Bulletin of the **S**ection of **L**ogic
Volume 51/2 (2022), pp. 197–205
https://doi.org/10.18778/0138-0680.2022.01

Lew Gordeev
E. Hermann Haeusler

PROOF COMPRESSION AND NP VERSUS PSPACE II: ADDENDUM

Abstract

In our previous work we proved the conjecture **NP** = **PSPACE** by advanced proof theoretic methods that combined Hudelmaier's cut-free sequent calculus for minimal logic (HSC) with the horizontal compressing in the corresponding minimal Prawitz-style natural deduction (ND). In this Addendum we show how to prove a weaker result **NP** = **coNP** without referring to HSC. The underlying idea (due to the second author) is to omit full minimal logic and compress only "naive" normal tree-like ND refutations of the existence of Hamiltonian cycles in given non-Hamiltonian graphs, since the Hamiltonian graph problem in NP-complete. Thus, loosely speaking, the proof of **NP** = **coNP** can be obtained by HSC-elimination from our proof of **NP** = **PSPACE**.

Keywords: Graph theory, natural deduction, computational complexity.

1. Introduction

Recall that in [2, 3] we proved that intuitionistically valid purely implicational formulas ρ have dag-like ND proofs ∂ whose weights (= the total numbers of symbols) are polynomial in the weights $|\rho|$ of ρ. ∂ were defined by a suitable two-fold horizontal compression of the appropriate tree-like ND ∂_1 obtained by standard conversion of basic tree-like HSC proofs π existing by the validity of ρ. We observed that the height and the total weight of distinct formulas occurring in (π, and hence also) ∂_1 are both

Presented by: Peter Schroeder-Heister
Received: December 1, 2020
Published online: January 07, 2022

polynomial in $|\rho|$. From this we inferred that the compressed dag-like ND proofs ∂ are weight-polynomial in $|\rho|$. Moreover, it is readily seen that the latter conclusion holds true for any tree-like ND ∂' with the polynomial upper bounds on the height and total weight of distinct formulas used. We just arrived at the following Theorem 1.3, where $\mathrm{NM}_{\to}$ is standard purely implicational ND for minimal logic (see also Appendix and [3] for more details).

DEFINITION 1.1. Tree-like $\mathrm{NM}_{\to}$-deduction ∂ with the root-formula (= conclusion) ρ is called *polynomial* if its weight (= total number of symbols) is polynomial in the weight of conclusion, $|\rho|$. ∂ is called *quasi-polynomial* if the height of ∂ plus total weight of distinct formulas occurring in ∂ is polynomial in $|\rho|$.

DEFINITION 1.2. A given (tree- or dag-like) $\mathrm{NM}_{\to}$-deduction is called a *proof* of its root-formula ρ iff every maximal thread connecting ρ with a leaf α is closed, i.e. it contains a "discharging" $(\to I)$ with conclusion $\alpha \to \beta$, for some β.

THEOREM 1.3. *In* $\mathrm{NM}_{\to}$*, any quasi-polynomial tree-like proof of* ρ *is compressible into a polynomial dag-like proof of* ρ.

Now let P be a NP-complete problem and suppose that ρ is valid iff P has no positive solution. From the existence of a tree-like ND proof ∂' as above we'll infer the existence of a polynomial dag-like ND proof ∂ of ρ, which will eventually imply $\mathbf{NP} = \mathbf{coNP}$. In particular, let P be the Hamiltonian Graph Problem. For any graph G consider purely implicational formula ρ expressing in standard way that G has no Hamiltonian cycles. Suppose that the canonical proof search in $\mathrm{NM}_{\to}$ yields a normal tree-like proof ∂' of ρ whose height is polynomial in $|G|$ (and hence in $|\rho|$), provided that G is non-Hamiltonian. Since normal ND proofs satisfy the subformula property, such ∂' will obey the requested polynomial upper bounds in question, and hence the weight of its horizontal dag-like compression ∂ will be polynomially bounded, as desired. That is, we argue as follows.

LEMMA 1.4. *Let* P *be the Hamiltonian graph problem and suppose that purely implicational formula* ρ *express in standard way that a given graph* G *has no Hamiltonian cycles. There exists a quasi-polynomial normal tree-like proof of* ρ *in* $\mathrm{NM}_{\to}$ *whose height is polynomial in* $|G|$ *(and hence* $|\rho|$*), provided that* G *is non-Hamiltonian.*

Recall that polynomial ND proofs (whether tree- or dag-like) have time-polynomial certificates ([3]: Appendix), while the non-hamiltoniancy of simple and directed graphs is coNP-complete. Hence Theorem 1.3 yields

Corollary 1.5. **NP** = **coNP** holds true.

This argument does not refer to sequent calculus. Summing up, in order to complete our HSC-free proof of **NP** = **coNP** it will suffice to prove Lemma 1.4. This will be elaborated in the rest of the paper.

2. Hamiltonian problem

Consider a simple[1] directed graph $G = \langle V_G, E_G \rangle$, $card\,(V_G) = n$. A *Hamiltonian path* (or *cycle*) in G is a sequence of nodes $\mathcal{X} = v_1 v_2 \dots v_n$, such that, the mapping $i \mapsto v_i$ is a bijection of $[n] = \{1, \cdots, n\}$ onto V_G and for every $0 < i < n$ there exists an edge $(v_i, v_{i+1}) \in E_G$. The (decision) problem whether or not there is a Hamiltonian path in G is known to be NP-complete (cf. e.g. [1]). If the answer is YES then G is called Hamiltonian. In order to verify that a given sequence of nodes $\mathcal{X}$, as above, is a Hamiltonian path it will suffice to confirm that:

1. There are no repeated nodes in $\mathcal{X}$,
2. No element $v \in V_G$ is missing in $\mathcal{X}$,
3. For each pair $\langle v_i, v_j \rangle$ in $\mathcal{X}$ there is an edge $(v_i, v_j) \in E_G$.

It is readily seen that the conjunction of $1, 2, 3$ is verifiable by a deterministic TM in n-polynomial time. Consider a natural formalization of these conditions (cf. e.g. [1]) in propositional logic with one constant $\bot$ (*falsum*) and three connectives $\wedge$, $\vee$, $\rightarrow$ (as usual $\neg F := F \rightarrow \bot$).

Definition 2.1. For any $G = \langle V_G, E_G \rangle$, $card(V_G) = n > 0$, as above, consider propositional variables $X_{i,v}$, $i \in [n]$, $v \in V_G$. Informally, $X_{i,v}$ should express that vertex v is visited in the step i in a path on G. Define propositional formulas $A - E$ as follows and let $\alpha_G := A \wedge B \wedge C \wedge D \wedge E$.

[1] A simple graph has no multiple edges. For every pair of nodes (v_1, v_2) in the graph there is at most one edge from v_1 to v_2.

1. $A = \bigwedge_{v\in V}(X_{1,v} \vee \ldots \vee X_{n,v})$ (: every vertex is visited in X).
2. $B = \bigwedge_{v\in V}\bigwedge_{i\neq j}(X_{i,v} \to (X_{j,v} \to \bot))$ (: there are no repetitions in X).
3. $C = \bigwedge_{i\in[n]}\bigvee_{v\in V} X_{i,v}$ (: at each step at least one vertex is visited).
4. $D = \bigwedge_{v\neq w}\bigwedge_{i\in[n]}(X_{i,v} \to (X_{i,w} \to \bot))$ (: at each step at most one vertex is visited).
5. $E = \bigwedge_{(v,w)\notin E}\bigwedge_{i\in[n-1]}(X_{i,v} \to (X_{i+1,w} \to \bot))$ (: if there is no edge from v to w then w can't be visited immediately after v).

Thus G is Hamiltonian iff α_G is satisfiable. Denote by SAT_{Cla} the set of satisfiable formulas in classical propositional logic and by $TAUT_{Int}$ the set of tautologies in intuitionistic propositional logic. Then the following conditions hold: (1) G is non-Hamiltonian iff $\alpha_G \notin SAT_{Cla}$, (2) G is non-Hamiltonian iff $\neg\alpha_G \in TAUT_{Cla}$, (3) G is non-Hamiltonian iff $\neg\alpha_G \in TAUT_{Int}$. Glyvenko's theorem yields the equivalence between (2) and (3). Hence G is non-Hamiltonian iff there is an intuitionistic proof of $\neg\alpha_G$. Such proof is called a certificate for the non-hamiltoniancy of G. [7] (also [4]) presented a translation from formulas in full propositional intuitionistic language into the purely implicational fragment of minimal logic whose formulas are built up from $\to$ and propositional variables. This translation employs new propositional variables q_γ for logical constants and complex propositional formulas γ (in particular, every $\alpha \vee \beta$ and $\alpha \wedge \beta$ should be replaced by $q_{\alpha\vee\beta}$ and $q_{\alpha\wedge\beta}$, respectively) while adding implicational axioms stating that q_γ is equivalent to γ . For any propositional formula γ, let $\gamma^\star$ denote its translation into purely implicational minimal logic in question. Note that $size(\gamma^\star) \leq (size(\gamma))^3$. Now let $\gamma := \neg\alpha_G$. So $\gamma \in TAUT_{Int}$ iff $\gamma^\star$ is provable in the minimal logic. Moreover, it follows from [7], [4] that for any normal intuitionistic ND proof ∂ of γ there is a normal proof $\partial_\to$ of $\gamma^\star$ in the corresponding ND system for minimal logic, $\mathrm{NM}_\to$, such that $height(\partial_\to) = \mathcal{O}(height(\partial))$. Thus in order to prove Lemma 1.4 it will suffice to establish

Claim 2.2. G is non-Hamiltonian iff there exists a normal intuitionistic tree-like ND proof of $\alpha_G \to \bot$, i.e. $\neg\alpha_G$, whose height is polynomial in n.

2.1. Proof of Claim 2.2

The sufficiency easily follows from the soundness of ND. Consider the necessity. In the sequel we suppose that a non-Hamiltonian graph G is fixed and $\alpha_G = A \wedge B \wedge C \wedge D \wedge E$ (cf. Definition 2.1). Let $p : \{1, \ldots, n\} \mapsto V_G$ be any sequence of nodes from V_G of the length n and let $\mathcal{X}_p := \left\{X_{1,p[1]}, \cdots, X_{n,p[n]}\right\}$ be corresponding set of propositional variables. $\mathcal{X}_p$ and p represent a path in G that starts by visiting vertex $p[1]$, encoded by $X_{1,p[1]}$, followed by $p[2]$, encoded by $X_{2,p[2]}$, etc., up to $p[n]$ encoded by $X_{n,p[n]}$. Since G is non-Hamiltonian, $\mathcal{X}_p$ is inconsistent with α_G.

Lemma 2.3. *For any p and $\mathcal{X}_p$ as above there is a normal intuitionistic tree-like ND Π_p with conclusion $\perp$, assumptions from $\mathcal{X}_p \cup \{\alpha_G\}$ and* height $(\Pi_p) = \mathcal{O}\left(n^2\right)$ *:*

$$\begin{array}{c} \mathcal{X}_p \cup \{\alpha_G\} \\ \Pi_p \\ \perp \end{array}$$

Proof: Π_p is defined as follows. Since G is non-Hamiltonian, we observe that at least one of the conditions 1, 3 to be a Hamiltonian path (see above in § 2) fails for $\mathcal{X}_p$. Hence at least one of the following is the case.

There are repeated nodes. There are $1 \leq i < j \leq n$, such that $p[i] = p[j] = v \in V_G$; let $i < j$ be the least such pair. Consider a deduction Γ_p :

$$\dfrac{X_{j,v} \qquad \dfrac{X_{i,v} \qquad X_{i,v} \to (X_{j,v} \to \perp)}{X_{j,v} \to \perp}}{\perp}$$

of $\perp$ from $X_{i,v}$, $X_{j,v}$ and $X_{i,v} \to (X_{j,v} \to \perp)$. Since $\{X_{i,v}, X_{j,v}\} \subset \mathcal{X}_p$, the assumption $X_{i,v} \to (X_{j,v} \to \perp)$ is a component of the conjunction B from α_G. So let Δ_p be a chain of $\wedge$-elimination rules deducing $X_{i,v} \to (X_{j,v} \to \perp)$ from α_G. Now let Π_p be the corresponding concatenation $\Delta_p \circ \Gamma_p$ deducing $\bot$ from $\{X_{i,v}, X_{j,v}, \alpha_G\} \subset \mathcal{X}_p \cup \{\alpha_G\}$. Clearly Π_p is normal and *height* $(\Pi_p) = \mathcal{O}\left(n^2\right)$.

There is a missing edge. There is $1 \leq i < n$, such that $p[i] = v \in V_G$, $p[i+1] = w \in V_G$ and $(v, w) \notin E_G$; Let i be the least such number. Consider a deduction Γ_p :

$$\dfrac{X_{i+1,w} \qquad \dfrac{X_{i,v} \qquad X_{i,v} \rightarrow (X_{i+1,w} \rightarrow \bot)}{X_{i+1,w} \rightarrow \bot}}{\bot}$$

of $\bot$ from $X_{i,v}$, $X_{i+1,w}$ and $X_{i,v} \rightarrow (X_{i+1,w} \rightarrow \bot)$. Since $\{X_{i,v}, X_{i+1,w}\} \subset \mathcal{X}_p$ and $(v, w) \notin E_G$, the assumption $X_{i,v} \rightarrow (X_{i+1,w} \rightarrow \bot)$ is a component of the conjunction E from α_G. So let Δ_p be a chain of $\wedge$-elimination rules deducing $X_{i,v} \rightarrow (X_{i+1,w} \rightarrow \bot)$ from α_G. Now let Π_p be the corresponding concatenation $\Delta_p \circ \Gamma_p$ deducing $\bot$ from $\{X_{i,v}, X_{i+1,w}, \alpha_G\} \subset \mathcal{X}_p \cup \{\alpha_G\}$. Clearly Π_p is normal and *height* $(\Pi_p) = \mathcal{O}\left(n^2\right)$. $\square$

In the sequel for the sake of brevity we let $V_G = \{1, \cdots, n\}$. Now consider the deductions Π_p^i, $1 \leq i \leq n$, in the extended ND that includes standard n-ary $\vee$-elimination rules. Π_p^i are defined by recursion on i using (in the initial case $i = 1$) the $\Pi_{p(1/k)}$ from the last lemma, where sequences $p\,(-j) : \{1, \ldots, n\} \mapsto V_G \cup \{0\}$ and $p\,(j/k) : \{1, \ldots, n\} \mapsto V_G$ are defined by

$$p\,(-j)\,[k] := \begin{cases} p\,[k]\,, & if \qquad k = j, \\ 0, & else, \end{cases}$$

and

$$p\,(j/k) := \begin{cases} p\,[k]\,, & if \qquad k = j, \\ p\,[j]\,, & else. \end{cases}$$

So let

$$\Pi_p^1 =$$

$$\dfrac{X_{1,v_1} \vee \cdots \vee X_{1,v_n} \qquad \begin{matrix} \mathcal{X}_{p(-1)} \cup \{\alpha_G\}\,, [X_{1,v_1}] \\ \Pi_{p(1/1)} \\ \bot \end{matrix} \qquad \cdots \qquad \begin{matrix} \mathcal{X}_{p(-1)} \cup \{\alpha_G\}\,, [X_{n,v_n}] \\ \Pi_{p(1/n)} \\ \bot \end{matrix}}{\bot},$$

$$\Pi_p^{j+1} :=$$

$$\cfrac{X_{j+1,v_1} \vee \cdots \vee X_{j+1,v_n} \qquad \begin{matrix} \mathcal{X}_{p(-(j+1))} \cup \{\alpha_G\}, [X_{j+1,v_1}] \\ \Pi^j_{p((j+1)/1)} \\ \bot \end{matrix} \qquad \cdots \qquad \begin{matrix} \mathcal{X}_{p(-(j+1))} \cup \{\alpha_G\}, [X_{j+1,v_n}] \\ \Pi^i_{p((j+1)/n)} \\ \bot \end{matrix}}{\bot}.$$

Thus for $i = n$ we obtain.

$$\Pi_p^n =$$

$$\cfrac{X_{n,v_1} \vee \cdots \vee X_{n,v_n} \qquad \begin{matrix} \mathcal{X}_{p(-(n-1))} \cup \{\alpha_G\}, [X_{n,v_1}] \\ \Pi^{n-1}_{p(n/1)} \\ \bot \end{matrix} \qquad \cdots \qquad \begin{matrix} \mathcal{X}_{p(-(n-1))} \cup \{\alpha_G\}, [X_{n,v_n}] \\ \Pi^{n-1}_{p(n/n)} \\ \bot \end{matrix}}{\bot}.$$

LEMMA 2.4. *For any $p : \{1, \ldots, n\} \mapsto V_G$, Π_p^n is a normal intuitionistic tree-like deduction with conclusion $\bot$ and (the only) open assumption α_G in the extended ND in question Moreover,* height $\left(\Pi_p^n\right) = \mathcal{O}\left(n^2\right)$.

PROOF: This easily follows from Lemma 2.4 by induction on n. □

Now let $\Pi := \Pi_{Id}^n$ where $Id : \{1, \ldots, n\} \mapsto V_G$ is the identity $Id\,[i] := i$. Denote by $\widehat{\Pi}$ the canonical tree-like embedding of Π into basic intuitionistic ND with plain (binary) $\vee$-eliminations that is obtained by successive unfolding of the n-ary $\vee$-elimination rules with premises $X_{j,v_1} \vee \cdots \vee X_{j,v_n}$ involved. Note that *height* $\left(\widehat{\Pi}\right) = \mathcal{O}\left(n^3\right)$. Moreover let ∂ denote $\widehat{\Pi}$ followed by the introduction of $\alpha_G \to \bot$:

$$\cfrac{\alpha_G \qquad \begin{matrix} [\alpha_G] \\ \widehat{\Pi} \\ \bot \end{matrix}}{\alpha_G \to \bot}$$

COROLLARY 2.5. ∂ is a normal intuitionistic tree-like ND proof of $\alpha_G \to \bot$ whose height is polynomial in n, as required.

Appendix: More on Theorem 1.3

THEOREM 1.3 (cf. Introduction). In standard ND for purely implicational minimal logic, $\mathrm{NM}_{\rightarrow}$, any quasi-polynomial tree-like proof ∂ of ρ is compressible into a polynomial dag-like proof ∂^* of ρ.

PROOF SKETCH[2]: The mapping $\partial \hookrightarrow \partial^*$ is obtained by a two-folded horizontal compression $\partial \hookrightarrow \partial^\flat \hookrightarrow \partial^*$, where $\partial^\flat$ is a polynomial dag-like deduction in $\mathrm{NM}^\flat_{\rightarrow}$ that extends $\mathrm{NM}_{\rightarrow}$ by a new *separation* rule (S)

$$\boxed{(S) : \frac{\overbrace{\alpha \quad \cdots \quad \alpha}^{n\ times}}{\alpha} \ (n \text{ arbitrary})}$$

whose identical premises are understood disjunctively: "*if at least one premise is proved then so is the conclusion*" (in contrast to ordinary inferences: "*if all premises are proved then so are the conclusions*"). The notion of provability in $\mathrm{NM}^\flat_{\rightarrow}$ is modified accordingly such that proofs are locally correct deductions assigned with appropriate sets of threads that are closed and satisfy special conditions of *local coherency*. Now $\partial^\flat$ arises from ∂ by ascending (starting from the root) merging of different occurrences of identical formulas occurring on the same level, followed by inserting instances of (S) instead of resulting multipremise inferences. Corresponding locally coherent threads in $\partial^\flat$ are inherited by the underlying (closed) threads in ∂ (in contrast to ordinary local correctness, the local coherency is not verifiable in polynomial time, as the total number of threads in question might be exponential in $|\rho|$). A desired "cleansed" $\mathrm{NM}_{\rightarrow}$-subdeduction $\partial^* \subset \partial^\flat$ arises by collapsing (S) to plain repetitions

$$\boxed{(R) : \frac{\alpha}{\alpha}}$$

with respect to the appropriately chosen premises of (S). The choice is made non-deterministically using the set of locally coherent threads in $\partial^\flat$. $\square$

[2]See [3] for more details.

References

[1] S. Arora, B. Barak, **Computational Complexity: A Modern Approach**, Cambridge University Press (2009).

[2] L. Gordeev, E. H. Haeusler, *Proof Compression and NP Versus PSPACE*, **Studia Logica**, vol. 107(1) (2019), pp. 55–83, DOI: https://doi.org/10.1007/s11225-017-9773-5.

[3] L. Gordeev, E. H. Haeusler, *Proof Compression and NP Versus PSPACE II*, **Bulletin of the Section of Logic**, vol. 49(3) (2020), pp. 213–230, DOI: https://doi.org/10.18778/0138-0680.2020.16.

[4] E. H. Haeusler, *Propositional Logics Complexity and the Sub-Formula Property*, [in:] **Proceedings of the Tenth International Workshop on Developments in Computational Models DCM** (2014), arXiv:1504.01927.

[5] J. Hudelmaier, *An $O(n \log n)$-space decision procedure for intuitionistic propositional logic*, **Journal of Logic and Computation**, vol. 3 (1993), pp. 1–13, DOI: https://doi.org/10.1093/logcom/3.1.63.

[6] D. Prawitz, **Natural deduction: A proof-theoretical study**, Almqvist & Wiksell (1965).

[7] R. Statman, *Intuitionistic propositional logic is polynomial-space complete*, **Theoretical Computer Science**, vol. 9 (1979), pp. 67–72, DOI: https://doi.org/10.1016/0304-3975(79)90006-9.

Lew Gordeev
University of Tübingen
Department of Computer Science
Nedlitzer Str. 4a
14612 Falkensee, Germany
e-mail: lew.gordeew@uni-tuebingen.de

E. Hermann Haeusler
Pontificia Universidade Católica do Rio de Janeiro – RJ
Department of Informatics
Rua Marques de São Vicente, 224
Gávea, Rio de Janeiro, Brazil
e-mail: hermann@inf.puc-rio.br