Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 193 (2020)

Average-case rigidity lower bounds

Xuangui Huang* Emanuele Viola*

April 9, 2021

Abstract

It is shown that there exists $f : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}$ in $\mathrm{E}^{\mathbf{NP}}$ such that for every $2^{n/2} \times 2^{n/2}$ matrix M of rank $\leq \rho$ we have $\mathbb{P}_{x,y}[f(x,y) \neq M_{x,y}] \geq 1/2 - 2^{-\Omega(k)}$, whenever $\log \rho \leq \delta n/k(\log n + k)$ for a sufficiently small $\delta > 0$, and n is large enough. This generalizes recent results which bound below the probability by $1/2 - \Omega(1)$ or apply to constant-depth circuits.

Starting with the seminal paper by Williams [Wil14b] a sequence of recent works have proved new lower bounds for functions in various classes which contain super-polynomial non-deterministic time [Wil11, Wil13, Wil14a, ACW16, Tam16, COS18, MW18, RSS18, AC19, Che19, CW19, VW20, CR20, Vio20, CLW20, BHPT20], lower bounds that we do not know how to prove by other means. Two sub-sequences of results are relevant to the present work. The first is the sub-sequence establishing *average-case hardness results* for various circuit classes. The concurrent works [CR20, Vio20] proved incomparable, new average-case lower bounds against AC^0 with parity gates. Both results were improved in [CLW20] to obtain a function that any such circuit of sub-exponential size cannot compute with a sub-exponentially small advantage over random guessing, for a uniform input.

The second is the sub-sequence constructing *rigid matrices* [Val77], that is, obtaining functions $f(x,y)$, where $|x| = |y| = n/2$ such that the corresponding $2^{n/2} \times 2^{n/2}$ matrix $M_{x,y} = f(x,y)$ is far from low-rank matrices. Using PCPs, [AC19] gave f such that $\mathbb{P}[M_{x,y} \neq f(x,y)] \geq \Omega(1)$ for any M of rank up to at most $2^{n^{1/4-\varepsilon}}$. Low-rank matrices are a generalization of low-degree polynomials [SV12], but the rank bound in [AC19] is not strong enough to improve the classic results on polynomials due to Razborov and Smolensky [Raz87, Smo87, Smo93] which hold up to degree $\sqrt{n}$. The subsequent paper [Vio20] achieved nearly-optimal probabilistic degree $n/\mathrm{poly}\log n$ relying on the PCP construction [BV14]. It also raised the question of constructing PCPs with stronger properties and showed that these would improve the rank bounds in [AC19] to $2^{n/\Omega(\log^2 n)}$ (under some distribution). Related PCPs were constructed in the subsequent work [BHPT20], finally obtaining f such that $\mathbb{P}[M_{x,y} \neq f(x,y)] \geq \Omega(1)$ for any M of rank up to $2^{n/\Omega(\log n)}$.

In this paper we prove a result that generalizes both sub-sequences. We simultaneously achieve the strong average-case hardness parameters of [CLW20] and work in the general model of low-rank matrices.

Theorem 1. *There exists a function $f\colon \{0,1\}^n \times \{0,1\}^n \to \{-1,1\}$ in $\mathrm{E}^{\mathbf{NP}}$ such that for any rank-ρ matrix M, we have*

$$\mathbb{P}_{x,y}[f(x,y) \neq M_{x,y}] \geq 1/2 - 2^{-\Omega(k)}$$

*Supported by NSF CCF award 1813930.

ISSN 1433-8092

for all large enough n, where $k(\log n + k)\log \rho \leq \delta n$ for a sufficiently small constant $\delta > 0$.

To illustrate the parameters, we can prove lower bounds whenever $k^2 \log \rho \leq \delta n$, for $k \geq \log n$. In particular we can for example bound below the probability by $1/2 - 2^{-n^{\Omega(1)}}$ for log rank $n^{0.99}$. We can also have $\log \rho = n/\Omega(\log n)$ whenever $k = O(1)$, recovering the result from [BHPT20].

It seems within reach to improve the tradeoff between k and ρ to obtain lower bounds whenever $k \log \rho \leq \delta n$. Improving the tradeoff even further to obtain lower bounds when $k \log \rho$ is $n^{1+\Omega(1)}$ would give new *data-structure lower bounds*, for functions in $\mathrm{E}^{\mathbf{NP}}$, via a connection established in [Vio20].

Independently, Chen and Lyu [CL21] proved lower bounds whenever $k^{1.5} \log \rho \leq \delta n$. Their proof proceeds in exactly the same way as ours, but in addition they prove a new derandomized XOR lemma where the seed length is just $\sqrt{k}n$ as opposed to kn in our Lemma 22. One can also plug their new XOR lemma in our proof and infer the stronger bound.

Techniques and organization. Our proof builds on the previous work mentioned earlier. We adapt a clever approach in [CLW20] which is based on Levin's proof of Yao's famous XOR lemma, cf. [GNW11]. The approach shows that to prove a strong average-case hardness result it suffices to prove a mild average-case hardness result *for an intermediate model*. The intermediate model in our case consists of *rational sums of low-rank matrices*. We show that a lower bound for this model can be obtained from the rectangular PCP in [BHPT20], see Theorem 19.

A little more in detail, we prove a constant-error lower bound for rational sums of low-rank matrices by contradiction using the non-deterministic time-hierarchy theorem following [Wil10]. We fix a unary language in $\mathbf{NTIME}(2^n) \setminus \mathbf{NTIME}(o(2^n))$, and let the lexicographically first rectangular PCP proof for this language be the hard function. Assuming that this hard function has constant correlation with a sum of low-rank matrices, we derive a contradiction by giving a quick non-deterministic algorithm. This algorithm first guesses a sum of low-rank matrices as an approximation of the hard function, i.e. the boolean proof, then performs a series of validity tests that are adapted from [CLW20] to guarantee that this sum is bounded and close to boolean. Then the rectangular property of the PCP is exploited to make sure that when the guessed sum is plugged in as a proof, the bits that the PCP verifier probes can also be written as sums of low-rank matrices, thus the algorithm can quickly evaluate the "acceptance probability" of the guessed sum, based on the fast counting algorithm for low-rank matrices in [CW16, AC19]. Now the boundedness and close-to-boolean properties will ensure that this "acceptance probability" is close to that of the boolean proof approximated by the guessed sum, so the algorithm can make a decision for the language based on this value.

We shall first prove our result for infinitely many input lengths n; at the end we shall explain what modifications are sufficient to obtain all sufficiently large n, using results in [CLW20].

1 Preliminaries

For any $n \in \mathbb{N}$, define $[n] = \{1, 2, \ldots, n\}$. For any matrix M, we use $M_{i,j}$ to denote its entry on row i column j. For any $n \times m$ matrix M define the matrix $(-1)^M$ by $\left((-1)^M\right)_{i,j} = (-1)^{M_{i,j}}$ for all $i \in [n]$, $j \in [m]$. For any matrix M, we define its ℓ_p-norm as $\|M\|_p = (\mathbb{E}_{i,j}[|M_{i,j}|^p])^{1/p}$, while the ℓ_∞-norm is defined as $\|M\|_\infty = \max_{i,j} |M_{i,j}|$. For any two matrices A and B with the same shape, we define $A \circ B$ to be the Hadamard product (entrywise product) of them over $\mathbb{R}$, which is distributive. We use $\widetilde{O}$ to hide $\mathrm{poly}(n)$ terms in runtime.

Definition 2. *For any $\alpha \in \mathbb{Q}$ we define its* bit-complexity *as the maximum of the bit lengths of the denominator and numerator. For a polynomial p with rational coefficients we define its bit complexity as the maximum bit complexity among the coefficients.*

Definition 3. *For any given function class $\mathcal{C}$, we call the sum $\widetilde{Q} = C\sum_{i=1}^{m} b_i \cdot f_i$ an m-sum of $\mathcal{C}$, for $b_i \in \{-1,1\}$ and $f_i \in \mathcal{C}$ for all $i \in [m]$ and $C \in \mathbb{Q}$. We define the* bit-complexity of $\widetilde{Q}$ *as the bit-complexity of C.*

*In particular, an m-*sum of rank-ρ $\mathbb{F}_2$-matrices *$\widetilde{Q} \in \mathbb{R}^{n\times n'}$ is given by $\widetilde{Q} = C\sum_{i=1}^{m} b_i \cdot (-1)^{M^{(i)}}$ where $M^{(i)} \in \mathbb{F}_2^{n\times n'}$ are rank-ρ matrices over $\mathbb{F}_2$.*

Definition 4. *Let $f, g\colon \{0,1\}^n \to [-1,1]$ be two functions. We define their* correlation *as $\mathsf{corr}(f,g) = \left|\mathbb{E}_{x\sim\{0,1\}^n}[f(x)g(x)]\right|$. We say f ε-*correlates with *g iff $\mathsf{corr}(f,g) \geq \varepsilon$.*

Definition 5. *We say a matrix M is* bounded *if $M_{i,j} \in [-1,1]$ for all i, j. Similarly, we say a function f is* bounded *if $f(x) \in [-1,1]$ for all x.*

Definition 6. *For any boolean function $f\colon \{-1,1\}^k \to \mathbb{R}$, we identify f with its* multilinear extension over domain $\mathbb{R}$*, defined by its Fourier expansion $f = \sum_{S\subseteq[k]} \beta_S \prod_{i\in S} x_i$, where $\beta_S \in \mathbb{R}$. For any sets X, Y and function $f\colon X^k \to Y$ we define its* extension over matrices *$\overline{f}\colon (X^{n\times m})^k \to Y^{n\times m}$ that maps matrices $M^{(1)}, M^{(2)}, \ldots, M^{(n)} \in X^{n\times m}$ to a matrix $M' \in Y^{n\times m}$ defined by $M'_{i,j} = f(M^{(1)}_{i,j}, M^{(2)}_{i,j}, \ldots, M^{(k)}_{i,j})$ for all $i \in [n], j \in [m]$.*

For example, the Hadamard product $A \circ B$ of matrices A and B is recovered as $\overline{f}(A,B)$ where f is multiplication.

Rectangular PCP. We need the following rectangular PCP to prove this theorem.

Definition 7 (Rectangular PCP, [BHPT20])**.** *For any language L, we say it has* an $(\ell^2, r, q, p, t, s, \tau)$-rectangular PCP verifier V over alphabet $\{-1,1\}$ *if we have the following properties:*

Proof. *the proof π of length ℓ^2 is viewed as a matrix in $\{-1,1\}^{\ell\times\ell}$.*

Randomness. *the random string $R \in \{0,1\}^r$ is partitioned into three parts*

$$R = (R_{\mathsf{row}}, R_{\mathsf{col}}, R_{\mathsf{shared}}) \in \{0,1\}^{r_{\mathsf{rect}}} \times \{0,1\}^{r_{\mathsf{rect}}} \times \{0,1\}^{r_{\mathsf{shared}}},$$

where $r_{\mathsf{rect}} = (1-\tau)r/2$ and $r_{\mathsf{shared}} = \tau r$.

Computation. *Given input x and proof oracle $\pi \in \{-1,1\}^{\ell\times\ell}$, with randomness R, $V^{\pi}(x;R)$ runs as follows:*

1. *Use shared randomness $R_{\mathsf{shared}} \in \{0,1\}^{r_{\mathsf{shared}}}$ to:*
   (a) *construct a decision function $D = D(x; R_{\mathsf{shared}})\colon \{-1,1\}^q \times \{-1,1\}^p \to \{0,1\}$,*
   (b) *construct randomness parity check $(C_1, \ldots, C_p) = (C_1(x; R_{\mathsf{shared}}), \ldots, C_p(x; R_{\mathsf{shared}}))$ where each $C_i\colon \{0,1\}^{r_{\mathsf{rect}}} \times \{0,1\}^{r_{\mathsf{rect}}} \to \{-1,1\}$ is a parity function, i.e. $C_i(R_{\mathsf{row}}, R_{\mathsf{col}}) = (-1)^{\langle R_{\mathsf{row}}, u\rangle + \langle R_{\mathsf{col}}, v\rangle + b}$ for some $u, v \in \{0,1\}^{r_{\mathsf{rect}}}$ and $b \in \{0,1\}$, where $\langle x, y\rangle$ is the inner product of x and y.*
2. *Use row randomness $R_{\mathsf{row}} \in \{0,1\}^{r_{\mathsf{rect}}}$ to construct row locations of queries*

$$i^{(1)} = i^{(1)}(x; R_{\mathsf{row}}, R_{\mathsf{shared}}), \ldots, i^{(q)} = i^{(q)}(x; R_{\mathsf{row}}, R_{\mathsf{shared}}).$$

3. Use column randomness $R_{\mathsf{col}} \in \{0,1\}^{r_{\mathsf{rect}}}$ to construct column locations of queries

$$j^{(1)} = j^{(1)}(x; R_{\mathsf{col}}, R_{\mathsf{shared}}), \ldots, j^{(q)} = j^{(q)}(x; R_{\mathsf{col}}, R_{\mathsf{shared}}).$$

4. Output the result

$$D(\pi_{i^{(1)},j^{(1)}}, \ldots, \pi_{i^{(q)},j^{(q)}}, C_1(R_{\mathsf{row}}, R_{\mathsf{col}}), \ldots, C_p(R_{\mathsf{row}}, R_{\mathsf{col}})).$$

Completeness. *If $x \in L$ then $\exists \pi \in \{-1,1\}^{\ell \times \ell}, \Pr_R[V^\pi(x;R) = 1] = 1$.*

Soundness. *If $x \notin L$ then $\forall \pi \in \{-1,1\}^{\ell \times \ell}, \Pr_R[V^\pi(x;R) = 1] < s$.*

Complexity *The verifier V runs in time $t \geq r$, the query complexity is q and parity-check complexity is p.*

Definition 8. *We say an $(\ell^2, r, q, p, t, s, \tau)$-rectangular PCP verifier is* smooth *if V queries uniformly on π over the choice of randomness $R \in \{0,1\}^r$ and queries $k \in [q]$.*

The above definition means that each location of the proof has equal probability of being queried by a *random* query. A stronger requirement would be that this holds for *each* query. The stronger notion is available in some PCPs (e.g. [Par20]), but as far as we know not for rectangular PCPs.

Lemma 9 ([BHPT20])**.** *For any constants $s \in (0, \frac{1}{2})$, $\tau \in (0,1)$, and language $L \in \mathbf{NTIME}(2^n)$, L has a smooth $(\ell^2, r, q, p, t, s, \tau)$-rectangular PCP verifier V over alphabet $\{-1,1\}$ with the following parameters:*

- $r = n + O(\log n)$.
- $q, p = O_s(1)$.
- $\ell^2 = O_s(2^r)$.
- $t = 2^{O(\tau n)}$.

2 Fast Algorithm for "Acceptance Probability"

In this section we prove and collect several facts that allow us to quickly compute the acceptance probability of a rectangular PCP verifier when its proof is a rational sum of low-rank matrices.

First we need the following result to quickly calculate number of 1's in low-rank matrices over $\mathbb{F}_2$ given low-rank decompositions.

Lemma 10 ([CW16, AC19])**.** *Given two matrices $A \in \mathbb{F}_2^{N \times \rho}$ and $B \in \mathbb{F}_2^{\rho \times N}$ where $\rho = N^{o(1)}$, there is a deterministic algorithm that computes the number of 1's in the product matrix AB over $\mathbb{F}_2$ in time $T(N, \rho) = N^{2 - \Omega(1/\log \rho)}$.*

We prove a general result on evaluating the expectation of a polynomial on sums of low-rank matrices.

Theorem 11. *Let $\left\{\widetilde{Q}_i\right\}_{i\in[k]}$ be k m-sums of rank-ρ $\mathbb{F}_2$ matrices with bit-complexity c, and let their low-rank decompositions be $\widetilde{Q}_i = C_i \sum_{i=1}^{m} b_{i,j}\cdot(-1)^{A^{(i,j)}B^{(i,j)}}$ where $C_i \in \mathbb{Q}$ has bit-complexity c, $b_{i,j}\in\{-1,1\}$, $A^{(i,j)}\in\mathbb{F}_2^{N\times\rho}$, and $B^{(i,j)}\in\mathbb{F}_2^{\rho\times N}$ for all $i\in[k]$ and $j\in[m]$. For any s-sparse degree-d polynomial on k variables $p\colon\mathbb{R}^k\to\mathbb{R}$ with bit complexity c', given the decompositions we can compute the value of $\mathbb{E}_{i,j\in[N]}\left[\left(\overline{p}\left(\widetilde{Q}_1,\dots,\widetilde{Q}_k\right)\right)_{i,j}\right]$ in time $O\big(sm^d(T(N,d\rho)+\mathrm{poly}(c,c',d,\log N))\big)$ if $d\rho = N^{o(1)}$. In particular for any boolean function $f\colon\{-1,1\}^k\to\{0,1\}$ it can be computed in time $O\big(2^k m^k(T(N,k\rho)+\mathrm{poly}(c,k,\log N))\big)$ if $k\rho = N^{o(1)}$.*

Proof. To calculate $\mathbb{E}_{i,j}\left[\left(\overline{p}\left(\widetilde{Q}_1,\dots,\widetilde{Q}_k\right)\right)_{i,j}\right]$, by linearity of expectation it suffices to calculate the expectation for each monomial of p. Wlog, let the monomial $p'(x) = x_1x_2\cdots x_d$. Then by the distributive property of Hadamard products we have

$$\begin{aligned}
\overline{p'}\left(\widetilde{Q}_1,\dots,\widetilde{Q}_k\right) &= \widetilde{Q}_1\circ\widetilde{Q}_2\circ\cdots\circ\widetilde{Q}_d\\
&= \circ_{i=1}^{d}\left(C_i\sum_{j=1}^{m} b_{i,j}\cdot(-1)^{A^{(i,j)}B^{(i,j)}}\right)\\
&= \sum_{(j_1,j_2,\dots,j_d)\in[m]^d}\left(\prod_{i=1}^{d} C_i b_{i,j_i}\right)\cdot\left(\circ_{i=1}^{d}(-1)^{A^{(i,j_i)}B^{(i,j_i)}}\right)\\
&= \sum_{(j_1,j_2,\dots,j_d)\in[m]^d}\left(\prod_{i=1}^{d} C_i b_{i,j_i}\right)\cdot\left((-1)^{\oplus_{i=1}^{d}A^{(i,j_i)}B^{(i,j_i)}}\right),
\end{aligned}$$

where '$\oplus$' is the addition of $\mathbb{F}_2$-matrices over $\mathbb{F}_2$. Hence by linearity of expectation, it suffices to calculate the expectation of $(-1)^{\oplus_{i=1}^{d}A^{(i,j_i)}B^{(i,j_i)}}$ for each $(j_1,\dots,j_d)\in[m]^d$. Note that for any $\mathbb{F}_2$-matrix M we have $\mathbb{E}_{\mathsf{row},\mathsf{col}}\left[\left((-1)^M\right)_{\mathsf{row},\mathsf{col}}\right] = 1-2\mathbb{E}_{\mathsf{row},\mathsf{col}}[M_{\mathsf{row},\mathsf{col}}]$, thus it suffices to calculate

$$\mathbb{E}_{\mathsf{row},\mathsf{col}}\left[\left(\oplus_{i=1}^{d}A^{(i,j_i)}B^{(i,j_i)}\right)_{\mathsf{row},\mathsf{col}}\right] = \frac{1}{N^2}\cdot\text{ number of 1's in }\oplus_{i=1}^{d}A^{(i,j_i)}B^{(i,j_i)}.$$

Note that $\oplus_{i=1}^{d}A^{(i,j_i)}B^{(i,j_i)}$ is just the product of an $N\times d\rho$ matrix and a $d\rho\times N$ matrix over $\mathbb{F}_2$, where the first matrix is obtained by concatenating the rows of $\left\{A^{(i,j_i)}\right\}_{i\in[d]}$ and the second matrix is obtained by concatenating the columns of $\left\{B^{(i,j_i)}\right\}_{i\in[d]}$. Hence by Lemma 10 the counting can be done in time $T(N,d\rho)$ if $d\rho = N^{o(1)}$. This expectation value has bit-complexity $O(\log N)$, so multiplying it by $\prod_{i=1}^{d}C_ib_{i,j_i}$ and adding to the running sum take time $\mathrm{poly}(c,d,\log N)$. We still need to multiply the result by the coefficients of the monomials in p, thus the runtime becomes $\mathrm{poly}(c,c',d,\log N)$. Therefore the total running time is $O\big(sm^d(T(N,d\rho)+\mathrm{poly}(c,c',d,\log N))\big)$.

For any boolean function f, it can be written as a degree-k multilinear polynomial so there are at most 2^k monomials. Fourier analysis shows that every coefficient of this polynomial is a multiple of 2^{-k}, so its bit complexity is $O(k)$. Therefore the total running time becomes $O(2^km^k(T(N,k\rho)+\mathrm{poly}(c,k,\log N)))$ if $k\rho = N^{o(1)}$. □

The following claim from [BHPT20] shows that randomness parity checks can be written as low-rank matrices.

Claim 12 ([BHPT20, Claim B.1])**.** *For any parity function $f\colon \{0,1\}^m \times \{0,1\}^m \to \{-1,1\}$ defined by $f(i,j) = (-1)^{\langle i,u\rangle+\langle j,v\rangle+b}$ for some $u,v \in \{0,1\}^m$ and $b \in \{0,1\}$, we can compute in time $O(m2^m)$ two matrices $A \in \mathbb{F}_2^{2^m\times 3}$ and $B \in \mathbb{F}_2^{3\times 2^m}$ such that $f(i,j) = \big((-1)^{AB}\big)_{i,j}$ for all $i,j \in \{0,1\}^m$.*

Proof. The first column of A is $\langle i,u\rangle$, row-indexed by $i \in \{0,1\}^m$. The second column of A is all 1, while the third column of A is all b. The second row of B is $\langle j,u\rangle$, column-indexed by $j \in \{0,1\}^m$, while every other entry in B is 1. □

We use the following lemma to quickly calculate the "acceptance probability" of a sum of low-rank matrices $\widetilde{\pi}$.

Lemma 13. *Let V be any $(\ell^2, r, q, p, t, s, \tau)$-rectangular PCP verifier over $\{-1,1\}$, and $\widetilde{V}$ be the same as V but with D multilinearly extended over $\mathbb{R}$. Given $\widetilde{\pi} = C\sum_{i=1}^m b_i\cdot(-1)^{A^{(i)}B^{(i)}}$ with $C \in \mathbb{Q}$ of bit-complexity $O(n)$, $b_i \in \{-1,1\}$, $A^{(i)} \in \mathbb{F}_2^{\ell\times\rho}$, and $B^{(i)} \in \mathbb{F}_2^{\rho\times\ell}$ for all $i \in [m]$. Assuming that $\log((q+p)\rho) = o(r)$, we can calculate $\mathbb{E}_R\Big[\widetilde{V}^{\widetilde{\pi}}(1^n;R)\Big]$ in time $\widetilde{O}\big(2^{r_{\mathsf{rect}}+r_{\mathsf{shared}}}\cdot(t+m\rho) + m^{q+p}\cdot 2^{q+p+r-\Omega(r/\log((q+p)\rho))}\big)$.*

Using the parameters of the PCP in Lemma 9, the time bound in the above lemma becomes

$$\widetilde{O}\big(m^{O(1)}\big(2^{0.51n}\rho + 2^{n-\Omega(n/\log\rho)}\big)\big), \tag{1}$$

which is $O(2^n/n)$ when $n/\log\rho \geq \kappa(\log m + \log n)$ for a constant κ. The proof of Lemma 13 follows closely from the computation process of the PCP in Definition 7, similar to parts of the proof of Lemma 3.1 in [BHPT20].

Proof of Lemma 13. The algorithm on input $\widetilde{\pi} = \sum_{i=1}^m \alpha_i\cdot(-1)^{A^{(i)}B^{(i)}}$ runs as follows:

1. Initialize the result res to be 0.
2. For each $R_{\mathsf{shared}} \in \{0,1\}^{r_{\mathsf{shared}}}$:
   (a) Compute the decision function $D = D(1^n; R_{\mathsf{shared}})$ and randomness parity check $(C_1,\dots,C_p) = (C_1(1^n;R_{\mathsf{shared}}),\dots,C_p(1^n;R_{\mathsf{shared}}))$.
   (b) For each $k \in [q]$, for each $i \in [m]$,
      i. Compute the $2^{r_{\mathsf{rect}}}\times\rho$ matrices $A^{(k,i)}$ whose R_{row}-th row is the row of $A^{(i)}$ indexed by $i^{(k)}(1^n;R_{\mathsf{row}},R_{\mathsf{shared}})$ for all $R_{\mathsf{row}} \in \{0,1\}^{r_{\mathsf{rect}}}$.
      ii. Compute the $\rho\times 2^{r_{\mathsf{rect}}}$ matrices $B^{(k,i)}$ whose R_{col}-th column is the column of $B^{(i)}$ indexed by $j^{(k)}(1^n;R_{\mathsf{col}},R_{\mathsf{shared}})$ for all $R_{\mathsf{col}} \in \{0,1\}^{r_{\mathsf{rect}}}$.
   (c) For each $j \in [p]$,
      i. Compute the $2^{r_{\mathsf{rect}}}\times 3$ matrix $A^{(q+j,1)}$ and the $3\times 2^{r_{\mathsf{rect}}}$ matrix $B^{(q+j,1)}$ with $\Big((-1)^{A^{(q+j,1)}B^{(q+j,1)}}\Big)_{R_{\mathsf{row}},R_{\mathsf{col}}} = C_j(R_{\mathsf{row}},R_{\mathsf{col}})$ given by Claim 12.
   (d) Now we define q m-sums of rank-ρ matrices, $\widetilde{Q}_k = C\sum_{i=1}^m b_i\cdot(-1)^{A^{(k,i)}B^{(k,i)}}$ for each $k \in [q]$, and p 1-sums of rank-3 matrices, $\widetilde{Q}_{q+j} = (-1)^{A^{(q+j,1)}B^{(q+j,1)}}$ for each $j \in [p]$. Apply Theorem 11 to calculate the following value and add it to res:

$$\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\Big(\overline{D}(\widetilde{Q}_1,\dots,\widetilde{Q}_q,\widetilde{Q}_{q+1},\dots,\widetilde{Q}_{q+p})\Big)_{R_{\mathsf{row}},R_{\mathsf{col}}}\right].$$

3. Return res as the value of $\mathbb{E}_R\Big[\widetilde{V}^{\widetilde{\pi}}(1^n;R)\Big]$.

Correctness of the algorithm follows from Definition 7.

Step 2(b) runs in time $O(2^{r_{\mathsf{rect}}}\cdot(t+m\rho))$, while Step 2(c) runs in $O(r2^{r_{\mathsf{rect}}})$ by Claim 12, which is dominated by the runtime of Step 2(b) since $t\geq r$. By Theorem 11, Step 2(d) takes time $O(2^{q+p}\cdot m^{q+p}\cdot(T(2^{r_{\mathsf{rect}}},(q+p)\rho)+\mathrm{poly}(n,q+p,r)))=O(2^{q+p}\cdot m^{q+p}\cdot T(2^{r_{\mathsf{rect}}},(q+p)\rho))\mathrm{poly}(n)$, if $(q+p)\rho=(2^{r_{\mathsf{rect}}})^{o(1)}$, i.e. $\log((q+p)\rho)=o(r)$. Therefore the running time of the above algorithm is

$$\begin{aligned}&O\big(2^{r_{\mathsf{shared}}}\cdot\big(2^{r_{\mathsf{rect}}}\cdot(t+m\rho)+2^{q+p}\cdot m^{q+p}\cdot T(2^{r_{\mathsf{rect}}},(q+p)\rho)\big)\big)\mathrm{poly}(n)\\=\;&O\big(2^{r_{\mathsf{shared}}+r_{\mathsf{rect}}}\cdot(t+m\rho)+m^{q+p}\cdot 2^{q+p+r-\Omega(r/\log((q+p)\rho))}\big)\mathrm{poly}(n).\end{aligned}$$

□

3 Validity Tests

In this section we discuss two tests on sums of low-rank matrices $\widetilde{\pi}$ to ensure that they are close to boolean and somewhat bounded. The following close-to-boolean test simplifies a similar test in [CLW20] due to the smoothness of the PCP verifier. Using the parameters of the PCP in Lemma 9, the time bound in the following lemma becomes $\widetilde{O}(m^4\cdot 2^{n-\Omega(n/\log\rho)})$, which is $O(2^n/n)$ for m and ρ satisfying $n/\log\rho\geq\kappa(\log m+\log n)$ for a constant κ.

Lemma 14 (Close-to-Boolean Test)**.** *Given $\widetilde{\pi}=C\sum_{i=1}^m b_i\cdot(-1)^{A^{(i)}B^{(i)}}$ with $C\in\mathbb{Q}$ of bit-complexity $O(n)$, $b_i\in\{-1,1\}$, $A^{(i)}\in\mathbb{F}_2^{\ell\times\rho}$, and $B^{(i)}\in\mathbb{F}_2^{\rho\times\ell}$. Assuming that $\rho=\ell^{o(1)}$, we can perform a test on $\widetilde{\pi}$ in time $\widetilde{O}\big(m^4\cdot\ell^{2-\Omega(1/\log\rho)}\big)$ such that:*

- *(Completeness) If $\widetilde{\pi}$ is bounded and there is a proof $\pi\in\{-1,1\}^{\ell\times\ell}$ with $\|\pi-\widetilde{\pi}\|_1\leq\varepsilon$, then we have $\|\pi-\widetilde{\pi}\|_2\leq\sqrt{2\varepsilon}$, and $\widetilde{\pi}$ passes the test.*
- *(Soundness) If $\widetilde{\pi}$ passes the test, there exists a proof $\pi\in\{-1,1\}^{\ell\times\ell}$ with $\|\pi-\widetilde{\pi}\|_2\leq 2\sqrt{2\varepsilon}$.*

Proof. We use Theorem 11 to evaluate the expectation of the degree-4 univariate polynomial $f(x)=(-1-x)^2(1-x)^2$ on $\widetilde{\pi}$. We accept $\widetilde{\pi}$ if $\mathbb{E}_{i,j}[f(\widetilde{\pi}_{i,j})]\leq 8\varepsilon$, and reject otherwise. It takes time $O(m^4\cdot(T(\ell,4\rho)+\mathrm{poly}(n,\log\ell)))=\widetilde{O}\big(m^4\cdot\ell^{2-\Omega(1/\log\rho)}\big)$ if $\rho=\ell^{o(1)}$.

For soundness, define $\pi\in\{-1,1\}^{\ell\times\ell}$ by $\pi_{i,j}=1$ if $\widetilde{\pi}_{i,j}\geq 0$, and -1 otherwise, for all $i,j\in[\ell]$. Then for all $i,j\in[\ell]$, we have $|(-\pi_{i,j})-\widetilde{\pi}_{i,j}|\geq 1$. As $\{\pi_{i,j},-\pi_{i,j}\}=\{-1,1\}$, we have

$$f(\widetilde{\pi}_{i,j})=(-1-\widetilde{\pi}_{i,j})^2(1-\widetilde{\pi}_{i,j})^2=((-\pi_{i,j})-\widetilde{\pi}_{i,j})^2(\pi_{i,j}-\widetilde{\pi}_{i,j})^2\geq(\pi_{i,j}-\widetilde{\pi}_{i,j})^2.$$

Therefore $\|\pi-\widetilde{\pi}\|_2=\sqrt{\mathbb{E}_{i,j}[(\pi_{i,j}-\widetilde{\pi}_{i,j})^2]}\leq\sqrt{\mathbb{E}_{i,j}[f(\widetilde{\pi}_{i,j})]}\leq 2\sqrt{2\varepsilon}$.

For completeness, observe that for $\widetilde{\pi}_{i,j}\in[-1,1]$ and $\pi_{i,j}\in\{-1,1\}$ we have $|(-\pi_{i,j})-\widetilde{\pi}_{i,j}|\leq 2$ and so $(\pi_{i,j}-\widetilde{\pi}_{i,j})^2\leq 2|\pi_{i,j}-\widetilde{\pi}_{i,j}|$. Therefore $f(\widetilde{\pi}_{i,j})\leq 2^2(\pi_{i,j}-\widetilde{\pi}_{i,j})^2\leq 8|\pi_{i,j}-\widetilde{\pi}_{i,j}|$, thus $\mathbb{E}_{i,j}[f(\widetilde{\pi}_{i,j})]\leq 8\|\pi-\widetilde{\pi}\|_1\leq 8\varepsilon$, so $\widetilde{\pi}$ passes the test. Moreover we have $\|\pi-\widetilde{\pi}\|_2=\sqrt{\mathbb{E}_{i,j}[(\pi_{i,j}-\widetilde{\pi}_{i,j})^2]}\leq\sqrt{2\mathbb{E}_{i,j}|\pi_{i,j}-\widetilde{\pi}_{i,j}|}=\sqrt{2\|\pi-\widetilde{\pi}\|_1}\leq\sqrt{2\varepsilon}$. □

We also need to test if the sum of low-rank matrices is somewhat bounded. Ideally we would like to ensure that the sum is point-wise bounded. However the quick algorithm in Theorem 11 can only calculate expectation so it is unlikely that we can use it to get a pointwise bound. Fortunately it turns out that for our purpose we don't really need pointwise boundedness. The test we present here generalizes a similar test in [CLW20]. We use the following notion of sampling from the lists I,J.

Definition 15. *Let I, J be any two lists of the same size taking (possibly duplicate) elements from $[\ell]$. We say a real matrix $\widetilde{\pi} \in \mathbb{R}^{\ell \times \ell}$ is* power-d bounded for (I, J) *if $\mathbb{E}_{i \sim I, j \sim J}[\widetilde{\pi}_{i,j}^d] \leq 1$, where $i \sim I$ means that i is sampled from I uniformly at random.*

Lemma 16 (Boundedness Test)**.** *Let $\widetilde{\pi} = C \sum_{i=1}^m b_i \cdot (-1)^{A^{(i)} B^{(i)}}$ be an m-sum with $C \in \mathbb{Q}$ of bit-complexity $O(\log n)$, $b_i \in \{-1, 1\}$, $A^{(i)} \in \mathbb{F}_2^{\ell \times \rho}$, and $B^{(i)} \in \mathbb{F}_2^{\rho \times \ell}$ for all $i \in [m]$. Let I, J be two lists of the same size taking elements from $[\ell]$. Let d be any number. Assuming that $d\rho = |I|^{o(1)}$, we can perform a test on $\widetilde{\pi}$ in time $\widetilde{O}\big(m\rho|I| + m^d |I|^{2-\Omega(1/\log(d\rho))}\big)$ such that:*

- *(Completeness) If $\widetilde{\pi}$ is bounded, it passes the test.*
- *(Soundness) If $\widetilde{\pi}$ passes the test, it is power-d bounded for (I, J).*

Jumping ahead, we will set I (and J) to be the list of the row (column, respectively) indices the verifier probes over row (column, respectively) randomness for each of the q queries and each choice of the shared randomness, so $|I| = |J| = 2^{r_{\mathsf{rect}}}$. Using the parameters of the PCP in Lemma 9, each boundedness test runs in time

$$\widetilde{O}(m^{O(1)}(2^{0.49n}\rho + 2^{0.98n - \Omega(n/\log \rho)})).$$

We will use $O(2^{0.02n})$-many boundedness tests so the total runtime is similar to (1), which becomes $O(2^n/n)$ when $n/\log \rho \geq \kappa(\log m + \log n)$ for a constant κ.

Proof. We construct an m-sum $\widetilde{Q} = C \sum_{i=1}^m b_i \cdot (-1)^{A'^{(i)} B'^{(i)}}$, where $A'^{(i)} \in \mathbb{F}_2^{|I| \times \rho}$ consists of the rows of $A^{(i)}$ indexed by elements in I and $B'^{(i)} \in \mathbb{F}_2^{\rho \times |I|}$ consists of the columns of $B^{(i)}$ indexed by elements in J. This step takes time $O(m\rho|I|)$.

Note that the uniform distribution over entries of $\widetilde{Q}$ is the same as the distribution over entries of $\widetilde{\pi}$ under I, J, so we have $\mathbb{E}_{i \sim I, j \sim J}[\widetilde{\pi}_{i,j}^d] = \mathbb{E}_{i,j}\left[\left(\widetilde{Q}\right)_{i,j}^d\right]$. Hence we use Theorem 11 to evaluate the expectation of the polynomial x^d on $\widetilde{Q}$. We accept $\widetilde{\pi}$ if the value is at most 1, and reject otherwise. This step takes time $O(m^d \cdot (T(|I|, d\rho) + \mathrm{poly}(n, d, \log |I|))$ if $d\rho = |I|^{o(1)}$. Therefore the total running time is $O\big(m\rho|I| + m^d|I|^{2-\Omega(1/\log(d\rho))}\big)\mathrm{poly}(n)$.

Completeness and soundness follow from the definition. □

We need the following technical lemma for the main theorem. Intuitively it shows that if a real-valued proof is bounded and close to a boolean proof, then its "acceptance probability" is also close to that of the boolean proof.

Definition 17. *Let V be any $(\ell^2, r, q, p, t, s, \tau)$-rectangular PCP verifier. We say a real matrix $\widetilde{\pi} \in \mathbb{R}^{\ell \times \ell}$ is* bounded for V *if for all $R_{\mathsf{shared}} \in \{0,1\}^{r_{\mathsf{shared}}}$, and all $S \subseteq [q]$, we have*

$$\mathbb{E}_{R_{\mathsf{row}}, R_{\mathsf{col}} \in \{0,1\}^{r_{\mathsf{rect}}}}\left[\prod_{k \in S} \widetilde{\pi}^2_{i^{(k)}, j^{(k)}}\right] \leq 1,$$

where $i^{(k)} = i^{(k)}(1^n; R_{\mathsf{row}}, R_{\mathsf{shared}})$ and $j^{(k)} = j^{(k)}(1^n; R_{\mathsf{row}}, R_{\mathsf{shared}})$ for all $k \in [q]$.

Lemma 18. *Let V be any smooth $(\ell^2, r, q, p, t, s, \tau)$-rectangular PCP verifier over $\{-1, 1\}$, and $\widetilde{V}$ be the same as V but with D multilinearly extended over $\mathbb{R}$. Let π be any matrix in $\{-1, 1\}^{\ell \times \ell}$ and $\widetilde{\pi}$ be any matrix in $\mathbb{R}^{\ell \times \ell}$ that is bounded for V. Then we have*

$$\left|\mathbb{E}_R[V^{\pi}(1^n; R)] - \mathbb{E}_R\left[\widetilde{V}^{\widetilde{\pi}}(1^n; R)\right]\right| \leq 2^{O(q+p)} \|\pi - \widetilde{\pi}\|_2.$$

Proof. Fix an arbitrary $R_{\mathsf{shared}} \in \{0,1\}^{r_{\mathsf{shared}}}$. By definition $\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\Big[\Big|V^{\pi}(1^n;R) - \widetilde{V}^{\widetilde{\pi}}(1^n;R)\Big|\Big]$ is

$$\begin{aligned}\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\big[\big|&D(\pi_{i^{(1)},j^{(1)}},\ldots,\pi_{i^{(q)},j^{(q)}},C_1(R_{\mathsf{row}},R_{\mathsf{col}}),\ldots,C_p(R_{\mathsf{row}},R_{\mathsf{col}}))\\ &-D(\widetilde{\pi}_{i^{(1)},j^{(1)}},\ldots,\widetilde{\pi}_{i^{(q)},j^{(q)}},C_1(R_{\mathsf{row}},R_{\mathsf{col}}),\ldots,C_p(R_{\mathsf{row}},R_{\mathsf{col}}))\big|\big],\end{aligned} \tag{2}$$

where $D = D(1^n;R_{\mathsf{shared}})$, $(C_1,\ldots,C_p) = (C_1(1^n;R_{\mathsf{shared}}),\ldots,C_p(1^n;R_{\mathsf{shared}}))$, $i^{(k)} = i^{(k)}(1^n;R_{\mathsf{row}},R_{\mathsf{shared}})$ and $j^{(k)} = j^{(k)}(1^n;R_{\mathsf{row}},R_{\mathsf{shared}})$ for all $k \in [q]$.

We write D in its Fourier expansion $D(z_1,\ldots,z_{q+p}) = \sum_{S\subseteq[q+p]}\beta_S\prod_{k\in S}z_k$, where for each $S\subseteq[q+p]$, $\beta_S = \mathbb{E}_{z\in\{-1,1\}^{q+p}}\big[D(z)\prod_{k\in S}z_k\big]$. For all $z\in\{-1,1\}^{q+p}$, $D(z)\in\{0,1\}$ and $\prod_{k\in S}z_k \in \{-1,1\}$, thus $|\beta_S|\le 1$ for any S. Hence by the triangular inequality we can bound (2) by

$$\begin{aligned}&\sum_{S\subseteq[q+p]}\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left|\left(\prod_{k\in S\cap[q]}\pi_{i^{(k)},j^{(k)}} - \prod_{k\in S\cap[q]}\widetilde{\pi}_{i^{(k)},j^{(k)}}\right)\prod_{k\in S\setminus[q]}C_k(R_{\mathsf{row}},R_{\mathsf{col}})\right|\right]\\ &= 2^p\sum_{S\subseteq[q]}\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left|\prod_{k\in S}\pi_{i^{(k)},j^{(k)}} - \prod_{k\in S}\widetilde{\pi}_{i^{(k)},j^{(k)}}\right|\right],\end{aligned} \tag{3}$$

as all the C_k's are $\{-1,1\}$-valued.

Fix any $S\subseteq[q]$. Wlog let $S=\{1,\ldots,d\}$ for some $d\le q$, then the expectation in (3) can be written as

$$\begin{aligned}&\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left|\prod_{u=1}^{d}\pi_{i^{(u)},j^{(u)}} - \prod_{u=1}^{d}\widetilde{\pi}_{i^{(u)},j^{(u)}}\right|\right]\\ &= \mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left|\sum_{v=1}^{d}\left(\prod_{u=1}^{v-1}\widetilde{\pi}_{i^{(u)},j^{(u)}}\prod_{u=v}^{d}\pi_{i^{(u)},j^{(u)}} - \prod_{u=1}^{v}\widetilde{\pi}_{i^{(u)},j^{(u)}}\prod_{u=v+1}^{d}\pi_{i^{(u)},j^{(u)}}\right)\right|\right]\\ &\le \sum_{v=1}^{d}\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left|\prod_{u=1}^{v-1}\widetilde{\pi}_{i^{(u)},j^{(u)}}\prod_{u=v}^{d}\pi_{i^{(u)},j^{(u)}} - \prod_{u=1}^{v}\widetilde{\pi}_{i^{(u)},j^{(u)}}\prod_{u=v+1}^{d}\pi_{i^{(u)},j^{(u)}}\right|\right]\\ &= \sum_{v=1}^{d}\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left|\prod_{u=1}^{v-1}\widetilde{\pi}_{i^{(u)},j^{(u)}}\cdot\left(\pi_{i^{(v)},j^{(v)}} - \widetilde{\pi}_{i^{(v)},j^{(v)}}\right)\cdot\prod_{u=v+1}^{d}\pi_{i^{(u)},j^{(u)}}\right|\right]\\ &\le \sum_{v=1}^{d}\left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left(\pi_{i^{(v)},j^{(v)}} - \widetilde{\pi}_{i^{(v)},j^{(v)}}\right)^2\right]\right)^{1/2}\left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\prod_{u=1}^{v-1}\widetilde{\pi}^2_{i^{(u)},j^{(u)}}\prod_{u=v+1}^{d}\pi^2_{i^{(u)},j^{(u)}}\right]\right)^{1/2}\\ &\le \sum_{v=1}^{d}\left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left(\pi_{i^{(v)},j^{(v)}} - \widetilde{\pi}_{i^{(v)},j^{(v)}}\right)^2\right]\right)^{1/2}\\ &= \sum_{k\in S}\left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left(\pi_{i^{(k)},j^{(k)}} - \widetilde{\pi}_{i^{(k)},j^{(k)}}\right)^2\right]\right)^{1/2},\end{aligned}$$

where the first inequality comes from the triangular inequality, the second inequality follows from the Cauchy-Schwarz inequality, and the last inequality follows from the assumptions that $\pi\in\{-1,1\}^{\ell\times\ell}$ and $\widetilde{\pi}$ is bounded for V.

Summing over S, we can bound (3) by

$$2^p\sum_{S\subseteq[q]}\sum_{k\in S}\left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\left(\pi_{i^{(k)},j^{(k)}} - \widetilde{\pi}_{i^{(k)},j^{(k)}}\right)^2\right]\right)^{1/2}$$

$$
\begin{aligned}
&= 2^{p+q-1} \sum_{k\in[q]} \left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}} \left[\left(\pi_{i^{(k)},j^{(k)}} - \widetilde{\pi}_{i^{(k)},j^{(k)}} \right)^2 \right] \right)^{1/2} \\
&= 2^{O(p+q)} \mathbb{E}_{k\in[q]} \left[\left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}} \left[\left(\pi_{i^{(k)},j^{(k)}} - \widetilde{\pi}_{i^{(k)},j^{(k)}} \right)^2 \right] \right)^{1/2} \right] \\
&\le 2^{O(p+q)} \left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}},k} \left[\left(\pi_{i^{(k)},j^{(k)}} - \widetilde{\pi}_{i^{(k)},j^{(k)}} \right)^2 \right] \right)^{1/2},
\end{aligned}
$$

where the first step uses double counting, and the last step follows from Jensen's inequality.

Therefore by averaging over R_{shared}, we have

$$
\begin{aligned}
\left| \mathbb{E}_R[V^\pi(1^n;R)] - \mathbb{E}_R\left[\widetilde{V}^{\widetilde{\pi}}(1^n;R)\right] \right| &\le \mathbb{E}_{R_{\mathsf{shared}}} \mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}} \left[\left| V^\pi(1^n;R) - \widetilde{V}^{\widetilde{\pi}}(1^n;R) \right| \right] \\
&\le 2^{O(p+q)} \mathbb{E}_{R_{\mathsf{shared}}} \left[\left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}},k} \left[\left(\pi_{i^{(k)},j^{(k)}} - \widetilde{\pi}_{i^{(k)},j^{(k)}} \right)^2 \right] \right)^{1/2} \right] \\
&\le 2^{O(p+q)} \left(\mathbb{E}_{R_{\mathsf{shared}},R_{\mathsf{row}},R_{\mathsf{col}},k} \left[\left(\pi_{i^{(k)},j^{(k)}} - \widetilde{\pi}_{i^{(k)},j^{(k)}} \right)^2 \right] \right)^{1/2} \\
&= 2^{O(p+q)} \left(\mathbb{E}_{i,j} \left[\left(\pi_{i,j} - \widetilde{\pi}_{i,j} \right)^2 \right] \right)^{1/2} \\
&= 2^{O(p+q)} \|\pi - \widetilde{\pi}\|_2,
\end{aligned}
$$

where the first step uses triangular inequality, the second step uses the above bound for every R_{shared}, the third step comes from Jensen's inequality, and the fourth step follows from the smoothness of V. □

4 Constant hardness for rational sums of low-rank matrices

In this section we prove our main hardness result against rational sums of low-rank matrices.

Theorem 19. *There is a function $f\colon \{0,1\}^{n+O(\log n)} \to \{-1,1\}$ in $\mathrm{E}^{\mathbf{NP}}$ that does not $(1-\Omega(1))$-correlate with any bounded m-sum of rank-ρ matrices with $O(n)$ bit-complexity, for infinitely many n, as long as $n/\log\rho \ge \kappa(\log m + \log n)$ for a constant κ.*

Proof. Fix L to be a unary language in $\mathbf{NTIME}(2^n) \setminus \mathbf{NTIME}(o(2^n))$ [Coo73, SFM78, Zák83]. Let V be the smooth $(\ell^2, r, q, p, t, s, \tau)$-rectangular PCP verifier over alphabet $\{-1,1\}$ for L given by Lemma 9, for s and τ to be determined later. Let $\widetilde{V}$ be the same as V but with D multilinearly extended over $\mathbb{R}$.

We use the lexicographically first proof oracle π as our hard function, i.e. our algorithm $f_n\colon [\ell]\times[\ell] \to \{-1,1\}$ on input (i,j) searches bit-by-bit for the lexicographically first proof π such that $\forall R$, $V^\pi(1^n;R) = 1$ if one exists, and outputs $\pi_{i,j}$. Clearly $f_n \in \mathrm{E}^{\mathbf{NP}}$. Note that f_n can also be seen as a family of matrices $f_n \in \{-1,1\}^{\ell\times\ell}$.

Now for the sake of contradiction, we assume that f_n $(1-\varepsilon)$-correlates with a bounded m-sum of rank-ρ matrices $\widetilde{\pi}$ with bit-complexity $O(n)$, for a constant ε to be determined later. We will show that $L \in \mathbf{NTIME}(2^n/n)$, thus deriving a contradiction.

Algorithm. The nondeterministic algorithm for L goes as follows:

1. Guess $\widetilde{\pi} = C\sum_{i=1}^m b_i \cdot (-1)^{A^{(i)}B^{(i)}}$ by guessing $b_i \in \{-1,1\}$, matrices $A^{(i)} \in \mathbb{F}_2^{\ell\times\rho}$, and $B^{(i)} \in \mathbb{F}_2^{\rho\times\ell}$ for all $i\in[m]$ and $C\in\mathbb{Q}$ with bit-complexity $O(n)$.

2. Perform the close-to-boolean test in Lemma 14 for ε on $\widetilde{\pi}$, reject if it doesn't pass.

3. For each $R_{\mathsf{shared}} \in \{0,1\}^{r_{\mathsf{shared}}}$, $k \in [q]$:

   (a) Compute the lists

   $$I^{(k)} = \left[i^{(k)}(1^n; R_{\mathsf{row}}, R_{\mathsf{shared}}) | R_{\mathsf{row}} \in \{0,1\}^{r_{\mathsf{rect}}}\right],$$
   $$J^{(k)} = \left[j^{(k)}(1^n; R_{\mathsf{col}}, R_{\mathsf{shared}}) | R_{\mathsf{col}} \in \{0,1\}^{r_{\mathsf{rect}}}\right].$$

   (b) For each $2 \le d \le 2q$:

      i. Perform the boundedness test in Lemma 16 for d and $(I^{(k)}, J^{(k)})$ on $\widetilde{\pi}$, reject if it doesn't pass.

4. Use Lemma 13 to calculate $\mathbb{E}_R[\widetilde{V}^{\widetilde{\pi}}(1^n; R)]$, and only accept if $\mathbb{E}_R[\widetilde{V}^{\widetilde{\pi}}(1^n; R)] > \gamma$ where the constant γ is to be determined later.

Runtime. Step 1 takes time $O(m\ell\rho + n)$.

By Lemma 14, Step 2 takes time $\widetilde{O}\big(m^4 \cdot \ell^{2-\Omega(1/\log\rho)}\big)$ if $\rho = \ell^{o(1)}$.

Step 3(a) takes time $\widetilde{O}(2^{r_{\mathsf{rect}}} \cdot t)$, and we have $|I| = 2^{r_{\mathsf{rect}}}$. Therefore by Lemma 16, Step 3(b) takes time $\widetilde{O}\big(qm\rho 2^{r_{\mathsf{rect}}} + qm^{2q}2^{2r_{\mathsf{rect}}-\Omega(r/\log(q\rho))}\big)$, if $q\rho = (2^{r_{\mathsf{rect}}})^{o(1)}$, i.e. $\log(q\rho) = o(r)$. Hence the total runtime for Step 3 is

$$\begin{aligned}&\widetilde{O}\big(2^{r_{\mathsf{shared}}} \cdot \big(2^{r_{\mathsf{rect}}} \cdot (t + qm\rho) + q \cdot m^{2q} \cdot 2^{2r_{\mathsf{rect}}-\Omega(r/\log(q\rho))}\big)\big)\\ =\ &\widetilde{O}\big(2^{r_{\mathsf{shared}}+r_{\mathsf{rect}}} \cdot (t + qm\rho) + qm^{2q} \cdot 2^{r-\Omega(r/\log(q\rho))}\big).\end{aligned}$$

By Lemma 13, Step 4 runs in time $\widetilde{O}\big(2^{r_{\mathsf{shared}}+r_{\mathsf{rect}}} \cdot (t + m\rho) + m^{q+p} \cdot 2^{q+p+r-\Omega(r/\log((q+p)\rho))}\big)$ if $\log((q+p)\rho) = o(r)$.

For the algorithm to run in time $O(2^n/n)$, it suffices to satisfy all the above requirements and make all the runtime to be $O(2^n/n)$. For convenience we take logarithms on all the time bounds. In summary, it is sufficient to satisfy the following conditions:

1. $\log(m\ell\rho + n) < n - \log n$.
2. $\rho = \ell^{o(1)}$.
3. $\log(m^4\ell^2) - \Omega(\log\ell/\log\rho) + O(\log n) < n - \log n$.
4. $\log(q\rho) = o(r)$.
5. $r_{\mathsf{shared}} + r_{\mathsf{rect}} + \log(t + qm\rho) + O(\log n) < n - \log n$.
6. $\log q + 2q\log m + r - \Omega\Big(\frac{r}{\log(q\rho)}\Big) + O(\log n) < n - \log n$.
7. $\log((q+p)\rho) = o(r)$.
8. $(q+p)(\log m + 1) + r - \Omega\Big(\frac{r}{\log((q+p)\rho)}\Big) + O(\log n) < n - \log n$.

We are going to set parameters to meet these conditions at the end.

Correctness. We first prove the following claim.

Claim 20. *If $\widetilde{\pi}$ passes all the tests in the definition of the algorithm then it is bounded for V.*

Proof. Fix any $R_{\mathsf{shared}} \in \{0,1\}^{r_{\mathsf{shared}}}$ and $S \subseteq [q]$. Let $d = |S|$. By Hölder's inequality, we get

$$\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\prod_{k\in S} \widetilde{\pi}^2_{i^{(k)},j^{(k)}}\right] \le \prod_{k\in S}\left(\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\widetilde{\pi}^{2d}_{i^{(k)},j^{(k)}}\right]\right)^{1/d} = \prod_{k\in S}\left(\mathbb{E}_{i\sim I^{(k)},j\sim J^{(k)}}\left[\widetilde{\pi}^{2d}_{i,j}\right]\right)^{1/d}.$$

We have $2d \le 2q$, therefore the boundedness tests in Step 3 can guarantee that all the terms in the product are bounded by 1, hence $\mathbb{E}_{R_{\mathsf{row}},R_{\mathsf{col}}}\left[\prod_{k\in S} \widetilde{\pi}^2_{i^{(k)},j^{(k)}}\right] \le 1$, thus by definition $\widetilde{\pi}$ is bounded for V. □

If $x = 1^n \in L$, let $\widetilde{\pi} \in \mathbb{R}^{\ell\times\ell}$ be any bounded m-sum of rank-ρ matrices with bit-complexity $O(\log n)$ that $(1-\varepsilon)$-correlates with the hard function f_n, which is the lexicographically first proof π in this case. We can assume wlog $\mathbb{E}_{i,j}[\pi_{i,j}\widetilde{\pi}_{i,j}] \ge 1-\varepsilon$, otherwise we can simply use $-\widetilde{\pi}$. Note that for any $x \in \{-1,1\}$, $y \in [-1,1]$ we have $|x-y| = 1-xy$. As $\pi_{i,j} \in \{-1,1\}$, $\widetilde{\pi}_{i,j} \in [-1,1]$, we have

$$\|\pi - \widetilde{\pi}\|_1 = \mathbb{E}_{i,j}[|\pi_{i,j} - \widetilde{\pi}_{i,j}|] = 1 - \mathbb{E}_{i,j}[\pi_{i,j}\widetilde{\pi}_{i,j}] \le \varepsilon.$$

Hence $\|\pi - \widetilde{\pi}\|_2 \le \sqrt{2\varepsilon}$, and moreover $\widetilde{\pi}$ passes the close-to-boolean test. Since $\widetilde{\pi}$ is bounded by assumption it is also bounded for V. Therefore by Lemma 18 we have

$$\begin{aligned}\mathbb{E}_R\left[\widetilde{V}^{\widetilde{\pi}}(1^n;R)\right] &\ge \mathbb{E}_R[V^{\pi}(1^n;R)] - \left|\mathbb{E}_R[V^{\pi}(1^n;R)] - \mathbb{E}_R\left[\widetilde{V}^{\widetilde{\pi}}(1^n;R)\right]\right| \\ &\ge 1 - 2^{O(p+q)}\|\pi - \widetilde{\pi}\|_2 \\ &\ge 1 - 2^{O(p+q)}\sqrt{\varepsilon}.\end{aligned}$$

If $x = 1^n \notin L$, then for any guessed m-sum of matrices $\widetilde{\pi}$ that passes all the tests, by soundness there exists a boolean proof $\pi \in \{-1,1\}^{\ell\times\ell}$ such that $\|\pi - \widetilde{\pi}\|_2 \le 2\sqrt{2\varepsilon}$, and by Claim 20 we know that $\widetilde{\pi}$ is bounded for V. Therefore by Lemma 18 we have

$$\begin{aligned}\mathbb{E}_R[\widetilde{V}^{\widetilde{\pi}}(1^n;R)] &\le \mathbb{E}_R[V^{\pi}(1^n;R)] + \left|\mathbb{E}_R[V^{\pi}(1^n;R)] - \mathbb{E}_R\left[\widetilde{V}^{\widetilde{\pi}}(1^n;R)\right]\right| \\ &\le s + 2^{O(p+q)}\|\pi - \widetilde{\pi}\|_2 \\ &\le s + 2^{O(p+q)}\sqrt{\varepsilon}.\end{aligned}$$

We can set γ to be any value between these two. Assuming Condition 1-8 are all met, the above nondeterministic algorithm decides L in time $O(2^n/n)$, a contradiction to our choice of L.

Setting parameters. We choose an arbitrary small constant s so both p,q are constants. Then we set ε to be any constant smaller than $\left(\frac{1-s}{2^{O(q+p)}}\right)^2$.

Now fix any ρ and m such that $n/\log\rho \ge \kappa(\log m + \log n)$ for a large constant κ to be determined. We are going to verify that Conditions 1-8 are satisfied. Note that by Lemma 9 we have $r = n + O(\log n)$, $\log \ell = n/2 + O(\log n)$, and $\log t = O(\tau n)$. First, $\log\rho \le n/(\kappa\log n) = o(r)$ and similarly $\rho = \ell^{o(1)}$, so Condition 2, 4, and 7 are all satisfied. As both $\log\rho$ and $\log m$ are at most n/κ, for Condition 1 we have

$$\log(m\ell\rho) + \log n \le 2n/\kappa + n/2 + O(\log n) < n - \log n,$$

for κ sufficiently large, while for Condition 5 we have

$$(1+\tau)r/2 + \log t + \log(qm\rho) + O(\log n) \le (1/2 + O(\tau))n + \log\rho + \log m < n - \log n,$$

for κ sufficiently large and τ sufficiently small. For Condition 8 we have

$$\begin{aligned}(q+p)(\log m+1)+r-\Omega\left(\frac{(1-\tau)r}{\log((q+p)\rho)}\right)+O(\log n) &\le O(\log m)+n+O(\log n)-\Omega(n/\log\rho)\\ &\le n+O(\log m+\log n)-\Omega(\kappa(\log m+\log n))\\ &< n-\log n,\end{aligned}$$

for κ sufficiently large. Similarly Condition 3, 5, and 6 are also satisfied, and we are done. □

5 Correlation bounds via XOR Lemma

In this section we adapt the approach in [CLW20] to our setting, and then prove the main result in this paper, Theorem 1.

Definition 21. *For any boolean function $f\colon \{0,1\}^n \to \{-1,1\}$ and number k, we define $f^{\oplus k}\colon \{0,1\}^{nk} \to \{-1,1\}$ by $f^{\oplus k}(x_1,\dots,x_k)=\prod_{i=1}^k f(x_i)$ for all $x_1,\dots,x_k\in\{0,1\}^n$.*

Lemma 22. *Let $f\colon \{0,1\}^n \to \{-1,1\}$ be any boolean function. Let rational $\varepsilon<1$ have constant bit-complexity, and for any number $k\ge 1$, let $\varepsilon_k=(\frac{1+\varepsilon}{2})^{k-1}\varepsilon$. Assume that $f^{\oplus k}$ ε_k-correlates with some function $h\colon \{0,1\}^{nk}\to[-1,1]$. Then f ε-correlates with a bounded m-sum of restrictions of h (by fixing some inputs), where $m=O\left(\frac{n}{\varepsilon_k^2}\right)$ and the bit-complexity is $O(k+\log n)$.*

Proof. We prove it by induction on k. For $k=1$ it is trivial as h is bounded. Now we assume that the hypothesis holds for $k-1$, and we are proving for k.

For all $x_1\in\{0,1\}^n$, define $g(x_1)=\mathbb{E}_{y\sim\{0,1\}^{n(k-1)}}\left[f^{\oplus k-1}(y)h(x_1,y)\right]$, where we use y for $(x_2,\dots,x_k)$ for convenience. If there exists $x_1\in\{0,1\}^n$ such that $|g(x_1)|\ge\varepsilon_{k-1}$, then we know that $f^{\oplus k-1}$ ε_{k-1}-correlates with h' defined by $h'(y)=h(x_1,y)$, so we can use the induction hypothesis for $k-1$ to get a bounded m-sum of functions obtained by fixing inputs of h', thus by fixing inputs of h.

Otherwise, for all $x_1\in\{0,1\}^n$ we have $|g(x_1)|\le\varepsilon_{k-1}=\frac{2\varepsilon_k}{1+\varepsilon}$. We take m i.i.d. samples $y_1,\dots,y_m$ uniformly from $\{0,1\}^{n(k-1)}$ for $m=O\left(\frac{n}{(\varepsilon_k)^2}\right)$, then define $\widetilde{g}(x_1)=\mathbb{E}_{i\in[m]}\left[f^{\oplus k-1}(y_i)h(x_1,y_i)\right]$. By Chernoff bound,

$$\Pr_{y_1,\dots,y_m}\left[|g(x_1)-\widetilde{g}(x_1)|\ge\frac{1-\varepsilon}{(1+\varepsilon)^2}\varepsilon_k\right]\le 2^{-n-1}.$$

By union bound, there exists a fix assignment to $y_1,\dots,y_m$ such that for all $x_1\in\{0,1\}^n$,

$$|g(x_1)-\widetilde{g}(x_1)|\le\frac{1-\varepsilon}{(1+\varepsilon)^2}\varepsilon_k, \tag{4}$$

thus $|\widetilde{g}(x_1)|\le|g(x_1)|+|g(x_1)-\widetilde{g}(x_1)|\le\left(\frac{2}{1+\varepsilon}+\frac{1-\varepsilon}{(1+\varepsilon)^2}\right)\varepsilon_k=\frac{3+\varepsilon}{(1+\varepsilon)^2}\varepsilon_k$.

Let $r=\frac{3+\varepsilon}{(1+\varepsilon)^2}\varepsilon_k$. We define $\widetilde{h}$ by

$$\widetilde{h}(x_1)=\frac{\widetilde{g}(x_1)}{r}=\frac{1}{mr}\sum_{i=1}^m f^{\oplus k-1}(y_i)h(x_1,y_i).$$

Now $|\widetilde{h}(x_1)| \leq 1$ for all x_1. We can write $\widetilde{h}$ as $C \sum_{i=1}^{m} b_i h_i$, where

$$\begin{aligned} C &= \frac{1}{mr}, \\ b_i &= f^{\oplus k-1}(y_i), \forall i \in [m], \\ h_i &\colon x_1 \mapsto h(x_1, y_i), \forall x_1 \in \{0,1\}^n, \forall i \in [m], \end{aligned}$$

which is a bounded $O(n/\varepsilon_k^2)$-sum of functions that can be obtained by fixing inputs of h. The bit-complexity of m is $O(k + \log n)$, and $O(k)$ for r, thus the bit-complexity of $\widetilde{h}$ is $O(k + \log n)$.

What remains is to prove that $\mathsf{corr}(f, \widetilde{h}) \geq \varepsilon$. By the definition of g and assumption we have $\mathsf{corr}(f, g) = \mathsf{corr}(f^{\oplus k}, h) \geq \varepsilon_k$. Therefore by the definition of $\widetilde{h}$, the fact that $f(x_1) \in \{-1, 1\}$ for all x_1, and (4), we have

$$\begin{aligned} \mathsf{corr}(f, \widetilde{h}) &= \frac{\mathsf{corr}(f, \widetilde{g})}{r} \\ &\geq \frac{1}{r}(\mathsf{corr}(f, g) - \mathbb{E}_{x_1}|g(x_1) - \widetilde{g}(x_1)|) \\ &\geq \frac{\varepsilon_k - \frac{1-\varepsilon}{(1+\varepsilon)^2}\varepsilon_k}{\frac{3+\varepsilon}{(1+\varepsilon)^2}\varepsilon_k} \\ &= \varepsilon. \end{aligned}$$

□

We first show a proof of a weaker version of Theorem 1 that only works for infinitely many n, by combining Theorem 19 and Lemma 22 directly.

Proof of Theorem 1 for infinitely many n. Let $f\colon \{0,1\}^{n+O(\log n)} \to \{-1,1\}$ in $\mathrm{E}^{\mathbf{NP}}$ be the function given by Theorem 19. We know that f does not ε-correlate with any bounded m-sum of rank-ρ matrices with $O(n)$ bit-complexity for infinitely many n, for a rational constant ε with constant bit-complexity.

Let $k \leq n$. We set $\varepsilon_k = (\frac{1+\varepsilon}{2})^{k-1}\varepsilon = 2^{-O(k)}$, and $F = f^{\oplus k}$ so $N = k(n + O(\log n))$. For the sake of contradiction we assume that F ε_k-correlates with some rank-ρ matrix h for infinitely many N. We view a matrix as the truth table of a function, so when we take restrictions on the function, we are taking some rows and columns of the matrix but keeping its dimensions, thus the rank doesn't increase. By Lemma 22 we know that f ε-correlates with a bounded m-sum of rank-ρ matrices $\widetilde{h}$, where $m = O(n/\varepsilon_k^2) = n2^{O(k)}$ and the bit complexity is $O(k + \log n) = O(n)$.

To get a contradiction for infinitely many n we still need to verify that $n/\log \rho \geq \kappa(\log m + \log n)$ for a sufficiently large constant κ given by Theorem 19. We have $\log n \leq \log N - \log k - O(\log \log n)$, thus

$$(\log m + \log n) \log \rho = (2 \log n + O(k)) \log \rho = O((\log N + k) \log \rho).$$

Let $c > 0$ be the constant hidden in the last big-O. We take $\delta = 1/2c\kappa$. Then

$$\kappa(\log m + \log n) \log \rho \leq c\kappa(\log N + k) \log \rho \leq \frac{N}{2k} = \frac{n + O(\log n)}{2} < n.$$

□

To prove the full version of Theorem 1 that works for all sufficiently large n, we need the following *refuter* from [CLW20].

Theorem 23. *There is a constant $c > 0$ such that the following holds.*

For any non-decreasing time-constructible function $T(n)$ such that $n \le T(n) \le 2^{\mathrm{poly}(n)}$, there is an $\mathbf{NTIME}(T(n))$ language L and an algorithm R such that:

> ***Input.*** *The input for R is a pair $(M, 1^n)$ where M is a nondeterministic algorithm running in time $\le cT(n)/\log T(n)$.*
>
> ***Output.*** *For any fixed M, for all large enough n, $R(M, 1^n)$ outputs a string x such that $|x| \in [n, n + T(n)]$ and $L(x) \neq M(x)$.*
>
> ***Complexity.*** *R is a deterministic algorithm running in $O(T(n) \cdot T(T(n) + n))$ time with an $\mathbf{NP}$ oracle.*

We also need a lemma on padding rigid matrices from [AC19].

Lemma 24. *Let $\mathbf{1}_m$ be the all-ones $m \times m$ matrix. For any square matrix A, A ε-correlates with some rank-ρ matrix if and only if $A \otimes \mathbf{1}_m$ ε-correlates with some rank-ρ matrix, where $\otimes$ is the tensor product of matrices.*

Proof of Theorem 1. We show how to remove the "infinitely often" part from the previous proof. Fix $T(n) = n^C$ for a large constant C. We are going to use the general version of Lemma 9 in [BHPT20] that works for $\mathbf{NTIME}(T(n))$ languages. Most importantly, we have $r = \log T(n) + O(\log\log T(n)) + O(\log n)$ and $2\log \ell = r + O(1)$. Then the proof of Theorem 19 shows that we have the following results:

1. For any $\mathbf{NTIME}(T(n))$ language L, let V be the smooth $(\ell^2, r, q, p, t, s, \tau)$-rectangular PCP verifier over alphabet $\{-1, 1\}$ for L given by the generalized version of Lemma 9, for small constants s and τ. We define the function $f_{L,x} \colon [\ell] \times [\ell] \to \{-1, 1\}$ such that on input (i, j) it searches bit-by-bit for the lexicographically first proof π such that $\forall R$, $V^\pi(x; R) = 1$ if one exists, and outputs $\pi_{i,j}$. Clearly $f_{L,x} \in \mathrm{E}^{\mathbf{NP}}$. Note that $f_{L,x}$ can also be seen as an $\ell \times \ell$ matrix.

2. For any $\mathbf{NTIME}(T(n))$ language L, there exists an explicit nondeterministic algorithm that decides if $x \in L$ in time $O(T(n)/\log T(n))$, for any input x such that $|x| = n$ and $f_{L,x}$ $(1 - \Omega(1))$-correlates with a bounded m-sum of rank-ρ matrices $\widetilde{\pi}$ with bit-complexity $O(\log T(n))$, as long as $\log T(n)/\log \rho \ge \kappa(\log m + \log\log T(n))$ for a constant κ.

We consider the language L for $\mathbf{NTIME}(T(n))$ from Theorem 23. Similarly as before, by combining Item 2 with Lemma 22, there exists an explicit nondeterministic $O(T(n)/\log T(n))$-time algorithm M deciding if $x \in L$ for any input x such that $|x| = n$ and $f_{L,x}^{\oplus k}$ ε_k-correlates with some rank-ρ matrix h, for any $k \le \log T(|x|) = C \log |x|$.

We aim to use the refuter R from Theorem 23 to get a contradiction. For all large enough n, R on $(1^n, M)$ will output an x such that $|x| \in [n, n^C]$ and $L(x) \neq M(x)$. Now the input length of $f_{L,x}^{\oplus k}$ is $k \cdot 2\log \ell = k(r + O(1)) = k(\log T(|x|) + O(\log\log T(|x|)) + O(\log |x|)) \in [k \cdot C \log n, k \cdot 2C^2 \log n]$. We view $f_{L,x}^{\oplus k}$ as a matrix and use Lemma 24 to get a function F_x with input length $k \cdot 2C^2 \log n$ such that F_x ε_k-correlates with some rank-ρ matrix iff $f_{L,x}^{\oplus k}$ ε_k-correlates with some rank-ρ matrix. Therefore if F_x ε_k-correlates with some rank-ρ matrix then M can decide if $x \in L$, a contradiction.

Our final hard function f works as follows. On input of length $N = k \cdot 2C^2 \log n$ it runs R on $(1^n, M)$ to get an x, then run F_x. Then for all large enough n, f does not ε_k-correlate with any rank-ρ matrices, for any $k \leq C \log n$. R runs in $O(n^{C^2}) = 2^{O(N/k)}$ time with an **NP** oracle and $f_{L,x} \in \mathrm{E}^{\mathbf{NP}}$, thus $f \in \mathrm{E}^{\mathbf{NP}}$. The condition $\log T(n)/\log \rho \geq \kappa(\log m + \log\log T(n))$ in Item 2 can be verified similarly as in the previous proof for a sufficiently small δ. □

References

[AC19] Josh Alman and Lijie Chen. Efficient construction of rigid matrices using an NP oracle. In David Zuckerman, editor, *60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019, Baltimore, Maryland, USA, November 9-12, 2019*, pages 1034–1055. IEEE Computer Society, 2019.

[ACW16] Josh Alman, Timothy M. Chan, and Ryan Williams. Polynomial representations of threshold functions and algorithmic applications. In *IEEE Symp. on Foundations of Computer Science (FOCS)*, 2016.

[BHPT20] Amey Bhangale, Prahladh Harsha, Orr Paradise, and Avishay Tal. Rigid matrices from rectangular PCPs. In *IEEE Symp. on Foundations of Computer Science (FOCS)*, 2020.

[BV14] Eli Ben-Sasson and Emanuele Viola. Short PCPs with projection queries. In *Coll. on Automata, Languages and Programming (ICALP)*, 2014.

[Che19] Lijie Chen. Non-deterministic quasi-polynomial time is average-case hard for ACC circuits. In *IEEE Symp. on Foundations of Computer Science (FOCS)*, 2019.

[CL21] Lijie Chen and Xin Lyu. Inverse-exponential correlation bounds and extremely rigid matrices from a new derandomized XOR lemma. In *ACM Symp. on the Theory of Computing (STOC)*, 2021.

[CLW20] Lijie Chen, Xin Lyu, and Ryan Williams. Almost everywhere circuit lower bounds from non-trivial derandomization. In *IEEE Symp. on Foundations of Computer Science (FOCS)*, 2020.

[Coo73] Stephen A. Cook. A hierarchy for nondeterministic time complexity. *J. of Computer and System Sciences*, 7(4):343–353, 1973.

[COS18] Ruiwen Chen, Igor Carboni Oliveira, and Rahul Santhanam. An average-case lower bound against ACC^0. In *LATIN*, volume 10807 of *Lecture Notes in Computer Science*, pages 317–330. Springer, 2018.

[CR20] Lijie Chen and Hanlin Ren. Strong average-case circuit lower bounds from non-trivial derandomization. In *ACM Symp. on the Theory of Computing (STOC)*, 2020.

[CW16] Timothy M. Chan and Ryan Williams. Deterministic APSP, orthogonal vectors, and more: Quickly derandomizing razborov-smolensky. In Robert Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 1246–1255. SIAM, 2016.

[CW19] Lijie Chen and R. Ryan Williams. Stronger connections between circuit analysis and circuit lower bounds, via PCPs of proximity. In Amir Shpilka, editor, *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA*, volume 137 of *LIPIcs*, pages 19:1–19:43. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[GNW11] Oded Goldreich, Noam Nisan, and Avi Wigderson. On Yao's XOR-lemma. In *Studies in Complexity and Cryptography*, volume 6650 of *Lecture Notes in Computer Science*, pages 273–301. Springer, 2011.

[MW18] Cody Murray and R. Ryan Williams. Circuit lower bounds for nondeterministic quasi-polytime: an easy witness lemma for NP and NQP. In *STOC*, pages 890–901. ACM, 2018.

[Par20] Orr Paradise. Smooth and strong PCPs. In Thomas Vidick, editor, *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*, volume 151 of *LIPIcs*, pages 2:1–2:41. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[Raz87] Alexander Razborov. Lower bounds on the dimension of schemes of bounded depth in a complete basis containing the logical addition function. *Akademiya Nauk SSSR. Matematicheskie Zametki*, 41(4):598–607, 1987. English translation in Mathematical Notes of the Academy of Sci. of the USSR, 41(4):333-338, 1987.

[RSS18] Ninad Rajgopal, Rahul Santhanam, and Srikanth Srinivasan. Deterministically counting satisfying assignments for constant-depth circuits with parity gates, with implications for lower bounds. In Igor Potapov, Paul G. Spirakis, and James Worrell, editors, *Symp. on Math. Foundations of Computer Science (MFCS)*, volume 117 of *LIPIcs*, pages 78:1–78:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

[SFM78] Joel I. Seiferas, Michael J. Fischer, and Albert R. Meyer. Separating nondeterministic time complexity classes. *J. of the ACM*, 25(1):146–167, 1978.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *19th ACM Symp. on the Theory of Computing (STOC)*, pages 77–82. ACM, 1987.

[Smo93] Roman Smolensky. On representations by low-degree polynomials. In *34th IEEE IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 130–138, 1993.

[SV12] Rocco A. Servedio and Emanuele Viola. On a special case of rigidity. Available at http://www.ccs.neu.edu/home/viola/, 2012.

[Tam16] Suguru Tamaki. A satisfiability algorithm for depth two circuits with a sub-quadratic number of symmetric and threshold gates. *Electronic Colloquium on Computational Complexity (ECCC)*, 23:100, 2016.

[Val77] Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In *6th Symposium on Mathematical Foundations of Computer Science*, volume 53 of *Lecture Notes in Computer Science*, pages 162–176. Springer, 1977.

[Vio20] Emanuele Viola. New lower bounds for probabilistic degree and AC0 with parity gates. *Electronic Colloquium on Computational Complexity (ECCC)*, 27:15, 2020.

[VW20] Nikhil Vyas and Ryan Williams. Lower bounds against sparse symmetric functions of ACC circuits: Expanding the reach of #SAT algorithms. In *Symp. on Theoretical Aspects of Computer Science (STACS)*, 2020.

[Wil10] Ryan Williams. Improving exhaustive search implies superpolynomial lower bounds. In *42nd ACM Symp. on the Theory of Computing (STOC)*, pages 231–240, 2010.

[Wil11] Ryan Williams. Guest column: a casual tour around a circuit complexity bound. *SIGACT News*, 42(3):54–76, 2011.

[Wil13] Ryan Williams. Natural proofs versus derandomization. In *ACM Symp. on the Theory of Computing (STOC)*, 2013.

[Wil14a] Ryan Williams. New algorithms and lower bounds for circuits with linear threshold gates. In *ACM Symp. on the Theory of Computing (STOC)*, 2014.

[Wil14b] Ryan Williams. Nonuniform ACC circuit lower bounds. *J. of the ACM*, 61(1):2:1–2:32, 2014.

[Zák83] Stanislav Zák. A turing machine time hierarchy. *Theoretical Computer Science*, 26:327–333, 1983.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il