Nisan–Wigderson Generators in Proof Complexity: New Lower Bounds

Erfan Khaniki
Faculty of Mathematics and Physics, Charles University, Prague, Czech Republic
Institute of Mathematics of the Czech Academy of Sciences, Prague, Czech Republic

Abstract
A map $g : \{0, 1\}^n \rightarrow \{0, 1\}^m$ ($m > n$) is a hard proof complexity generator for a proof system $P$ iff for every string $b \in \{0, 1\}^m \setminus \text{Rng}(g)$, formula $\gamma_b(g)$ naturally expressing $b \not\in \text{Rng}(g)$ requires superpolynomial size $P$-proofs. One of the well-studied maps in the theory of proof complexity generators is Nisan–Wigderson generator. Razborov [37] conjectured that if $A$ is a suitable matrix and $f$ is a $\text{NP} \cap \text{CoNP}$ function hard-on-average for $P/\text{poly}$, then $\text{NW}_{f,A}$ is a hard proof complexity generator for Extended Frege. In this paper, we prove a form of Razborov’s conjecture for $\text{AC}^0$-Frege. We show that for any symmetric $\text{NP} \cap \text{CoNP}$ function $f$ that is exponentially hard for depth two $\text{AC}^0$ circuits, $\text{NW}_{f,A}$ is a hard proof complexity generator for $\text{AC}^0$-Frege in a natural setting. As direct applications of this theorem, we show that:
1. For any $f$ with the specified properties, $\gamma_b(\text{NW}_{f,A})$ (for a natural formalization) based on a random $b$ and a random matrix $A$ with probability $1 - O(1)$ is a tautology and requires superpolynomial (or even exponential) $\text{AC}^0$-Frege proofs.
2. Certain formalizations of the principle $f_n \not\in (\text{NP} \cap \text{CoNP})/\text{poly}$ requires superpolynomial $\text{AC}^0$-Frege proofs.

These applications relate to two questions that were asked by Krajíček [21].

2012 ACM Subject Classification Theory of computation → Proof complexity; Theory of computation → Complexity theory and logic

Keywords and phrases Proof complexity, Bounded arithmetic, Bounded depth Frege, Nisan-Wigderson generators, Meta-complexity, Lower bounds

Digital Object Identifier 10.4230/LIPIcs.CCC.2022.17

Funding This work was supported by the GACR grant 19-27871X, the institute grant RVO: 67985840, and the Specific university research project SVV-2020-260589. Part of this work was done while the author was participating in the program Satisfiability: Theory, Practice, and Beyond at the Simons Institute for the Theory of Computing.

Acknowledgements We are grateful to Jan Bydžovský, Susanna de Rezende, Emil Jeřábek, Jan Krajíček, Jan Fich and Pavel Pudlišák for their different forms of help in different stages of this work. We are also indebted to anonymous referees for their helpful suggestions, which led to a better presentation of the paper.

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 [21] 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 $\text{AC}^0(\oplus)$-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 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 [21]). 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 [23, 35]). The third candidate is proof complexity generators.

### 1.1 Proof complexity generators

Let \( g : \{0,1\}^n \rightarrow \{0,1\}^m \) be a function which is computable in a reasonable low complexity class such as \( \text{FP/poly} \). As \( m > n \), \( \{0,1\}^m \setminus \text{Rng}(g) \) is nonempty. Let \( b \in \{0,1\}^m \setminus \text{Rng}(g) \), then as \( g \) is computable in \( \text{FP/poly} \), we can naturally express the true statement \( b \notin \text{Rng}(g) \) 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 \( b \in \{0,1\}^m \setminus \text{Rng}(g) \), then \( g \) is a hard proof complexity generator for \( P \). The concept of proof complexity generators were defined independently by Alekhnovich et al. [2] and Krajíček [11].

As pseudorandom generators are an important topic in computational complexity, Alekhnovich et al. [2] asked the following natural question: which mappings \( g : \{0,1\}^n \rightarrow \{0,1\}^m \) should be considered hard from the point of view of proof complexity? To understand this concept, different mappings were investigated from different aspects in [2]. In particular, they investigated conditions that make a Nisan–Wigderson generator hard for proof systems such as Resolution and Polynomial Calculus.

Krajíček [11] 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 \( \text{dWPHP}_{2n}^n \) which says that for every function \( g : [n] \rightarrow [2n] \), \( g \) cannot be onto. An interesting theory of bounded arithmetic is \( \text{BT} := S^1_2 + \text{dWPHP}(\text{PV}) \) which has several nice properties (see [7, 8]). Here \( S^1_2 \) is the base bounded arithmetic theory in the Buss’s Bounded arithmetic hierarchy which is related to the polynomial-time reasoning (see [5]) and \( \text{dWPHP}(\text{PV}) \) consists of \( \text{dWPHP}_{2n}(f) \) for every polynomial-time computable function \( f \). A natural question is whether \( S^1_2 \) and \( \text{BT} \) are actually the same theory. Krajíček introduced the concept of proof complexity generators as functions which violate \( \text{dWPHP}(\text{PV}) \) and formulated a conjecture about them in the setting of model theory of arithmetic that implies \( S^1_2 \neq \text{BT} \) (see [22] for a proof of separation of \( \text{PV} \) and \( \text{PV} + \text{dWPHP}(\text{PV}) \) under a different assumption). Moreover, this conjecture implies that proof complexity generators are hard for Extended Frege.

Later, Krajíček [12, 13, 14, 15, 16, 18, 19] investigated proof complexity generators from different aspects, developed the theory of proof complexity generators in great length and proposed some conjectures. In particular, Krajíček [18] defined the generator \( \text{nw}_{n,c} \) based on the gadget generators of [16] and conjectured that \( \text{nw}_{n,c} \) is a hard proof complexity generator for any proof system.

Razborov [37] 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 [2, 14]. Moreover, he formulated the following intriguing conjecture:
Conjecture 1 (Razborov [37]). Any Nisan–Wigderson generator based on suitable matrices and any function in \( \text{NP} \cap \text{CoNP} \) that is hard on average for \( \text{P/poly} \), is hard for Extended Frege.

Conjecture 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 [18] and Section 19.4 of [21].

Regarding Razborov’s conjecture, Pich [28] 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 was done by Krajíček in [19]. He proved that assuming the existence of a function \( f \in \text{NP} \cap \text{CoNP} \) which is hard on average for \( \text{P}/\text{poly} \); it is consistent with the universal theory \( \text{PV} \) that for any Nisan–Wigderson generator based on \( f \) (or for a function closely related to \( f \)) and suitable matrices is an onto function. It is worth noting that the arithmetical sentence that Krajíček used to formalize the sentence \( \text{Nisan–Wigderson generator is onto} \) is a natural one. However, it is not clear whether this consistency result based on this formalization implies Razborov’s conjecture or not. Note that \( \text{PV} \) is a fairly strong theory as it proves a reasonable fragment of computational complexity theorems (see [30] for more information). It is worth mentioning that those investigations of the Nisan–Wigderson generators in proof complexity led to advancements in other areas as well, such as [29, 32] which proved unprovability of circuit lower bounds in bounded arithmetic and [31] 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 [10] 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 [34]. Unfortunately, this property does not hold for strong proof systems such as Extended Frege [24], and even \( \text{AC}^0 \)-Frege [4] assuming cryptographic hardness assumptions (for more information, see chapter 17 of [21]). 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 [17] proved a form of feasible interpolation for \( \text{AC}^0 \)-Frege that is different from the original definition of the feasible interpolation property. Moreover, he developed the method of Forcing with random variables in [18] intending to prove hardness of computation to hardness of proofs theorems for strong proof systems (bounded arithmetics) and proved types of this theorem for \( \text{AC}^0 \)-Frege and \( \text{AC}^0(\oplus) \)-Frege (for a finitary proof of the theorem for \( \text{AC}^0(\oplus) \)-Frege see [20]). Pudlák [36] characterized the canonical disjoint \( \text{NP} \)-pairs of \( \text{AC}^0 \)-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 \( \text{AC}^0 \)-Frege. Our main contribution is the proof of Razborov’s conjecture for \( \text{AC}^0 \)-Frege in a natural setting which was not known before. The following theorem states a natural restriction of Razborov’s conjecture.
Theorem 2 (Main theorem, informal version). Let \( f \in \text{NP} \cap \text{CoNP} \) be a symmetric function that requires \( 2^{\Omega(n)} \) depth two \( \text{AC}^0 \) circuits. Then for any \( \Sigma^1 \cap \Pi^1 \) pair \((\phi_0, \phi_1)\) that defines \( f \), any suitable matrix \( A \), and any \( b \notin \text{Rng}(\text{NW}_{f,A}) \), \( \tau_b(\text{NW}_{f,A}) \) requires superpolynomial or exponential size \( \text{AC}^0 \)-Frege proofs based on whether the stretch is exponential or polynomial when the Paris-Wilkie translation of \((\phi_0, \phi_1)\) is used to form the formula \( \tau_b(\text{NW}_{f,A}) \).

Theorem 2 unconditionally implies that \( \text{NW}_{f,A} \) for suitable functions \( f \) (such as Parity or Majority) and suitable matrices \( A \) are hard proof complexity generators for \( \text{AC}^0 \)-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 \( \text{AC}^0 \)-Frege, were the PHP-generator of [16] and the more general generator \( n \text{ww}_{n,c} \) of [18]. Moreover, Theorem 2 implies the following results:

1. For any \( f \) that satisfies the conditions of Theorem 2 such as Parity, the formula \( \tau_b(\text{NW}_{f,A}) \)
   (for a natural formalization) based on a random \( b \) and a random matrix \( A \) is a tautology with probability \( 1 - o(1) \) and requires superpolynomial (exponential) \( \text{AC}^0 \)-Frege proofs.
2. Certain formalizations of the principle \( f_n \notin (\text{NTIME}(n^k) \cap \text{CoNTIME}(n^k))/\text{poly} \) requires superpolynomial \( \text{AC}^0 \)-Frege proofs.

These results relate to two questions asked by Krajíček [21] (problems 19.4.5 and 19.6.1). The first problem asks whether random linear generators (random systems of linear equations over \( F_2 \)) are hard for \( \text{AC}^0 \)-Frege or not. The second problem asks whether linear generators are iterable for \( \text{AC}^0 \)-Frege or not, which relates to the question of the hardness of proving the principle \( f_n \notin \text{SIZE}(n^k) \) in \( \text{AC}^0 \)-Frege. It seems that because of the formalization that we used in the main theorem, our lower bounds do not imply the hardness of proving the principle \( f_n \notin \text{SIZE}(n^k) \) for \( \text{AC}^0 \)-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 \( [r_1, r_2) := \{ i \in \mathbb{N} : [r_1] \leq i < [r_2] \} \) and \( [r_1, r_2] := \{ i \in \mathbb{N} : [r_1] \leq i \leq [r_2] \} \).

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 \( f : \{0,1\}^l \to \{0,1\} \) is a Boolean function and \( A \) is a \( m \times n \) \( l \)-sparse matrix, Nisan and Wigderson [26] defined the generator \( \text{NW}_{f,A} : \{0,1\}^n \to \{0,1\}^m \) as follows:

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

It was proved in the seminal paper [26] that if \( f \) is a hard function (depending on the application) and \( A \) satisfies specific combinatorial properties, then \( \text{NW}_{f,A} \) is a good pseudorandom generator (depending on the parameters).

Let \( f \in \text{NP} \cap \text{CoNP} \). 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. \((\sigma_0, \sigma_1)\) defines the function \( f_n \) which means:
   a. \( \neg \sigma_0 \lor \neg \sigma_1 \) is a tautology.
   b. For every \( a \in \{0,1\}^n \), \( f(a) = i \) iff \( \sigma_i(a, \mathbf{t}) \) is satisfiable where \( i \in \{0,1\} \).

Note that as \( f \in \text{NP} \cap \text{CoNP} \), for every \( n \), \( f_n \) has a representation.
Suppose $f \in \text{NP} \cap \text{CoNP}$, $(\sigma_0, \sigma_1)$ is a representation for $f$, and $A$ is a $m \times n$-sparse matrix. Then for any $b \in \{0,1\}^m$, $\tau_b(\text{NW}_{f,A})$ based on $(\sigma_0, \sigma_1)$ is the following propositional formula:

$$
\bigvee_{b_i=1} \neg \sigma_1(p|J_i(A), q_i) \lor \bigvee_{b_i=0} \neg \sigma_0(p|J_i(A), q_i)
$$

where $q_i$'s are disjoint variables. Note that if $b \not\in \text{Rng}(\text{NW}_{f,A})$, then $\tau_b(\text{NW}_{f,A})$ is tautology.

As it was discussed in previous works [2, 15, 37, 19], $\text{NW}_{f,A}$ 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 $\tau_b(\text{NW}_{f,A})$.
- The string $b \not\in \text{Rng}(\text{NW}_{f,A})$.

As we will see, our main result also imposes different conditions on $\tau_b(\text{NW}_{f,A})$ 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 $\tau_b(\text{NW}_{f,A})$ can depend on the pair $(\sigma_0, \sigma_1)$ that is used in it. This matter has been investigated in [2], and they examined different representations. Recently, Sokolov [38] answered one of the open problems that was stated about a representation of $\tau_b(\text{NW}_{f,A})$ in [2]. Here we investigate representations based on definability over finite structures in logic, which is a well-studied concept in descriptive complexity and finite model theory.

$\Sigma^1_1 \cap \Pi^1_1$ representation

Let $\mathcal{L}$ be a finite relational language and $X$ be a unary relational symbol which is not in $\mathcal{L}$. A $\Sigma^1_1$ formula $\psi(X)$ in the language $\mathcal{L} \cup \{X\}$ with equality defines a function $f \in \text{NP}$ iff:

1. $\psi := \exists Y \phi(X, Y)$ where $\phi(X, Y)$ is a first-order formula in the language $\mathcal{L} \cup \{X\}$ with equality.
2. $X$ is not in $Y$.
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 [6] directly implies that for every symmetric $f \in \text{NP}$, a $\Sigma^1_1$ formula $\psi_f(X)$ exists in a language $\mathcal{L} \cup \{X\}$ that defines $f$. Therefore, the set of functions that are $\Sigma^1_1$ definable is exactly symmetric $\text{NP}$ and hence this set is quite rich. As an example, we explain how the negation of Parity function can be defined as a $\Sigma^1_1$ formula. Let $\mathcal{L} = \{Y\}$ where $Y$ is a binary relation symbol. Then

$$
\tilde{\oplus}(X, Y) := \forall i (X(i) \rightarrow \exists j (j \neq i \land X(j) \land Y(i, j) \land Y(j, i) \land \forall k (k = i \lor \neg Y(i, k) \lor j = k))).
$$

Then $\psi_{\tilde{\oplus}}(X) := \exists Y \tilde{\oplus}(X, Y)$ 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 $\Sigma^1_1$ 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 [17]).
To prove Theorem 2, the following lemma is needed. This lemma states that the truth of first-order formulas in a relational language does not change under permutations.

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 \( h(Q) := \{(h(a_0), \ldots, h(a_{k-1})) : (a_0, \ldots, a_{k-1}) \in Q \} \).

**Lemma 3.** Let \( L = \{Y_0, \ldots, Y_k\} \) be a finite relational language and \( A_0 = (A, \{Q_0^0, \ldots, Q_k^0\}) \) be an \( L \)-structure. Let \( h \) be a bijective function from \( A \) onto \( A \). Consider the \( L \)-structure \( A_1 := (A, \{Q_0^1, \ldots, Q_k^1\}) \) where \( Q_i^1 = h(Q_i^0) \), for every \( i \in [0, k] \). Then for every first-order formula \( \phi(x_0, \ldots, x_{p-1}) \) in \( L \) with equality, every \( (a_0, \ldots, a_{p-1}) \in A^p \):

\[ A_0 \models \phi(a_0, \ldots, a_{p-1}) \iff A_1 \models \phi(h(a_0), \ldots, h(a_{p-1})). \]

**Proof.** This lemma can be proved by induction on the complexity of \( \phi \). ▶

Let \( \exists Y \phi(X, Y) \) be a \( \Sigma_1^1 \) formula. Then for any \( n \), the Paris-Wilkie translation [27] (see also Section 8.2 of [21]) of \( \phi^{<n}(X, Y) \) (\( \phi^{<n} \) is \( \phi \) when every first-order quantifier is bounded by \( n \)) is denoted by \( \langle \phi \rangle_n(p, q) \) 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 \( \exists Y(X, Y) \) in the universe of size \( n \) is

\[ \langle \exists Y(X, Y) \rangle_n := \bigwedge_{i=0}^{n-1} \left( \neg p_i \lor \bigvee_{j=0, j \neq i}^{n-1} \left( p_j \land q_{i,j} \land q_{j,i} \land \bigwedge_{k=0, k \neq i, k \neq j}^{n-1} \neg q_{i,k} \right) \right). \]

Let \( f \in \text{NP} \cap \text{CoNP} \) be a symmetric function. Then a pair of \( \Sigma_1^1 \) formulas \( (\exists Y\phi_0(X, Y), \exists Z\phi_1(X, Z)) \) defines \( f \) iff:

1. \( \exists Y \phi_0(X, Y) \) defines \( f \).
2. \( \exists Z \phi_0(X, Z) \) 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 \( \psi(X) := \exists Y \phi(X, Y) \) is a \( \Sigma_1^1 \) 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 [21, 9]). Here we state some useful facts about \( \text{AC}^0 \)-Frege, which will be used in the results.

**2.2.1 \( \text{AC}^0 \)-Frege**

\( \text{AC}^0 \)-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 \( \text{AC}^0 \)-Frege proof system of depth \( d \), which is the Frege proof system that works with formulas of depth at most \( d \).

To prove Theorem 2, we need some known relations between \( \text{AC}^0 \)-Frege and \( V_0^1 \), which is a two-sorted bounded arithmetic (see [5, 9]). These relations are related to the model theory of \( V_0^1 \).

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

\[ M_n := \{ a \in M : \text{There exists a } b \in M \setminus \mathbb{N} \text{ such that } a < 2^n b^{1/n} \}. \]
The following theorems explain the relationship between $\mathbf{AC}^0$-Frege and $\mathbf{V}^0_1$ from the point of view of proof complexity. These theorems state that lower bounds for $\mathbf{AC}^0$-Frege correspond to unprovability in $\mathbf{V}^0_1$ in a certain sense.

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

**Theorem 4** (Section 9.4 of [9]). Let $(\mathcal{M}, \chi) \models \mathbf{V}^0_1$ and $\sigma \in \chi$ be a constant depth propositional formula (depth of $\sigma$ is standard). If $\neg \sigma$ is satisfiable by an assignment in $\chi$, then for every standard $d$, there is no $\mathbf{F}_d$-proof of $\sigma$ in $(\mathcal{M}, \chi)$.

Note that Theorem 4 also holds in the case where $\sigma$ is the Paris-Wilkie translation of a bounded arithmetical formula such as $\phi(x, R)$ ($\sigma = \langle \phi(n, R) \rangle_n$ 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 $\chi$ and therefore $\sigma$ does not have any $\mathbf{F}_d$-proof in $\mathcal{M}$.

**Theorem 5** (Section 9.4 of [9]). Let $\mathcal{M}$ be a countable nonstandard model of true arithmetical 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 $\mathbf{F}_d$-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 $\chi$.
2. $(\mathcal{M}_m, \chi) \models \mathbf{V}^0_1$.
3. There is an $\alpha \in \chi$ such that $(\mathcal{M}_m, \chi) \models \neg \phi(m, \alpha)$.

### 3 Razborov’s conjecture for $\mathbf{AC}^0$-Frege

In this section, we state and prove the main result of the paper.

A Boolean function $f$ is symmetric iff for every $n$, $f_n$ is invariant under any permutation of its inputs. Let $S_{\mathbf{AC}^0_2}$ denote the depth two $\mathbf{AC}^0$ circuit complexity of functions, then:

**Theorem 6.** Let $f \in \mathbf{NP} \cap \mathbf{CoNP}$ be a symmetric function such that $S_{\mathbf{AC}^0_2}(f) = 2^{O(n)}$ and $(\phi_0, \phi_1)$ 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 $0 < \epsilon < 1$, there exists an $\epsilon' > 0$ such that for every large enough $n$, every $n^\epsilon \times n$ $n^\epsilon$-sparse matrix $A$, any $b \not\in \text{Rng}_2(\tau_\mathbb{N}(\mathbf{NW}_{f,A})$ based on $\langle (\phi_0)_{\lfloor n^\epsilon \rfloor}, (\phi_1)_{\lfloor n^\epsilon \rfloor} \rangle$ does not have $\mathbf{F}_d$-proofs of size less than $2^{2n^\epsilon'}$.
2. For every positive $r \in \mathbb{N}$, every large enough $s$, every $t \in [s/r, s]$, every $c \in \mathbb{N}$, every large enough $n$, every $2^n \times n^c$ $n^c$-sparse matrix $A$, any $b \not\in \text{Rng}_2(\tau_\mathbb{N}(\mathbf{NW}_{f,A})$ based on $\langle (\phi_0)_{n^{c'}}, (\phi_1)_{n^{c'}} \rangle$ does not have $\mathbf{F}_d$-proofs of size less than $2^{2n}$.

Note that in Theorem 6, the size of the formula $\tau_b(\mathbf{NW}_{f,A})$ is $n^{O(1)}$ in the first part and it is $2^{O(n)}$ in the second part. 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 $\mathbf{AC}^0$-Frege. Model theoretic arguments have been used previously in proof complexity and they were very fruitful (for example see [1, 11, 17] and [9] for a detailed explanation). See [30, 12] 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 6 is that $\mathbf{NW}_{f,A}$ based on a hard enough function $f$ with suitable parameters is a hard proof complexity generator for $\mathbf{AC}^0$-Frege. As the Parity function or the Majority function satisfies the required assumptions of Theorem 6, we get that $\mathbf{NW}$-generators based on these functions are hard proof complexity generators for $\mathbf{AC}^0$-Frege.
Proof of Theorem 6

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, \([n] := [0, n]\).

Intuitively, the proof goes as follows. Let \(n\) be large enough. As \(f\) is symmetric and has high depth two circuit complexity, then there is a \(u\) such that \(f_{n'}\) on strings with \(u\) many 1’s is different from \(f_{n'}\) on strings with \(u + 1\) many 1’s and moreover, \(u\) is not too big and not too small. This implies that there is an input \(a\) for the NW generator such that the number of 1’s of \(a\) restricted to each row is close to \(u\). Now, assuming PHP fails, for every row \(i\) we can find a witness for \(\phi_n(a|J_i(A))\) by constructing permutations between sets that actually have different sizes and this forces any string \(b\) into the range of the generator and this is possible as the truth of representations are closed under permutations. The next lemmas formalize this intuitive proof and their combination proves the theorem.

Lemma 7. Let \(f : \{0, 1\}^* \to \{0, 1\}\) be a symmetric Boolean function such that \(S_{\text{AC}}(f_n) = \Omega(2^n)\) for an \(\epsilon > 0\). Then there is a natural \(m\) such that for every \(n \geq m\) there is natural number \(u \in [n^{t/2}, n - n^{t/2}]\) such that

\[
f_n(1^n0^{n-u}) \neq f_n(1^{u+1}0^{n-u-1}).
\]

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 \(r \leq k \leq n - r\), \(g(1^n0^{n-k}) = 0\), then

\[
S_{\text{DNF}}(g) \leq 2n \sum_{i=0}^{r} \binom{n}{i} \leq 2n\left(\frac{en}{r}\right)^r
\]

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

\[
c2^{n'} \leq 2n(en^{1-\delta})^n \leq 2en^{n^\delta}n^{1+n^\delta} \leq 2n^{1+2n^\delta} = 2^{(2n^\delta+1)\log n+1}.
\]

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 \(v \in [n^{t/2}, n - n^{t/2}]\) such that \(f_n(1^n0^{n-v}) = 1\). Following the same argument for \(\neg f_n\), we can deduce that for every large enough \(n\), there exists a \(v' \in [n^{t/2}, n - n^{t/2}]\) such that \(\neg f_n(1^{v'}0^{n-v'}) = 1\). So we have found \(v, v' \in [n^{t/2}, n - n^{t/2}]\) such that \(f_n(1^n0^{n-v}) \neq f_n(1^{v'}0^{n-v'})\), hence there exists a \(u \in [n^{t/2}, n - n^{t/2}]\) such that

\[
f_n(1^n0^{n-u}) \neq f_n(1^{u+1}0^{n-u-1}). \n
\]

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 \(n^s2^n \leq 2^nt^s\) for a nonstandard \(n\).
3. \(b \in \mathcal{M} \setminus \mathbb{N}\) is a binary string of length \(2^n\) such that \(b \notin \text{Rng}(\text{NW}_f, A)\).

Let \(\chi\) be the set of all bounded subsets of \(\mathcal{M}_{nt}\) encoded in \(\mathcal{M}\). So in particular \(A, b \in \chi\). As \(S_{\text{AC}}(f_n) = 2^{nt^s}(n^t)\), there is a standard rational \(\epsilon > 0\) such that \(S_{\text{AC}}(f_m) = \Omega(2^{nt^s})\). Let \(\delta := \epsilon/2\), then there exists \(u \in [n^{t\delta}, n^t - n^{t\delta}]\) that is guaranteed to exist by Lemma 7 for \(f_{n'}\). Let \(v := \min\{u, n^t - u\}\), then...
Lemma 8. There exists a binary string $\alpha \in \chi$ of length $n^s$ such that for every $i \in [2^n]$, 

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

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 $i$, $Pr[X_i = 1] = \frac{v}{\sqrt{v}}$. For every $i \in [2^n]$, let $Y_i = \sum_{j \in J_i(A)} X_j$ and hence $E[Y_i] = v$.

By the Chernoff bound we have the following inequalities for every $i \in [2^n]$:

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

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:

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

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

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

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

Lemma 9. The following functions exist in $\chi$:

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 $i \in [2^n]$, $\omega(i, \cdot)$ defines a permutation over $[n^t]$ and moreover $\beta_j = (\alpha | J_i(A))_{\omega(i,j)}$ where $\beta = 1^{\gamma(i)}0^{n^t-\gamma(i)}$.

Proof.

1. The function $\gamma$ exists in $\mathcal{M}$ as it is definable by an arithmetical formula with parameter $\alpha$. To prove that $\gamma$ is in $\chi$, we observe that encoding of $\gamma$ as a binary string requires at most $c2^n \cdot \log n^t$ (for some $c \in N$) which is less than $2^{n^\gamma}$, hence $\gamma \in \chi$.

2. Like the previous part, $\omega$ exists in $\mathcal{M}$ as it is definable by an arithmetical formula with parameters $\alpha$ and $\gamma$, and its bit representation requires at most $c2^n \cdot n^t \log n^t$ (for some $c \in N$) which is again less than $2^{n^\gamma}$, and therefore $\omega \in \chi$.

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

Theorem 10 ([1, 25, 33]). For any natural number $d$, there exists an $\epsilon_d > 0$ such that for large values of $n$, any $F_d$-proof of $\text{PHP}_{n+1}$ has size at least $2^{\Omega(n^d)}$. 

CCC 2022
Now let \( l = \lfloor \sqrt{n} \rfloor \), then we have the following lemma.

**Lemma 11.** There exists \( \chi' \subseteq \mathcal{P}(\mathcal{M}_n) \) such that:

1. \( \chi \subseteq \chi' \).
2. There exists a function \( \sigma \in \chi' \) such that \( \sigma \) is a bijection from \([l]\) onto \([l - 1]\).
3. \( (\mathcal{M}_n, \chi') \models \mathcal{V}_0^l \).

**Proof.** By Theorem 10 we know that \( \text{PHP}_{m-1}^n \) requires exponential size \( F_d \)-proofs for every \( d \). Therefore by Theorem 5, there exists a \( \chi' \subseteq \mathcal{P}(\mathcal{M}_l) \) such that every bounded subset of \( \mathcal{M}_l \) is in \( \chi' \), \( (\mathcal{M}_l, \chi') \models \mathcal{V}_0^l \) and there exists a \( \sigma \in \chi' \) such that it is bijection from \([l]\) onto \([l - 1]\). Note that if \( a \in \mathcal{M}_n \), then there exists a \( b \in \mathcal{M} \setminus \mathbb{N} \) such that \( a < 2^{n^{t/4}} \). Let \( b' = \lfloor \frac{a}{2} \rfloor \), then \( a < 2^{t/4} \) as we know \( l \geq n^{t/4} \). This implies that \( \mathcal{M}_l = \mathcal{M}_n \), and moreover \( \chi \subseteq \chi' \) which completes the proof. \( \square \)

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

**Lemma 12.** There exists a function \( F : [2^n] \times \{-1, 0, 1\} \times [n^l] \rightarrow [n'] \) in \( \chi' \) such that for every \( i \in [2^n] \)

1. \( F(i, a, \cdot) \) restricted to \([v + a]\), is a bijection from \([v + a]\) onto \([\gamma(i)]\).
2. \( F(i, a, \cdot) \) restricted to \([v + a, n']\), is a bijection from \([v + a, n']\) onto \([\gamma(i), n']\).

**Proof.** Let \( \sigma \in \chi' \) be the function that Lemma 11 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:

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

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

Note that \( v - 1 \leq M_{i,a} \), hence

\[
w_{i,a} \leq \frac{v - 1}{\sqrt{n}} \leq \frac{v - 1}{l} \leq \frac{M_{i,a}}{l}
\]

as \( w_{i,a} \leq \sqrt{n^2 + 1} \) by Lemma 8. So \( G_0(i, a, \cdot) \) 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 \( G(i, a, \cdot) \) 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 \( G_1(i, a, \cdot) \) 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 \( H_0(i, a, \cdot) \) 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:

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

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

Note that \( n^t - v - 1 \leq M_{i,a}' \) and moreover \( v \leq n^t/2 \), therefore \( n^t/2 - 1 \leq M_{i,a}' \). This implies that

\[
w_{i,a} \leq \sqrt[n^t]{v} + 1 \leq \sqrt[n^t/2]{v} + 1 \leq \sqrt[n^t/2]{(n^t/2)^2} - 1 \leq \frac{n^t/2 - 1}{\sqrt[n^t/2]{v}} \leq \frac{n^t/2 - 1}{l} \leq \frac{M_{i,a}'}{l}.
\]

Therefore \( H_0(i, a, \cdot) \) 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 \( H_0(i, a, \cdot) \) 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 \( H_1(i, a, \cdot) \) is a bijection from \([m_{i,a}']\) onto \([M_{i,a}]\).

Now \( F(i, a, b) \) is:

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

As \( G_0, G_1, H_0, H_1 \) are definable by a bounded arithmetical formula based on \( \gamma \) and \( \sigma \), therefore \( F \) is also definable by a bounded arithmetical formula based on \( \gamma \) and \( \sigma \) and this implies that \( F \in \chi' \) as \( (\mathcal{M}_{n,t}, \chi') \models \mathcal{V}_1^0 \). ▶

Without the loss of generality we can assume \( f_{n,t}(1^{v0^{n'-u}}) = 0 \). Consider the following relations in \( \chi' \):

1. \( \theta_0 = 1^{u0^{n'-v}}. \)
2. \( \theta_0' = 0^{n-1}1^u. \)
3. \( \theta_1 = 1^{v+1}0^{n'-u-1}. \)
4. \( \theta_1' = 0^{n'-u-1}1^{u+1}. \)
5. \( \bar{\lambda}_0 \) such that \( \phi_0(\theta_0, \lambda_0) \) holds in \( (\mathcal{M}_{n,t}', \chi) \).
6. \( \bar{\lambda}_0' \) such that \( \phi_0(\theta_0', \lambda_0') \) holds in \( (\mathcal{M}_{n,t}', \chi) \).
7. \( \bar{\lambda}_1 \) such that \( \phi_1(\theta_1, \lambda_1) \) holds in \( (\mathcal{M}_{n,t}, \chi) \).
8. \( \bar{\lambda}_1' \) such that \( \phi_1(\theta_1', \lambda_1') \) holds in \( (\mathcal{M}_{n,t}, \chi) \).

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

\[
(\mathcal{M}_{n,t}, \chi') \models \forall i < 2^n \ (b_i = 0 \rightarrow \phi_0(\mathcal{X}[J_i(A), \bar{\lambda}_i]) \land (b_i = 1 \rightarrow \phi_1(\mathcal{X}[J_i(A), \bar{\lambda}_i]))
\]

which implies that \( \tau_{\chi}((\mathcal{N}W_{f,A}) \) based on \((\phi_0)_{n,t}, (\phi_1)_{n,t}\) 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. \( \bar{\mathcal{Y}}_i = \omega(i, F(i, 0, \bar{\alpha}_0)) \).
   c. \( \bar{\mathcal{Z}}_i = \omega(i, F(i, 1, \bar{\alpha}_1)) \).

2. If \( u = n^t - v \):
   a. \( \mathcal{X} \) is the complement of \( \alpha \), i.e., \( \mathcal{X}_j = 1 - \alpha_j \) \( j \in [n^t] \).
   b. \( \bar{\mathcal{Y}}_i = \omega(i, F(i, 0, \bar{\alpha}_0)) \).
   c. \( \bar{\mathcal{Z}}_i = \omega(i, F(i, -1, \bar{\alpha}_1)) \).

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 3 as \( \omega(i, F(i, 0, \cdot)) \) is a bijection from \([n^t]\) onto itself and the fact that \( \sigma_0(\mathcal{X}|J_i(A), \bar{\mathcal{Z}}_i) \) 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 \( \theta_0', \theta_1', \bar{\mathcal{Y}}_0', \bar{\mathcal{Y}}_1' \).

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 \( \mathbb{N} \):
\[
\mathcal{H} := \forall \exists t \exists 3 s \geq s_1, \exists t \in [s/r, s], \exists c > 0, \forall m, \exists n > m \exists 2^n \times n^t \text{-sparse matrix } A, \exists b \notin \text{Rng}(NW_{f,A}), \exists F_{d'}-\text{proof } \pi \text{ for } \tau_b(NW_{f,A}) \text{ such that } |\pi| \leq |\tau_b(NW_{f,A})|^{c}.
\]
Let \( \mathcal{M} \) be a countable nonstandard model of true arithmetic. This means that \( \mathcal{M} \models \mathcal{H} \). To simplify the presentation let
\[
\mathcal{H} := \forall \exists t \exists 3 s, t, c \forall m \exists n, A, b, \pi \Phi(s_1, s, t, c, m, n, A, b, \pi).
\]
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 \( m_1 \geq m \), \( m_1^{2^{m_1}} \leq 2^{m_1^{2^{m_1}}} \), hence there exist an \( n > m \), a \( 2^n \times n^t \text{-sparse matrix } A \in \mathcal{M} \setminus \mathbb{N} \), a \( b \in \mathcal{M} \setminus \mathbb{N} \) such that \( b \notin \text{Rng}(NW_{f,A}) \), and an \( F_{d'}-\text{proof } \pi \in \mathcal{M} \) for \( \tau_b(NW_{f,A}) \) such that \( |\pi| \leq |\tau_b(NW_{f,A})|^{c} \). Now we consider \( M_n' \) and by the argument in this section, there exists a \( \chi' \subseteq P(M_n') \) such that it has every bounded \( M \)-definable subset of \( M_n' \) and moreover
1. \( (M_n', \chi') \models \forall \).
2. There exists an \( \alpha \in \chi' \) which falsifies \( \tau_b(NW_{f,A}) \).

Then by Theorem 4 there is no \( F_{d'}-\text{proof } \tau_b(NW_{f,A}) \) in \( (M_n', \chi') \). Note that there is a standard number \( e \) such that
\[
|\pi| \leq |\tau_b(NW_{f,A})|^c \leq (n^{ct}2^{cn})^{c} \leq 2^{cn^{ct/2}}
\]
which implies that \( \pi \in \chi \), but this leads to a contradiction and completes the proof.

### 4 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 hardness 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 $1 - o(1)$, $b \not\in \text{Rng}(\text{NW}_{\oplus,A})$. Now, if we choose a random $A$ and a random $b$ uniformly, then with probability $1 - o(1)$ $\tau_b(\text{NW}_{\oplus,A})$ is a tautology (here we use DNF representation of the Parity function in the definition of the $\tau$ formula). The interesting point about these formulas is that if $\tau_b(\text{NW}_{\oplus,A})$ 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 [14, 3]). For more information, see Section 13.4 of [21].

In this regard, Krajíček [21] asked whether random systems of linear equations over $\mathbb{F}_2$ are hard for $\text{AC}^0$-Frege or not (problem 19.4.5). We note that Theorem 6 partially answers this question as follows.

Let $(\phi_0, \phi_1)$ be a $\Sigma^1_1 \cap \Pi^1_2$ definition of a function $f \in \text{NP} \cap \text{CoNP}$ (for example we can take $f$ as the Parity function). Then a random formula $F \sim F(\phi_0, \phi_1, m, n, l)$ 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 $F := \tau_b(\text{NW}_{f,A})$ based on $(\langle \phi_0 \rangle_1, \langle \phi_1 \rangle_1)$.

The following corollary partially answers Krajíček’s question.

**Corollary 13.** Let $f \in \text{NP} \cap \text{CoNP}$ be a symmetric function such that $S_{\text{AC}^0_2}(f_n) = 2^nO(1)$. Let $(\phi_0, \phi_1)$ be a $\Sigma^1_1 \cap \Pi^1_1$ definition of $f$. Then for every $d$, for every $c > 1$ and every $0 < \epsilon < 1$, if $n$ is large enough, then $F \sim F(\phi_0, \phi_1, n^c, n, [n^c])$ is a tautology with probability $1 - o(1)$ and it requires exponential $F_d$-proofs.

Another implication of the hardness of $\text{NW}$-generators for a proof system $P$ is that it implies that it is hard for $P$ to prove circuit lower bounds effectively. Razborov [37] pointed out that if the base function is in $P/\text{poly}$ and the $2^n \times n^{O(1)}$ matrix $A$ is efficiently constructible (an example of such matrices was constructed in [26]), and moreover $\text{NW}_{f,A}$ is a hard proof complexity generator for a proof system $P$, the $P$ cannot prove circuit lower bounds effectively. Moreover, this implies that $\text{NP} \not\subseteq P/\text{poly}$ does not have efficient proofs in $P$. Razborov proved such a result for $k$-DNF Resolution in [37]. 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 $\text{AC}^0$-Frege was asked by Krajíček [21] (problem 19.6.1). Let $f \in \text{NTime}(n^k) \cap \text{CoNTime}(n^k)$ and $A$ be a $2^n \times n^k$ $n^k$-sparse matrix which is effectively constructible. Then for any fixed $w \in \{0,1\}^n$, $\text{NW}_{f,A}(w)$ defines a function $C_w \in (\text{NTime}(n^k) \cap \text{CoNTime}(n^k))/\text{poly}$ as follows:

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

This means that if $\tau_b(\text{NW}_{f,A})$ 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 $w \in \{0,1\}^n$. As Theorem 6 (part 2) implies that $\text{NW}$-generators based on suitable $\text{NP} \cap \text{CoNP}$ functions, suitable matrices, and suitable representations are hard proof complexity generators $\text{AC}^0$-Frege, we get the fact that proving certain $(\text{NP} \cap \text{CoNP})/\text{poly}$ lower bounds ($b$ does not have $C_w$ circuits) for Boolean functions are hard for $\text{AC}^0$-Frege. Note that in contrast with with the principle $f_n \not\in \text{SIZE}(n^k)$ which can be written as a propositional formula, it is not clear how the principle $f_n \not\in (\text{NTime}(n^k) \cap \text{CoNTime}(n^k))/\text{poly}$ can be written as a propositional formula. So one way of considering this principle in proof complexity is to consider $\tau_{f_n}(\text{NW}_{f,A})$ for any
$g \in \text{NTime}(n^k) \cap \text{CoNTime}(n^k)$, any representation of $g$ and any effectively constructible $A$. In this regard, Theorem 6 states lower bounds for a lot of possible natural formalizations (but not all) of the principle $f_n \notin (\text{NTime}(n^k) \cap \text{CoNTime}(n^k))/\text{poly}$.

References