Nisan–Wigderson generators in Proof Complexity: New lower bounds

Erfan Khaniki[*1,2]

[1]Faculty of Mathematics and Physics, Charles University
[2]Institute of Mathematics, Czech Academy of Sciences

February 19, 2022

Abstract

A map $g : \{0,1\}^n \to \{0,1\}^m$ ($m > n$) is a hard proof complexity generator for a proof system P iff for every string $b \in \{0,1\}^m \setminus \mathsf{Rng}(g)$, formula $\tau_b(g)$ naturally expressing $b \notin \mathsf{Rng}(g)$ requires superpolynomial size P-proofs. One of the well-studied maps in the theory of proof complexity generators is Nisan–Wigderson generator. Razborov [Raz15] conjectured that if A is a suitable matrix and f is a $\mathsf{NP} \cap \mathsf{CoNP}$ function hard-on-average for $\mathsf{P/poly}$, then $\mathsf{NW}_{f,A}$ is a hard proof complexity generator for Extended Frege. In this paper, we prove a form of Razborov's conjecture for AC^0-Frege. We show that for any symmetric $\mathsf{NP} \cap \mathsf{CoNP}$ function f that is exponentially hard for depth two AC^0 circuits, $\mathsf{NW}_{f,A}$ is a hard proof complexity generator for AC^0-Frege in a natural setting. As direct applications of this theorem, we show that:

1. For any f with the specified properties, $\tau_b(\mathsf{NW}_{f,A})$ based on a random b and a random matrix A with probability $1 - o(1)$ is a tautology and requires superpolynomial (or even exponential) AC^0-Frege proofs.

2. Certain formalizations of the principle $f_n \notin (\mathsf{NP} \cap \mathsf{CoNP})/\mathsf{poly}$ requires superpolynomial AC^0-Frege proofs.

These applications relate to two questions that were asked by Krajíček [Kra19].

1 Introduction

Proving superpolynomial lower bounds for every proof system is one of the ultimate goals in proof complexity. For this matter, we need to prove that for every proof system P, there exists an infinite family of tautologies $\{\phi_n\}_{n\in\mathbb{N}}$ such that P does not have polynomial-size proofs for $\{\phi_n\}_{n\in\mathbb{N}}$. It is known that some weak proof systems require superpolynomial (or even exponential) size proofs for some families of tautologies (see [Kra19] for more information). No superpolynomial lower bounds are known for strong proof systems such as Frege or Extended Frege. We do not even know superpolynomial lower bounds for $\mathsf{AC}^0(\oplus)$-Frege. It seems that one of the main issues in proving lower bounds is the lack of good candidate hard formulas. There are three prominent candidates of

---

*e.khaniki@gmail.com

formulas that are believed to be hard for any proof system. The first candidate of these formulas is random CNFs. Some experts believe that these formulas should be hard for any proof system (see [Kra19]). Another family of conjectured hard formulas is finite consistency statements. These formulas have tight connections to important conjectures in proof complexity and experts believed that they are hard for any proof system (For a detailed discussion, see [KP89, Pud17]). The third candidate is proof complexity generators.

1.1 Proof complexity generators

Let $g : \{0,1\}^n \to \{0,1\}^m$ $(m > n)$ be a function which is computable in a *reasonable low complexity class* such as $\mathsf{FP/poly}$. As $m > n$, $\{0,1\}^m \setminus \mathsf{Rng}(g)$ is nonempty. Let $b \in \{0,1\}^m \setminus \mathsf{Rng}(g)$, then as g is computable in $\mathsf{FP/poly}$, we can naturally express the true statement $b \notin \mathsf{Rng}(g)$ as a propositional formula which is denoted by $\tau_b(g)$. If for a proof system P, $\tau_b(g)$ requires superpolynomial size P-proofs for every $b \in \{0,1\}^m \setminus \mathsf{Rng}(g)$, then g is a hard proof complexity generator for P. The concept of proof complexity generators were defined independently by Alekhnovich *et. al.* [ABRW04] and Krajíček [Kra01a].

As pseudorandom generators are an important topic in computational complexity, Alekhnovich *et al.* [ABRW04] asked the following natural question: *which mappings $g : \{0,1\}^n \to \{0,1\}^m$ should be considered hard from the point of view of proof complexity?* To understand this concept, different mappings were investigated from different aspects in [ABRW04]. In particular, they investigated conditions that make a Nisan–Wigderson generator hard for proof systems such as Resolution and Polynomial Calculus.

Krajíček [Kra01a] investigated the hardness of different variants of the Pigeonhole principle in proof systems and their provability in related theories of bounded arithmetic. One of these variants is the dual weak Pigeonhole principle (dWPHP_{2n}^n) which says that for every function $g : [n] \to [2n]$, g cannot be onto. An interesting theory of bounded arithmetic is $\mathsf{BT} := \mathsf{S}_2^1 + \mathsf{dWPHP}(\mathsf{PV})$ which has several nice properties (see [Jeř04, Jeř07]). Here S_2^1 is the base bounded arithmetic theory in the Buss's Bounded arithmetic hierarchy which is related to the polynomial-time reasoning (see [Bus86]) and $\mathsf{dWPHP}(\mathsf{PV})$ consists of $\mathsf{dWPHP}_{2n}^n(f)$ for every polynomial-time computable function f. A natural question is whether S_2^1 and BT are actually the same theory. Krajíček introduced the concept of proof complexity generators as functions which violate $\mathsf{dWPHP}(\mathsf{PV})$ and formulated a conjecture about them in the setting of model theory of arithmetic that implies $\mathsf{S}_2^1 \neq \mathsf{BT}$ (see [Kra21] for a proof of separation of PV and $\mathsf{PV} + \mathsf{dWPHP}(\mathsf{PV})$ under a different assumption). Moreover, this conjecture implies that proof complexity generators are hard for Extended Frege.

Later, Krajíček [Kra01b, Kra04a, Kra04b, Kra05, Kra09, Kra11a, Kra11b] investigated proof complexity generators from different aspects, developed the theory of proof complexity generators in great length and proposed some conjectures. In particular, Krajíček [Kra11a] defined the generator $\mathsf{nw}_{n,c}$ based on the gadget generators of [Kra09] and conjectured that $\mathsf{nw}_{n,c}$ is a hard proof complexity generator for any proof system.

Razborov [Raz15] made a significant contribution to the lower bound problem for proof complexity generators. He proved that Nisan–Wigderson generators based on suitable matrices and suitable functions are hard not only for Resolution but also for k-DNF Resolution, which improved the previous lower bounds in terms of the stretch of the generator and the strength of the proof system in [ABRW04, Kra04b]. Moreover, he formulated the following intriguing conjecture:

Conjecture 1.1 *(Razborov [Raz15]) Any Nisan–Wigderson generator based on suitable matrices and any function in* NP ∩ CoNP *that is hard on average for* P/poly*, is hard for Extended Frege.*

Conjecture 1.1 initiated new investigations in the theory of proof complexity generators from different aspects. We refer the reader for comprehensive dissections of the conjectures about the proof complexity generators to read Chapter 30 of [Kra11a] and Section 19.4 of [Kra19].

Regarding Razborov's conjecture, Pich [Pic11] proved that this conjecture is true for proof systems that enjoy different forms of the feasible interpolation property.

The strongest argument that supports Conjecture 1.1 was done by Krajíček in [Kra11b]. He proved that assuming the existence of a function $f \in$ NP∩CoNP which is hard on average for P/poly; it is consistent with the universal theory PV that any Nisan–Wigderson generator based on f (or for a function closely related to f) and suitable matrices is hard not only for Extended Frege but also for any proof system. Note that PV is a fairly strong theory as it proves a reasonable fragment of computational complexity theorems (see [Pic15b] for more information). It is worth mentioning those investigations of the Nisan–Wigderson generators in proof complexity led to advancements in other areas as well, such as [Pic15a, PS21] which proved unprovability of circuit lower bounds in bounded arithmetic and [Pic20] which proved the existence of learning algorithms from circuit lower bounds.

Razborov's conjecture is inherently different from other conjectures in proof complexity that imply that strong proof systems are not p-bounded. The reason is that this conjecture describes a situation where *the hardness of computation implies the hardness of proof* for strong proof systems. For weak proof systems, such a relation exists, which is called *feasible interpolation property*. Krajíček defined this property in [Kra97] and proved that several proof systems such as Resolution have the feasible interpolation property, which implied lower bounds for new formulas. Proving lower bounds using feasible interpolation proved to be very fruitful and led to several lower bounds for different proof systems such as Cutting Planes [Pud97]. Unfortunately, this property does not hold for strong proof systems such as Extended Frege [KP98], and even AC^0-Frege [BDG$^+$04] assuming cryptographic hardness assumptions (for more information, see chapter 17 of [Kra19]). To overcome the barrier against the feasible interpolation property, different attempts were made to prove *hardness of computation implies hardness of proof* theorems for strong proof systems. Krajíček [Kra10] proved a form of feasible interpolation for AC^0-Frege that is different from the original definition of the feasible interpolation property. Moreover, he developed the method of *Forcing with random variables* in [Kra11a] intending to prove *hardness of computation to hardness of proofs* theorems for strong proof systems (bounded arithmetics) and proved types of this theorem for AC^0-Frege and $\mathsf{AC}^0(\oplus)$-Frege (for a finitary proof of the theorem for $\mathsf{AC}^0(\oplus)$-Frege see [Kra15]). Pudlák [Pud21] characterized the canonical disjoint NP-pairs of AC^0-Frege and proved a generalized feasible interpolation theorem for them.

1.2 Our results

This paper aims to find sufficient conditions that make a Nisan–Wigderson generator hard for proof systems such as AC^0-Frege. Our main contribution is the proof of Razborov's conjecture for AC^0-Frege in a natural setting which was not known before.

Theorem 1.1 *(Main theorem, informal version) Let $f \in$ NP ∩ CoNP be a symmetric function that requires $2^{n^{\Omega(1)}}$ depth two AC^0 circuits. Then for any $\Sigma_1^1 \cap \Pi_1^1$ pair (ϕ_0, ϕ_1) that defines f, any suitable*

matrix A, and any $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$, $\tau_b(\mathsf{NW}_{f,A})$ *requires superpolynomial (exponential)* AC^0*-Frege proofs when the Paris-Wilkie translation of* (ϕ_0, ϕ_1) *is used to form the formula* $\tau_b(\mathsf{NW}_{f,A})$.

Theorem 1.1 unconditionally implies that $\mathsf{NW}_{f,A}$ for suitable functions f (such as Parity or Majority) and suitable matrices A are hard proof complexity generators for AC^0-Frege even when the stretch is exponential. No lower bounds for Nisan–Wigderson generators were known for this system. It is worth noting that before this work, the only known hard proof complexity generators for AC^0-Frege, were the PHP-generator of [Kra09] and the more general generator $\mathsf{nw}_{n,c}$ of [Kra11a]. Moreover, Theorem 1.1 implies the following results:

1. For any f that satisfies the conditions of Theorem 1.1 such as Parity, the formula $\tau_b(\mathsf{NW}_{f,A})$ based on a random b and a random matrix A is a tautology with probability $1 - o(1)$ and requires superpolynomial (exponential) AC^0-Frege proofs.

2. Certain formalizations of the principle $f_n \notin (\mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k))/\mathsf{poly}$ requires superpolynomial AC^0-Frege proofs.

These results relate to two questions asked by Krajíček [Kra19] (problems 19.4.5 and 19.6.1). The first problem asks whether random linear generators (random systems of linear equations over $\mathbb{F}_2$) are hard for AC^0-Frege or not. The second problem asks whether linear generators are iterable for AC^0-Frege or not, which relates to the question of the hardness of proving the principle $f_n \notin \mathsf{SIZE}(n^k)$ in AC^0-Frege.

2 Preliminaries

2.1 Nisan–Wigderson generators

For the rest of the paper for any two real numbers $r_1 \leq r_2$, define $[r_1, r_2) := \{i \in \mathbb{N} : \lfloor r_1 \rfloor \leq i < \lceil r_2 \rceil\}$ and $[r_1, r_2] := \{i \in \mathbb{N} : \lfloor r_1 \rfloor \leq i \leq \lceil r_2 \rceil\}$.

Let $f : \{0,1\}^* \to \{0,1\}$ be a Boolean function. For a natural number n, f_n denotes the function f restricted to $\{0,1\}^n$. Let A be an $m \times n$ $0-1$ matrix such that each row of A has exactly l ones. Such a matrix is called an l-sparse matrix. For such a $m \times n$ l-sparse matrix A, $J_i(A) := \{j \in [0,n) : A_{i,j} = 1\}$.

For every pair (f, A) where f is a Boolean function and A is a $m \times n$ l-sparse matrix, Nisan and Wigderson [NW94] defined the generator $\mathsf{NW}_{f,A} : \{0,1\}^l \to \{0,1\}^m$ as follows:

- For every input $a \in \{0,1\}^l$, the i'th bit of the output of $\mathsf{NW}_{f,A}(a)$ is $f(a|J_i(A))$.

It was proved in the seminal paper [NW94] that if f is a hard function (depending on the application) and A satisfies specific combinatorial properties, then $\mathsf{NW}_{f,A}$ is a *good* pseudorandom generator (depending on the parameters).

Let $f \in \mathsf{NP} \cap \mathsf{CoNP}$. A pair of propositional formulas $(\sigma_0(\mathbf{p}, \mathbf{q}), \sigma_1(\mathbf{p}, \mathbf{r}))$ is a representation of f_n for a natural number n iff:

1. $|\mathbf{p}| = n$ and moreover $\mathbf{p}$, $\mathbf{q}$, and $\mathbf{r}$ variables are disjoint.

2. (σ_0, σ_1) defines the function f_n which means:

   (a) $\neg\sigma_0 \vee \neg\sigma_1$ is a tautology.

(b) For every $a \in \{0,1\}^n$, $f(a) = i$ iff $\sigma_i(a, \mathbf{t})$ is satisfiable where $i \in [0, 2)$.

Note that as $f \in \mathsf{NP} \cap \mathsf{CoNP}$, for every n, f_n has a representation.

Suppose $f \in \mathsf{NP} \cap \mathsf{CoNP}$, (σ_0, σ_1) is a representation for f_l, and A is a $m \times n$ l-sparse matrix. Then for any $b \in \{0,1\}^m$, $\tau_b(\mathsf{NW}_{f,A})$ based on (σ_0, σ_1) is the following propositional formula:

$$\bigvee_{b_i=1} \neg\sigma_1(\mathbf{p}|J_i(A), \mathbf{q}_i) \vee \bigvee_{b_i=0} \neg\sigma_0(\mathbf{p}|J_i(A), \mathbf{q}_i)$$

where $\mathbf{q}_i$'s are disjoint variables. Note that if $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$, then $\tau_b(\mathsf{NW}_{f,A})$ is tautology.

As it was discussed in previous works [ABRW04, Kra05, Raz15, Kra11b], $\mathsf{NW}_{f,A}$ can be a hard proof complexity generator for a proof system P for the following four reasons:

- The complexity of f.

- The properties that A satisfies.

- The representation of f that is used in the formula $\tau_b(\mathsf{NW}_{f,A})$.

- The string $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$.

As we will see, our main result also imposes different conditions on $\tau_b(\mathsf{NW}_{f,A})$ to make sure that it requires long proofs.

The following parts explain the properties that we need for the matrices and representations to prove our theorems.

2.1.1 Representations

The hardness of $\tau_b(\mathsf{NW}_{f,A})$ can depend on the pair (σ_0, σ_1) that is used in it. This matter has been investigated in [ABRW04] and they examined different representations. Recently, Sokolov [Sok21] answered one of the open problems that was stated about a representation of $\tau_b(\mathsf{NW}_{f,A})$ in [ABRW04].

$\Sigma_1^1 \cap \Pi_1^1$ representation

Let $\mathcal{L}$ be a finite relational language and X be a unary relational symbol which is not in $\mathcal{L}$. A Σ_1^1 formula $\psi(X)$ in the language $\mathcal{L} \cup \{X\}$ with equality defines a function $f \in \mathsf{NP}$ iff:

1. $\psi := \exists \bar{Y} \phi(X, \bar{Y})$ where $\phi(X, \bar{Y})$ is a first order formula in the language $\mathcal{L} \cup \{X\}$ with equality.

2. X is not in $\bar{Y}$.

3. For every n, every $a \in \{0,1\}^n$, $f_n(a) = 1$ iff $([0, n), a) \models \psi(X)$ when X is interpreted by a.

Fagin's theorem [Fag74] directly implies that for every symmetric $f \in \mathsf{NP}$, a Σ_1^1 formula $\psi_f(X)$ exists in a language $\mathcal{L} \cup \{X\}$ that defines f. Therefore, the set of functions that are Σ_1^1 definable is exactly symmetric NP and hence this set is quite rich. As an example, we explain how the negation of Parity function can be defined as a Σ_1^1 formula. Let $\mathcal{L} = \{Y\}$ where Y is a binary relation symbol. Then

$$\bar{\oplus}(X, Y) := \forall i \, (X(i) \rightarrow \exists j (j \neq i \wedge X(j) \wedge Y(i,j) \wedge Y(j,i) \wedge \forall k (k = i \vee \neg Y(i,k) \vee j = k)).$$

5

Then $\psi_{\bar{\oplus}}(X) := \exists Y \bar{\oplus}(X, Y)$ defines the negation of Parity function (parity of $a \in \{0, 1\}^n$ is 0 iff the number of 1's in a is even).

The class of Σ_1^1 formulas is a natural and important class in finite model theory and descriptive complexity. Moreover, this class has appeared in different places in proof complexity, too (for example, see [Kra10]).

To prove Theorem 1.1, the following lemma is needed. If A is a set and Q is a relation on it, i.e. $Q \subseteq A^k$ for some k, and $h : A \to A$ is a function, then $h(Q) := \{(h(a_1), ..., h(a_k)) : (a_1, ..., a_k) \in A^k\}$.

Lemma 2.1 *Let $\mathcal{L} = \{Y_0, ..., Y_k\}$ be a finite relational language and $\mathcal{A}_0 = (A, \{Q_0^0, ..., Q_k^0\})$ be an $\mathcal{L}$-structure. Let h be a bijective function from A onto A. Consider the $\mathcal{L}$-structure $\mathcal{A}_1 := (A, \{Q_0^1, ..., Q_k^1\})$ where $Q_i^1 = h(Q_i^0)$, for every $i \in [0, k]$. Then for every first-order formula $\phi(x_0, ..., x_p)$ in $\mathcal{L}$ with equality, every $(a_0, ..., a_p) \in A^p$:*

$$\mathcal{A}_0 \models \phi(a_0, ..., a_p) \Leftrightarrow \mathcal{A}_1 \models \phi(h(a_0), ..., h(a_p)).$$

Proof. This lemma can be proved by induction on the complexity of ϕ. ∎

Let $\exists \bar{Y} \phi(X, \bar{Y})$ be a Σ_1^1 formula. Then for any n, the Paris–Wilkie translation [PW85] (see also Section 8.2 of [Kra19]) of $\phi^{<n}(X, \bar{Y})$ ($\phi^{<n}$ is ϕ when every first order quantifier is bounded by n) is denoted by $\langle \phi \rangle_n(\mathbf{p}, \mathbf{q})$ which is a constant depth formula (without loss of generality we can assume that it is a CNF using extension variables). The number n indicates the size of the universe in which $\phi(X, Y)$ has been considered. For example the Paris-Wilkie translation of $\bar{\oplus}(X, Y)$ in the universe of size n is

$$\langle \bar{\oplus}(X, Y) \rangle_n := \bigwedge_{i=0}^{n-1} \left(\neg p_i \vee \bigvee_{j=0, j \neq i}^{n-1} \left(p_j \wedge q_{i,j} \wedge q_{j,i} \wedge \bigwedge_{k=0, k \neq i, k \neq j}^{n-1} \neg q_{i,k} \right) \right).$$

Let $f \in \mathsf{NP} \cap \mathsf{CoNP}$ be a symmetric function. Then a pair of Σ_1^1 formulas $(\exists \bar{Y} \phi_0(X, \bar{Y}), \exists \bar{Z} \phi_1(X, \bar{Z}))$ defines f iff:

1. $\exists \bar{Y} \phi_1(X, \bar{Y})$ defines f.

2. $\exists \bar{Z} \phi_0(X, \bar{Z})$ defines $\neg f$.

Such a pair is called a $\Sigma_1^1 \cap \Pi_1^1$ definition of f. Moreover, for any n, $(\langle \phi_0 \rangle_n, \langle \phi_1 \rangle_n)$ is a representation of f_n. For the sake of easiness, by $\langle \psi \rangle_n$ we mean $\langle \phi \rangle_n$ where $\psi(X) := \exists \bar{Y} \phi(X, \bar{Y})$ is a Σ_1^1 formula.

2.2 Proof systems

We assume the reader knows the basic facts about proof complexity, proof systems, and bounded arithmetics (for a detailed discussion, see [Kra19, Kra95]). Here we state some useful facts about AC^0-Frege, which will be used in the results.

2.2.1 AC^0-Frege

AC^0-Frege is the name for a family of proof systems that work with constant-depth de morgan formulas. For each $d \geq 1$, F_d denotes AC^0-Frege proof system of depth d.

To prove Theorem 1.1, we need some known relations between AC^0-Frege and V_1^0, which is a two-sorted bounded arithmetic (see [Bus86, Kra95]). These relations are related to the model theory of V_1^0.

Let $\mathcal{M}$ be an arbitrary nonstandard model of true arithmetic and $n \in \mathcal{M} \setminus \mathbb{N}$. Then

$$\mathcal{M}_n := \{a \in \mathcal{M} : \text{There exists a } b \in \mathcal{M} \setminus \mathbb{N} \text{ such that } a < 2^{n^{1/b}}\}.$$

The following theorems explain the relationship between AC^0-Frege and V_1^0 from the point of view of proof complexity.

For a set A, $\mathcal{P}(A)$ denotes the power set of A.

Theorem 2.2 *([Kra95]) Let $(\mathcal{M}, \chi) \models \mathsf{V}_1^0$ and $\sigma \in \chi$ be a constant depth propositional formula (depth of σ is standard). If $\neg\sigma$ is satisfiable by an assignment in χ, then for every standard d, there is no F_d-proof of σ in $(\mathcal{M}, \chi)$.*

Note that Theorem 2.2 also holds in the case where σ is the Paris-Wilkie translation of a bounded arithmetical formula such as $\phi(x, \bar{R})$ ($\sigma = \langle \phi(n, \bar{R}) \rangle_n$ for some $n \in \mathcal{M}$), i.e. if there is an $\bar{\alpha} \in \chi$ such that $(\mathcal{M}, \chi) \models \neg\phi(n, \bar{\alpha})$, then $\neg\sigma$ is satisfiable by an assignment from χ and therefore it does not have any F_d-proof in $\mathcal{M}$.

Theorem 2.3 *([Kra95]) Let $\mathcal{M}$ be a countable nonstandard model of true arithmetic and $\phi(x, R)$ be a bounded arithmetical formula such that for every d, the family $\{\langle \phi(n, R) \rangle_n\}_{n \in \mathbb{N}}$ requires exponential F_d-proofs. Then for every $m \in \mathcal{M} \setminus \mathbb{N}$, there exists a $\chi \subseteq \mathcal{P}(\mathcal{M}_m)$ such that:*

1. *Every bounded subset of $\mathcal{M}_m$ which is definable in $\mathcal{M}$ is in χ.*

2. *$(\mathcal{M}_m, \chi) \models \mathsf{V}_1^0$.*

3. *There is an $\alpha \in \chi$ such that $(\mathcal{M}_m, \chi) \models \neg\phi(m, \alpha)$.*

3 Razborov's conjecture for AC^0-Frege

In this section, we estate the main result of the paper. Let $\mathsf{S}_{\mathsf{AC}_2^0}$ denote the depth two AC^0 circuit complexity of functions, then:

Theorem 3.1 *Let $f \in \mathsf{NP} \cap \mathsf{CoNP}$ be a symmetric function such that $\mathsf{S}_{\mathsf{AC}_2^0}(f) = 2^{n^{\Omega(1)}}$ and (ϕ_0, ϕ_1) be a $\Sigma_1^1 \cap \Pi_1^1$ definition of f. Then for every d:*

1. *For every positive $c \in \mathbb{N}$, every $0 < \varepsilon < 1$, every large enough n, every $n^c \times n \lfloor n^\varepsilon \rfloor$-sparse matrix A, any $b \notin \mathsf{Rng}$, $\tau_b(\mathsf{NW}_{f,A})$ based on $(\langle \phi_0 \rangle_{\lfloor n^\varepsilon \rfloor}, \langle \phi_1 \rangle_{\lfloor n^\varepsilon \rfloor})$ does not have sub-exponential F_d-proofs.*

2. *For every positive $r \in \mathbb{N}$, every large enough s, every $t \in [s/r, s]$, every large enough n, every $2^n \times n^s$ n^t-sparse matrix A, $\tau_b(\mathsf{NW}_{f,A})$ based on $(\langle \phi_0 \rangle_{n^t}, \langle \phi_1 \rangle_{n^t})$ does not have polynomial size F_d-proofs.*

We prove this theorem in Section 4. This theorem is proved by a model-theoretic argument based on the relations explained in Preliminaries in combination with the hardness of the Pigeonhole principle in AC^0-Frege. Model theoretic arguments have been used previously in proof complexity and they were very fruitful (for example see [Ajt94, Kra01a, Kra10] and [Kra95] for a detailed explanation). See [Woo97, Kra01b] for discussions about the importance and benefits of the model-theoretic arguments (and in general, the logical point of view) in proof complexity.

Note that an immediate consequence of Theorem 3.1 is that $\mathsf{NW}_{f,A}$ based on a hard enough function f with suitable parameters is a hard proof complexity generator for AC^0-Frege. As the Parity function or the Majority function satisfies the required assumptions of Theorem 3.1, we get that NW-generators based on these functions are hard proof complexity generators for AC^0-Frege.

4   Proof of Theorem 3.1

In this section, we prove Theorem 3.1. We state the proof as a series of lemmas for more clarity. We prove the second part of this theorem. The first part can be proved in the same way. For the rest of the paper, $[n] := [0, n)$.

Lemma 4.1 *Let $f : \{0,1\}^* \to \{0,1\}$ be a symmetric Boolean function such that $\mathsf{S}_{\mathsf{AC}^0_2}(f_n) = \Omega(2^{n^\epsilon})$ for an $\epsilon > 0$. Then there is a natural m such that for every $n \geq m$ there is natural number $u \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that*

$$f_n(1^u 0^{n-u}) \neq f_n(1^{u+1} 0^{n-u-1}).$$

Proof. Let $g : \{0,1\}^n \to \{0,1\}$ be a symmetric function. If there exists a $r \leq n/2$ such that for every $r \leq k \leq n - r$, $g(1^k 0^{n-k}) = 0$, then

$$\mathsf{S}_{\mathsf{DNF}}(g) \leq 2n \cdot \sum_{i=0}^{r} \binom{n}{i} \leq 2n(\frac{en}{r})^r$$

where $\mathsf{S}_{\mathsf{DNF}}$ denotes the DNF complexity of functions. Writing this inequality (1) for f_n, we get $c2^{n^\epsilon} \leq 2n(\frac{en}{r})^r$ for a $c > 0$. So if we put $r = n^\delta$ and rewriting this inequality we have

$$c2^{n^\epsilon} \leq 2n(en^{1-\delta})^{n^\delta} \leq 2e^{n^\delta} n^{1+n^\delta} \leq 2n^{1+2n^\delta} = 2^{(2n^\delta+1)\log n+1}.$$

So assuming $\delta = \epsilon/2$, we have $(2n^\delta + 1)\log n + 1 = o(n^\epsilon)$. Therefore for every large enough n, there exists a $v \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that $f_n(1^v 0^{n-v}) = 1$. Following the same argument for $\neg f_n$, we can deduce that for every large enough n, there exists a $v' \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that $\neg f_n(1^{v'} 0^{n-v'}) = 1$. So we have found $v, v' \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that $f_n(1^v 0^{n-v}) \neq f_n(1^{v'} 0^{n-v'})$, hence there exists a $u \in [n^{\epsilon/2}, n - n^{\epsilon/2}]$ such that

$$f_n(1^u 0^{n-u}) \neq f_n(1^{u+1} 0^{n-u-1}).$$

∎

Now let $\mathcal{M}$ be a countable nonstandard model of true arithmetic. Let n, s, t, A, b be arbitrary elements of $\mathcal{M}$ such that:

1. $n, t \in \mathcal{M} \setminus \mathbb{N}$.

2. $A \in \mathcal{M} \setminus \mathbb{N}$ encodes a $2^n \times n^s$ n^t-sparse matrix where $t \in [s/r, s]$, $n^s < 2^n$, and $n^s 2^n \leq 2^{n^{t/u}}$ for a nonstandard u.

3. $b \in \mathcal{M} \setminus \mathbb{N}$ is a binary string of length 2^n such that $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$.

Let χ be the set of all bounded subset of $\mathcal{M}_{n^t}$ encoded in $\mathcal{M}$. So in particular $A, b \in \chi$.

As $\mathsf{S}_{\mathsf{AC}_2^0}(f_m) = 2^{m^{\Omega(1)}}$, there is a standard rational $\varepsilon > 0$ such that $\mathsf{S}_{\mathsf{AC}_2^0}(f_m) = \Omega(2^{m^\varepsilon})$. Let $\delta := \epsilon/2$, then there exists $u \in [n^{\delta t}, n^t - n^{\delta t}]$ that is guaranteed to exist by Lemma 4.1 for f_{n^t}. Let $v := \min\{u, n^t - u\}$, then

Lemma 4.2 *There exists a binary string $\alpha \in \chi$ of length n^s such that for every $i \in [2^n]$,*

$$\#_1(\alpha|J_i(A)) \in [v(1 - \frac{1}{\sqrt[3]{v}}), v(1 + \frac{1}{\sqrt[3]{v}})]$$

where $\#_s(w)$ is the number of occurrences of symbol s in the string w.

Proof. Let $X_0, ..., X_{n^s-1}$ be independent random variables taking values in $\{0, 1\}$ such that for every i, $Pr[X_i = 1] = \frac{v}{n^t}$. For every $i \in [2^n]$, let $Y_i = \sum_{j \in J_i(A)} X_j$ and hence $\mathbb{E}[Y_i] = v$. By the Chernoff bound we have the following inequalities for every $i \in [2^n]$:

1. $Pr[Y_i \leq v(1 - \frac{1}{\sqrt[3]{v}})] \leq e^{-\frac{\sqrt[3]{v}}{2}}$.

2. $Pr[Y_i \geq v(1 + \frac{1}{\sqrt[3]{v}})] \leq e^{-\frac{\sqrt[3]{v}}{3}}$.

Let X' be the concatenation of $X_0, ..., X_{n^s-1}$, hence it is a random string of length of n^s. Now combining the above inequalities with the union bound we get:

$$\mathbf{P} = Pr\left[\bigvee_{i=0}^{2^n-1} \#_1\left(X'|J_i(A)\right) \notin [v(1 - \frac{1}{\sqrt[3]{v}}), v(1 + \frac{1}{\sqrt[3]{v}})]\right] \leq$$

$$\sum_{i=0}^{2^n-1} Pr\left[\#_1\left(X'|J_i(A)\right) \notin [v(1 - \frac{1}{\sqrt[3]{v}}), v(1 + \frac{1}{\sqrt[3]{v}})]\right] \leq$$

$$\sum_{i=0}^{2^n-1} \left(Pr[Y_i \leq v(1 - \frac{1}{\sqrt[3]{v}})] + Pr[Y_i \geq v(1 + \frac{1}{\sqrt[3]{v}})]\right) \leq$$

$$2^n \cdot 2e^{-\frac{\sqrt[3]{v}}{3}}.$$

We know that $v \geq n^{\delta t}$, t is a nonstandard number, and δ is a standard rational, so

$$n + 1 < \frac{n^{\delta t/3}}{3} \leq \frac{\sqrt[3]{v}}{3}$$

which implies $2^n \cdot 2e^{-\frac{\sqrt[3]{v}}{3}} < 1$, and hence $\mathbf{P} < 1$. This implies that there exists a string $\alpha \in \chi$ that satisfies the desired property. $\blacksquare$

Lemma 4.3 *The following functions exist in χ:*

1. $\gamma : [2^n] \to [n^t + 1]$ such that for every $i \in [2^n]$, $\gamma(i) = \#_1(\alpha | J_i(A))$.

2. $\omega : [2^n] \times [n^t] \to [n^t]$ such that for every $i \in [2^n]$, $\omega(i, .)$ defines a permutation over $[n^t]$ and moreover $\beta_j = \left(\alpha | J_i(A)\right)_{\omega(i,j)}$ where $\beta = 1^{\gamma(i)} 0^{n^t - \gamma(i)}$.

Proof. 1. The function γ exists in $\mathcal{M}$. To prove that γ is in χ, we observe that encoding of γ as a binary string requires at most $c2^n \cdot \log n^t$ (for some $c \in \mathbb{N}$) which is less than $2^{n^{\sqrt{t}}}$, hence $\gamma \in \chi$.

2. Like the previous part, ω exists in $\mathcal{M}$, and its bit representation requires at most $c2^n \cdot n^t \log n^t$ (for some $c \in \mathbb{N}$) which is again less than $2^{n^{\sqrt{t}}}$, and therefore $\omega \in \chi$.

$\blacksquare$

To continue the proof, we need the celebrated result about the hardness of the Pigeonhole principle for AC^0-Frege.

Theorem 4.4 *([Ajt94, KPW95, PBI93]) For any natural number d, there exists an $\varepsilon_d > 0$ such that for large values of n, any F_d-proof of PHP_n^{n+1} has size at least $2^{\Omega(n^{\varepsilon_d})}$.*

Now let $l = \lfloor \sqrt[4]{v} \rfloor$, then we have the following lemma.

Lemma 4.5 *There exists $\chi' \subseteq \mathcal{P}(\mathcal{M}_{n^t})$ such that:*

1. $\chi \subseteq \chi'$.

2. *There exists a function $\sigma \in \chi'$ such that σ is a bijection from $[l]$ onto $[l-1]$.*

3. $(\mathcal{M}_{n^t}, \chi') \models \mathsf{V}_1^0$.

Proof. By Theorem 4.4 we know that PHP_{m-1}^m requires exponential size F_d-proofs for every d. Therefore by Theorem 2.3, there exists a $\chi' \subseteq \mathcal{P}(\mathcal{M}_l)$ such that every bounded subset of $\mathcal{M}_l$ is in χ', $(\mathcal{M}_l, \chi') \models \mathsf{V}_1^0$ and there exists a $\sigma \in \chi'$ such that it is bijection from $[l]$ onto $[l-1]$. Note that if $a \in \mathcal{M}_{n^t}$, then there exists a $b \in \mathcal{M} \setminus \mathbb{N}$ such that $a < 2^{n^{t/b}}$. Let $b' = \lfloor \frac{\delta b}{4} \rfloor$, then $a < 2^{l^{1/b'}}$ as we know $l \geq n^{\delta t/4}$. This implies that $\mathcal{M}_l = \mathcal{M}_{n^t}$, and moreover $\chi \subseteq \chi'$ which completes the proof. $\blacksquare$

The following lemma shows that we can simultaneously falsify some weak Pigeonhole principle instances.

Lemma 4.6 *There exists a function $F : [2^n] \times \{-1, 0, 1\} \times [n^t] \to [n^t]$ in χ' such that for every $i \in [2^n]$*

1. $F(i, a, .)$ *restricted to $[v + a]$, is a bijection from $[v + a]$ onto $[\gamma(i)]$.*

2. $F(i, a, .)$ *restricted to $[v + a, n^t)$, is a bijection from $[v + a, n^t)$ onto $[\gamma(i), n^t)$.*

Proof. Let $g \in \chi'$ be the function that Lemma 4.5 provides. Let

1. $w_{i,a} = |\gamma(i) - v - a|$.

2. $M_{i,a} = \max\{v + a, \gamma(i)\}$.

3. $m_{i,a} = \min\{v + a, \gamma(i)\}$.

Then we define the function $G_0(i, a, b)$ as follows:

$$G_0(i, a, b) := \begin{cases} \sigma(b - lk) + (l-1)k & b \in [lk, l(k+1)) \wedge k \in [w_{i,a}] \\ b - w_{i,a} & b \in [lw_{i,a}, M_{i,a}) \end{cases}$$

where $i \in [2^n]$, $a \in \{-1, 0, 1\}$, and $b \in [M_{i,a}]$.

Note that $v - 1 \le M_{i,a}$, hence

$$w_{i,a} \le \frac{v-1}{\sqrt[4]{v}} \le \frac{v-1}{l} \le \frac{M_{i,a}}{l}$$

as $w_{i,a} \le \sqrt[3]{v^2} + 1$ by Lemma 4.2. So $G_0(i, a, .)$ is a bijection from $[lw_{i,a}]$ onto $[(l-1)w_{i,a}]$ and moreover is a bijection from $[lw_{i,a}, M_{i,a})$ onto $[(l-1)w_{i,a}, m_{i,a})$ as

$$M_{i,a} - lw_{i,a} = m_{i,a} - (l-1)w_{i,a}.$$

Therefore the conclusion is that $G(i, a, .)$ is a bijection from $[M_{i,a}]$ onto $[m_{i,a}]$ for every $i \in [2^n]$ and $a \in \{-1, 0, 1\}$. Now, we define the function $G_1(i, a, b)$ as the inverse of G_0 which means that

$$G_1(i, a, G_0(i, a, b)) = b$$

where $i \in [2^n]$, $a \in \{-1, 0, 1\}$, and $b \in [M_{i,a}]$. So $G_1(i, a, .)$ is a bijection from $[m_{i,a}]$ onto $[M_{i,a}]$.

Using G_0 and G_1, we can fulfill (1) from the lemma. Now we want to construct two other functions H_0 and H_1 to fulfill (2).

The task is to define $H_0(i, a, .)$ as a function that defines a bijection from $[\max\{n^t - v - a, n^t - \gamma(i)\}]$ onto $[\min\{n^t - v - a, n^t - \gamma(i)\}]$ where $i \in [2^n]$ and $a \in \{-1, 0, 1\}$ and moreover H_1 would be the inverse of H_0. Let

1. $M'_{i,a} = \max\{n^t - v - a, n^t - \gamma(i)\}$.

2. $m'_{i,a} = \min\{n^t - v - a, n^t - \gamma(i)\}$.

Then we define $H_0(i, a, b)$ as follows:

$$H_0(i, a, b) := \begin{cases} \sigma(b - lk) + (l-1)k & b \in [lk, l(k+1)) \wedge k \in [w_{i,a}] \\ b - w_{i,a} & b \in [lw_{i,a}, M'_{i,a}) \end{cases}$$

where $i \in [2^n]$, $a \in \{-1, 0, 1\}$, and $b \in [M'_{i,a}]$.

Note that $n^t - v - 1 \le M'_{i,a}$ and moreover $v \le n^t/2$, therefore $n^t/2 - 1 \le M'_{i,a}$. This implies that

$$w_{i,a} \le \sqrt[3]{v^2} + 1 \le \sqrt[3]{(n^t/2)^2} + 1 \le \sqrt[4]{(n^t/2)^3} - 1 \le \frac{n^t/2 - 1}{\sqrt[4]{n^t/2}} \le \frac{n^t/2 - 1}{\sqrt[4]{v}} \le \frac{n^t/2 - 1}{l} \le \frac{M'_{i,a}}{l}.$$

Therefore $H_0(i, a, .)$ is a bijection from $[lw_{i,a}]$ onto $[(l-1)w_{i,a}]$ and moreover is a bijection $[lw_{i,a}, M'_{i,a})$ onto $[(l-1)w_{i,a}, m'_{i,a})$. Hence $H_0(i, a, .)$ is a bijection from $[M'_{i,a}]$ onto $[m'_{i,a}]$ for every $i \in [2^n]$ and $a \in \{-1, 0, 1\}$. Now we define the function $H_1(i, a, b)$ as the inverse again as follows:

$$H_1(i, a, H_0(i, a, b)) = b$$

where $i \in [2^n]$, $a \in \{-1, 0, 1\}$, and $b \in [M'_{i,a}]$. Hence $H_1(i, a, .)$ is a bijection from $[m'_{i,a}]$ onto $[M'_{i,a}]$. Now $F(i, a, b)$ is:

$$
F(i, a, b) := \begin{cases}
G_0(i, a, b) & b \in [v + a] \wedge v + a = M_{i,a} \\
G_1(i, a, b) & b \in [v + a] \wedge v + a = m_{i,a} \\
H_0(i, a, b - v - a) & b \in [v + a, n^t) \wedge n^t - v - a = M'_{i,a} \\
H_1(i, a, b - v - a) & b \in [v + a, n^t) \wedge n^t - v - a = m'_{i,a}
\end{cases}
$$

As G_0, G_1, H_0, H_1 are definable by a bounded arithmetical formula based on γ and σ, therefore F is also definable by a bounded arithmetical formula based on γ and σ and this implies that $F \in \chi'$ as $(\mathcal{M}_{n^t}, \chi') \models V_1^0$. ∎

Without the loss of generality we can assume $f_{n^t}(1^u 0^{n^t - u}) = 0$. Consider the following relations in χ:

1. $\theta_0 = 1^u 0^{n^t - u}$.

2. $\theta'_0 = 0^{n^t - u} 1^u$.

3. $\theta_1 = 1^{u+1} 0^{n^t - u - 1}$.

4. $\theta'_1 = 0^{n^t - u - 1} 1^{u+1}$.

5. $\bar{\lambda}_0$ such that $\phi_0(\theta_0, \bar{\lambda}_0)$ holds in $(\mathcal{M}_{n^t}, \chi)$.

6. $\bar{\lambda}'_0$ such that $\phi_0(\theta'_0, \bar{\lambda}'_0)$ holds in $(\mathcal{M}_{n^t}, \chi)$.

7. $\bar{\lambda}_1$ such that $\phi_1(\theta_1, \bar{\lambda}_1)$ holds in $(\mathcal{M}_{n^t}, \chi)$.

8. $\bar{\lambda}'_1$ such that $\phi_1(\theta'_1, \bar{\lambda}'_1)$ holds in $(\mathcal{M}_{n^t}, \chi)$.

Now we are ready to describe the assignments $\mathcal{X}$, $\{\bar{\mathcal{Y}}_i\}_{i \in [2^n]}$, and $\{\bar{\mathcal{Z}}_i\}_{i \in [2^n]}$ such that

$$
(\mathcal{M}_{n^t}, \chi') \models \forall i < 2^n \left(b_i = 0 \rightarrow \phi_0(\mathcal{X}|J_i(A), \bar{\mathcal{Y}}_i) \right) \wedge \left(b_i = 1 \rightarrow \phi_1(\mathcal{X}|J_i(A), \bar{\mathcal{Z}}_i) \right)
$$

which implies that $\tau_b(\mathsf{NW}_{f,A})$ based on $(\langle \phi_0 \rangle_{n^t}, \langle \phi_1 \rangle_{n^t})$ fails under an assignment in $(\mathcal{M}_{n^t}, \chi')$. We define these assignments as follows:

1. If $u = v$:

   (a) $\mathcal{X} = \alpha$.
   (b) $\bar{\mathcal{Y}}_i = \omega(i, F(i, 0, \bar{\lambda}_0))$.
   (c) $\bar{\mathcal{Z}}_i = \omega(i, F(i, 1, \bar{\lambda}_1))$.

2. If $u = n^t - v$:

   (a) $\mathcal{X}$ is the complement of α, i.e., $\mathcal{X}_j = 1 - \alpha_j \; j \in [n^s]$.
   (b) $\bar{\mathcal{Y}}_i = \omega(i, F(i, 0, \bar{\lambda}'_0))$.
   (c) $\bar{\mathcal{Z}}_i = \omega(i, F(i, -1, \bar{\lambda}'_1))$.

Without loss of generality assume $v = u$. Then for an arbitrary $i \in [2^n]$, we know that

$$\mathcal{X}|J_i(A) = \omega(i, F(i, 0, \theta_0)),$$

hence $\sigma_0(\mathcal{X}|J_i(A), \bar{\mathcal{Y}}_i)$ holds by Lemma 2.1 as $\omega(i, F(i, 0, .))$ is a bijection from $[n^t]$ onto itself and the fact that $\sigma_0(\theta_0, \bar{\lambda}_0)$ holds. The same argument works for $\sigma_1(\mathcal{X}|J_i(A), \bar{\mathcal{Z}}_i)$. Moreover if $v = n^t - u$, the same argument works by using $\theta_0', \theta_1', \bar{\lambda}_0', \bar{\lambda}_1'$.

To complete the proof, we argue as follows. Suppose the statement of the theorem is not true. This means that there exist standard d and r such that the following arithmetical sentence is true in $\mathbb{N}$:

- $\mathbf{H} := \forall s_1 \exists s \geq s_1, \exists t \in [s/r, s], \exists c > 0, \forall m, \exists n > m \exists\ 2^n \times n^s\ n^t$-sparse matrix A, $\exists b \notin$ $\mathsf{Rng}(\mathsf{NW}_{f,A})$, $\exists\ \mathsf{F}_d$-proof π for $\tau_b(\mathsf{NW}_{f,A})$ such that $|\pi| \leq |\tau_b(\mathsf{NW}_{f,A})|^c$.

Let $\mathcal{M}$ be a countable nonstandard model of true arithmetic. This means that $\mathcal{M} \models \mathbf{H}$. To simplify the presentation let

$$\mathbf{H} := \forall s_1 \exists s, t, c \forall m \exists n, A, b, \pi \Phi(s_1, s, t, c, m, n, A, b, \pi).$$

Let $s_1 \in \mathcal{M} \setminus \mathbb{N}$, then there exist $s, t \in \mathcal{M} \setminus \mathbb{N}$ and $c \in \mathcal{M}$ such that

$$\mathcal{M} \models \forall m \exists n, A, b, \pi \Phi(s_1, s, t, c, m, n, A, b, \pi).$$

We choose an $m \in \mathcal{M} \setminus \mathbb{N}$ such that for all $m_1 \geq m$, $m_1^{ct} 2^{cm_1} \leq 2^{m_1^{\sqrt{t}/2}}$, hence there exist an $n > m$, a $2^n \times n^s\ n^t$-sparse matrix $A \in \mathcal{M} \setminus \mathbb{N}$, a $b \in \mathcal{M} \setminus \mathbb{N}$ such that $b \notin \mathsf{Rng}(\mathsf{NW}_{f,A})$, and an F_d-proof $\pi \in \mathcal{M}$ for $\tau_b(\mathsf{NW}_{f,A})$ such that $|\pi| \leq |\tau_b(\mathsf{NW}_{f,A})|^c$. Now we consider $\mathcal{M}_{n^t}$ and by the argument in this section, there exists a $\chi' \subseteq \mathcal{P}(\mathcal{M}_{n^t})$ such that it has every bounded $\mathcal{M}$-definable subset of $\mathcal{M}_{n^t}$ and moreover

1. $(\mathcal{M}_{n^t}, \chi') \models \mathsf{V}_1^0$.

2. There exists an $\alpha \in \chi'$ which falsifies $\tau_b(\mathsf{NW}_{f,A})$.

Then by Theorem 2.2 there is no F_d-proof of $\tau_b(\mathsf{NW}_{f,A})$ in $(\mathcal{M}_{n^t}, \chi')$. Note that there is a standard number e such that

$$|\pi| \leq |\tau_b(\mathsf{NW}_{f,A})|^c \leq (n^{ct} 2^{cn})^e \leq 2^{en^{\sqrt{t}/2}}$$

which implies that $\pi \in \chi$, but this leads to a contradiction and completes the proof.

5   What are the implications of the hardness of NW-generators for a proof system?

Some experts believe that random DNFs with suitable parameters give hard formulas to prove in any proof system. The hardness of random DNFs has been proved for several proof systems. One way of proving the hardness of these formulas is by proving the harness of certain NW-generators. Let A be a $m \times n$ l-sparse matrix such that $m \geq 2n$ and l is a constant or it is at most $O(\log n)$. Let the base function be the Parity function $\oplus$. Then if we choose a random $b \in \{0,1\}^m$ uniformly, with probability $1 - o(1)$, $b \notin \mathsf{Rng}(\mathsf{NW}_{\oplus,A})$. Now, if we choose a random A and a random b uniformly, then with probability $1 - o(1)$ $\tau_b(\mathsf{NW}_{\oplus,A})$ is a tautology (here we use DNF representation of the

Parity function in the definition of the τ formula). The interesting point about these formulas is that if $\tau_b(\mathsf{NW}_{\oplus,A})$ is hard with probability $1 - o(1)$ for a proof system P, then random l-DNFs are hard with probability $1 - o(1)$ for P. This strategy was used to prove the hardness of random DNFs for some proof systems (for example, see [Kra04b, BI10]). For more information, see Section 13.4 of [Kra19]. In this regard, Krajíček [Kra19] asked whether random systems of linear equations over $\mathbb{F}_2$ are hard for AC^0-Frege or not (problem 19.4.5). We note that Theorem 3.1 partially answers this question as follows.

Let (ϕ_0, ϕ_1) be a $\Sigma_1^1 \cap \Pi_1^1$ definition of a function $f \in \mathsf{NP} \cap \mathsf{CoNP}$ (for example we can take f as the Parity function). Then a random formula $F \sim \mathcal{F}(\phi_0, \phi_1, m, n, l)$ is generated as follows:

1. we choose m subsets $J_0, ..., J_{m-1}$ independently uniformly randomly such that $J_i \subseteq [n]$ and $|J_i| = l$ for every $i \in [m]$. These subsets specify a random $m \times n$ l-sparse matrix A.

2. We choose a random $b \in \{0, 1\}^m$ uniformly randomly.

3. Then $F := \tau_b(\mathsf{NW}_{f,A})$ based on $(\langle \phi_0 \rangle_l, \langle \phi_1 \rangle_l)$.

The following corollary partially answers Krajíček's question.

Corollary 5.1 *Let $f \in \mathsf{NP} \cap \mathsf{CoNP}$ be a symmetric function such that $\mathsf{S}_{\mathsf{AC}_2^0}(f_n) = 2^{n^{\Omega(1)}}$. Let (ϕ_0, ϕ_1) be a $\Sigma_1^1 \cap \Pi_1^1$ definition of f. Then for every d, for every $c > 1$ and every $0 < \varepsilon < 1$, if n is large enough, then $F \sim \mathcal{F}(\phi_0, \phi_1, n^c, n, \lfloor n^\varepsilon \rfloor)$ is a tautology with probability $1 - o(1)$ and it requires exponential F_d-proofs.*

Another implication of the hardness of NW-generators for a proof system P is that it implies that it is hard for P to prove circuit lower bounds effectively. Razborov [Raz15] pointed out that if the base function is in P/poly and the $2^n \times n^{O(1)}$ matrix A is *efficiently constructibe* (an example of such matrices was constructed in [NW94]), and moreover $\mathsf{NW}_{f,A}$ is a hard proof complexity generator for a proof system P, the P cannot prove circuit lower bounds effectively. Moreover, this implies that $\mathsf{NP} \not\subseteq \mathsf{P}/\mathsf{poly}$ does not have efficient proofs in P. Razborov proved such a result for k-DNF Resolution in [Raz15]. In this regard, our results imply a partial answer for the question of the hardness of circuit lower bounds for proof systems. A related question about AC^0-Frege was asked by Krajíček [Kra19] (problem 19.6.1). Let $f \in \mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k)$ and A be a $2^n \times n^s$ n^t-sparse matrix which is *effectively constructible*. Then for any fixed $w \in \{0, 1\}^{n^c}$, $\mathsf{NW}_{f,A}(w)$ defines a function $C_w \in (\mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k))/\mathsf{poly}$ as follows:

- For every $i \in \{0, 1\}^n$, $C_w(i) = f\left(w|_{J_{n(i)}}(A)\right)$ where $n(i)$ is the number with the binary representation i.

This means that if $\tau_b(\mathsf{NW}_{f,A})$ is a tautology (for a fixed representation of f), then the function with the truth-table b does not have a C_w circuit for any $w \in \{0, 1\}^{n^s}$. As Theorem 3.1 (part 2) implies that NW-generators based on suitable $\mathsf{NP} \cap \mathsf{CoNP}$ functions, suitable matrices, and suitable representations are hard proof complexity generators AC^0-Frege, we get the fact that proving certain $(\mathsf{NP} \cap \mathsf{CoNP})/\mathsf{poly}$ lower bounds (b does not have C_w circuits) for Boolean functions are hard for AC^0-Frege. Note that in contrast with with the principle $f_n \notin \mathsf{SIZE}(n^k)$ which can be written as a propositional formula, it is not clear how the principle $f_n \notin (\mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k))/\mathsf{poly}$ can be written as a propositional formula. So one way of considering this principle in proof complexity is to consider $\tau_{f_n}(\mathsf{NW}_{f,A})$ for any $g \in \mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k)$, any representation of g and any effectively constructible A. In this regard, Theorem 3.1 includes a lot of possible natural formalizations (but not all) of $f_n \notin (\mathsf{NTime}(n^k) \cap \mathsf{CoNTime}(n^k))/\mathsf{poly}$.

Acknowledgment

References

[ABRW04] M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal on Computing*, 34(1):67–88, 2004.

[Ajt94] M. Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, 1994.

[BDG+04] M. L. Bonet, C. Domingo, R. Gavaldà, A. Maciel, and T. Pitassi. Non-automatizability of bounded-depth Frege proofs. *Computational Complexity*, 13(1-2):47–68, 2004.

[BI10] E. Ben-Sasson and R. Impagliazzo. Random CNF's are hard for the polynomial calculus. *Computational Complexity*, 19(4):501–519, 2010.

[Bus86] S. R. Buss. Bounded arithmetic. Studies in Proof Theory. Lecture Notes, 3. Napoli: Bibliopolis. VII, 221 p. (1986)., 1986.

[Fag74] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. Complexity of Comput., Proc. Symp. appl. Math., New York City 1973, 43-73 (1974)., 1974.

[Jeř04] E. Jeřábek. Dual weak pigeonhole principle, Boolean complexity, and derandomization. *Annals of Pure and Applied Logic*, 129(1-3):1–37, 2004.

[Jeř07] E. Jeřábek. Approximate counting in bounded arithmetic. *The Journal of Symbolic Logic*, 72(3):959–993, 2007.

[KP89] J. Krajíček and P. Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54(3):1063–1079, 1989.

[KP98] J. Krajíček and P. Pudlák. Some consequences of cryptographical conjectures for S_2^1 and EF. *Information and Computation*, 140(1):82–94, 1998.

[KPW95] J. Krajíček, P. Pudlák, and A. Woods. An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures & Algorithms*, 7(1):15–39, 1995.

[Kra95] J. Krajíček. *Bounded arithmetic, propositional logic, and complexity theory*, volume 60. Cambridge: Cambridge Univ. Press, 1995.

[Kra97]   J. Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.

[Kra01a] J. Krajíček. On the weak pigeonhole principle. *Fundamenta Mathematicae*, 170(1-2):123–140, 2001.

[Kra01b] J. Krajíček. Tautologies from pseudo-random generators. *The Bulletin of Symbolic Logic*, 7(2):197–212, 2001.

[Kra04a] J. Krajíček. Diagonalization in proof complexity. *Fundamenta Mathematicae*, 182(2):181–192, 2004.

[Kra04b] J. Krajíček. Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. *The Journal of Symbolic Logic*, 69(1):265–286, 2004.

[Kra05]   J. Krajíček. Structured pigeonhole principle, search problems and hard tautologies. *The Journal of Symbolic Logic*, 70(2):616–630, 2005.

[Kra09]   J. Krajíček. A proof complexity generator. In *Logic, methodology and philosophy of science. Proceedings of the 13th international congress, Beijing, China, August 2007*, pages 185–190. London: College Publications, 2009.

[Kra10]   J. Krajíček. A form of feasible interpolation for constant depth Frege systems. *The Journal of Symbolic Logic*, 75(2):774–784, 2010.

[Kra11a] J. Krajíček. *Forcing with random variables and proof complexity*, volume 382. Cambridge: Cambridge University Press, 2011.

[Kra11b] J. Krajíček. On the proof complexity of the Nisan-Wigderson generator based on a hard $NP \cap coNP$ function. *Journal of Mathematical Logic*, 11(1):11–27, 2011.

[Kra15]   J. Krajíček. A reduction of proof complexity to computational complexity for $AC^0[p]$ Frege systems. *Proceedings of the American Mathematical Society*, 143(11):4951–4965, 2015.

[Kra19]   J. Krajíček. *Proof complexity*, volume 170. Cambridge: Cambridge University Press, 2019.

[Kra21]   J. Krajíček. Small Circuits and Dual Weak PHP in the Universal Theory of P-Time Algorithms. *ACM Transactions on Computational Logic*, 22(2), 2021.

[NW94]   N. Nisan and A. Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994.

[PBI93]   T. Pitassi, P. Beame, and R. Impagliazzo. Exponential lower bounds for the pigeonhole principle. *Computational Complexity*, 3(2):97–140, 1993.

[Pic11]   J. Pich. Nisan-Wigderson generators in proof systems with forms of interpolation. *Mathematical Logic Quarterly (MLQ)*, 57(4):379–383, 2011.

[Pic15a] J. Pich. Circuit lower bounds in bounded arithmetics. *Annals of Pure and Applied Logic*, 166(1):29–45, 2015.

[Pic15b] J. Pich. Logical strength of complexity theory and a formalization of the PCP theorem in bounded arithmetic. *Logical Methods in Computer Science*, 11(2):38, 2015.

[Pic20] J. Pich. Learning algorithms from circuit lower bounds . *arXiv*, (2012.14095), 2020.

[PS21] J. Pich and R. Santhanam. Strong Co-Nondeterministic Lower Bounds for NP Cannot Be Proved Feasibly. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2021, page 223–233, 2021.

[Pud97] P. Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *The Journal of Symbolic Logic*, 62(3):981–998, 1997.

[Pud17] P. Pudlák. Incompleteness in the finite domain. *The Bulletin of Symbolic Logic*, 23(4):405–441, 2017.

[Pud21] P. Pudlák. The canonical pairs of bounded depth Frege systems. *Annals of Pure and Applied Logic*, 172(2):42, 2021. Id/No 102892.

[PW85] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. Methods in mathematical logic, Proc. 6th Latin Amer. Symp., Caracas/Venez. 1983, Lect. Notes Math. 1130, 317-340 (1985)., 1985.

[Raz15] A. A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Annals of Mathematics. Second Series*, 181(2):415–472, 2015.

[Sok21] D. Sokolov. Pseudorandom Generators, Resolution and Heavy Width . *ECCC*, (TR21-076), 2021.

[Woo97] A. R. Woods. Approximating the structures accepted by a constant depth circuit or satisfying a sentence – a nonstandard approach. In *Logic and random structures. DIMACS workshop, November 5–7, 1995*, pages 109–130. 1997.