Electronic Colloquium on Computational Complexity, Report No. 8 (2026)

A Note on Natural-Proofs for Super-Linear Lower Bounds for Linear Functions

Ran Raz *

Abstract

Proving super-linear lower bounds on the size of circuits computing explicit linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$ is a fundamental long-standing open problem in circuit complexity. We focus on the case where $\mathbb{F}$ is a finite field. The circuit can be either a Boolean circuit or an arithmetic circuit with scalar products and sum gates over $\mathbb{F}$.

We extend the notion of natural proofs [RR97] to the context of proving circuit lower bounds for linear functions. Let $L_n = \mathbb{F}^{n^2}$ denote the set of all linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$, represented by their corresponding $n \times n$ matrices over $\mathbb{F}$. We say that a lower bound proof for the circuit complexity of a linear function $A : \mathbb{F}^n \to \mathbb{F}^n$ is *natural*, if either implicitly or explicitly, the proof defines for every n a subset $C_n \subset L_n$, such that, there exists a polynomial-time recognizable subset $C'_n \subseteq C_n$, such that, $|C'_n| \geq \frac{1}{\text{poly}(n)} \cdot |L_n|$ and the lower bound applies for every function $A \in C'_n$. This definition is analogous to the original definition of natural proofs by Razborov and Rudich [RR97], modified to the study of linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$, represented by their corresponding $n \times n$ matrices, rather than general Boolean functions, represented by their truth tables.

We observe that recent works on *trapdoored matrices*, by Vaikuntanathan and Zamir [VZ26] and Braverman and Newman [BN25], imply that, assuming (strong but plausible) cryptographic assumptions, natural proofs cannot establish circuit lower bounds higher than $n \cdot \text{polylog}(n)$ for linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$.

We study the problem of proving super-linear lower bounds on the size of circuits computing explicit linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$. We focus on the case where $\mathbb{F}$ is a finite field. The circuit can be either a Boolean circuit (that uses the Boolean gates $\wedge, \vee, \neg$), or an arithmetic circuit (that uses scalar products and sum gates[1] over $\mathbb{F}$). Since a linear function $A : \mathbb{F}^n \to \mathbb{F}^n$ can be represented as an $n \times n$ matrix over $\mathbb{F}$, a simple counting argument implies that the circuit complexity of most linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$ is at least $\Omega(n^2/\log n)$. However, for explicit linear functions, no lower bound better than $\Omega(n)$ is known. In this note, we investigate whether there are natural-proofs barriers for proving super-linear lower bounds for such functions.

*Department of Computer Science, Princeton University. Research supported by a Simons Investigator Award. Email: ran.raz.mail@gmail.com

[1] It is well known that non-scalar product gates do not decrease the arithmetic circuit complexity of a linear function.

ISSN 1433-8092

A landmark work by Razborov and Rudich introduced the notion of Natural Proofs in the context of proving circuit lower bounds [RR97]. Let $F_n = \{0,1\}^{2^n}$ denote the set of all Boolean functions $f : \{0,1\}^n \to \{0,1\}$, represented by their truth tables. A lower bound proof for the circuit complexity of a function $f : \{0,1\}^n \to \{0,1\}$ is called *natural*, if either implicitly or explicitly, the proof defines for every n a subset $C_n \subset F_n$, such that, there exists a subset $C'_n \subseteq C_n$, satisfying the following three properties:

1. Usefulness: The lower bound applies for every function $f \in C'_n$.
2. Constructivity: There is a polynomial time algorithm that given the truth table of a function $f : \{0,1\}^n \to \{0,1\}$, determines whether $f \in C'_n$.
3. Largeness: $|C'_n| \geq 2^{-O(n)} \cdot |F_n|$.

These conditions formalize the idea that a natural proof identifies a large, efficiently recognizable class of functions for which the lower bound holds. Razborov and Rudich proved that, assuming standard cryptographic assumptions, natural proofs cannot establish super-polynomial circuit lower bounds, or other strong circuit lower bounds [RR97]. This result is often viewed as a barrier for proving strong circuit lower bounds.

While the view of natural proofs as a barrier for proving strong circuit lower bounds is highly controversial (see for example [For24]), natural proofs have been extensively studied in numerous works from a wide range of perspectives, and were found to be relevant to many other issues in computational complexity theory (see for example [Razb95, Cho11, MV15, Wil16, CIKK16, GKSS17, FSV18, KPI25, KLMS25]).

We extend the notion of natural proofs to the context of proving circuit lower bounds for linear functions. Let $L_n = \mathbb{F}^{n^2}$ denote the set of all linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$, represented by their corresponding $n \times n$ matrices over $\mathbb{F}$. We say that a lower bound proof for the circuit complexity of a linear function $A : \mathbb{F}^n \to \mathbb{F}^n$ is *natural*, if either implicitly or explicitly, the proof defines for every n a subset $C_n \subset L_n$, such that, there exists a subset $C'_n \subseteq C_n$, satisfying the following three properties:

1. Usefulness: The lower bound applies for every function $A \in C'_n$.
2. Constructivity: There is a polynomial time algorithm that given the $n \times n$ matrix over $\mathbb{F}$ corresponding to a linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$, determines whether $A \in C'_n$.
3. Largeness: $|C'_n| \geq \frac{1}{\text{poly}(n)} \cdot |L_n|$.

These conditions are analogous to the corresponding usefulness, constructivity and largeness conditions in the original definition of natural proofs. Note that while the description of a Boolean function $f : \{0,1\}^n \to \{0,1\}$ by its truth table is of exponential length, the description of a linear function $A : \mathbb{F}^n \to \mathbb{F}^n$ by its corresponding $n \times n$ matrix is of quadratic length. It is hence reasonable to scale-up the fraction $2^{-O(n)}$ in the largeness condition in the original definition of natural proofs to $\frac{1}{\text{poly}(n)}$ in our new definition, as they are both inverse polynomial in the length of description of the corresponding function.

Striking recent works by Vaikuntanathan and Zamir [VZ26] and Braverman and Newman [BN25] introduced the concept of *trapdoored matrices*. A distribution of $n \times n$

trapdoored matrices is a distribution D_n over L_n, satisfying the following two properties: (See Definition 2.1, Definition 2.2 and Definition 2.3 in [VZ26])[2]

1. Efficiency: Every function $A : \mathbb{F}^n \to \mathbb{F}^n$ in the support of D_n has a circuit of size almost linear in n.

2. Indistinguishability: D_n is indistinguishable from the uniform distribution over L_n by a polynomial time algorithm. Specifically, for any polynomial time algorithm T, the probability that T outputs 1 on a matrix A drawn from the distribution D_n is almost equal to the probability that T outputs 1 on a matrix A drawn from the uniform distribution over L_n, where *almost equal* means that the difference between them vanishes faster than any inverse polynomial in n.

Our main result is the following observation:

Corollary 1. *Assume that there exists a family of distributions $\{D_n : n \in \mathbb{N}\}$, such that, for every n, D_n is a distribution over L_n, and:*

1. *Efficiency: Every function $A : \mathbb{F}^n \to \mathbb{F}^n$ in the support of D_n has an arithmetic circuit of size at most $s(n)$.*

2. *Indistinguishability: The distribution D_n is indistinguishable from the uniform distribution over L_n by a polynomial time algorithm.*

Then, natural proofs cannot establish lower bounds higher than $s(n)$ on the arithmetic circuit complexity of linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$.

Proof. Similarly to [RR97], assume for a contradiction that there exists a natural proof that establishes a lower bound higher than $s(n)$ on the arithmetic circuit complexity of linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$. Let $C'_n \subseteq L_n$ be the corresponding subset that satisfies the three required properties: Usefulness, Constructivity and Largeness. Denote by D'_n the support of D_n.

By the Efficiency property of D_n and the Usefulness property of C'_n, the subsets C'_n and D'_n are disjoint. By the Constructivity property of C'_n, there is a polynomial time algorithm T that determines whether a matrix A is in C'_n. Thus, T is a polynomial time algorithm that outputs 1 on inputs in C'_n and 0 on inputs in D'_n. By the Largeness property of C'_n, we have that T outputs 1 with non-negligible probability over L_n (that is, T outputs 1 with probability larger than some inverse polynomial in n), while it outputs 0 on inputs in D'_n, and thus violates the Indistinguishability property of D_n. □

Note that a lower bound higher than $c \cdot s(n)$ on the Boolean circuit complexity of a function $A : \mathbb{F}^n \to \mathbb{F}^n$ implies a lower bound higher than $s(n)$ on the arithmetic circuit complexity of the same function (when $\mathbb{F}$ is a finite field and c is a sufficiently large constant). Hence, Corollary 1 also implies that natural proofs cannot establish lower bounds higher than $c \cdot s(n)$ on the Boolean circuit complexity of linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$.

[2] We ignore here the requirement of *efficient sampleability* in [VZ26], as this requirement is immaterial for our work.

Explicit constructions of distributions of trapdoored matrices (under cryptographic assumptions) were given in [VZ26, BN25, BCHIKMRR25]. For example, Vaikuntanathan and Zamir proved the following theorem: (Theorem 3.1 in [VZ26]. A similar construction was given by Braverman and Newman [BN25])

Theorem 2. *[VZ26, BN25] There exists a family of distributions $\{D_n : n \in \mathbb{N}\}$, such that, for every n, D_n is a distribution over L_n, and:*

1. *Efficiency: Every function $A : \mathbb{F}^n \to \mathbb{F}^n$ in the support of D_n has an arithmetic circuit of size $O(n \cdot \mathrm{polylog}(n))$.*
2. *Indistinguishability: Assuming the sub-exponential hardness of learning parity with noise, generalized to the field $\mathbb{F}$ (for exact statement and parameters, see Section 3 in [VZ26]), the distribution D_n is indistinguishable from the uniform distribution over L_n by a polynomial time algorithm.*[3]

Corollary 3. *Assuming the sub-exponential hardness of learning parity with noise, generalized to the field $\mathbb{F}$ (for exact statement and parameters, see Section 3 in [VZ26]), natural proofs cannot establish lower bounds higher than $n \cdot \mathrm{polylog}(n)$ on the arithmetic circuit complexity of linear functions $A : \mathbb{F}^n \to \mathbb{F}^n$ (for some $\mathrm{polylog}(n)$).*

Proof. The proof follows immediately from Corollary 1 and Theorem 2. □

As before, since lower bounds on Boolean circuit complexity imply lower bounds on arithmetic circuit complexity, Corollary 3 applies to Boolean circuits as well.

References

[BCHIKMRR25] Fabrice Benhamouda, Caicai Chen, Shai Halevi, Yuval Ishai, Hugo Krawczyk, Tamer Mour, Tal Rabin, Alon Rosen: Encrypted Matrix-Vector Products from Secret Dual Codes. CCS 2025: 394-408 4

[BN25] Mark Braverman, Stephen Newman: Practical Secure Delegated Linear Algebra with Trapdoored Matrices. TCC 2025 1, 2, 4

[Cho11] Timothy Y. Chow: Almost-Natural Proofs. J. Comput. Syst. Sci. 77(4): 728-737 (2011) 2

[CIKK16] Marco L. Carmosino, Russell Impagliazzo, Valentine Kabanets, Antonina Kolokolova: Learning Algorithms from Natural Proofs. CCC 2016: 10:1-10:24 2

[For24] Lance Fortnow: Natural Proofs is Not the Barrier You Think It Is. Computational Complexity Blog. https://blog.computationalcomplexity.org/2024/09/natural-proofs-is-not-barrier-you-think.html 2

[3] Under the *polynomial* hardness of learning parity with noise, generalized to the field $\mathbb{F}$, the obtained efficiency is $O(n^{1+\epsilon})$, for an arbitrary small $\epsilon > 0$, rather than $O(n \cdot \mathrm{polylog}(n))$.

[FSV18] Michael A. Forbes, Amir Shpilka, Ben Lee Volk: Succinct Hitting Sets and Barriers to Proving Lower Bounds for Algebraic Circuits. Theory Comput. 14(1): 1-45 (2018) 2

[GKSS17] Joshua A. Grochow, Mrinal Kumar, Michael E. Saks, Shubhangi Saraf: Towards an Algebraic Natural Proofs Barrier via Polynomial Identity Testing. Electron. Colloquium Comput. Complex. TR17 (2017) 2

[KLMS25] Michal Koucky, Bruno Loff, Tulasimohan Molli, Mike Saks: The Natural-Proofs Barrier Against Data Structure Lower Bounds. Manuscript (2025) 2

[KPI25] Oliver Korten, Toniann Pitassi, Russell Impagliazzo: Stronger Cell Probe Lower Bounds via Local PRGs. FOCS 2025 2

[MV15] Eric Miles, Emanuele Viola: Substitution-Permutation Networks, Pseudorandom Functions, and Natural Proofs. J. ACM 62(6): 46:1-46:29 (2015) 2

[Razb95] Alexander A. Razborov: Unprovability of Lower Bounds on Circuit Size in Certain Fragments of Bounded Arithmetic. Izvestiya: Mathematics 59(1), 205-227 (1995) 2

[RR97] Alexander A. Razborov, Steven Rudich: Natural Proofs. J. Comput. Syst. Sci. 55(1): 24-35 (1997) 1, 2, 3

[VZ26] Vinod Vaikuntanathan, Or Zamir: Improving Algorithmic Efficiency Using Cryptography. SODA 2026 1, 2, 3, 4

[Wil16] Ryan Williams: Natural Proofs versus Derandomization. SIAM J. Comput. 45(2): 497-529 (2016) 2

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il