Seminar in Logic: Upper bounds on Frege proofs of the pigeonhole principle via the Paris-Wilkie translation

Fabian Regen

SS22

1 Prerequisites

We will consider propositional logic consisting of atoms, constants 1 and 0 representing true and false respectively and the unary logical connective negation $\neg$ and the binary connectives disjunction $\vee$ and conjunction $\wedge$. Formulas are defined in the usual inductive manner: atoms and constants are formulas and for a and b formulas also $\neg a$, $a \vee b$, $a \wedge b$ are formulas.

A Frege proof system F refers to a finite set of Frege rules that is sound and complete. Since we will use a different proof system which is equivalent to Frege systems but more elegant to reason with, we will refer to [Krajíček, 2019, Chapter 2] for details.

Definition 1.1. Given a language L and a formula a in the language L the logical depth ldp is defined inductively:

- $\mathrm{ldp}(b) = 0$ if b is an atom or a constant,
- $\mathrm{ldp}(\circ(b_1, \ldots, b_k)) = 1 + max_i \ \mathrm{ldp}(b_i)$ for a k-ary connective $\circ$ in L.

TC^0 defines the languages computed on $\{0,1\}^n$ by boolean circuits C_n with conjunctions and disjunctions of unbounded arity, logical depth bounded by a constant d, a size bound $|C_n| \leq n^c$ and using unbounded arity connectives $\mathrm{TH}_{n,k}$. The connectives $\mathrm{TH}_{n,k}$ are defined for $0 \leq k \leq n$:

$$\mathrm{TH}_{n,k}(a_1, \ldots, a_n) = 1 \quad \text{if and only if} \quad \sum_i a_i \geq k$$

Definition 1.2. The depth $\mathrm{dp}(A)$ of a propositional formula A is defined inductively:

- $\mathrm{dp}(B) = 0$ for B being an atom or a constant,
- if B starts with $\neg$ then $\mathrm{dp}(\neg B) = \mathrm{dp}(B)$ otherwise $\mathrm{dp}(\neg B) = \mathrm{dp}(B) + 1$,

- if A can be written as $B(C_1, \ldots, C_t)$ where $B(q_1, \ldots, q_t)$ is built from atoms and disjunctions only and neither of the formulas $C_1, \ldots, C_t$ do have a disjunction as their top connective then $\mathrm{dp}(A) = \max_i \mathrm{dp}(C_i) + 1$,

- Analogously for conjunctions.

The depth is a notion of the length of the longest chain of subformulas for which the top connective changes its type.

The depth of a Frege proof is the maximum depth of the formulas that occur in the proof. By TC^0-Frege systems we denote the bounded depth Frege subsystem operating on TC^0 formulas.

L_{BA} will denote the language of bounded arithmetic as defined in [Krajíček, 2019, Chapter 9.1]. It can be considered an extension of the language of peano with its symbols $0, 1, +, \cdot, \leq$ by adding function symbols for bit-length and bit-operations. We will only consider theories in L_{BA} which contain the BASIC axioms, described in the same chapter, and axioms that give the added functions their intended meaning.

By $L_{BA}(R)$ we denote the extension of L_{BA} by a relation symbol R, and we possibly added some axioms about said symbol to the theory we consider. With $\Sigma_0^{1,b}$ we denote the class of $L_{BA}(R)$ formulas with only bounded quantifiers. The Theory $I\Sigma_0^{1,b}$ is axiomatized by adding the IND scheme for all $\Sigma_0^{1,b}$ formulas A:

$$\neg A(0) \vee (\exists y \leq x, y < x \wedge A(y) \wedge \neg A(y+1)) \vee A(x),$$

which is obtained by taking the usual induction axiom, replacing quantifiers with their bounded versions and translating inferences into disjunctions and negations.

2 Sequent Calculus

Because of its simple inference rules we introduce the Sequent Calculus LKB, which we will later use to reason about proofs. We assume familiarity with LK but refer to [Krajíček, 2019, Chapter 3.1] for a detailed explanation. We now introduce a version of the Sequent Calculus LK for bounded arithmetic. We extend LK by inference rules for bounded quantifiers:

$$\frac{a \leq t, \Gamma \longrightarrow \Delta, A(a)}{\Gamma \longrightarrow \Delta, \forall x \leq t A(x)} \qquad \frac{a \leq t, A(a), \Gamma \longrightarrow \Delta}{\exists x \leq t A(x), \Gamma \longrightarrow \Delta}$$

$$\frac{A(s), \Gamma \longrightarrow \Delta}{s \leq t, \forall x \leq t A(x), \Gamma \longrightarrow \Delta} \qquad \frac{\Gamma \longrightarrow \Delta, A(s)}{s \leq t, \Gamma \longrightarrow \Delta, \exists x \leq t A(x)}$$

for which s and t are terms and a is a free variable not appearing in the lower sequent. We also add the induction inference rule

$$\frac{A(y), \Gamma \longrightarrow \Delta, A(y+1)}{A(0), \Gamma \longrightarrow \Delta, A(x)}$$

for $A \in \Sigma_0^{1,b}$. We will refer to this version of Sequent Calculus as LKB.

3 Correspondence

We say that a proof system P **p-simulates** a theory T if and only if there exists a translation $\langle \cdot \rangle_n$ such that the following conditions are satisfied:

1. The translation of Δ_0 formulas A (in the language of T) into sequences of propositional formulas $\langle A \rangle_n$, $n \geq 1$, satisfies:
   - there is a p-time algorithm that computes $\langle A \rangle_n$,
   - $|\langle A \rangle_n|$ is polynomially bounded and $\mathrm{dp}(\langle A \rangle_n)$ is constant,
   - $\forall x A(x)$ is true for all interpretations of the added relation symbols iff $\langle A \rangle_n$ are tautologies.
2. If T proves $\forall x A(x)$ then there are P-proofs of $\langle A \rangle_n$ of polynomial size and there is a p-time algorithm that constructs a P-proof of $\langle A \rangle_n$ from $1^{(n)}$.

This implies that in order to establish a polynomial upper bound for P-proofs of $\langle A \rangle_n$ for $n \geq 1$ it suffices to prove $\forall x A(x)$ in T. We will now introduce a proof system P and a theory T and show that P p-simulates T.

4 TC^0-Frege Systems

Consider an extension of a Frege system F by n-ary counting connectives $C_{n,k}$ which holds true if exactly k of its arguments are true and false otherwise. For $0 \leq k \leq n$ we define $C_{n,k}$ by the axiom schemes

- $C_{1,1}(p) \equiv p$,
- $C_{n,0}(p_1, \ldots, p_n) \equiv \wedge_{i \leq n} \neg p_i$,
- $C_{n+1,k+1}(\bar{p}, q) \equiv (C_{n,k}(\bar{p}) \wedge q) \vee (C_{n,k+1}(\bar{p}) \wedge \neg q)$ for all $k < n$,
- $C_{n+1,n+1}(\bar{p}, q) \equiv C_{n,n}(\bar{p}) \wedge q$.

This extension will be denoted by FC which stands for Frege with counting. FC_d will denote the subsystem allowing in proofs only formulas of depth at most d. Using a $C_{n,k}$ connective increases the depth of a subformula by 1.

FC_d systems serve as examples of TC^0-Frege systems, since both counting and threshold connectives can be expressed by the other:

$$C_{n,k}(\bar{p}) \equiv \mathrm{TH}_{n,k}(\bar{p}) \wedge \neg \mathrm{TH}_{n,k+1}(\bar{p}) \quad \text{and} \quad \mathrm{TH}_{n,k}(\bar{p}) \equiv \bigvee_{k \leq l \leq n} C_{n,l}(\bar{p}).$$

To construct a theory that gets p-simulated by FC_d systems we introduce a bounded counting quantifier $\exists^{=}$ for which

$$\exists^{=s} y \leq t\ A(y) \quad \text{holds if and only if} \quad |\{b \leq t | A(b)\}| = s$$

where s and t are terms not involving y.

Analogously to the counting connectives $C_{n,k}$ we define $\exists^{=}$ by the following axiom schemes:

- $\forall y \leq t\ \neg A(y) \rightarrow \exists^{=0} y \leq t A(y)$,
- $(A(t+1) \wedge \exists^{=s} y \leq t\ A(y)) \rightarrow \exists^{=s+1} y \leq t+1\ A(y)$,
- $(\neg A(t+1) \wedge \exists^{=s} y \leq t\ A(y)) \rightarrow \exists^{=s} y \leq t+1\ A(y)$.

The class of bounded $L_{BA}(R)$ formulas allowing the $\exists^{=}$ quantifier will be denoted by $\exists^{=}\Sigma_0^{1,b}$. The theory $I\exists^{=}\Sigma_0^{1,b}$ is defined as the theory $I\Sigma_0^{1,b}$ but allows the IND scheme $\exists^{=}\Sigma_0^{1,b}$ formulas.

5 The Paris-Wilkie Translation

Originally the Paris-Wilkie translation maps a $\Delta_0(R)$ formula $A(x_1, \ldots, x_k)$ and $n_i \geq 0$ for $i \in \{1, \ldots, k\}$ to a propositional formula $\langle A(\bar{x}) \rangle_{n_1, \ldots, n_k}$. We will formulate an extension of the translation that operates on closed $\exists^{=}\Sigma_0^{1,b}$ formulas. It is defined inductively on the complexity of A:

- If B is an atomic formula $B \equiv t(\bar{x}) = s(\bar{x})$ or $B \equiv t(\bar{x}) \leq s(\bar{x})$ for terms t and s the translation is defined as

$$\langle B \rangle_{\bar{n}} := \begin{cases} 1 & B(\bar{n}) \text{ is true,} \\ 0 & \text{otherwise.} \end{cases}$$

- For an atomic formula $B \equiv R(t(\bar{x}), s(\bar{x}))$ and the terms $t(\bar{x})$ and $s(\bar{x})$ having values i and j for $\bar{x} := \bar{n}$ then the translation is defined as a propositional atom r_{ij}.
- The translation commutes with negation, conjunction and disjunction:
  - $\langle A \vee B \rangle := \langle A \rangle \vee \langle B \rangle$,
  - $\langle \neg A \rangle := \neg \langle A \rangle$,
  - $\langle A \wedge B \rangle := \langle A \rangle \wedge \langle B \rangle$.
- For bounded quantifiers $A(\bar{x}) = \exists y \leq t(\bar{x}) B(\bar{x}, y)$ we define

$$\langle A \rangle_{\bar{n}} := \bigvee_{m \leq t(\bar{n})} \langle B(\bar{x}, y) \rangle_{\bar{n}, m}.$$

- Analogously for $A(\bar{x}) = \forall y \leq t(\bar{x}) B(\bar{x}, y)$

$$\langle A \rangle_{\bar{n}} := \bigwedge_{m \leq t(\bar{n})} \langle B(\bar{x}, y) \rangle_{\bar{n},m}.$$

- For the counting quantifier $A(\bar{x}) = \exists^{=s} y \leq t B(\bar{x}, y)$ we define

$$\langle A \rangle_{\bar{n}} := C_{m+1,k}(\langle B(\bar{x}, y) \rangle_{\bar{n},0}, \ldots, \langle B(\bar{x}, y) \rangle_{\bar{n},m})$$

  for s and t terms and $k = s(\bar{n})$, $m = t(\bar{n})$.

This translation will be used to show that FC_d p-simulates $I\exists^{=}\Sigma_0^{1,b}$.

Lemma 5.1. *For a $\exists^{=}\Sigma_0^{1,b}$-formula A there exist $c, d \geq 1$ such that for all $\bar{n} = (n_1, \ldots, n_k)$ it holds that*

- $|\langle A \rangle_{\bar{n}}| \leq (n_1 + \cdots + n_k + 2)^c$,
- $dp(\langle A \rangle_{\bar{n}}) \leq d$.

and $A(\bar{n})$ is true for all interpretations of R if and only if $\langle A \rangle_{\bar{n}}$ is a tautology.

Proof. By induction on the complexity of A: for atomic formulas the depth is 0 and the size is constant, therefore bounded by a polynomial. The propositional connectives might increase the depth by 1 and the size bound holds by the induction hypothesis. For bounded quantifiers, since every term $t(n)$ is a polynomial, the size of the translation is bounded by the size of the subformulas, which are bounded by the induction hypothesis, times the polynomial bounding $t(n)$. Analogously the depth may increase by 1, depending on the formulas B and the quantifier at hand. The counting quantifier increases the depth by 1 and the size of the formula stays polynomially bounded. □

The following statement was adapted from Krajíček [2019] which proves the statement in a model-theoretic way. We are going to provide a proof-theoretic proof as can be found in [Cook and Nguyen, 2010, VII.2.3].

Theorem 5.2. *For FC_d, $d \geq 1$, and $A(\bar{x})$ being a $\exists^{=}\Sigma_0^{1,b}$ formula and assuming $I\exists^{=}\Sigma_0^{1,b}$ proves $\forall \bar{x} A(\bar{x})$ then there exist $c, d \geq 1$ such that for every $\bar{n}$ there is an FC_d-proof $\pi_{\bar{n}}$ of $\langle A(\bar{x}) \rangle_{\bar{n}}$ such that*

- $dp(\pi_{\bar{n}}) \leq d$ *and*
- $|\pi_{\bar{n}}| \leq (n_1 + \cdots + n_k + 2)^c$.

Proof. The idea is to take a LKB proof consisting of bounded formulas only in $I\exists^{=}\Sigma_0^b$ and translate each formula via the translation defined above. A proof consisting of bounded formulas only exists due to cut-elimination. Details about this result can be found in Cook and Nguyen [2010]. We will then find a set of rules on how to translate each of the inference rules such that the result of the translation is a proof of $\langle A(\bar{x}) \rangle_{\bar{n}}$. Let π be a $I\exists^{=}\Sigma_0^b$ proof with bounded formulas only in LKB of $A(x)$. We will construct a proof of $\langle A\rangle_n$ for $n \geq 0$ with polynomial size and constant depth. For all free variables a proof can be found. We therefore in each step only consider sequents with values assigned to all the free variables. We prove by induction on the number of lines above a sequent in π:

If A is an axiom, we replace it with a short Frege proof of $\langle A\rangle$. For example we prove the first axiom of the $\exists^{=}$ quantifier: $\forall y \leq t\ \neg A(y) \rightarrow \exists^{=0} y \leq tA(y)$. The translation works as follows:

$$\langle \forall y \leq t\ \neg A(y)\rangle_n \ \longrightarrow\ \langle \exists^{=0} y \leq t\ A(y)\rangle_n$$

is per definition

$$\bigwedge_{i=0}^{t(n)} \langle \neg A\rangle_{n,i} \ \longrightarrow\ C_{t(n)+1,0}(\langle A\rangle_{n,0}, \ldots, \langle A\rangle_{n,t(n)})$$

which by the definition of $C_{n,k}$ is

$$\bigwedge_{i=0}^{t(n)} \langle \neg A\rangle_{n,i} \ \longrightarrow\ \bigwedge_{i=0}^{t(n)} \neg\langle A\rangle_{n,i}.$$

This sequent has a proof of size polynomial in n since $t(n)$ is a polynomial and we apply the inference rules for introducing conjunctions left and right for $t(n)$ times starting from initial sequents of the form $B \longrightarrow B$. Since $\langle A\rangle_{n,i}$ has bounded depth, this proof has $\max_i \langle A\rangle_{n,i} + 1$ as an upper bound on its depth. The other axioms can be replaced by a short proof with said size and depth requirement in a similar manner.

For the induction step we consider all the possibilities of how the proof is structured:

1. The propositional inference rules of LK translate naturally, for example:

$$\frac{\Gamma, C \ \longrightarrow\ \Delta}{\Gamma \ \longrightarrow\ \Delta, \neg C}$$

   has the translation

$$\frac{\langle\Gamma\rangle, \langle C\rangle \ \longrightarrow\ \langle\Delta\rangle}{\langle\Gamma\rangle \ \longrightarrow\ \langle\Delta\rangle, \langle\neg C\rangle}$$

   which coincides with a propositional inference rule because $\langle \neg C\rangle = \neg\langle C\rangle$. Other inference rules like the introduction of conjunctions or disjunctions also translate naturally.

2. When the cut rule

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Pi \longrightarrow \Lambda}{\Gamma, \Pi \longrightarrow \Delta, \Lambda}$$

is applied with A being the cut formula, since $\langle A \rangle$ has bounded depth by the induction hypothesis, this proof step translates naturally into a cut with $\langle A \rangle$ being the cut formula.

3. For the bounded-quantifier inference rule $\forall$-right with a value assigned to the free variable a

$$\frac{a \leq t, \Gamma \longrightarrow \Delta, A(a)}{\Gamma \longrightarrow \Delta, \forall x \leq t A(x)}$$

translates to

$$\frac{\langle \Gamma \rangle \longrightarrow \langle \Delta \rangle, \langle A \rangle_{n,0} \qquad \ldots \qquad \langle \Gamma \rangle \longrightarrow \langle \Delta \rangle, \langle A \rangle_{n,t(n)}}{\langle \Gamma \rangle \longrightarrow \langle \Delta \rangle, \bigwedge_{i=0}^{t(n)} \langle A \rangle_{n,i}}$$

where the bottom line is the translation of

$$\langle \Gamma \rangle \longrightarrow \langle \Delta \rangle, \langle \forall y \leq t(x) A(x,y) \rangle_n.$$

This is a proof by applying the $\wedge$-right rule $t(n)$ times. By the induction hypothesis the formulas $\langle A \rangle_{n,i}$ have constant depth and therefore this proof has a constant upper bound on its depth.

4. Consider the $\exists$-left rule

$$\frac{a \leq t, A(a), \Gamma \longrightarrow \Delta}{\exists x \leq t A(x), \Gamma \longrightarrow \Delta}$$

which gets translated into

$$\frac{\langle A \rangle_{n,0}, \langle \Gamma \rangle \longrightarrow \langle \Delta \rangle \qquad \ldots \qquad \langle A \rangle_{n,t(n)}, \langle \Gamma \rangle \longrightarrow \langle \Delta \rangle}{\bigvee_{i=0}^{t(n)} \langle A \rangle_{n,i}, \langle \Gamma \rangle \longrightarrow \langle \Delta \rangle}$$

Where each of the $t(n)$ sequents on top has a proof thats polynomially bounded by the induction hypothesis. Therefore this proof consists of polynomially many proofs with polynomial size together with polynomially many applications of the $\vee$-left rule. The depth bound holds for the same reason as in the last case.

5. The $\forall$-left rule

$$\frac{A(s), \Gamma \longrightarrow \Delta}{s \leq t, \forall x \leq t A(x), \Gamma \longrightarrow \Delta}$$

translates in the case $s \leq t$ to

$$\frac{\langle A \rangle_{n,s}, \langle \Gamma \rangle \longrightarrow \langle \Delta \rangle}{\bigwedge_{i=0}^{t(n)} \langle A \rangle_{n,i}, \langle \Gamma \rangle \longrightarrow \langle \Delta \rangle}$$

by applying the $\wedge$-left rule polynomially many times. For $s > t$ the bottom sequent can be simplified to 1. The bound on the depth might increase by 1.

6. The $\exists$-right inference rule

$$\frac{\Gamma \longrightarrow \Delta, A(s)}{s \leq t, \Gamma \longrightarrow \Delta, \exists x \leq t A(x)}$$

translates in the case $s \leq t$ to

$$\frac{\langle \Gamma \rangle \longrightarrow \langle \Delta \rangle, \langle A \rangle_{n,s}}{\langle \Gamma \rangle \longrightarrow \langle \Delta \rangle, \bigvee_{i=0}^{t(n)} \langle A \rangle_{n,i}}$$

by applying the $\vee$-right inference rule polynomially many times. While the case $s > t$ can be simplified to 1 like we mentioned above.

7. The IND inference rule

$$\frac{A(y), \Gamma \longrightarrow \Delta, A(y+1)}{A(0), \Gamma \longrightarrow \Delta, A(x)}$$

translates to

$$\frac{\langle A(y) \rangle_0, \langle \Gamma \rangle \rightarrow \langle \Delta \rangle, \langle A(y+1) \rangle_0 \qquad \ldots \qquad \langle A(y) \rangle_{t-1}, \langle \Gamma \rangle \rightarrow \langle \Delta \rangle, \langle A(y+1) \rangle_{t-1}}{\langle A(y) \rangle_0, \langle \Gamma \rangle \rightarrow \langle \Delta \rangle, \langle A(y) \rangle_t}$$

by applying the Cut-Rule $t(n)$ times. By the induction hypothesis each of the sequents on top has a polynomial size proof therefore so does the sequent on the bottom. The same argument holds for the depth.

$\square$

Therefore by Theorem 5.2 and Lemma 5.1 it holds that FC_d p-simulates $I\Sigma_0^{1,b}$.

6 PHP in TC^0-Frege

Let $PHP(z, R)$ be the disjunction of the formulas

1. $\exists x \leq z+1 \forall y \leq z\ \neg R(x,y)$,
2. $\exists w \leq z+1 \exists u \neq v \leq z\ R(w,u) \wedge R(w,v)$,
3. $\exists u \neq v \leq z+1 \exists w \leq z\ R(u,w) \wedge R(v,w)$.

We will show $\neg(1) \wedge \neg(2) \rightarrow (3)$ by proving in $I\exists^{=}\Delta_0(R)$ the formulas

$$\exists^{=t+1} y \leq z \exists x \leq t\ R(x,y) \quad \text{and} \quad \exists^{=z+1} u \leq z\ u = u.$$

The former will be shown by induction on t. Because $\neg(1) \wedge \neg(2)$ means that R is the Graph of a function with domain $\{0, \ldots, z+1\}$ and image $\{0, \ldots, z\}$ we can prove for $t = 0$ the base case $\exists^{=1} y \leq z R(0,y)$. For the induction step since

$$|\{y \leq z : \exists x \leq t\ R(x,y)\}| = |\{x \leq t : \exists y \leq z\ R(x,y)\}|$$

holds, we show

$$\exists^{=t+1} x \leq t \exists y \leq z R(x,y) \rightarrow \exists^{=t+2} x \leq t+1 \exists y \leq z R(x,y).$$

Due to R defining the Graph of a function, $\exists y \leq z R(t+1, y)$ has a proof for appropriate t, which in combination with the second $\exists^{=}$ axiom yields a proof of the induction step. The IND axiom for $\exists^{=}\Delta_0$ formulas then yields a proof of the first formula.

The latter we show by induction on z. The base case $\exists^{=1} u \leq 0 : u = u$ follows from 0 being the smallest element in the linear order and using the first two axioms of the $\exists^{=}$ quantifier. A proof for the induction step consists of a proof of $z+1 = z+1$ and the second axiom of the $\exists^{=}$ quantifier. Since both the initial formula and the induction step formula are $\exists^{=}\Delta_0$ by the IND axiom we obtain a proof of $\exists^{=z+1} u \leq z\ u = u$.

The propositional translation PHP_n of $PHP(z-1, R)$ is the formula

$$\neg(\bigwedge_i \bigvee_j p_{ij} \wedge \bigwedge_i \bigwedge_{j \neq j'} (\neg p_{ij} \vee \neg p_{ij'}) \wedge \bigwedge_{i \neq i'} \bigwedge_j (\neg p_{ij} \vee \neg p_{i'j}))$$

for which by Theorem 5.2 we obtain:

Lemma 6.1. *The PHP_n formulas have polynomial-size TC^0-Frege proofs.*

7 Simulation of TC^0-Frege by Frege

What's left to be shown is that we can translate a FC proof to an F proof such that the new proof is polynomial in size. This is done by defining counting functions for Frege systems and showing that their main properties have polynomial size proofs.

The straightforward way of implementing addition and thus counting does not lead to formulas with polynomial size. Therefore carry-save addition is used, which is a technique for computing the sum of a vector of numbers with a logarithmic depth circuit. It can be used to compute the sum of n n-bit numbers by a propositional formula with polynomial size in n. This carry-save addition will be used to define the counting connectives $C_{n,k}(p_1, \ldots, p_n)$.

We will present the high level idea and refer the reader to [Krajíček, 2019, Chapter 11.3] for more details or [Buss, 1987, Chapter 4] for an in-depth description. Interpreting $p_1, \ldots, p_n$ as n one-bit numbers and using the $\log n$ bits $r_0, \ldots, r_{|n|-1}$ of the output of the carry save addition formula to define $\sum_i p_i$ we then get

$$C_{n,k}(p_1, \ldots, p_n) \equiv \bigwedge_{j \in K_0} \neg r_j \wedge \bigwedge_{j \in K_1} r_j$$

where K_0 and K_1 are the positions j where the bit of k is 0 or 1.

This polynomial simulation of TC^0-Frege by Frege implies the polynomial simulation of FC_d by Frege.

Lemma 7.1. *The size of formulas $C_{n,k}$ is polynomial in n and the axioms of FC have polynomial size Frege proofs.*

Combining Theorem 6.1 and Lemma 7.1 yields:

Corollary 7.1.1. *The PHP_n-formulas have polynomial size Frege proofs.*

References

Jan Krajíček. *Proof Complexity.* Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2019.

Stephen Cook and Phuong Nguyen. *Logical Foundations of Proof Complexity.* Cambridge University Press, 2010.

Samuel R. Buss. Polynomial size proofs of the propositional pigeonhole principle. *Journal of Symbolic Logic*, 52(4):916–927, December 1987.