L-CF proofs of

$$\alpha_n(\Box\vec{p},\vec{q}) \to \Box A_{\exists\vec{r}\,\alpha_n(\vec{p},\vec{r})}(\vec{p},\vec{r}),$$

where we may assume w.l.o.g. that $L = \mathbf{S4GrzBB_2}$ or $L = \mathbf{GLBB_2}$. By Theorem 6.1, there exist poly-size monotone circuits $C_n^{\forall}(\vec{p},\vec{s})$ such that (72) has poly-size **CPC**-CF proofs, and

$$\bigwedge_{\substack{l<m_n\\ r<3}} \Big(s_{l,r} \wedge \boxdot\psi_{l,r} \to \bigvee_{i\neq r} \boxdot\psi_{l,i}\Big) \wedge \bigwedge_{i<n}(p_i \to \Box p_i) \wedge C_n^{\forall}(\vec{p},\vec{s}) \to \boxdot A_{\exists\vec{r}\,\alpha_n(\vec{p},\vec{r})}(\vec{p},\vec{r}) \tag{75}$$

has poly-size L-CF proofs. We claim that this makes

$$\forall\vec{s}\,\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j}) \to C_n^{\forall}(\vec{p},\vec{s})\Big) \to \exists\vec{q}\,\alpha_n(\vec{p},\vec{q})$$

a quantified Boolean tautology, which together with (72) implies (66) and (67). Indeed, let $w \in \mathbf{2}^n$ be such that

$$\forall\vec{s}\,\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j}) \to C_n^{\forall}(w,\vec{s})\Big)$$

is true. Substituting the bits of w as truth constants into (75), we see that

$$\vdash_L \bigwedge_{\substack{l<m_n\\ r<3}} \Big(s_{l,r} \wedge \boxdot\psi_{l,r}(\vec{p}/w) \to \bigvee_{i\neq r} \boxdot\psi_{l,i}(\vec{p}/w)\Big) \wedge \bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j}) \to \boxdot A_{\exists\vec{r}\,\alpha_n(\vec{p},\vec{r})}(w,\vec{r}).$$

Further substituting $\boxdot\psi_{l,r}(\vec{p}/w) \to \bigvee_{i\neq r}\boxdot\psi_{l,i}(\vec{p}/w)$ for $s_{l,r}$, we obtain

$$\vdash_L A_{\exists\vec{r}\,\alpha_n(\vec{p},\vec{r})}(w,\vec{r}),$$

which implies the truth of $\exists\vec{q}\,\alpha_n(w,\vec{q})$ by Lemma 4.5.

The dual language $P^{\mathrm{d}} = \big\{w \in \mathbf{2}^* : (\neg w) \notin P\big\}$ is also monotone, hence by the already proved part, there exist monotone circuits $C_n^{\forall,\mathrm{d}}$ such that

$$\begin{aligned} w \in P^{\mathrm{d}} &\iff \forall\vec{s}\,\Big(\bigwedge_{l<m_n}\bigvee_{r<3} s_{l,r} \to C_n^{\forall,\mathrm{d}}(w,\vec{s})\Big)\\ &\iff \forall\vec{s}\,\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j}) \to C_n^{\forall,\mathrm{d}}(w,\vec{s})\Big). \end{aligned}$$

(The m_n here is a priori different from the one for P, but we can enlarge one of them to make them equal.) Then

$$C_n^{\exists}(\vec{p},\vec{s}) = \neg C_n^{\forall,\mathrm{d}}(\neg\vec{p},\neg\vec{s})$$

is (equivalent to) a monotone circuit, and it satisfies (68) and (69). Moreover, given (73), we can arrange $C_n^{\exists}$ to satisfy (74); as a special case, we obtain (70) by taking (66) for (73).

In order to prove the last sentence of the theorem, if $P \in \mathrm{PSPACE}$ is not necessarily monotone, it can be still defined as in (71) with α_n poly-size Boolean formulas. Writing α_n in negation normal form, we have

$$w \in P \iff \exists\vec{q}\,\alpha_n'(w,\neg w,\vec{q})$$

for $\alpha'_n(\vec{p}, \vec{p}', \vec{q})$ monotone in $\vec{p}$ and $\vec{p}'$. Thus,

$$\langle w, w' \rangle \in P' \iff \exists \vec{q}\, \alpha'_n(w, w', \vec{q})$$

defines a monotone language, hence we can apply the results above to P', and substitute $\neg\vec{p}$ back for $\vec{p}'$. $\square$

Remark 6.4 Since (70) implies

$$\bigwedge_{l<m_n} \bigvee_{r<3} s_{l,r} \to \neg C_n^{\exists}(\vec{p}, \neg\vec{s}) \vee C_n^{\forall}(\vec{p}, \vec{s}),$$

Theorem 6.3 further strengthens Corollary 5.11 and Remark 5.12.

7 Negation-free lower bounds

Our results apply to a fairly limited class of logics. This is unavoidable in Theorem 4.1 as the Ext_t^* rules are not admissible in most other extensions of $\mathbf{K4BB}_k$ in the first place, but our separations between EF and SF may in principle be applicable to a broader class of logics. In this section, we will show how to generalize them to logics such as $\mathbf{S4.2BB_2}$ (which does not even have the disjunction property), using a reformulation of the tautologies we used for the separations as positive formulas, and a proof-theoretic analogue of preservation of positive formulas by dense subreductions. A similar approach was used in [14] to generalize separations from logics of depth 2 to logics of unbounded branching.

Definition 7.1 For any $h \geq 0$, let BT_h denote the perfect binary tree of height h (where the tree consisting of a single node has height 0), and let $\mathrm{BT}_{h,\bullet}$ ($\mathrm{BT}_{h,\circ}$) denote the irreflexive (reflexive, resp.) Kripke frame with skeleton BT_h. We will number the levels of BT_h bottom-up such that the root is at level 0, and leaves at level h.

Lemma 7.2 *Let $L \supseteq \mathbf{K4}$ be a logic such that for every $h \geq 0$, there exists a dense subreduction from an L-frame to a Kripke frame with skeleton BT_h.*

Then there exists $* \in \{\bullet, \circ\}$ such that for every $h \geq 0$, there exists a dense subreduction from an L-frame to $\mathrm{BT}_{h,*}$.

Proof: Since $\mathrm{BT}_{h',*}$ is a generated subframe of $\mathrm{BT}_{h,*}$ for $h' < h$, it is enough if the conclusion holds for infinitely many h; thus, by the infinitary pigeonhole principle, it suffices to show that for arbitrarily large h, there exists a dense subreduction from an L-frame to $\mathrm{BT}_{h,\bullet}$ or to $\mathrm{BT}_{h,\circ}$. This in turn follows from transitivity of dense subreductions and the fact that any Kripke frame F with skeleton $\mathrm{BT}_{(h+1)(g+1)}$ densely subreduces onto $\mathrm{BT}_{h,\bullet}$ or $\mathrm{BT}_{g,\circ}$.

To see this, notice that either F includes $\mathrm{BT}_{h,\bullet}$ as a dense subframe, or for every $x \in F$ of depth $> h$, there exists a reflexive $y \geq x$ at most h levels above x. In the latter case, we can construct a meet-preserving embedding $f \colon \mathrm{BT}_{g,\circ} \to F$ by a bottom-up approach: we map the root of $\mathrm{BT}_{g,\circ}$ to a reflexive point of F at level $\leq h$, and if $f(u) = x$ is already defined, u_0 and u_1 are the immediate successors of u, and x_0 and x_1 the immediate successors of x, we fix reflexive points $y_0 \geq x_0$ and $y_1 \geq x_1$ at most $h+1$ levels above x, and we put $f(u_i) = y_i$, $i = 0, 1$. We extend f^{-1} to a dense subreduction from F to $\mathrm{BT}_{g,\circ}$ as follows: if $x \in f[\mathrm{BT}_{g,\circ}]{\downarrow}$, we map x to $\min\{u \in \mathrm{BT}_{h,\circ} : x \leq f(u)\}$, which exists as f is meet-preserving. $\square$

Lemma 7.3 *Let $* \in \{\bullet, \circ\}$, and $L \supseteq \mathbf{K4}$ be a logic such that for every $h \geq 0$, there exists a dense subreduction from an L-frame to $\mathrm{BT}_{h,*}$.*

Then for every finite set Φ of variable-free formulas, there exists $e\colon \Phi \to \mathbf{2}$ such that for every $h \geq 0$, there exists an L-frame F and a dense subreduction f from F to $\mathrm{BT}_{h,*}$ such that

$$F, u \vDash \bigwedge_{\varphi \in \Phi} (\Box\varphi)^{e(\varphi)} \tag{76}$$

for all $u \in \mathrm{dom}(f)$, where we write $\varphi^1 = \varphi$, $\varphi^0 = \neg\varphi$.

Proof: By induction on $|\Phi|$. The base case $\Phi = \varnothing$ is trivial. Assuming the statement holds for Φ, we will show it holds for $\Phi \cup \{\psi\}$; as in Lemma 7.2, it suffices to prove it with reversed order of quantifiers (for arbitrarily large h, there exists e, etc.).

Let $h \geq 0$. By the induction hypothesis, there exist $e\colon \Phi \to \mathbf{2}$, an L-frame F, and a dense subreduction from F to $T_{2h,*}$ satisfying (76). Observe that $\{u \in F : u \vDash \Box\psi\}$ is an upper subset of F. Thus, if there exists $v \in \mathrm{dom}(f)$ such that $v \vDash \Box\psi$ and $f(v)$ is one of the points at level h of $\mathrm{BT}_{2h,*}$, the restriction $g = f \restriction v{\Uparrow}$ is a dense subreduction from the L-frame $\{v\}{\Uparrow}$ to $\{f(v)\}{\Uparrow} \simeq \mathrm{BT}_{h,*}$ such that, in addition to (76), we have $u \vDash \Box\psi$ for all $u \in \mathrm{dom}(g)$. Otherwise, let T be the copy of $\mathrm{BT}_{h,*}$ consisting of the points of $\mathrm{BT}_{2h,*}$ at levels $\leq h$; then $g = f \restriction f^{-1}[T]$ is a dense subreduction from F to $\mathrm{BT}_{h,*}$ that satisfies (76) as well as $u \vDash \neg\Box\psi$ for all $u \in \mathrm{dom}(g)$. $\square$

Theorem 7.4 *Let $* \in \{\bullet, \circ\}$, and $L \supseteq \mathbf{K4}$ be a logic such that for every $h \geq 0$, there exists a dense subreduction from an L-frame to $\mathrm{BT}_{h,*}$. Put $\overline{L} = \mathbf{GLBB_2}$ if $* = \bullet$, and $\overline{L} = \mathbf{S4GrzBB_2}$ if $* = \circ$. Then $\overline{L}$-CF weakly simulates L-CF proofs of positive formulas or circuits.*

Proof: If S is a set of circuits and $e\colon S \to \mathbf{2}$, we define a translation φ^e for circuits φ such that $\{\psi : \Box\psi \in \mathrm{Sub}(\varphi)\} \subseteq S$ as follows: $p_i^e = p_i$ for all variables p_i, the translation commutes with Boolean connectives, and

$$(\Box\varphi)^e = \begin{cases} \Box\varphi^e, & e(\varphi) = 1, \\ \bot, & e(\varphi) = 0. \end{cases}$$

In other words, we replace top-most occurrences of subcircuits $\Box\psi$ such that $e(\psi) = 0$ with $\bot$. Notice that $|\varphi^e| \leq |\varphi|$.

Assume we are given an L-CF proof $\pi = \langle \theta_0, \dots, \theta_z \rangle$, where θ_z is positive. Let ν be the substitution such that $\nu(p_i) = \top$ for all variables p_i, and put $\Phi = \{\nu(\varphi) : \Box\varphi \in \mathrm{Sub}(\pi)\}$. Let $e\colon \Phi \to \mathbf{2}$ satisfy the conclusion of Lemma 7.3. Notice that $\varphi^{e\circ\nu}$ is defined for all $\varphi \in \mathrm{Sub}(\pi)$, where $e \circ \nu$ denotes the composite assignment $(e \circ \nu)(\varphi) = e(\nu(\varphi))$.

Since θ_z is positive, $\vdash_L \nu(\varphi)$ for all $\varphi \in \mathrm{Sub}(\theta_z)$, thus we must have $e(\nu(\varphi)) = 1$ whenever $\Box\varphi \in \mathrm{Sub}(\theta_z)$. It follows that $\theta_z^{e\circ\nu} = \theta_z$, hence it suffices to show that the sequence

$$\theta_0^{e\circ\nu}, \dots, \theta_z^{e\circ\nu}$$

can be extended to a polynomially larger $\overline{L}$-CF proof.

By Corollary 2.3, we may assume the L-CF system is axiomatized by axioms and rules of **CPC** (which are trivially preserved by the $(-)^{e\circ\nu}$ translation), (Nec), and a single axiom schema consisting of substitution instances of a formula α. For (Nec), notice that $\vdash_L \nu(\theta_i)$, hence $e(\nu(\theta_i)) = 1$, i.e., $\theta_i^{e\circ\nu} \,/\, (\Box\theta_i)^{e\circ\nu}$ is again an instance of (Nec).

Concerning instances of α, let $X = \{\beta : \Box\beta \in \mathrm{Sub}(\alpha)\}$, and if σ is a substitution such that $\sigma(\alpha) \in \pi$, define $e_\sigma \colon X \to \mathbf{2}$ by $e_\sigma = e \circ \nu \circ \sigma$. Let $\sigma^{e\circ\nu}$ be the substitution such that $\sigma^{e\circ\nu}(p_i) = \big(\sigma(p_i)\big)^{e\circ\nu}$. Unwinding the definition of the translation, we find

$$\big(\sigma(\alpha)\big)^{e\circ\nu} = \sigma^{e\circ\nu}(\alpha^{e_\sigma}).$$

Since there is only a constant number of choices for e_σ, the translations of all instances of α in the proof are instances of a constant number of axiom schemata, and as such have linear-size $\overline{L}$-CF proofs by Observation 2.2, as long as these schemata are valid in $\overline{L}$. Thus, it remains to show that

$$\vdash_{\overline{L}} \alpha^{e_\sigma}$$

for all σ such that $\sigma(\alpha) \in \pi$.

Let $M = \langle V, <, v_M\rangle$ be a finite Kripke $\overline{L}$-model, which we may assume to be a (binary) tree; we will show $M \vDash \alpha^{e_\sigma}$. We embed the underlying frame $\langle V, <\rangle$ as a dense subframe in $\mathrm{BT}_{h,*}$ for some h, in such a way that the root of $\langle V, <\rangle$ is the root of $\mathrm{BT}_{h,*}$, and all leaves of $\mathrm{BT}_{h,*}$ are outside V, i.e., every point of V sees an element of $\mathrm{BT}_{h,*} \smallsetminus V$. Using Lemma 7.3, let us fix an L-frame $F = \langle W, <, A\rangle$ and a dense subreduction f from F to $\mathrm{BT}_{h,*}$ that satisfies (76). We may assume that F is rooted and its root r is mapped to the root of $\langle V, <\rangle$ by f, hence $f^{-1}[V]$ is a lower subset of W. We endow F with an admissible valuation as follows:

$$F, u \vDash p_i \iff \begin{cases} M, f(u) \vDash p_i, & \text{if } u \in f^{-1}[V],\\ \quad F, u \vDash \nu(\sigma(p_i)), & \text{otherwise.}\end{cases}$$

Since $W \smallsetminus f^{-1}[V]$ is an upper subset of W, we obtain

$$F, u \vDash \varphi \iff F, u \vDash \nu(\sigma(\varphi)) \tag{77}$$

for all φ and $u \notin f^{-1}[V]$. We claim that

$$F, u \vDash \beta \iff M, f(u) \vDash \beta^{e_\sigma} \tag{78}$$

for all $u \in f^{-1}[V]$ and $\beta \in \mathrm{Sub}(\alpha)$. Since $F \vDash \alpha$, this implies $M \vDash \alpha^{e_\sigma}$, finishing the proof.

We prove (78) by induction on the complexity of β. It holds for variables by definition, and the induction steps for Boolean connectives follow immediately as they commute with $(-)^{e_\sigma}$.

Assume that (78) holds for $\beta \in X$, we will prove it for $\Box\beta$.

If $e_\sigma(\beta) = 1$, we have $F, r \vDash \Box\nu(\sigma(\beta))$ by (76), thus $F, v \vDash \beta$ for all $v \notin f^{-1}[V]$ by (77). It follows that for any $u \in f^{-1}[V]$, we have

$$\begin{aligned} F, u \vDash \Box\beta &\iff \forall v > u\, \big(v \in f^{-1}[V] \implies F, v \vDash \beta\big)\\ &\iff \forall v > u\, \big(v \in f^{-1}[V] \implies M, f(v) \vDash \beta^{e_\sigma}\big)\\ &\iff \forall y > f(u)\; M, y \vDash \beta^{e_\sigma}\\ &\iff M, f(u) \vDash (\Box\beta)^{e_\sigma}, \end{aligned}$$

using the induction hypothesis and f's being a subreduction.

If $e_\sigma(\beta) = 0$, $(\Box\beta)^{e_\sigma} = \bot$ is false in $f(u)$. On the other hand, there exists $v > u$ such that $v \in f^{-1}[\mathrm{BT}_{h,*} \smallsetminus V]$, and $F, v \nvDash \Box\nu(\sigma(\beta))$ by (76), hence there exists $w > v$ such that $F, w \nvDash \beta$ by (77). Thus, $F, u \nvDash \Box\beta$. $\Box$

In order to apply Theorem 7.4, we need a convenient supply of positive tautologies. In fact, there is a simple general method of converting any tautology to a positive one:

Definition 7.5 Given a formula or circuit $\varphi(\vec{p})$, we define a positive formula or circuit $\varphi^+(\vec{p}, r)$ using a new variable r as follows. We first rewrite all negations $\neg\psi$ inside φ as $\psi \to \bot$, so that w.l.o.g. φ uses only the connectives $\{\wedge, \vee, \to, \top, \bot, \Box\}$. Let $\varphi'(\vec{p}, r)$ be the circuit obtained from φ by replacing $\bot$ with r, thus φ' is positive and $\varphi(\vec{p}) = \varphi'(\vec{p}, \bot)$. Then we put

$$\varphi^+(\vec{p}, r) = \bigwedge_i \boxdot(r \to p_i) \to \varphi'(\vec{p}, r).$$

Lemma 7.6 *Let L be an extension of* **K4** *by positive axiom schemata, and φ a circuit.*

(i) *There is a poly-time constructible L-*CF *proof of $\sigma(\varphi^+) \to \varphi$, where σ is the substitution $\sigma(r) = \bot$.*

(ii) *Given an L-*CF *or L-*SCF *proof of φ, we can construct in polynomial time an L-*CF *or L-*SCF *proof (respectively) of φ^+.*

Proof: (i) is obvious. Observe that L can be axiomatized by (MP), (Nec), positive axiom schemata, and the schema $\bot \to \psi$. With this in mind, (ii) can be shown by virtually the same proof as [16, Thm. 3.8]; we leave the details to the reader. $\Box$

Theorem 7.7 *Let $L \supseteq$* **K4** *be a logic such that for every $h \geq 0$, there exists a dense subreduction from an L-frame to a Kripke frame with skeleton BT_h.*

*Then L-*SF *has superpolynomial speed-up over L-*EF*, unless* PSPACE = NP = coNP*, and unless the conclusion of Theorem 6.3 holds.*

Proof: Let $* \in \{\bullet, \circ\}$ be as in Lemma 7.2, and put $\overline{L} = \mathbf{GLBB_2}$ if $* = \bullet$, and $\overline{L} = \mathbf{S4GrzBB_2}$ if $* = \circ$. By the proofs of Theorems 4.6 and 6.3, there exists a sequence of tautologies $\{\varphi_n : n < \omega\}$ that have polynomial-size **K4**-SCF proofs, while the conclusion of the theorem holds if they have polynomial-size $\overline{L}$-CF proofs. Now, by Lemma 7.6 (ii), the tautologies φ_n^+ also have polynomial-size **K4**-SCF proofs, and if we assume they have polynomial-size L-CF proofs, then they have polynomial-size $\overline{L}$-CF proofs by Theorem 7.4, thus φ_n have polynomial-size $\overline{L}$-CF proofs by Lemma 7.6 (i). $\Box$

Example 7.8 Theorem 7.7 applies to all transitive logics included in $\mathbf{S4.2GrzBB_2}$ or in $\mathbf{GL.2BB_2}$: indeed, $\mathrm{BT}_{h,\bullet}$ with an extra irreflexive point on top is a $\mathbf{GL.2BB_2}$-frame for any h, and similarly in the reflexive case.

Remark 7.9 Logics L satisfying the assumption of Theorem 7.7 are PSPACE-hard by Theorem 2.12, hence PSPACE $\neq$ NP implies superpolynomial lower bounds on all Cook–Reckhow proof systems for L, in particular on L-SF.

8 Superintuitionistic logics

Intuitionistic logic (**IPC**) and its extensions (superintuitionistic logics) behave in many respects analogously to transitive modal logics; in particular, many interesting properties are preserved by the Blok–Esakia isomorphism between extensions of **IPC** and extensions of **S4Grz**. We will now indicate how to transfer our results to the case of superintuitionistic logics. Our basic tool will be an efficient transformation of proofs from superintuitionistic logics to modal logics by means of the Gödel–Tarski–McKinsey translation, which reduces the decision problems associated with DP and similar rules to the modal case; in this way, we will obtain analogues of the extension rule complexity estimates from Theorem 4.1 and the first equivalence in Theorem 5.8, and of the conditional separations from Theorem 4.6, Corollary 5.11, and (a monotone form of) Remark 5.12.

There is not much point in formally introducing an intuitionistic analogue of the class of $*$-extensible logics, as the only such logic is **IPC** itself (being complete w.r.t. finite trees). The intuitionistic equivalent of the bounded branching logics are the *Gabbay–de Jongh logics*[6] $\mathbf{T}_k$, axiomatized by

$$\begin{aligned}\mathbf{T}_k &= \mathbf{IPC} + \bigwedge_{i\le k}\Bigl[\Bigl(\varphi_i \to \bigvee_{j\ne i}\varphi_j\Bigr) \to \bigvee_{j\ne i}\varphi_i\Bigr] \to \bigvee_{i\le k}\varphi_j \\ &= \mathbf{IPC} + \Bigl[\bigvee_{i\le k}\Bigl(\varphi_i \to \bigvee_{j\ne i}\varphi_j\Bigr) \to \bigvee_{i\le k}\varphi_i\Bigr] \to \bigvee_{i\le k}\varphi_j.\end{aligned}$$

As in Lemma 2.1, the logic $\mathbf{T}_k$ is complete w.r.t. finite trees (or more general finite intuitionistic Kripke frames) of branching $\le k$, and a frame F validates $\mathbf{T}_k$ iff there is no dense subreduction from F to Ψ_{k+1}.

The disjunction property for superintuitionistic logics is defined by L-admissibility of the multi-conclusion rules

$$(\mathrm{DP}_n) \qquad \varphi_0 \vee \cdots \vee \varphi_{n-1} \ / \ \varphi_0, \dots, \varphi_{n-1}.$$

The intuitionistic analogue of the extension rules are *Visser's rules*

$$(\mathrm{V}_n) \qquad \bigwedge_{i<n}(\varphi_i \to \psi_i) \to \bigvee_{i<n}\varphi_i \Bigm/ \bigwedge_{i<n}(\varphi_i \to \psi_i) \to \varphi_0, \dots, \bigwedge_{i<n}(\varphi_i \to \psi_i) \to \varphi_{n-1}.$$

We mention that similarly to Theorem 2.15, Visser's rules are constructively feasible for **IPC**-CF [20, 12] by an argument using an efficient version of Kleene's slash in place of Boolean assignments.

We assume **IPC** is formulated in a language using connectives $\{\wedge, \vee, \to, \bot\}$, with $\neg\varphi$ being defined as $\varphi \to \bot$, and $\top$ as $\neg\bot$. The *Gödel–McKinsey–Tarski translation* of intuitionistic formulas (or circuits) to modal formulas (circuits, resp.) is defined such that $\mathsf{T}(p_i) = \Box p_i$ for propositional variables p_i, T commutes with the monotone connectives $\wedge$, $\vee$, and $\bot$, and

$$\mathsf{T}(\varphi \to \psi) = \Box\bigl(\mathsf{T}(\varphi) \to \mathsf{T}(\psi)\bigr).$$

[6] Introduced as $\mathbf{D}_{k-1}$ in Gabbay and de Jongh [7]. We find the off-by-one error in the subscript too distressing, hence we follow the notation of [4] instead.

A modal logic $L' \supseteq \mathbf{S4}$ is a *modal companion* of a superintuitionistic logic L if

$$\vdash_L \varphi \iff \vdash_{L'} \mathsf{T}(\varphi) \tag{79}$$

for all formulas φ. If $L = \mathbf{IPC} + \{\varphi_i : i \in I\}$, then $\tau L = \mathbf{S4} \oplus \{\mathsf{T}(\varphi_i) : i \in I\}$ is the smallest modal companion of L, while $\sigma L = \tau L \oplus \mathbf{Grz}$ is the largest modal companion of L. (See [4, §9.6] for details.) We have $\tau \mathbf{T}_k = \mathbf{S4BB}_k$ and $\sigma \mathbf{T}_k = \mathbf{S4GrzBB}_k$.

Lemma 8.1 *Given a formula or circuit φ, we can construct in polynomial time an* $\mathbf{S4}$-CF *proof of* $\mathsf{T}(\varphi) \leftrightarrow \Box \mathsf{T}(\varphi)$.

Proof: By induction on the complexity of φ. $\Box$

Lemma 8.2 *Let L' be a modal companion of a superintuitionistic logic L. Given an* L-CF *proof (or* L-SCF *proof) of φ, we can construct in polynomial time an* L'-CF *proof (*L'-SCF *proof, resp.) of* $\mathsf{T}(\varphi)$.

Proof: Using Lemma 8.1, the T translation commutes with substitution up to shortly provable equivalence. This means we can just apply T to the whole proof line by line, and fix it up to make a valid proof; we leave the details to the reader. $\Box$

Lemma 8.3 *Let $k \geq 2$. Given n, there are* poly(n)*-time constructible* $\mathbf{T}_k$-F *proofs of*

$$\Big[\bigwedge_{l<n}\bigvee_{i\leq k}\Big(q_{l,i} \to \bigvee_{j\neq i} q_{l,j}\Big) \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}\Big] \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}.$$

Proof: Put $\beta_{l,i} = q_{l,i} \to \bigvee_{j\neq i} q_{l,j}$. We prove

$$\Big(\bigwedge_{l<m}\bigvee_{i\leq k}\beta_{l,i} \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}\Big) \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i} \tag{80}$$

by induction on $m \leq n$. The base case $m = 0$ is trivial. Assuming we have a proof of (80) for m, we derive it for $m + 1$ by

$$\begin{aligned}
\Big(\bigwedge_{l\leq m}\bigvee_{i\leq k}\beta_{l,i} \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}\Big) &\to \Big[\bigvee_{i\leq k}\beta_{m,i} \to \Big(\bigwedge_{l<m}\bigvee_{i\leq k}\beta_{l,i} \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}\Big)\Big]\\
&\to \Big(\bigvee_{i\leq k}\beta_{m,i} \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}\Big)\\
&\to \Big(\bigvee_{i\leq k}\beta_{m,i} \to \bigvee_{i\leq k} q_{m,i}\Big)\\
&\to \bigvee_{i\leq k} q_{m,i}\\
&\to \bigvee_{i\leq k} \beta_{m,i}\\
&\to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}
\end{aligned}$$

using an instance of $\mathbf{T}_k$. $\Box$

Lemma 8.4 *For any $k \geq t \geq 2$,* $\mathrm{Dec}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF}) \leq_s \mathrm{Dec}(\mathrm{V}_t, \mathbf{T}_k\text{-CF})$*.*

Proof: Assume we are given a $\mathbf{CPC}$-CF proof of

$$\bigwedge_{l<n} \bigvee_{i\leq k} p_{l,i} \to \bigvee_{u<t} \varphi_u(\vec{p}),$$

where φ_u are monotone circuits. We can make it an $\mathbf{IPC}$-CF proof by [14, Thm. 3.9], hence we can construct an $\mathbf{IPC}$-CF proof of the substitution instance

$$\bigwedge_{l<n} \bigvee_{i\leq k} \beta_{l,i} \to \bigvee_{u<t} \varphi_u(\dots, \beta_{l,i}, \dots), \tag{81}$$

where $\beta_{l,i} = q_{l,i} \to \bigvee_{j\neq i} q_{l,j}$. Using (81) and Lemma 8.3, we can construct a $\mathbf{T}_k$-CF proof of

$$\begin{aligned}\bigwedge_{u<t}\Bigl(\varphi_u(\dots,\beta_{l,i},\dots) \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}\Bigr) \to \Bigl(\bigwedge_{l<n}\bigvee_{i\leq k}\beta_{l,i} \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}\Bigr) \\ \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i} \\ \to \bigwedge_{l<n}\bigvee_{i\leq k} \beta_{l,i} \\ \to \bigvee_{u<t} \varphi_u(\dots,\beta_{l,i},\dots),\end{aligned}$$

which gives a reduction to $\mathrm{Dec}(\mathrm{V}_t, \mathbf{T}_k\text{-CF})$. In order to see that it is sound, if $u < t$ is such that

$$\vdash_{\mathbf{T}_k} \bigwedge_{v<t}\Bigl(\varphi_v(\dots,\beta_{l,i},\dots) \to \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i}\Bigr) \to \varphi_u(\dots,\beta_{l,i},\dots),$$

then

$$\vdash_{\mathbf{T}_k} \bigwedge_{l<n}\bigvee_{i\leq k} q_{l,i} \to \varphi_u\Bigl(\dots,\bigvee_{j\neq i} q_{l,j},\dots\Bigr).$$

By substituting $\bigwedge_{j\neq i} p_{l,j}$ for $q_{l,i}$, we obtain

$$\vdash_{\mathbf{T}_k} \bigwedge_{l<n}\bigwedge_{i<j\leq k} (p_{l,i} \vee p_{l,j}) \to \varphi_u(\vec{p})$$

as in the proof of Lemma 5.7. □

We note that the same argument also shows $\mathrm{Cons}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF}) \leq \mathrm{Cons}(\mathrm{V}_t, \mathbf{T}_k\text{-CF})$. However, we will not obtain any upper bound on the complexity of $\mathrm{Cons}(\mathrm{V}_t, \mathbf{T}_k\text{-CF})$.

Theorem 8.5 *If $k \geq t \geq 2$, then* $\mathrm{Dec}(\mathrm{V}_t, \mathbf{T}_k\text{-CF})$*, and therefore* $\mathrm{Dec}(\mathrm{DP}_t, \mathbf{T}_k\text{-CF})$*, is subsumed by a total* coNP *search problem. Specifically,* $\mathrm{Dec}(\mathrm{V}_t, \mathbf{T}_k\text{-CF}) \equiv_s \mathrm{Dec}(\mathrm{R}_{k,t}, \mathbf{CPC}\text{-CF})$*.*

Proof: In view of Theorems 4.1 and 5.8 and Lemma 8.4, it suffices to construct a reduction of $\mathrm{Dec}(\mathrm{V}_t, \mathbf{T}_k\text{-CF})$ to $\mathrm{Dec}(\mathrm{Ext}^\circ_t, \mathbf{S4BB}_k\text{-CF})$. Given a $\mathbf{T}_k$-CF proof of

$$\bigwedge_{u<t} (\varphi_u \to \psi_u) \to \bigvee_{u<t} \varphi_u,$$

we can construct an $\mathbf{S4BB}_k$-CF proof of

$$\bigwedge_{u<t} \Box\big(\Box\mathsf{T}(\varphi_u) \to \Box\mathsf{T}(\psi_u)\big) \to \bigvee_{u<t} \Box\mathsf{T}(\varphi_u)$$

by Lemmas 8.2 and 8.1. Using

$$\Big[\big(\Box\mathsf{T}(\varphi_u) \to \Box\mathsf{T}(\psi_u)\big) \to \Box\big(\Box\mathsf{T}(\varphi_u) \to \Box\mathsf{T}(\psi_u)\big)\Big] \to \Box\big(\Box\mathsf{T}(\varphi_u) \to \Box\mathsf{T}(\psi_u)\big) \vee \Box\mathsf{T}(\varphi_u),$$

we obtain an $\mathbf{S4BB}_k$-CF proof of

$$\bigwedge_{u<t} B^\circ\big(\Box\mathsf{T}(\varphi_u) \to \Box\mathsf{T}(\psi_u)\big) \to \bigvee_{u<t} \Box\mathsf{T}(\varphi_u).$$

This is a sound reduction, as

$$\vdash_{\mathbf{S4BB}_k} \bigwedge_{u<t} \Box\big(\Box\mathsf{T}(\varphi_u) \to \Box\mathsf{T}(\psi_u)\big) \to \mathsf{T}(\varphi_v) \implies \vdash_{\mathbf{T}_k} \bigwedge_{u<t} (\varphi_u \to \psi_u) \to \varphi_v$$

by (79) and Lemma 8.1. $\Box$

Remark 8.6 The logics $\mathbf{T}_k$ in fact admit Visser's rules in a more general form

$$(\mathrm{V}_{t,m}) \qquad \bigwedge_{i<t}(\varphi_i \to \psi_i) \to \bigvee_{i<t+m} \varphi_i \Big/ \bigwedge_{i<t}(\varphi_i \to \psi_i) \to \varphi_0, \dots, \bigwedge_{i<t}(\varphi_i \to \psi_i) \to \varphi_{t+m-1}$$

for $t \le k$ and all $m \ge 0$; it is possible to derive $\mathrm{V}_{t,m}$ by iteration of $\mathrm{V}_{t,0} = \mathrm{V}_t$. However, as in Remark 5.9, we do not get any nontrivial bounds on the complexity of $\mathrm{Dec}(\mathrm{V}_{t,m}, \mathbf{T}_k\text{-CF})$ for $t + m > k$.

Remark 8.7 We do not know if a full analogue of Theorem 5.8 holds for $\mathbf{T}_k$. Instead of using translation to modal logic as in our proof of Theorem 8.5, it is straightforward to give a self-contained argument with efficient Kleene's slash taking the role of Boolean assignments as in [12, 4.11–4.13]. This in turn can be internalized along the lines of Section 5, and we can prove analogues of Lemmas 5.2 and 5.3 with no particular difficulty. Unfortunately, this does not seem to lead anywhere, as $\mathbf{T}_k$ does not prove the crucial tautology (61), i.e.,

$$\bigwedge_{\substack{l<m\\ i_0<i_1\le k}} \Big[\Big(\psi_{l,i_0} \to \bigvee_{j\ne i_0} \psi_{l,j}\Big) \vee \Big(\psi_{l,i_1} \to \bigvee_{j\ne i_1} \psi_{l,j}\Big)\Big],$$

just like $\mathbf{S4BB}_k$ does not prove the boxed version of (61):

$$\bigwedge_{\substack{l<m\\ i_0<i_1\le k}} \Big[\Box\Big(\Box\psi_{l,i_0} \to \bigvee_{j\ne i_0} \Box\psi_{l,j}\Big) \vee \Box\Big(\Box\psi_{l,i_1} \to \bigvee_{j\ne i_1} \Box\psi_{l,j}\Big)\Big].$$

Our inability to circumvent this problem is directly related to our failure to solve Remark 5.10.

We now turn to lower bounds. We define the intuitionistic versions A^I_Φ of the A_Φ circuits by dropping all boxes from Definition 4.2. It is straightforward to adapt the proofs of Lemmas 4.3, 4.4, and 4.5 (again, by essentially dropping all boxes) to show the following:

Lemma 8.8 *Given a QBF $\Phi(p_0,\dots,p_{n-1})$, there are poly-time constructible* **IPC**-SCF *proofs of*

$$\bigwedge_{i<n}(p_i\vee\neg p_i)\to A^I_\Phi\vee A^I_{\overline{\Phi}}. \qquad \Box$$

Lemma 8.9 *Let Φ be a QBF in free variables $\vec p$, let $\vec a$ be a Boolean assignment to $\vec p$, and $\vec p/\vec a$ denote the corresponding substitution. If L is a superintuitionistic logic with DP, and*

$$\vdash_L A^I_\Phi(\vec p/\vec a),$$

then $\Phi(\vec a)$ is true. $\Box$

As with the notion of extensible logics, in the superintuitionistic case there is not much point in considering a complicated condition on logics as in Theorem 7.7: one can check that a superintuitionistic logic L has the property that for each h there exists a subreduction from an L-frame to B_h if and only if $L\subseteq \mathbf{T}_2+\mathbf{KC}$, where $\mathbf{KC}$ is the logic of weak excluded middle

$$\mathbf{KC}=\mathbf{IPC}+\neg\varphi\vee\neg\neg\varphi,$$

hence we may as well just directly state the results for sublogics of $\mathbf{T}_2+\mathbf{KC}$.

The superintuitionistic analogues of Lemma 7.6 and Theorem 7.4 were already proved in Jeřábek [16]. Given a formula or circuit $\varphi(\vec p)$, let $\varphi'(\vec p,r)$ be the positive circuit obtained by replacing all occurrences of $\bot$ with r, so that $\varphi(\vec p)=\varphi'(\vec p,\bot)$. Then we put $\varphi^+(\vec p,r)=\bigwedge_i(r\to p_i)\to\varphi'(\vec p,r)$. The following is Theorem 3.8 in [16].

Lemma 8.10 *Let L be an extension of* **IPC** *by positive axioms, and φ a circuit.*

(i) *There is a poly-time constructible* **IPC**-CF *proof of $\sigma(\varphi^+)\to\varphi$, where σ is the substitution $\sigma(r)=\bot$.*

(ii) *Given an L-*CF *or L-*SCF *proof of φ, we can construct in polynomial time an L-*CF *or L-*SCF *proof (respectively) of φ^+.* $\Box$

The next lemma is a special case of Theorem 4.5 in [16].

Lemma 8.11 *Given a $(\mathbf{T}_2+\mathbf{KC})$-*CF *proof of a positive formula or circuit φ, we can construct in polynomial time a $\mathbf{T}_2$-*CF *proof of φ.* $\Box$

Theorem 8.12 *If $\mathbf{IPC}\subseteq L\subseteq\mathbf{T}_2+\mathbf{KC}$, then L-*SF *has superpolynomial speed-up over L-*EF *unless* PSPACE = NP = coNP*, and unless the disjoint* NP *pair version of* $\mathrm{Dec}(\mathrm{R}_{2,2},\mathbf{CPC}\text{-CF})$ *is a complete disjoint* PSPACE *pair under nonuniform poly-time reductions.*

Proof: As before, it suffices to show a conditional separation between L-CF and L-SCF proofs of circuits using intuitionistic variants of Lemmas 2.5 and 2.6.

For any QBF Φ, the circuits $(A^I_\Phi)^+$ have polynomial-time constructible **IPC**-SCF proofs by Lemmas 8.8 and 8.10. Thus, if L-CF weakly simulates L-SCF, then the circuits A^I_Φ have polynomial-size $\mathbf{T}_2$-CF proofs π_Φ by Lemmas 8.11 and 8.10. In view of Theorem 8.5 amd Lemma 8.9, this implies that PSPACE = NP by guessing π_Φ nondeterministically as in the proof of Theorem 4.6, and that all disjoint PSPACE pairs nonuniformly reduce to $\mathrm{Dec}(\mathrm{R}_{2,2},\mathbf{CPC}\text{-CF})$ by using the π_Φ as advice as in the proof of Corollary 5.11. $\Box$

We will also show a monotone lower bound. We are not able to extend the full statement of Theorem 6.3 to $\mathbf{T}_2 + \mathbf{KC}$, but we will prove a monotone version of Remark 5.12.

Definition 8.13 If Φ is a QBF in negation normal form, its *dual* Φ^{d} is constructed by replacing each $\wedge$ with $\vee$, $\top$ with $\bot$, $\forall$ with $\exists$, and vice versa.

Lemma 8.14

(i) *Given a monotone formula or circuit* $\varphi(p_0, \dots, p_{n-1})$*, we can construct in polynomial time an* **IPC**-CF *proof of*

$$\bigwedge_{i<n} (p_i \vee q_i) \to \varphi(\vec{p}) \vee \varphi^{\mathrm{d}}(\vec{q}).$$

(ii) *Given a QBF* $\Phi(p_0, \dots, p_{n-1})$ *in negation normal form which is monotone in* $\vec{p}$*, and uses quantified variables* $\{r_i : i < d\}$*, we can construct in polynomial time an* **IPC**-SCF *proof of*

$$\bigwedge_{i<n} (p_i \vee q_i) \to A^I_\Phi(\vec{p}, \vec{r}) \vee A^I_{\Phi^{\mathrm{d}}}(\vec{q}, \vec{r}).$$

Proof: (i): By straightforward induction on the complexity of φ.

(ii): By induction on d. The base case $d = 0$ is (i). For the induction step from d to $d+1$, assume w.l.o.g. that Φ is existentially quantified. We can write $\Phi(\vec{p}) = \exists r_d\, \Phi_0(\vec{p}, r_d, \neg r_d)$, where $\Phi_0(\vec{p}, r, r')$ is monotone in r and r'. It is easy to check that

$$A^I_{\Phi_0(\vec{p}, r_d, \neg r_d)}(\vec{p}, r_d, \vec{r}) = A^I_{\Phi_0(\vec{p}, r, r')}(\vec{p}, r_d, \neg r_d, \vec{r}),$$

hence

$$A^I_\Phi(\vec{p}, \vec{r}, r_d) = \big[\big(r_d \to A^I_{\Phi_0(\vec{p}, r, r')}(\vec{p}, r_d, \neg r_d, \vec{r})\big) \vee \big(\neg r_d \to A^I_{\Phi_0(\vec{p}, r, r')}(\vec{p}, r_d, \neg r_d, \vec{r})\big)\big], \tag{82}$$

and likewise,

$$A^I_{\Phi^{\mathrm{d}}}(\vec{p}, \vec{r}, r_d) = \big(r_d \vee \neg r_d \to A^I_{\Phi_0^{\mathrm{d}}(\vec{p}, r, r')}(\vec{p}, r_d, \neg r_d, \vec{r})\big). \tag{83}$$

By the induction hypothesis, we have an **IPC**-SCF proof of

$$\bigwedge_{i<n} (p_i \vee q_i) \wedge (r \vee s) \wedge (r' \vee s') \to A^I_{\Phi_0}(\vec{p}, r, r', \vec{r}) \vee A^I_{\Phi_0^{\mathrm{d}}}(\vec{q}, s, s', \vec{r}).$$

Using the substitution rule, we obtain

$$\bigwedge_{i<n} (p_i \vee q_i) \to \Big(A^I_{\Phi_0}(\vec{p}, \top, \bot, \vec{r}) \vee A^I_{\Phi_0^{\mathrm{d}}}(\vec{q}, \bot, \top, \vec{r})\Big),$$
$$\bigwedge_{i<n} (p_i \vee q_i) \to \Big(A^I_{\Phi_0}(\vec{p}, \bot, \top, \vec{r}) \vee A^I_{\Phi_0^{\mathrm{d}}}(\vec{q}, \top, \bot, \vec{r})\Big),$$

hence (suppressing the variables $\vec{p}, \vec{r}$ in $A^I_{\Phi_0}$ and $\vec{q}, \vec{r}$ in $A^I_{\Phi_0^{\mathrm{d}}}$ for readability)

$$\begin{aligned}\bigwedge_{i<n}(p_i \vee q_i) &\to \big(A^I_{\Phi_0}(\top,\bot) \vee A^I_{\Phi_0}(\bot,\top)\big) \vee \big(A^I_{\Phi_0^{\mathrm{d}}}(\top,\bot) \wedge A^I_{\Phi_0^{\mathrm{d}}}(\bot,\top)\big)\\ &\to \big[\big(r_d \to A^I_{\Phi_0}(r_d,\neg r_d)\big) \vee \big(\neg r_d \to A^I_{\Phi_0}(r_d,\neg r_d)\big)\big] \vee \big(r_d \vee \neg r_d \to A^I_{\Phi_0^{\mathrm{d}}}(r_d,\neg r_d)\big)\\ &\to A^I_{\Phi}(\vec{p},\vec{r},r_d) \vee A^I_{\Phi^{\mathrm{d}}}(\vec{p},\vec{r},r_d)\end{aligned}$$

by (82) and (83). $\square$

Theorem 8.15 *Let* **IPC** $\subseteq L \subseteq \mathbf{T}_2 + \mathbf{KC}$, *and assume that* L-EF *weakly simulates* L-SF.

Then for every monotone PSPACE *language* P, *there exists a sequence of polynomial-size monotone Boolean circuits* $\{C^\forall_n, C^\exists_n : n \in \omega\}$ *such that* $C^\forall_n$ *and* $C^\exists_n$ *use variables* $\{p_i : i < n\}$ *and* $\{s_{l,r} : l < m_n, r < 3\}$, *and for every* $w \in \mathbf{2}^n$, *we have*

$$w \in P \iff \forall \vec{s}\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i} \vee s_{l,j}) \to C^\forall_n(w,\vec{s})\Big) \tag{84}$$

$$\iff \exists \vec{s}\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i} \vee s_{l,j}) \wedge C^\exists_n(w,\neg\vec{s})\Big), \tag{85}$$

while the circuits

$$\bigwedge_{l<m_n}\bigvee_{r<3} s_{l,r} \wedge C^\exists_n(\vec{p},\neg\vec{s}) \to C^\forall_n(\vec{p},\vec{s}) \tag{86}$$

have polynomial-size **CPC**-CF *proofs.*

If $P \in$ PSPACE *is not necessarily monotone, the above holds with* $C^\forall_n$ *and* $C^\exists_n$ *monotone in* $\vec{s}$.

Proof: Using Lemmas 8.10 and 8.11 and intuitionistic versions of Lemmas 2.5 and 2.6, we may assume that $\mathbf{T}_2$-CF weakly simulates **IPC**-SCF on circuits. Let $P \in$ PSPACE be monotone. There exists a polynomial-time constructible sequence of QBF $\{\Phi_n(p_0,\dots,p_{n-1}) : n \in \omega\}$ in negation normal form such that Φ_n is monotone in $\vec{p}$, and

$$w \in P \iff \Phi_n(w)$$

for all $w \in \mathbf{2}^n$. By Lemma 8.14 and the assumption, there are polynomial-size $\mathbf{T}_2$-CF proofs of

$$\bigwedge_{i<n}(p_i \vee q_i) \to A^I_{\Phi_n}(\vec{p},\vec{r}) \vee A^I_{\Phi_n^{\mathrm{d}}}(\vec{q},\vec{r}),$$

hence using Lemmas 8.2 and 8.1, there are polynomial-size $\mathbf{S4BB_2}$-CF proofs of

$$\bigwedge_{i<n}(\Box p_i \vee \Box q_i) \to \Box\mathsf{T}(A^I_{\Phi_n})(\vec{p},\vec{r}) \vee \Box\mathsf{T}(A^I_{\Phi_n^{\mathrm{d}}})(\vec{q},\vec{r}).$$

By Theorem 6.1, there exist polynomial-size monotone circuits $C^u_n(\vec{p},\vec{q},\vec{s})$, $u = 0,1$, polynomial-size **CPC**-CF proofs of

$$\bigwedge_{i<n}(p_i \vee q_i) \wedge \bigwedge_{l<m_n}\bigvee_{r<3} s_{l,r} \to \bigvee_{u<2} C^u_n(\vec{p},\vec{q},\vec{s}), \tag{87}$$

and polynomial-size $\mathbf{S4BB_2}$-CF proofs of

$$\bigwedge_{\substack{l<m\\r<3}}\Big(s_{l,r}\wedge\Box\psi_{l,r}\to\bigvee_{i\neq r}\Box\psi_{l,i}\Big)\wedge\bigwedge_{i<n}(p_i\to\Box p_i)\wedge\bigwedge_{i<n}(q_i\to\Box q_i)\wedge C^1_n(\vec p,\vec q,\vec s)\to\Box\mathsf{T}(A^I_{\Phi_n})(\vec p,\vec r),$$

$$\bigwedge_{\substack{l<m\\r<3}}\Big(s_{l,r}\wedge\Box\psi_{l,r}\to\bigvee_{i\neq r}\Box\psi_{l,i}\Big)\wedge\bigwedge_{i<n}(p_i\to\Box p_i)\wedge\bigwedge_{i<n}(q_i\to\Box q_i)\wedge C^0_n(\vec p,\vec q,\vec s)\to\Box\mathsf{T}(A^I_{\Phi^{\mathrm d}_n})(\vec q,\vec r),$$

for some formulas $\{\psi_{l,i} : l < m_n,\ i < 3\}$. Using the same argument as in the proof of Theorem 6.3, this implies the validity of the QBF

$$\forall\vec s\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j})\to C^1_n(\vec p,\vec q,\vec s)\Big)\to\Phi_n(\vec p),$$

$$\forall\vec s\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j})\to C^0_n(\vec p,\vec q,\vec s)\Big)\to\Phi^{\mathrm d}_n(\vec q).$$

Observe $\Phi^{\mathrm d}(\vec p)\equiv\neg\Phi(\neg\vec p)$. Thus, putting $C^{\forall}_n(\vec p,\vec s)=C^1_n(\vec p,\vec\top,\vec s)$, $C^{\exists}_n(\vec p,\vec s)=(C^0_n)^{\mathrm d}(\vec\bot,\vec p,\vec s)\equiv\neg C^0_n(\vec\top,\neg\vec p,\neg\vec s)$, and using the monotonicity of C^u_n, we have

$$\forall\vec s\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j})\to C^{\forall}_n(\vec p,\vec s)\Big)\to\Phi_n(\vec p),$$

$$\forall\vec s\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j})\to\neg C^{\exists}_n(\vec p,\neg\vec s)\Big)\to\neg\Phi_n(\vec p),$$

i.e.,

$$\Phi_n(\vec p)\to\exists\vec s\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j})\wedge C^{\exists}_n(\vec p,\neg\vec s)\Big).$$

Using the monotonicity of C^u_n, substitution of $\neg p_i$ for q_i in (87) yields (86). This in turn implies

$$\exists\vec s\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j})\wedge C^{\exists}_n(\vec p,\neg\vec s)\Big)\to\forall\vec s\Big(\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j})\to C^{\forall}_n(\vec p,\vec s)\Big),$$

hence (84) and (85): indeed,

$$\begin{aligned}\bigwedge_{l<m_n}\bigwedge_{i<j<3}(t_{l,i}\vee t_{l,j})\wedge C^{\exists}_n(\vec p,\neg\vec t)\wedge\bigwedge_{l<m_n}\bigwedge_{i<j<3}(s_{l,i}\vee s_{l,j})&\\ \to\bigwedge_{l<m_n}\bigvee_{r<3}(s_{l,r}\wedge t_{l,r})\wedge C^{\exists}_n\big(\vec p,\neg(\vec t\wedge\vec s)\big)&\\ \to C^{\forall}_n(\vec p,\vec t\wedge\vec s)&\\ \to C^{\forall}_n(\vec p,\vec s),&\end{aligned}$$

using once again the monotonicity of $C^{\exists}_n$ and $C^{\forall}_n$.

For nonmonotone $P\in$ PSPACE, we proceed as in Theorem 6.3. $\Box$

Remark 8.16 That (86) has short proofs, and in particular, is a tautology, is a crucial part of Theorem 8.15: the existence of $C_n^\forall$ and $C_n^\exists$ satisfying (84) and (85) already follows from PSPACE = NP. Indeed, if $P \in \mathrm{coNP}$ is monotone, there exists a polynomial-time constructible sequence of monotone formulas $\alpha_n(p_0, \dots, p_{n-1}, q_0, \dots, q_{m-1}, q'_0, \dots, q'_{m-1})$ such that

$$w \in P \iff \forall \vec{q}\, \alpha_n(w, \vec{q}, \neg\vec{q})$$

for all $w \in \mathbf{2}^n$. (Note that α_n can be made monotone in $\vec{p}$ as in the beginning of the proof of Theorem 6.3.) Then

$$w \in P \iff \forall \vec{s} \Big(\bigwedge_{l<m} \bigwedge_{i<j<3} (s_{l,i} \lor s_{l,j}) \to C_n^\forall(w, \vec{s}) \Big),$$

where $C_n^\forall(\vec{p}, \vec{s})$ is the monotone formula

$$\alpha_n(\vec{p}, s_{0,0}, \dots, s_{m-1,0}, s_{0,1}, \dots, s_{m-1,1}) \lor \bigvee_{l<m} (s_{l,0} \land s_{l,1}).$$

9 Conclusion

We have characterized the decision complexity of extension rules in basic transitive modal logics of bounded branching and the corresponding superintuitionistic logics, and as a consequence, we proved superpolynomial separation of EF and SF systems for these logics under plausible hypotheses, solving Problem 7.1 from [14]. Our work raises a few questions. First, we did not manage to obtain *unconditional* separations or lower bounds, but it is not clear if this is a result of insufficiency of our methods, or if the problems are fundamentally hard (say, as hard as lower bounds on classical Frege-like systems). Several additional problems were mentioned in Remark 5.10:

Question 9.1 *Let* $* \in \{\bullet, \circ\}$, $k \ge t \ge 2$, *and* $L = L_0 \oplus \mathbf{BB}_k$, *where* L_0 *is a* $*$*-extensible logic.*

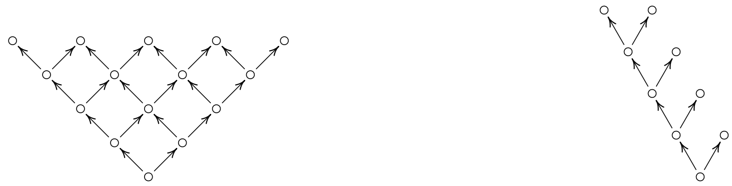
(i) *What is the complexity of* $\mathrm{Dec}(\mathrm{DP}_t, L\text{-CF})$*? Is it equivalent to* $\mathrm{Dec}(\mathrm{Ext}_t^*, L\text{-CF})$*? Is it feasible?*

(ii) *Are the single-conclusion extension rules* $\mathrm{Ext}_t^{*,\lor}$ *feasible for* L-CF*? Are all* EF (*or* CF) *systems for* L *p-equivalent even if allowed to use non-derivable admissible rules?*

Similar questions also concern the superintuitionistic logics $\mathbf{T}_k$.

On a more general note, our results only apply to $*$-extensible logics augmented with the $\mathbf{BB}_k$ axioms, which are among the weakest logics of bounded branching. They do not show much light on other logics of bounded branching and unbounded width, especially strong logics such as the logic of square grids $\langle \{0, \dots, n\} \times \{0, \dots, n\}, \le \rangle$ (or the similar logic of "clipped" grids as in Fig. 1 (a), which even has the disjunction property) and the logic of binary caterpillars (Fig. 1 (b)).

The results of [14] were consistent with the mental picture of a clear dividing line between weak logics for which we can prove unconditional exponential separations between EF and SF



(a) (b)

Figure 1: Some frames of branching two: (a) clipped grid, (b) binary caterpillar.

using some forms of feasible disjunction properties, and strong logics for which—at least if they are sufficiently well-behaved—SF and EF are p-equivalent, and up to a translation, p-equivalent to **CPC**-EF.

The results here rather seem to suggest a more complicated landscape where, as logics get stronger, the complexity of disjunction properties goes up until it perhaps becomes irrelevant for separation of proof systems, while perhaps the gap between EF and SF gradually becomes smaller, or perhaps it becomes dominated by tautologies of a completely different nature than seen here. In any case, there seems to be a law of diminishing returns at play, as it took us quite a lot of effort to get a modest improvement over [14], and it appears even more effort would be needed for further progress; at the same time, we are moving into a territory where the number of natural modal logics is quite underwhelming.

We now have a decent understanding of the relationship between EF and SF, but we know nothing much about what happens below or above these proof systems. These might be currently the most important problems in the proof complexity of nonclassical logics:

Question 9.2 *Can we separate L-*F *from L-*EF *for some modal or superintuitionistic logics L?*

Question 9.3 *Can we unconditionally* (*or at least, less trivially than by assuming* PSPACE $\neq$ NP) *prove superpolynomial lower bounds on the lengths of L-*SF *proofs for some modal or superintuitionistic logics L?*

Acknowledgements

I want to thank Pavel Pudlák and Pavel Hrubeš for clarifying discussion, and the anonymous reviewer for helpful suggestions to improve the presentation.

Supported by grant 19-05497S of GA ČR. The Institute of Mathematics of the Czech Academy of Sciences is supported by RVO: 67985840.

References

[1] 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.

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

[3] Alexander V. Chagrov, *On the complexity of propositional logics*, in: Complexity problems in Mathematical Logic, Kalinin State University, 1985, pp. 80–90 (in Russian).

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

[5] 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.

[6] 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.

[7] Dov M. Gabbay and Dick H. J. De Jongh, *A sequence of decidable finitely axiomatizable intermediate logics with the disjunction property*, Journal of Symbolic Logic 39 (1974), no. 1, pp. 67–78.

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

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

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

[11] Emil Jeřábek, *Dual weak pigeonhole principle, Boolean complexity, and derandomization*, Annals of Pure and Applied Logic 129 (2004), pp. 1–37.

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

[13] ———, *Independent bases of admissible rules*, Logic Journal of the IGPL 16 (2008), no. 3, pp. 249–267.

[14] ———, *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.

[15] ———, *Rules with parameters in modal logic I*, Annals of Pure and Applied Logic 166 (2015), no. 9, pp. 881–933.

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

[17] ———, *Rules with parameters in modal logic II*, Annals of Pure and Applied Logic 171 (2020), no. 10, article no. 102829, 59 pp.

[18] Jan Krajíček, *Proof complexity*, Encyclopedia of Mathematics and its Applications vol. 170, Cambridge University Press, 2019.

[19] Richard E. Ladner, *The computational complexity of provability in systems of modal propositional logic*, SIAM Journal on Computing 6 (1977), no. 3, pp. 467–480.

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

[21] Pavel Pudlák, *On reducibility and symmetry of disjoint NP pairs*, Theoretical Computer Science 295 (2003), pp. 323–339.

[22] ———, *Incompleteness in the finite domain*, Bulletin of Symbolic Logic 23 (2017), no. 4, pp. 405–441.

[23] Alexander A. Razborov, *On provably disjoint NP-pairs*, Technical Report RS-94-36, BRICS Report Series, 1994.

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

[25] J. Jay Zeman, *Modal logic: The Lewis-modal systems*, Oxford University Press, 1973.