Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 133 (2012)

On Rigid Matrices and U-Polynomials

Noga Alon* Gil Cohen†

October 29, 2012

Abstract

We introduce a class of polynomials, which we call *U-polynomials* and show that the problem of explicitly constructing a rigid matrix can be reduced to the problem of explicitly constructing a small hitting set for this class. We prove that small-bias sets are hitting sets for the class of U-polynomials, though their size is larger than desired. Furthermore, we give two alternative proofs for the fact that small-bias sets induce rigid matrices.

Finally, we construct rigid matrices from unbalanced expanders, with essentially the same size as the construction via small-bias sets.

*Sackler School of Mathematics and Blavatnik School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. Email: nogaa@tau.ac.il. Research supported in part by an ERC Advanced grant, by a USA-Israeli BSF grant and by the Israeli I-Core program.

†Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel. Email: gil.cohen@weizmann.ac.il. Research supported by Israel Science Foundation (ISF) grant.

ISSN 1433-8092

1 Introduction

Motivated by the problem of proving lower bounds for arithmetic circuits, Valiant [Val77] introduced the notion of *matrix rigidity*. Let A be an $m \times n$ matrix over a finite field $\mathbb{F}$. We consider the linear mapping $x \mapsto Ax$, and ask how hard is it to compute in the following natural model of computation. Consider a circuit on n inputs and m outputs composed of the following gates: for every $a, b \in \mathbb{F}$ the gate $G_{a,b}$ on inputs $x, y \in \mathbb{F}$ outputs $ax + by$. The *size* of a circuit is the number of gates it contains. The *depth* of a circuit is the number of gates in the longest path from an input to an output. In this paper we will focus on $\mathbb{F} = \mathbb{F}_2$. Note that in this case the only allowed gate is the Parity gate.

A simple counting argument shows that most linear mappings with $m = \Theta(n)$ have size $\Omega(n^2/\log n)$. Nevertheless, currently there is no explicit linear mapping we know of, that has size $\omega(n)$. In fact, even after more than three decades of study, there is no known linear mapping that cannot be computed by a circuit with linear size and logarithmic depth simultaneously. Valiant [Val77] suggested a route for resolving the latter problem by giving a sufficient conditions for a matrix A that ensure it corresponds to a difficult instance. The property suggested by Valiant essentially requires that the rank of A is robust against alternations of a small number of entries. There are a few variants of this notion. For more information, we refer the reader to a recent survey by Lokam [Lok09].

Definition 1.1 (Matrix Rigidity)**.** *Let A be an $m \times n$ matrix over $\mathbb{F}_2$. A is called* (r, s)-rigid *if for every $m \times n$ matrix R with rank at most r, $A - R$ contains a row with at least s non-zero entries.*

The above definition states that a matrix A is (r, s)-rigid if one cannot decrease the rank of A to r by altering less than s entries in each row of A. The following theorem, due to Valiant, has motivated the study of matrix rigidity.

Theorem 1.2 (Valiant [Val77])**.** *Let A be an $m \times n$ matrix over $\mathbb{F}_2$, where $m = O(n)$. If A is $(\Omega(n), n^{\Omega(1)})$-rigid, then any linear arithmetic circuit with logarithmic depth that computes A, has size $\Omega(n \cdot \log\log n)$.*

In [APY09], Alon, Panigrahy and Yekhanin present the problem of constructing rigid matrices in an equivalent, yet conceptually different way. To describe it, we need the following standard definition of distance between a point and a set.

Definition 1.3. *For $x \in \mathbb{F}_2^n$ and $U \subseteq \mathbb{F}_2^n$, define the* Hamming distance of x from U *by*

$$\mathsf{dist}_{\mathsf{H}}(x, U) = \min_{u \in U} |x + u|,$$

where $|v|$ denotes the Hamming weight of the vector v.

Definition 1.4 (Rigid Sets)**.** *A* set $S \subseteq \mathbb{F}_2^n$ *is called* (n, k, d)-rigid *if for every subspace $U \subseteq \mathbb{F}_2^n$ of dimension k,*

$$\max_{s \in S} \mathsf{dist}_{\mathsf{H}}(s, U) \geq d.$$

It is an easy exercise to show that an (n, k, d)-rigid set S with size m induces a (k, d)-rigid matrix with size $m \times n$, and vice versa. We will also discuss the following stronger variant of rigid sets.

Definition 1.5 (Strong Rigid Sets)**.** *A* set $S \subseteq \mathbb{F}_2^n$ *is called* strong (n, k, d)-rigid *if for every subspace* $U \subseteq \mathbb{F}_2^n$ *of dimension* k*,*

$$\mathbb{E}_{s \sim S} \left[\mathsf{dist}_{\mathsf{H}}(s, U) \right] \geq d.$$

For implications to complexity theory using Valiant's Theorem (Theorem 1.2), one needs to construct an $(n, \Omega(n), n^{\Omega(1)})$-rigid set with size $O(n)$. Thus, historically, the study of matrix rigidity focused on the tradeoff between k and d while fixing $m = O(n)$ [Fri93, Lok95, SSS97, KR98]. Given that after more than three decades of research we seem to be far from achieving a tradeoff between k, d that would suffice for establishing Theorem 1.2, the authors of [APY09] initiated the study of the tradeoff between m and d while fixing $k = n/2$. In this setting one no longer insists on $m = O(n)$, but aims at getting m as small as possible as a function of d, with the goal of achieving $m = \mathrm{poly}(d)$.

1.1 Our Results

In this work we suggest a new approach for constructing rigid sets (or equivalently, rigid matrices). Throughout the paper we let $\rho \in (0, 1)$ be a constant parameter. Central to our approach are polynomials with a special structure, which we call U*-polynomials*.

U-polynomials. For a subspace $U \subset \mathbb{F}_2^n$ define the polynomial $p_U \colon \mathbb{F}_2^n \to \mathbb{R}$ [1] as follows

$$p_U(x) = \frac{1}{\mathsf{W}_\rho(U)} \cdot \sum_{u \in U} \rho^{|u|} \cdot (-1)^{<u,x>},$$

where $\mathsf{W}_\rho(U) = \sum_{u \in U} \rho^{|u|}$ is the *weight enumerator* of U with parameter ρ, and serves for normalization. We call such polynomial a U*-polynomial*. We emphasize that this is indeed a polynomial if one chooses to work over the domain $\{1, -1\}$ rather than $\mathbb{F}_2$.

Let $\mathcal{P}_k$ be the class of all U-polynomials p_U, where $U \subset \mathbb{F}_2^n$ has dimension k. One can show that for any subspace U and for any $x \in \mathbb{F}_2^n$, $0 < p_U(x) \leq 1$ [2], where equality to 1 holds iff $x \in U^\perp$. Our first main theorem shows that $p_{U^\perp}(x)$ is related to the Hamming distance of x from U.

Theorem 1. *Let* $\rho \in (0, 1)$ *be an arbitrary constant parameter. Let* $U \subseteq \mathbb{F}_2^n$ *be a subspace. Then, for every* $x \in \mathbb{F}_2^n$*,*

$$\mathsf{dist}_{\mathsf{H}}(x, U) = \Omega\left(\log \frac{1}{p_{U^\perp}(x)} \right).$$

[1] For the sake of readability, we suppress ρ in the notation when it is clear from context.

[2] The upper bound is trivial, while the lower bound is implicit in the proof of Theorem 1.

By Theorem 1, the problem of explicitly constructing an $(n, k, \Omega(d))$-rigid set is reduced to that of explicitly constructing a set S such that for every $U \subset \mathbb{F}_2^n$ with dimension $n-k$, there exists $s \in S$ such that $p_U(s) \leq 2^{-\Omega(d)}$. We informally refer to such sets as *hitting sets for* $\mathcal{P}_{n-k}$, as for values of k of interest (say, $k = \alpha n$ for a constant $\alpha \in (0,1)$), p_U evaluated on a random point is exponentially small in n.

Similarly, by Theorem 1, the problem of explicitly constructing a *strong* $(n, k, \Omega(d))$-rigid set is reduced to the problem of explicitly constructing a set S such that for every $U \subset \mathbb{F}_2^n$ of dimension $n-k$, for at least, say, half of the elements $s \in S$ it holds that $p_U(s) \leq 2^{-\Omega(d)}$. If $\mathcal{A}$ is an algorithm that given n, k, d as inputs, constructs such a set S, then we informally refer to $\mathcal{A}$ as a *pseudorandom generator for* $\mathcal{P}_{n-k}$.

For simplicity of presentation we set $k = n/2$ and discuss the case of general k in Section 6, where we show how to reduce the problem of constructing (n, k, d)-strong rigid sets for general k to the case $k = n/2$.

One may ask whether there is a quantitative loss in the reduction from the problem of constructing rigid sets to the problem of constructing hitting sets for U-polynomials. Similarly, is there a quantitative loss in the reduction from the problem of constructing strong rigid sets to the problem of constructing pseudorandom generators for U-polynomials ? The following claim gives a negative answer to these questions.

Claim 2. *Let $\rho \in (\sqrt{2}-1, 1)$ be a constant parameter. Then, with high probability, a random set $S \subset \mathbb{F}_2^n$ of size $O(n)$ has the following property: for every $p_U \in \mathcal{P}_{n/2}$, for at least half of the elements $s \in S$ it holds that $p_U(s) \leq 2^{-\Omega(n)}$.*

Unfortunately, we are unable to give an explicit construction of a set S that satisfies the property of Claim 2 (by Theorem 1, such a set would be a strong rigid set). However, we hope that this reduction will be used as a starting point for future constructions of rigid sets. In this paper we make use of Theorem 1 to show that small-bias sets are strong rigid sets, however, their size is larger than desired.

Theorem 3. *Let n, d be such that $d \leq c \cdot n$ for some suitable constant $0 < c < 1$. Let $S \subset \mathbb{F}_2^n$ be an $\exp(-d)$-biased set. Then S is an $(n, n/2, d)$-strong rigid set.*

In the theorem above, and throughout the rest of the paper, the notation $\exp(z)$ always means e^{cz} for an appropriate constant c.

Using, for example, the construction of [ABN+92] for small-bias sets, Theorem 3 yields an $(n, n/2, d)$-strong rigid set with size $n \cdot \exp(d)$. This matches the construction of [APY09]. Applying the reduction described in Section 6 we get an explicit construction of a strong (n, k, d)-rigid set with size $n \cdot \exp(d \cdot k/n)$. In Section 4 we present two alternative proofs for Theorem 3. Each of these proofs applies different arguments.

In Section 5 we show how to construct rigid sets from unbalanced expanders (see Section 5 for a formal definition of unbalanced expanders). Specifically, we prove the following theorem.

Theorem 4. *Let $G = (L, R, E)$ be a $(k_{max}, 2/3)$-bipartite expander with $L = [m]$, $R = [n]$ and left-degree $4d$. For every $\ell \in L$ define a vector $c_\ell \in \mathbb{F}_2^n$ as follows: for $i \in [n]$,*

$$(c_\ell)_i = \begin{cases} 1, & \ell i \in E; \\ 0, & \textit{otherwise.} \end{cases}$$

If

$$\sum_{i=0}^{k_{max}/2} \binom{m}{i} > 2^k,$$

then the set $C = \{c_\ell : \ell \in L\}$ is (n, k, d)-rigid.

The proof of Theorem 4 applies a different argument than any of the proofs for Theorem 3. In particular, it does not use the reduction to the problem of constructing hitting sets for U-polynomials. Moreover, it is interesting to note that the two rigid sets constructed in Theorem 3 and Theorem 4 have a different structure. Indeed, a typical element in a small-bias set $S \subseteq \mathbb{F}_2^n$ has weight roughly $n/2$. On the other hand, every element in the construction that is based on unbalanced expanders has weight at most $4d$. Nevertheless, plugging the unbalanced expander that is obtained by the probabilistic method [3] yields an (n, k, d)-rigid set with size $n \cdot \exp(d \cdot k/n)$ - exactly the size we get by applying the reduction in Section 6 to Theorem 3.

1.2 Recent Related Work

Recently, two papers have suggested new approaches for constructing rigid matrices. Dvir [Dvi10] related the problem of constructing rigid matrices to the problem of proving lower bounds for locally self-correctable codes. Specifically, he showed that if the generating matrix of a locally decodable code is not rigid, then the code has rate close to one. Hence, proving that such codes do not exist will give rise to explicit construction of rigid matrices.

Barak, Dvir, Wigderson and Yehudayoff [BDWY11] showed that some combinatorial [4] property of the zero/non-zero entries in a matrix implies high rank. The hope is that a combinatorial property will be more robust against small number of alternations than an algebraic property, and thus, a matrix satisfying this combinatorial property will be rigid. The result of [BDWY11] holds for a field of characteristic zero and for fields of large finite characteristic.

1.3 Organization

The rest of the paper is organized as follows. In Section 2 we give basic definitions and results we shall later use. As different parts of the paper require different, almost non-intersecting, tools, we postpone some of the preliminary results and describe them once they are required. In Section 3 we

[3] The state of the art explicit construction for unbalanced expanders due to Guruswami, Umans and Vadhan [GUV09] falls short from achieving the parameters of the probabilistic construction. This in turn gives a rigid set with a somewhat larger size. We elaborate on this in Section 5.

[4] Combinatorial in the sense that one only counts the number of zero/non-zero entries in various patterns.

study U-polynomials and their application to the construction of rigid sets. Specifically, we prove Theorem 1, Claim 2 and Theorem 3. In Section 4 we give two alternative proofs for Theorem 3. In Section 5 we prove Theorem 4 and in Section 6 we prove a lemma that reduces the problem of constructing (n, k, d)-rigid sets to that of constructing $(n, n/2, d')$-rigid sets.

2 Preliminaries

In this section we cover some preliminary definitions, facts and theorems used in the rest of the paper. As mentioned, since each of our proofs uses a different set of tools, for the sake of readability, we defer some of the preliminaries to the relevant sections. We start by giving some general remarks. To avoid cumbersome presentation we omit all floor and ceiling signs whenever these are not crucial. All logarithms in the paper are in base 2. We denote by $\mathsf{SD}(X, Y)$ the statistical distance between two distributions on the same support. Formally, if X, Y have support S, then

$$\mathsf{SD}(X, Y) = \max_{A \subseteq S} \big|\mathsf{Pr}[X \in A] - \mathsf{Pr}[Y \in A]\big|.$$

Let S, T be two distributions on $\mathbb{F}_2^n$. The distribution $S + T$ is defined as follows. To sample from $S + T$ one samples two elements s, t independently from S, T respectively, and outputs $s + t$. The definition can be naturally extended to any finite number of distributions. In particular, for an integer $c \geq 1$, and a distribution S on $\mathbb{F}_2^n$, we define $c \cdot S$ to be $S + \cdots + S$ where c summands participate in the sum.

2.1 Fourier Analysis

In this section we cover the required tools needed from Fourier analysis. We refer the reader to the book of O'Donnell [O'D] for a comprehensive treatment.

Consider all functions of the form $f : \mathbb{F}_2^n \to \mathbb{R}$. These form a vector space $\mathcal{F}$, where addition is conducted in a point-wise manner, that is, for every $f, g \in \mathcal{F}$, the function $f + g$ is defined by $(f + g)(x) = f(x) + g(x)$. For every $\alpha \in \mathbb{F}_2^n$, $\chi_\alpha : \mathbb{F}_2^n \to \mathbb{R}$ is defined by $\chi_\alpha(x) = (-1)^{<\alpha, x>}$. It is easy to see that $\{\chi_\alpha : \alpha \in \mathbb{F}_2^n\}$ is a basis for $\mathcal{F}$. This basis is called the *Fourier basis* for $\mathcal{F}$. Define an inner product over $\mathcal{F}$: for every $f, g \in \mathcal{F}$,

$$< f, g >= \frac{1}{2^n} \cdot \sum_{x \in \mathbb{F}_2^n} f(x)g(x).$$

It is easy to see that

$$< \chi_\alpha, \chi_\beta >= \begin{cases} 1, & \alpha = \beta; \\ 0, & \text{otherwise.} \end{cases}$$

Under the above inner product, the Fourier basis is an orthonormal basis. Thus, every $f \in \mathcal{F}$ can be expanded according to the Fourier basis as follows

$$f = \sum_{\alpha \in \mathbb{F}_2^n} \hat{f}(\alpha)\chi_\alpha,$$

where $\hat{f}(\alpha) =< f, \chi_\alpha >$ is called *the Fourier coefficient* of f on point α.

The noise operator. Let $0 \leq \varepsilon \leq 1$. The *noise operator* $T_\varepsilon : \mathcal{F} \to \mathcal{F}$ is defined as follows

$$T_\varepsilon(f)(x) = \sum_{y \in \mathbb{F}_2^n} \left(\frac{1-\varepsilon}{2}\right)^{|y|} \cdot \left(\frac{1+\varepsilon}{2}\right)^{n-|y|} f(x+y).$$

Fact 2.1. *For every $f \in \mathcal{F}$, $0 \leq \varepsilon \leq 1$ and $\alpha \in \mathbb{F}_2^n$,*

$$\widehat{T_\varepsilon(f)}(\alpha) = \varepsilon^{|\alpha|} \cdot \widehat{f}(\alpha).$$

2.2 Small-Bias Sets

Small-Bias sets, introduced by Naor and Naor [NN93], are pseudorandom objects that have found numerous applications in theoretical computer science.

Definition 2.2. *Let $S \subseteq \mathbb{F}_2^n$. We say that S is an ε-biased set if for every $0 \neq \alpha \in \mathbb{F}_2^n$ it holds that*

$$\left| \mathbb{E}_{s \sim S} \left[(-1)^{<\alpha, s>} \right] \right| \leq \varepsilon.$$

A minor technicality when working with small-bias sets is repetition of elements in the set. To avoid ambiguity, when working with small-bias sets we do not ignore repetitions of elements, that is, we consider small-bias sets as multi-sets. In other words, we think of small-bias sets as sample spaces, where an element is sampled with probability that is proportional to the element's multiplicity in the set.

A simple probabilistic argument shows that there exist ε-biased sets in $\mathbb{F}_2^n$ with size $O(n/\varepsilon^2)$. Several explicit constructions of small-bias sets were introduced in [AGHP92, ABN+92, NN93, BT09]. Unfortunately, none of the explicit constructions achieves the size obtained by the probabilistic argument.

3 U-Polynomials

In this section we discuss U-polynomials and their application for the construction of rigid sets and strong rigid sets. Specifically, we prove Theorem 1, Claim 2 and Theorem 3.

3.1 Proof of Theorem 1

The following theorem readily implies Theorem 1. Indeed, it is simply Theorem 1 for the case where ρ is not necessarily a constant.

Theorem 5. *Let $U \subset \mathbb{F}_2^n$ be a subspace. Then, for any $\rho \in (0,1)$ and for any $x \in \mathbb{F}_2^n$,*

$$\mathsf{dist}_{\mathsf{H}}(x, U) \geq \left(\log \frac{1+\rho}{1-\rho}\right)^{-1} \cdot \log \frac{1}{p_{U^\perp, \rho}(x)}.$$

The main intuition behind the proof of Theorem 5 is to work with "scalar fields"[5] rather than with "distances". We now elaborate on this. Let $U \subseteq \mathbb{F}_2^n$ be a subspace. Imagine that at every point $u \in U$ we place a source of light that emits radiation to its surrounding, with intensity that decays with distance. Then, every point $x \in \mathbb{F}_2^n$ senses the superposition of radiations coming to it from all points in U. From this perspective, finding a point that is far from U boils down to locating a point that senses a small amount of radiation, that is, a dark point. The formal definition of this energy function is as follows.

Definition 3.1. *For a parameter $\rho \in (0,1)$ and a subspace $U \subseteq \mathbb{F}_2^n$, define the function $\mathsf{energy}_{U,\rho} : \mathbb{F}_2^n \to \mathbb{R}$ as follows*

$$\mathsf{energy}_{U,\rho}(x) = \frac{1}{\mathsf{W}_\rho(U)} \cdot \sum_{u \in U} \rho^{|u+x|}.$$

When it is not needed to specify one or more of the parameters ρ, U, we omit them. We note that $\mathsf{energy}_U(x) \in (0,1]$, and that $\mathsf{energy}_U(x) = 1$ if and only if $x \in U$. (The lower bound is obvious, whereas the upper bound and the characterization of equality follows from equation 3.3 below.) Thus, not surprisingly, a maximum amount of radiation is sensed on the subspace U itself. Moreover, for a uniformly sampled $x \in \mathbb{F}_2^n$, $\mathsf{energy}_U(x)$ is exponential in $\Omega(k-n)$. That is, a typical point in $\mathbb{F}_2^n$ senses a small amount of radiation, and so most of $\mathbb{F}_2^n$ is dark.

We will need the following theorem, due to MacWilliams (see, e.g., [MS77]), that relates the weight enumerator of a subspace with that of its dual. We state the theorem for the binary field only.

Theorem 3.2 (MacWilliams's Theorem)**.** *Let $U \subseteq \mathbb{F}_2^n$ be a subspace of dimension k. Then for every $0 < \rho < 1$ it holds that*

$$\mathsf{W}_\rho(U^\perp) = \frac{(1+\rho)^n}{2^k} \cdot \mathsf{W}_{\frac{1-\rho}{1+\rho}}(U).$$

We are now ready to prove Theorem 5.

Proof of Theorem 5: Let $1_U : \mathbb{F}_2^n \to \{0,1\}$ be the characteristic function for U. That is, $1_U(x) = 1$ if and only if $x \in U$. Then,

$$\begin{aligned}
T_\rho(1_U)(x) &= \sum_{y \in \mathbb{F}_2^n} \left(\frac{1-\rho}{2}\right)^{|y|} \cdot \left(\frac{1+\rho}{2}\right)^{n-|y|} \cdot 1_U(x+y) \\
&= \left(\frac{1+\rho}{2}\right)^n \cdot \sum_{y \in \mathbb{F}_2^n} \left(\frac{1-\rho}{1+\rho}\right)^{|y|} \cdot 1_U(x+y) \\
&= \left(\frac{1+\rho}{2}\right)^n \cdot \sum_{u \in U} \left(\frac{1-\rho}{1+\rho}\right)^{|u+x|} \\
&= \left(\frac{1+\rho}{2}\right)^n \cdot \mathsf{W}_{\frac{1-\rho}{1+\rho}}(U) \cdot \mathsf{energy}_{U,\frac{1-\rho}{1+\rho}}(x). \qquad (3.1)
\end{aligned}$$

[5]Here the word field takes its meaning from physics and has nothing to do with algebraic fields.

On the other hand, it is easy to see that

$$\widehat{1_U}(\alpha) = \begin{cases} 2^{k-n}, & \alpha \in U^\perp; \\ 0, & \text{otherwise.} \end{cases}$$

Hence, by Fact 2.1

$$\begin{aligned} T_\rho(1_U)(x) &= \sum_{\alpha \in \mathbb{F}_2^n} \widehat{T_\rho(1_U)}(\alpha) \cdot (-1)^{<\alpha,x>} \\ &= \sum_{\alpha \in \mathbb{F}_2^n} \widehat{1_U}(\alpha) \cdot \rho^{|\alpha|} \cdot (-1)^{<\alpha,x>} \\ &= 2^{k-n} \cdot \sum_{\alpha \in U^\perp} \rho^{|\alpha|} \cdot (-1)^{<\alpha,x>} \\ &= 2^{k-n} \cdot \mathsf{W}_\rho(U^\perp) \cdot p_{U^\perp,\rho}(x) \\ &= \left(\frac{1+\rho}{2}\right)^n \cdot \mathsf{W}_{\frac{1-\rho}{1+\rho}}(U) \cdot p_{U^\perp,\rho}(x), \end{aligned} \tag{3.2}$$

where the last equality follows by Theorem 3.2. By equations (3.1), (3.2) we have that

$$\mathsf{energy}_{U,\frac{1-\rho}{1+\rho}}(x) = p_{U^\perp,\rho}(x).\ ^6 \tag{3.3}$$

Assume now that $\mathsf{dist}_{\mathsf{H}}(x, U) = d$. Then there exists $w \in U$ such that $|x + w| = d$. Therefore,

$$\begin{aligned} \mathsf{W}_{\frac{1-\rho}{1+\rho}}(U) \cdot \mathsf{energy}_{U,\frac{1-\rho}{1+\rho}}(x) &= \sum_{u \in U} \left(\frac{1-\rho}{1+\rho}\right)^{|u+x|} \\ &\overset{(1)}{=} \sum_{u \in U} \left(\frac{1-\rho}{1+\rho}\right)^{|u+x+w|} \\ &\overset{(2)}{\geq} \sum_{u \in U} \left(\frac{1-\rho}{1+\rho}\right)^{|u|+|x+w|} \\ &= \left(\frac{1-\rho}{1+\rho}\right)^d \cdot \sum_{u \in U} \left(\frac{1-\rho}{1+\rho}\right)^{|u|} \\ &= \left(\frac{1-\rho}{1+\rho}\right)^d \cdot \mathsf{W}_{\frac{1-\rho}{1+\rho}}(U). \end{aligned}$$

Equality (1) uses the fact that U is a subspace, and in particular, the fact that for every $w \in U$, the function $f(u) = u + w$ is a bijection from U to U. Inequality (2) holds by the triangle inequality, and the fact that $(1 - \rho)/(1 + \rho) < 1$. Thus, by Equation (3.3),

$$p_{U^\perp,\rho}(x) \geq \left(\frac{1-\rho}{1+\rho}\right)^d,$$

which concludes the proof of the theorem. □

[6] By this equality, it is easy to see that U-polynomials are positive.

3.2 Proof of Claim 2

To prove Claim 2 we make use of the following claim, which gives a lower bound for the weight enumerator.

Claim 3.3. *For any $\rho \in (0,1)$ and for any subspace $U \subseteq \mathbb{F}_2^n$ of dimension $n/2$*

$$\mathsf{W}_\rho(U) \geq \left(\frac{1+\rho}{\sqrt{2}}\right)^n.$$

Proof: There are $2^{n/2}$ cosets $x+U$ of the subspace U, and for each of them $\sum_{w\in x+U}\rho^{|w|} \leq \sum_{u\in U}\rho^{|u|}$, whereas the summation of these $2^{n/2}$ sums over all cosets is exactly $\sum_{w\in\mathbb{F}_2^n}\rho^{|w|} = (1+\rho)^n$. □

Proof of Claim 2: Let $p_U \in \mathcal{P}_{n/2}$. Then

$$\begin{aligned}\mu \triangleq \mathbb{E}_{x\sim\mathbb{F}_2^n}\left[p_U(x)\right] &= \mathbb{E}_{x\sim\mathbb{F}_2^n}\left[\frac{1}{\mathsf{W}_\rho(U)}\cdot\sum_{u\in U}\rho^{|u|}(-1)^{<u,x>}\right] \\ &= \frac{1}{\mathsf{W}_\rho(U)}\cdot\sum_{u\in U}\rho^{|u|}\cdot\mathbb{E}_{x\sim\mathbb{F}_2^n}[(-1)^{<u,x>}] = \frac{1}{\mathsf{W}_\rho(U)},\end{aligned}$$

where the last equality holds as all summands are zero but for $u=0$, which contributes 1 to the sum. By Claim 3.3,

$$\mu = \frac{1}{\mathsf{W}_\rho(U)} \leq \left(\frac{\sqrt{2}}{1+\rho}\right)^n.$$

For any $\rho > \sqrt{2}-1$ the base of the exponent in the above equation is smaller than 1, and so, for any such ρ, there exists a constant $\alpha = \alpha(\rho) > 0$ such that $\mu < 2^{-\alpha n}$. Thus, by Markov's inequality,

$$\mathsf{Pr}_{x\sim\mathbb{F}_2^n}\left[p_U(x) > 2^{-\alpha n/2}\right] \leq 2^{-\alpha n/2}.$$

Let m to be an integer to be determined later.

$$\mathsf{Pr}_{x_1,\ldots,x_m\sim\mathbb{F}_2^n}\left[\exists S\subseteq[m], |S| = \frac{m}{2} \text{ s.t. } \forall i\in S\ \ p_U(x_i) > 2^{-\alpha n/2}\right] \leq \binom{m}{m/2}\cdot\left(2^{-\alpha n/2}\right)^{m/2}. \tag{3.4}$$

The number of subspaces of dimension $n/2$ in $\mathbb{F}_2^n$ is bounded by $\binom{2^n}{n/2}$ [7], and so by the union bound, the probability that there exists U of dimension $n/2$ for which the event in Equation (3.4) holds is bounded by

$$\binom{2^n}{n/2}\cdot\binom{m}{m/2}\cdot\left(2^{-\alpha n/2}\right)^{m/2} < 2^{n^2/2}\cdot 2^m\cdot 2^{-\alpha n m/4}.$$

For $m = (7/\alpha)n$ the right hand side in the above expression is bounded by 2^{-n^2}, for large enough n. This concludes the proof of the claim. □

[7] In fact, a tighter bound of roughly $2^{n^2/4}$ can be easily proven.

3.3 Proof of Theorem 3

We end this section by deriving Theorem 3 from Theorem 1.

Proof of Theorem 3: Let $S \subseteq \mathbb{F}_2^n$ be an ε-biased set. It can be, for example, be the one constructed in [ABN+92] which has size $m = O(n/\varepsilon^3)$, but the proof works for any such set. Let U be a subspace of dimension $n/2$. Then,

$$\begin{aligned}\mathbb{E}_{x\sim S}[p_U(x)] &= \frac{1}{\mathsf{W}_\rho(U)} \cdot \mathbb{E}_{x\sim S}\left[\sum_{u\in U} \rho^{|u|} \cdot (-1)^{<u,x>}\right] \\ &= \frac{1}{\mathsf{W}_\rho(U)} \cdot \sum_{u\in U} \rho^{|u|} \cdot \mathbb{E}_{x\sim S}\left[(-1)^{<u,x>}\right].\end{aligned}$$

Any summand except for $u = 0$ is bounded in absolute value by ε. Thus,

$$\mathbb{E}_{x\sim S}[p_U(x)] < \varepsilon + \frac{1}{\mathsf{W}_\rho(U)}.$$

Assume for now that we will pick $\varepsilon > 1/\mathsf{W}_\rho(U)$, and so we can further simplify to get $\mathbb{E}_{x\sim S}[p_U(x)] < 2\varepsilon$. Since $\log(1/x)$ is a convex function, we get, by Jensen's inequality that

$$\mathbb{E}_{x\sim S}\left[\log\left(\frac{1}{p_U(x)}\right)\right] \geq \log\left(\frac{1}{\mathbb{E}_{x\sim S}[p_U(x)]}\right) \geq \log\left(\frac{1}{2\varepsilon}\right).$$

Since we are working with subspaces of dimension $n/2$, the above equation also holds for the dual of every subspace of dimension $n/2$. Thus, by Theorem 1, for every subspace $U \subset \mathbb{F}_2^n$ with dimension $n/2$

$$\mathbb{E}_{x\sim S}\left[\mathsf{dist}_{\mathsf{H}}(x, U)\right] = \Omega\left(\log\frac{1}{\varepsilon}\right).$$

Recall that in our case $m = O(n/\varepsilon^3)$, and so setting $m = n \cdot 2^{\Theta(d)}$ would give that S is an $(n, n/2, d)$-strong rigid set with size m.

We now return to the assumption we made, namely, that $\varepsilon > 1/\mathsf{W}_\rho(U)$. Eventually we chose $\varepsilon = \exp(-d)$, and so to justify the assumption, it is enough to show that $\mathsf{W}_\rho(U) > \exp(d)$. By Claim 3.3 we have that $\mathsf{W}_\rho(U) \geq ((1+\rho)/\sqrt{2})^n$. For $\rho > \sqrt{2} - 1$, the base of the exponent is larger than 1. For any such ρ, there exists a constant $c = c(\rho) > 0$ such that our assumption is met as long as $d \leq c \cdot n$. □

4 Strong Rigid Sets from Small-Bias Sets - Alternative Proofs

In this section we give two alternative proofs for Theorem 3. We refer to the two proofs as *the bias-reduction proof* and *the covering proof*.

4.1 The Bias-Reduction Proof

This proof relies on the Parity Lemma (c.f., for example, [NN93]).

Lemma 4.1 (The Parity Lemma)**.** *Let $S \subseteq \{0,1\}^n$ be an ε-biased set. Let $T \subseteq [n]$ be a non-empty set of size k. Denote by S_T the projection of S on the index set T. Then,*

$$\mathsf{SD}(S_T, \mathrm{U}_k) \leq \varepsilon \cdot 2^{k/2}.$$

Lemma 4.1 roughly states that the projection of a small-bias set on a small number of coordinates is close, in statistical distance, to the uniform distribution. Since a random vector is, with high probability, far from any given subspace with small dimension, one would hope that a typical vector in a small-bias set would also be far from any given subspace. This idea fails because although the bound on the statistical distance guaranteed by the Parity Lemma depends linearly on the bias of the small-bias set, it depends exponentially on n, the length of the vectors.

A natural suggestion for circumventing this problem is to partition the set of indices $[n]$ to blocks and apply the argument above for each block separately. This way, the statistical distance guaranteed by the Parity Lemma will be exponential in the block length, which can be controlled, as opposed to being exponential in n. However, this suggestion fails as well since one must take the block size large enough so that the projection of the subspace on a block would still have small dimension with respect to the block length. Indeed, otherwise a random vector would not necessarily be far from the projection.

As mentioned, the statistical distance guaranteed by the Parity Lemma depends linearly on the bias of the small-bias set and exponentially on n. The natural idea above tried to obtain a better guarantee on the statistical distance by decreasing the exponential part as it naturally seems to cause the problem. However, this idea failed. The idea behind the "bias-reduction proof" as its name suggests, is to reduce the bias enough so as to cancel the exponential loss incurred by the Parity Lemma. The way we reduce the bias is by applying the above argument not to the original small-bias set S, but rather to the set $S + \cdots + S$, where the number of summands depends on the distance, d, that we want to achieve. The bias of this sum decreases exponentially with the number of summands (see Claim 4.2 below). This cancels out the exponential loss we absorb by the Parity Lemma, as desired. This shows that $S + \cdots + S$ is a strong rigid set with good parameters. We then show that this implies that S itself must also be a strong rigid set (with weaker parameters). We now make this formal. We need the following claim.

Claim 4.2. *Let S be an ε-biased set. Then, for every integer $c \geq 1$, $c \cdot S$ is an ε^c-biased set.*

Proof: For any $0 \neq \alpha \in \mathbb{F}_2^n$

$$\begin{aligned}
\left|\mathbb{E}_{x \sim c \cdot S}\left[(-1)^{<\alpha,x>}\right]\right| &= \left|\mathbb{E}_{s_1,\ldots,s_c \sim S}\left[(-1)^{<\alpha,s_1+\cdots+s_c>}\right]\right| \\
&= \left|\mathbb{E}_{s_1,\ldots,s_c \sim S}\left[\prod_{i=1}^{c}(-1)^{<\alpha,s_i>}\right]\right| \\
&= \prod_{i=1}^{c}\left|\mathbb{E}_{s_i \sim S}\left[(-1)^{<\alpha,s_i>}\right]\right| \leq \varepsilon^c.
\end{aligned}$$

□

We are now ready to give the bias-reduction proof for Theorem 3.

Proof of Theorem 3: Let S be a $2^{-c'd}$-biased set for a constant $c' > 0$ to be determined later on. Let $S' = (n/20d) \cdot S$. By Claim 4.2, S' is a $2^{-c'n/20}$-biased set. Let $U \subset \mathbb{F}_2^n$ be a subspace of dimension $n/2$. By standard counting arguments one can show that

$$\mathsf{Pr}_{x \sim \mathbb{F}_2^n}\left[\mathsf{dist}_{\mathsf{H}}(x, U) > \frac{n}{10}\right] > 0.6.$$

By the Parity Lemma (Lemma 4.1), we have that

$$\mathsf{SD}\left(S', \mathbb{F}_2^n\right) \leq 2^{-c'n/20 + n/2} < 0.1,$$

where the last inequality holds for a sufficiently large constant c'. We choose c' accordingly. Thus,

$$\mathsf{Pr}_{x \sim S'}\left[\mathsf{dist}_{\mathsf{H}}(x, U) > \frac{n}{10}\right] > 0.5.$$

In particular, the latter implies that

$$\mathbb{E}_{x \sim S'}[\mathsf{dist}_{\mathsf{H}}(x, U)] > \frac{n}{20}.$$

Recall that $S' = (n/20d) \cdot S$, and so the above equation can be written as

$$\mathbb{E}_{s_1, \ldots, s_{n/20d} \sim S}\left[\mathsf{dist}_{\mathsf{H}}\left(\sum_{i=1}^{n/20d} s_i, U\right)\right] > \frac{n}{20}. \tag{4.1}$$

At this point we note that for every $s_1, \ldots, s_{n/20d} \in S$

$$\sum_{i=1}^{n/20d} \mathsf{dist}_{\mathsf{H}}(s_i, U) \geq \mathsf{dist}_{\mathsf{H}}\left(\sum_{i=1}^{n/20d} s_i, U\right).$$

Indeed, for $i \in [n/20d]$, let $u_i \in U$ be such that $\mathsf{dist}_{\mathsf{H}}(s_i, U) = |s_i + u_i|$. Then,

$$\sum_{i=1}^{n/20d} \mathsf{dist}_{\mathsf{H}}(s_i, U) = \sum_{i=1}^{n/20d} |s_i + u_i| \geq \left|\sum_{i=1}^{n/20d} s_i + \sum_{i=1}^{n/d} u_i\right| \geq \mathsf{dist}_{\mathsf{H}}\left(\sum_{i=1}^{n/20d} s_i, U\right),$$

where the last inequality follows since U is closed under addition. Plugging this into Equation (4.1) and using linearity of expectation, we get

$$\mathbb{E}_{s \sim S}[\mathsf{dist}_{\mathsf{H}}(s, U)] > d.$$

□

4.2 The Covering Proof

In this section we give a third proof for Theorem 3. We need some preliminary definitions and results regarding expander graphs. For more information regarding expander graphs we refer the reader to the survey by Hoory, Linial and Wigderson [HLW06].

Let $G = (V, E)$ be an undirected D-regular graph on N vertices. Let A_G be the normalized adjacency matrix of G. That is, for $u, v \in V$, $(A_G)_{uv}$ equals the number of edges connecting the vertices u, v, divided by D. It is well-known that the eigenvalues of A_G are all real numbers, and that the maximum eigenvalue is 1. The graph G is called (N, D, λ)-expander if the second largest eigenvalue in absolute value is at most λ.

For a subset $S \subset V$, let $e(S)$ be the number of edges in the induced subgraph of G on S. The quantity $e(S)$ measures the density of this induced subgraph. In [AC88] Alon and Chung proved the following lemma, which states that induced subgraphs of expanders have approximately the "right" density.

Theorem 4.3 (Lemma 2.3 in [AC88])**.** *Let $G = (V, E)$ be an (N, D, λ)-expander. Then, for any set $S \subseteq V$ with size $|S| = \alpha N$*

$$\left| e(S) - \frac{1}{2} D\alpha^2 N \right| \leq \frac{1}{2} \lambda D\alpha(1-\alpha)N.$$

We also need the following theorem proved in [AR94].

Theorem 4.4. *Let $S \subseteq \mathbb{F}_2^n$ be an ε-biased set. Define the graph $G_S = (V, E)$ as follows. $V = \mathbb{F}_2^n$, and an edge connects a pair of vertices u, v if and only if $u + v \in S$. Then, G_S is a $(2^n, |S|, \varepsilon)$-expander.*

With the two theorems above we are ready to prove the following lemma. A similar lemma was proved by Arvind and Srinivasan [AS10]. Here we give a somewhat simpler proof.

Lemma 4.5. *Let $S \subseteq \mathbb{F}_2^n$ be an ε-biased set. Then, for any subspace $U \subseteq \mathbb{F}_2^n$ of dimension k*

$$\frac{|S \cap U|}{|S|} \leq 2^{k-n} + \varepsilon.$$

Proof: Define the graph $G_S = (V, E)$ as in Theorem 4.4. That is $V = \mathbb{F}_2^n$, and an edge connects a pair of vertices u, v if and only if $u + v \in S$. By Theorem 4.4, G_S is a $(2^n, |S|, \varepsilon)$-expander. Let $U \subset \mathbb{F}_2^n = V$ be a subspace of dimension k. For $u \in U$, the degree of u in the induced subgraph of G_S on U is

$$|\{s \in S : u + s \in U\}| = |\{s \in S : s \in U\}| = |U \cap S|.$$

Thus,

$$|e(S)| = \frac{1}{2} \cdot |U| \cdot |U \cap S|.$$

By Theorem 4.3,

$$|U| \cdot |U \cap S| \leq |S| \cdot \left(\frac{|U|}{2^n} \right)^2 \cdot 2^n + \varepsilon \cdot |S| \cdot |U|,$$

or equivalently,

$$\frac{|U \cap S|}{|S|} \leq \frac{|U|}{2^n} + \varepsilon,$$

which concludes the proof of the lemma as $|U| = 2^k$. □

Proof of Theorem 3: Let $U \subset \mathbb{F}_2^n$ be a subspace of dimension $n/2$. We now describe the covering of the neighborhood of U, proposed in [APY09]. Partition the n unit vectors of $\mathbb{F}_2^n$ into $8d$ sets $B_1, \ldots, B_{8d}$ of size $n/8d$ each. For every set $I \subseteq [8d]$ with size $|I| = 2d$, define

$$U_I = \mathsf{Span}\left(U \cup \bigcup_{i \in I} B_i\right).$$

We note that $\mathsf{dim}(U_I) \leq 3n/4$ for every I, as we add to U, which has dimension $n/2$, $(n/8d) \cdot 2d$ unit vectors, thus increasing U's dimension by at most $n/4$. Moreover, it is easy to see that every vector x satisfying $\mathsf{dist}_{\mathsf{H}}(x, U) \leq 2d$ is contained in U_I for some I. Let S be an ε-biased set. By Lemma 4.5, for every I as above,

$$|S \cap U_I| \leq |S| \cdot \left(2^{-n/4} + \varepsilon\right).$$

There are $\binom{8d}{2d} < 120^d$ such sets I, and as mentioned, they cover the $2d$-neighborhood of U. Therefore, S intersects the $2d$-neighborhood of U in at most $120^d \cdot |S| \cdot \left(2^{-n/4} + \varepsilon\right)$ vectors. As we assume $d \leq c \cdot n$, for small enough constant c, setting $\varepsilon = 120^{-d}/4$ implies that at most half of the vectors in S are contained in the $2d$-neighborhood of U. Thus,

$$\mathbb{E}_{s \sim S}\left[\mathsf{dist}_{\mathsf{H}}(s, U)\right] \geq d.$$

□

5 Rigid Sets from Unbalanced Expanders

In this section we prove Theorem 4. First we give some preliminary definitions and results regarding bipartite expanders. For more information we refer the reader to [HLW06]. Let $G = (L, R, E)$ be a bipartite graph with $|L| = m$, $|R| = n$, and left-degree d. For a set $S \subseteq L$ define

$$\Gamma(S) = \{r \in R : \exists s \in S \text{ such that } sr \in E\},$$

and

$$\Gamma_1(S) = \{r \in R : \exists! s \in S \text{ such that } sr \in E\}.$$

G is called $(k_{max}, 1-\varepsilon)$-*bipartite-expander* if for every $S \subseteq L$ with size at most $k_{\max}$, it holds that $|\Gamma(S)| \geq (1-\varepsilon)d|S|$. G is called $(k_{max}, 1-\varepsilon)$-*unique neighbor expander* if for every $S \subseteq L$ with size at most $k_{\max}$, it holds that $|\Gamma_1(S)| \geq (1-\varepsilon)d|S|$. The following simple well known fact relates the two definitions.

Fact 5.1. *Every $(k_{max}, 1-\varepsilon)$-bipartite expander is a $(k_{max}, 1-2\varepsilon)$-unique neighbor expander.*

We will be interested in the case where $m >> n$. Such bipartite expanders are called *unbalanced expanders*. It can be shown, using a standard probabilistic argument, that for every $n, d, k_{\max}$ such that $k_{\max} = O(n/d)$ and for every constant $\varepsilon > 0$, there exists a $(k_{\max}, 1-\varepsilon)$-bipartite expander with

$$m = k_{\max} \cdot \left(\frac{n}{d \cdot k_{\max}}\right)^{\Omega(d)}.$$

In particular, by Fact 5.1, this bipartite expander is a $(k_{\max}, 1-2\varepsilon)$-unique neighbor expander. The state of the art explicit construction for unbalanced expanders is due to Guruswami et al. [GUV09]. Unfortunately, it falls short of achieving the same parameters as the probabilistic construction above. We are now ready to prove Theorem 4.

Proof of Theorem 4: By Fact 5.1, we have that G is a $(k_{\max}, 1/3)$-unique neighbor expander. Let $U \subseteq \mathbb{F}_2^n$ be a subspace of dimension k. Assume for contradiction that for every $c \in C$ there exists $u_c \in U$ such that $|c + u_c| \leq d$. In case there is more than one element in U that is of distance at most d from c, we choose one such element arbitrarily. Define $U' = \{u_c : c \in C\}$.

Claim 5.2. $|U'| = |C| = m$

Proof: Let c, c' be two distinct elements in C. To prove the claim it is enough to show that $u_c \neq u_{c'}$. Assume for contradiction that $u_c = u_{c'}$. Then, by the triangle inequality,

$$|c + c'| \leq |c + u_c| + |c' + u_{c'}| + |u_c + u_{c'}| \leq 2d. \tag{5.1}$$

On the other hand, G is a $(k_{\max}, 1/3)$-unique neighbor expander. Hence,

$$|c + c'| \geq \frac{1}{3} \cdot 4d \cdot 2 > 2d,$$

contradicting Equation (5.1). □

Define

$$U'' = \left\{ \sum_{i=1}^{t} u_i \;\middle|\; t \in [k_{\max}/2] \text{ and } u_1, \ldots, u_t \in U' \right\}.$$

Claim 5.3.

$$|U''| = \sum_{i=0}^{k_{max}/2} \binom{m}{i}$$

Before proving Claim 5.3 we note that it completes the proof of Theorem 4. Indeed, on one hand $U'' \subseteq U$, and so $|U''| \leq |U|$. On the other hand, by Claim 5.3 and by the assumption of Theorem 4, $|U''| > |U|$.

Proof of Claim 5.3: We first note that it is enough to prove that for every $\emptyset \neq S \subseteq U''$ with size at most $k_{\max}$, it holds that

$$\sum_{u \in S} u \neq 0. \tag{5.2}$$

Indeed, assume that there exist two distinct subsets $R, T \subseteq U''$ such that $R = \{u_1, \ldots, u_r\}$, $T = \{v_1, \ldots, v_t\}$, and $r, t \leq k_{\max}/2$. If

$$\sum_{i=1}^{r} u_i = \sum_{j=1}^{t} v_j,$$

then the symmetric difference of R, T is a non-empty set of size at most $k_{\max}$ such that the sum of its elements is 0, contradicting Equation 5.2. As in Claim 5.2, assume by contradiction that there exists a set S as above for which Equation (5.2) does not hold. Then, by the triangle inequality,

$$\left| \sum_{u \in S} c_u \right| \leq \sum_{u \in S} |u + c_u| + \left| \sum_{u \in S} u \right| \leq d \cdot |S|. \tag{5.3}$$

On the other hand, since G is $(k_{\max}, 1/3)$ unique-neighbor expander,

$$\left| \sum_{u \in S} c_u \right| \geq \frac{1}{3} \cdot 4d \cdot |S| > d \cdot |S|,$$

contradicting Equation (5.3). □

This completes the proof of Theorem 4. □

As mentioned above, a standard probabilistic argument shows that there exists a bipartite expander G as above with

$$m = k_{\max} \cdot \left(\frac{n}{d \cdot k_{\max}} \right)^{\Omega(d)}.$$

For any $k \leq c \cdot n$, for some suitable constant c, one can choose $k_{\max}$ such that $n/(d \cdot k_{\max}) = \exp(k/n)$ which suffices for the assumption of Theorem 4 to hold. This gives an (n, k, d)-rigid set with size $m = n \cdot \exp(d \cdot k/n)$ - exactly the size one gets by applying Lemma 6 of the next section to Theorem 3 (see Corollary 7). This construction however is not explicit. Plugging the unbalanced expanders of [GUV09] only gives rigid sets with size $m = n \cdot \exp(d^{O(1)} \cdot k/n)$.

6 General k

In this section we discuss the problem of constructing (n, k, d)-rigid sets for an arbitrary k. A natural approach would be to reduce this problem to the problem of constructing $(n, n/2, d')$-rigid sets. However, it is not clear whether or not there exists such a reduction. More formally, it is not clear how can one use a $\mathrm{poly}(n)$-time algorithm that is given n, d as inputs and computes an

$(n, n/2, d)$-rigid set in $\mathbb{F}_2^n$ to devise a $\mathrm{poly}(n)$-time algorithm that given n, k, d as inputs, where $k < n/2$, computes an (n, k, d)-rigid set with small size. However, it turns out that for strong rigid sets such a reduction exists. This is the statement of the following lemma.

Lemma 6. *Assume that there exists an algorithm $\mathcal{A}$ that given inputs n, d, runs in $\mathrm{poly}(n)$-time and computes a strong $(n, n/2, d)$-rigid set with size $m = m(n, d)$. Then there exists an algorithm $\mathcal{A}'$ that given n, k, d as inputs, such that $k \leq n/2$, runs in $\mathrm{poly}(n)$-time and computes a strong (n, k, d)-rigid set with size $m(2k, d \cdot 2k/n)$.*

Proof: The algorithm $\mathcal{A}'$ works as follows. $\mathcal{A}'$ makes a call to $\mathcal{A}$ on input $2k, d \cdot 2k/n$ to compute a strong $(2k, k, d \cdot 2k/n)$-rigid set S. The output of $\mathcal{A}'$ is the set

$$S' = \left\{ \underbrace{s \circ s \cdots \circ s}_{n/2k \text{ copies}} : s \in S \right\},$$

where $\circ$ denotes string concatenation. Note that $|S'| = |S| = m(2k, d \cdot 2k/n)$ as stated. We now show that S' is a strong (n, k, d)-rigid set. Let $U \subseteq \mathbb{F}_2^n$ be a subspace of dimension k. Partition the set of indices $[n]$ into $n/2k$ consecutive blocks of size $2k$ each. For $i \in [n/2k]$ denote by $U|_i$ the projection of U on the i^{th} block. Note that for every $i \in [n/2k]$, $U|_i \subseteq \mathbb{F}_2^{2k}$ is a subspace of dimension at most k. For $s \in S$ let $u_s \in U$ be a closest vector in U to $s \circ \cdots \circ s$, namely,

$$\mathsf{dist}_{\mathsf{H}}(s \circ \cdots \circ s, U) = |s \circ \cdots \circ s + u_s|.$$

For $i \in [n/2k]$, let $u_s|_i$ be the projection of u_s to the i^{th} block. Then,

$$\mathsf{dist}_{\mathsf{H}}(s \circ \cdots \circ s, U) = \sum_{i=1}^{n/2k} \left| u_s|_i + s \right| \geq \sum_{i=1}^{n/2k} \mathsf{dist}_{\mathsf{H}}(s, U|_i).$$

Thus, by linearity of expectation

$$\begin{aligned}
\mathbb{E}_{s' \sim S'} \left[\mathsf{dist}_{\mathsf{H}}(s', U) \right] &= \mathbb{E}_{s \sim S} \left[\mathsf{dist}_{\mathsf{H}}(s \circ \cdots \circ s, U) \right] \\
&\geq \mathbb{E}_{s \sim S} \left[\sum_{i=1}^{n/2k} \mathsf{dist}_{\mathsf{H}}(s, U|_i) \right] \\
&= \sum_{i=1}^{n/2k} \mathbb{E}_{s \sim S} \left[\mathsf{dist}_{\mathsf{H}}(s, U|_i) \right] \\
&\geq \frac{n}{2k} \cdot \frac{2kd}{n} = d.
\end{aligned}$$

□

Theorem 3 together with Lemma 6 yield the following corollary.

Corollary 7. *Let n, k, d be such that $k \leq n/2$ and $d \leq c \cdot n$ for some suitable constant $0 < c < 1$. Then there exists an explicit construction of an (n, k, d)-strong rigid set with size $n \cdot \exp(d \cdot k/n)$.*

In fact, one can generalize each of the proofs we gave for Theorem 3 to show that an $\exp(-d \cdot k/n)$-biased set is an (n, k, d)-strong rigid set. Nevertheless, the reduction in Lemma 6 might be of use in the construction of (n, k, d)-strong rigid sets from arbitrary $(n, n/2, d)$-rigid sets.

Acknowledgements

The second author is grateful for his advisor Ran Raz for his continuous support and encouragement, and for helpful discussions regarding this work. He would also like to thank Amir Shpilka for introducing him to the paper [APY09] and Avraham Ben-Aroya and Igor Shinkar for stimulating discussions.

References

[ABN+92] N. Alon, J. Bruck, J. Naor, M. Naor, and R. Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on Information Theory*, 38:509–516, 1992.

[AC88] N. Alon and F.R.K. Chung. Explicit construction of linear sized tolerant networks. *Discrete Mathematics*, 72(1):15–19, 1988.

[AGHP92] N. Alon, O. Goldreich, J. Håstad, and R. Peralta. Simple construction of almost k-wise independent random variables. *Random Structures and Algorithms*, 3(3):289–304, 1992.

[APY09] N. Alon, R. Panigrahy, and S. Yekhanin. Deterministic approximation algorithms for the nearest codeword problem. In *APPROX 09 / RANDOM 09: Proceedings of the 12th International Workshop and 13th International Workshop on Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 339–351, 2009.

[AR94] N. Alon and Y. Roichman. Random cayley graphs and expanders. *Random Structures and Algorithms*, 5(2):271–285, 1994.

[AS10] V. Arvind and S. Srinivasan. The remote point problem, small bias spaces, and expanding generator sets. In *27th STACS*, pages 59–70, 2010.

[BDWY11] B. Barak, Z. Dvir, A. Wigderson, and A. Yehudayoff. Rank bounds for design matrices with applications to combinatorial geometry and locally correctable codes. In *Proceedings of the 43rd annual ACM symposium on Theory of computing*, pages 519–528. ACM, 2011.

[BT09] A. Ben-Aroya and A. Ta-Shma. Constructing small-bias sets from algebraic-geometric codes. In *Proceedings of the 50th annual IEEE symposium on foundations of computer science (FOCS)*, pages 191–197, 2009.

[Dvi10] Z. Dvir. On matrix rigidity and locally self-correctable codes. In *Proceedings of the 25th Annual CCC*, pages 291–298, 2010.

[Fri93] J. Friedman. A note on matrix rigidity. *Combinatorica*, 13(2):235–239, 1993.

[GUV09] V. Guruswami, C. Umans, and S. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *J. ACM*, 56(4):1–34, 2009.

[HLW06] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *Bulleting of the American Mathematical Society*, 43:439–561, 2006.

[KR98] B.S. Kashin and A.A. Razborov. Improved lower bounds on the rigidity of Hadamard matrices. *Mathematical Notes*, 63(4):471–475, 1998.

[Lok95] S. V. Lokam. Spectral methods for matrix rigidity with applications to size-depth tradeoffs and communication complexity. In *36th Annual FOCS*, pages 6–15, 1995.

[Lok09] S. V. Lokam. Complexity lower bounds using linear algebra. *Foundations and Trends in Theoretical Computer Science*, 4(1-2):1–155, 2009.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes, Part II*. North-Holland, 1977.

[NN93] J. Naor and M. Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM J. on Computing*, 22(4):838–856, 1993.

[O'D] R. O'Donnell. Analyis of boolean functions. http://analysisofbooleanfunctions.org/.

[SSS97] M.A. Shokrollahi, D. Spielman, and V. Stemann. A remark on matrix rigidity. *Information Processing Letters*, 64(6):283–285, 1997.

[Val77] L. G. Valiant. Graph-theoretic arguments in low-level complexity. In *Lecture notes in Computer Science*, volume 53, pages 162–176. Springer, 1977.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de