An Additive Combinatorics Approach Relating Rank to Communication Complexity

ELI BEN-SASSON, Technion - Israel Institute of Technology
SHACHAR LOVETT, University of California, San Diego
NOGA RON-ZEWI, Technion - Israel Institute of Technology

Identifying complexity measures that bound the communication complexity of a $\{0,1\}$-valued matrix M is one the most fundamental problems in communication complexity. Mehlhorn and Schmidt [1982] were the first to suggest matrix-rank as one such measure. Among other things, they showed

$$\log \mathrm{rank}_{\mathbb{F}}(M) \leq \mathrm{CC}(M) \leq \mathrm{rank}_{\mathbb{F}_2}(M),$$

where $\mathrm{CC}(M)$ denotes the (deterministic) communication complexity of the function associated with M, and the rank on the left-hand side is over any field $\mathbb{F}$ and on the right-hand side it is over the two-element field $\mathbb{F}_2$. For certain matrices M, communication complexity equals the right-hand side, and this completely settles the question of "communication complexity vs. $\mathbb{F}_2$-rank".

Here we reopen this question by pointing out that, when M has an additional natural combinatorial property—high discrepancy with respect to distributions which are uniform over submatrices—then communication complexity can be sublinear in $\mathbb{F}_2$-rank. Assuming the Polynomial Freiman-Ruzsa (PFR) conjecture in additive combinatorics, we show that

$$\mathrm{CC}(M) \leq O(\mathrm{rank}_{\mathbb{F}_2}(M)/\log \mathrm{rank}_{\mathbb{F}_2}(M))$$

for any matrix M which satisfies this combinatorial property.

We also observe that if M has low rank over the reals, then it has low rank over $\mathbb{F}_2$ and it additionally satisfies this combinatorial property. As a corollary, our results also give the first (conditional) sublinear bound on communication complexity in terms of rank over the reals, a result improved later by Lovett [2014].

Our proof is based on the study of the "approximate duality conjecture" which was suggested by Ben-Sasson and Zewi [2011] and studied there in connection to the PFR conjecture. First, we improve the bounds on approximate duality assuming the PFR conjecture. Then, we use the approximate duality conjecture (with improved bounds) to get our upper bound on the communication complexity of low-rank matrices.

Categories and Subject Descriptors: F.1.2 [**Computation by Abstract Devices**]: Modes of Computation—*Interactive and reactive computation*; F.1.3 [**Computation by Abstract Devices**]: Complexity Measures and Classes—*Relations among complexity measures*

General Terms: Algorithms

Additional Key Words and Phrases: Communication complexity, log-rank conjecture, additive combinatorics, polynomial Freiman-Ruzsa conjecture, approximate duality, low-rank matrices

The research leading to these results received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement numbers 240258 and 257575, by NSF grant DMS-0835373, NSF CAREER award 1350481 and by the Israel Ministry of Science and Technology.

Authors' addresses: E. Ben-Sasson, Department of Computer Science, Technion, Haifa, Israel and Microsoft Research New-England, Cambridge, MA; email: eli@cs.technion.ac.il; S. Lovett, Computer Science and Engineering Department, University of California, San Diego, CA; email: slovett@ucsd.edu; N. Ron-Zewi, Department of Computer Science, Technion, Haifa; email: nogaz@cs.technion.ac.il.

DOI:http://dx.doi.org/10.1145/2629598

ACM Reference Format:
Ben-Sasson, E., Lovett, S., and Ron-Zewi, N. 2014. Additive combinatorics approach relating rank to communication complexity. *J. ACM* 61, 4, Article 22 (July 2014), 18 pages.
DOI:http://dx.doi.org/10.1145/2629598

1. INTRODUCTION

This article revisits the question of the relation between communication complexity and matrix rank over the two-element field $\mathbb{F}_2$, a question that has laid dormant for the past 30 years. It presents a new connection between communication complexity and additive combinatorics, showing that a well-known conjecture from additive combinatorics known as the *Polynomial Freiman-Ruzsa conjecture* (PFR, in short) implies nontrivial upper bounds on the deterministic communication complexity of a $\{0,1\}$-valued matrix M in terms of its rank over $\mathbb{F}_2$ and its discrepancy with respect to distributions that are uniform on submatrices. We view this result as interesting not only because it reopens what in our mind is a fundamental problem, but also because (1) it is the first advance since 1997 on the so-called "log rank conjecture"[1] explained in this article, and (2) it shows a new connection between the two vibrant, yet seemingly unrelated, fields of communication complexity and additive combinatorics.

Our analysis relies on the study of *approximate duality*, a concept closely related to the PFR conjecture, which was introduced in Ben-Sasson and Zewi [2011]. Our main technical contribution improves the bounds on approximate duality, assuming the PFR conjecture, and it does so with simpler a proof than in Ben-Sasson and Zewi [2011]. We view this contribution as being of independent interest because of the growing number of applications of the "approximate duality method" to theoretical computer science. So far, these include the construction of two-source extractors [Ben-Sasson and Zewi 2011], communication complexity (this work), and the subsequent lower bounds for matching vector codes [Bhowmick et al. 2013] (cf. the survey [Lovett 2013]).

1.1. On Communication Complexity and Matrix Rank over $\mathbb{F}_2$

In the two-party communication complexity model two parties — Alice and Bob — wish to compute a function $f : X \times Y \to \{0,1\}$ on inputs $x \in X$ and $y \in Y$ where x is known only to Alice and y is known only to Bob. In order to compute the function f, they must exchange bits of information between each other according to some (deterministic) protocol. The (deterministic) communication complexity of a protocol is the maximum total number of bits sent between the two parties, where the maximum is taken over all pairs of inputs x, y. We henceforth omit the adjective "deterministic" from our discourse because our results deal only with the deterministic model. The communication complexity of the function f, denoted by $\mathrm{CC}(f)$, is the minimum communication complexity of a protocol for f.

For many applications, it is convenient to associate the function $f : X \times Y \to \{0,1\}$ with the matrix $M \in \{0,1\}^{X\times Y}$ whose (x,y) entry equals $f(x,y)$. For a $\{0,1\}$-valued matrix M, let $\mathrm{CC}(M)$ denote the communication complexity of the Boolean function associated with M. For an arbitrary field $\mathbb{F}$, let $\mathrm{rank}_{\mathbb{F}}(M)$ denote the rank of M over $\mathbb{F}$; we shall mostly consider the two-element field $\mathbb{F}_2$ and the field of reals $\mathbb{R}$.

It is well known since the work of Mehlhorn and Schmidt [1982] that

$$\log \mathrm{rank}_{\mathbb{F}}(M) \leq \mathrm{CC}(M) \leq \mathrm{rank}_{\mathbb{F}_2}(M). \tag{1}$$

(Notice the left-hand side is rank over any field $\mathbb{F}$.) Furthermore, for the inner-product function IP given by $\mathrm{IP(x, y)} = \langle \mathrm{x, y} \rangle \pmod 2$, it holds that $\mathrm{CC(IP)} = \mathrm{rank}_{\mathbb{F}_2}(\mathrm{IP})$. So that, in the worst case, the upper bound mentioned previously is tight for $\mathbb{F}_2$-rank, and

[1] Recently, the second author made further progress on this problem [Lovett 2014], cf. Section 1.2.

this completely resolves the question of the worst-case relation between communication complexity and $\mathbb{F}_2$-rank.

The premise of this work is that the previously mentioned result actually leads to an interesting question, to the best of our knowledge addressed here for the first time:

Under what conditions is communication complexity sublinear in $\mathbb{F}_2$-rank?

Our answer to this question is that — assuming the PFR conjecture — one such condition is that M has high discrepancy with respect to distributions which are uniform over submatrices. In technical terms, our main contribution is as follows.

Let M be a $\{0, 1\}$-valued matrix. For a distribution μ over the entries of M, the *discrepancy of M with respect to* μ is defined as

$$\mathrm{disc}_\mu(M) = \max_{M'} \left| \sum_{(x,y)\in M'} (-1)^{M_{x,y}} \mu(x, y) \right|,$$

where M' ranges over all submatrices of M. For a set $\mathcal{D}$ of distributions over the entries of M, we define the *discrepancy of M with respect to* $\mathcal{D}$ as

$$\mathrm{disc}_{\mathcal{D}}(M) = \min_{\mu\in\mathcal{D}} \mathrm{disc}_\mu(M).$$

Our main theorem uses $\mathrm{disc}_{\mathcal{U}}(\mathrm{M})$, where $\mathcal{U}$ denotes the set of uniform distributions over submatrices of M.

THEOREM 1.1 (MAIN). *For every constant $\eta > 0$ there exists a constant $c = c(\eta)$ such that the following holds. Suppose that M is a $\{0, 1\}$-valued matrix of rank at most r over $\mathbb{F}_2$ which satisfies that $\mathrm{disc}_{\mathcal{U}}(\mathrm{M}) \geq 2^{-\mathrm{r}^{1-\eta}}$. Then, assuming the PFR Conjecture* 1.7*,* $\mathrm{CC}(M) \leq c \cdot r/\log r$.

We remark that the IP function mentioned previously does not contradict Theorem 1.1 because it satisfies $\mathrm{disc}_{\mathcal{U}}(\mathrm{IP}) \leq 2^{-\mathrm{rank}_{\mathbb{F}_2}(\mathrm{IP})/2}$ [Babai et al. 1986; Chor and Goldreich 1988].

1.2. On Communication Complexity and Matrix Rank over $\mathbb{R}$

The question of rank vs. communication complexity has received much attention over the field of reals. This is because $\mathrm{rank}_{\mathbb{F}_2}(M) \leq \mathrm{rank}_{\mathbb{R}}(M)$ for a $\{0, 1\}$-valued matrix M, so equation (1) implies that

$$\log \mathrm{rank}_{\mathbb{R}}(M) \leq \mathrm{CC}(M) \leq \mathrm{rank}_{\mathbb{R}}(M) \qquad (2)$$

and it is a fundamental question to find out what is the true worst-case dependency of $\mathrm{CC}(M)$ on the real-rank. The famous log-rank conjecture due to Lovász and Saks [1988] postulates that communication complexity is always closer to the left hand side of (2). (And recall that this is false for $\mathrm{rank}_{\mathbb{F}_2}$.)

Conjecture 1.2 (*Log-Rank*). $\mathrm{CC}(M) = \log^{O(1)} \mathrm{rank}_{\mathbb{R}}(M)$ for every $\{0, 1\}$-valued matrix M.

Lovász and Saks [1988] also point out that Conjecture 1.2 has several other interesting equivalent formulations. One of them, due to Van Nuffelen [1976] and Fajtlowicz [1988], is the following.

Conjecture 1.3. For every graph G, $\chi(\overline{G}) \leq \log^{O(1)} \mathrm{rank}_{\mathbb{R}}(G)$, where $\chi(\overline{G})$ is the chromatic number of the complement of G, and $\mathrm{rank}_{\mathbb{R}}(G)$ is the rank of the adjacency matrix of G over the reals.

Though considerable effort has been made since 1982 in an attempt to narrow the gap between lower and upper bounds in (2), till recently the state of the art was not far from where it was 30 years ago and stood at

$$\mathrm{CC}(M) = \Omega(\log^{\log_3 6} \mathrm{rank}_{\mathbb{R}}(M)) = \Omega(\log^{1.63\cdots} \mathrm{rank}_{\mathbb{R}}(M))$$

for some matrix M, and

$$\mathrm{CC}(M) \le \log(4/3)\mathrm{rank}_{\mathbb{R}}(M) = (0.41\cdots)\mathrm{rank}_{\mathbb{R}}(M) \tag{3}$$

for every matrix M. The first bound is due to Kushilevitz (unpublished, cf. Nisan and Wigderson [1995]) and improves on a previous bound of $\Omega(\log^{\log_2 3} \mathrm{rank}_{\mathbb{R}}(M)) = \Omega(\log^{1.58\cdots} \mathrm{rank}_{\mathbb{R}}(M))$ due to Nisan and Wigderson [1995]. The second bound is due to Kotlov [1997] and improves on the previous best bound of $\mathrm{CC}(M) \le \mathrm{rank}_{\mathbb{R}}(M)/2$ by Kotlov and Lovász [1996].

Our main Theorem 1.1 leads to the first (conditional) sublinear bound on communication complexity in terms of rank.

COROLLARY 1.4. *Assuming the PFR Conjecture* 1.7*, for every* $\{0,1\}$*-valued matrix M,*

$$\mathrm{CC}(M) = O(\mathrm{rank}_{\mathbb{R}}(M)/\log \mathrm{rank}_{\mathbb{R}}(M)).$$

Recently, Lovett [2014] improved considerably on this by proving the following.

THEOREM 1.5 [LOVETT 2014]. *For every* $\{0,1\}$*-valued matrix M,*

$$\mathrm{CC}(M) = O(\sqrt{\mathrm{rank}_{\mathbb{R}}(M)} \log \mathrm{rank}_{\mathbb{R}}(M)).$$

The proof of Corollary 1.4 differs significantly from that of Theorem 1.5; hence, we provide it in Section 3.2. In a nutshell, Corollary 1.4 uses as its starting point the result of Nisan and Wigderson [1995] which shows that low rank over the reals implies that $\mathrm{disc}_{\mathcal{U}}(M) = \min_{\mu\in\mathcal{U}} \mathrm{disc}_{\mu}(M)$ is high, where $\mathcal{U}$ denotes the set of uniform distributions over submatrices of M. Observing that $\mathrm{rank}_{\mathbb{F}_2}(M) \le \mathrm{rank}_{\mathbb{R}}(M)$ for a $\{0,1\}$-valued matrix M, we quickly move to the two-element field and apply Theorem 1.1.

In contrast, Lovett [2014] starts with a much stronger observation due to Linial et al. [2007] and Linial and Shraibman [2009]: that low rank over the reals implies high discrepancy with respect to *any distribution* μ over the entries of M, namely that $\mathrm{disc}(M) := \min_{\mu} \mathrm{disc}_{\mu}(M)$ is high where μ ranges over all distributions over the entries of M. As such, it leads to stronger and unconditional bounds on communication complexity in terms of real rank. We stress however that Theorem 1.5 does not impact our Main Theorem 1.1.

1.3. Additive Combinatorics and the Polynomial Freiman-Ruzsa Conjecture

Additive combinatorics is the area of mathematics which studies the combinatorial estimates associated with the arithmetic operations of addition and subtraction. As such, it deals with a variety of problems that aim to “quantify” the amount of additive structure in subsets of additive groups. One such a problem is that which is addressed by the Polynomial Freiman-Ruzsa conjecture (we shall encounter a different problem in additive combinatorics when we get to “approximate duality” later on).

For $A \subseteq \mathbb{F}_2^n$, let $A + A$ denote the sum-set of A

$$A + A := \{a + a' \mid a, a' \in A\},$$

where addition is over $\mathbb{F}_2$. It is easy to see that $|A + A| = |A|$ if and only if A is an affine subspace of $\mathbb{F}_2^n$. The question addressed by the Freiman-Ruzsa theorem is whether the ratio of $|A + A|$ to $|A|$ also “approximates” the closeness of A to being a subspace, or in other words, whether the fact that $A+A$ is small with respect to the size of A also implies that $\operatorname{span}(A)$ is small with respect to the size of A. The Freiman-Ruzsa theorem [Ruzsa 1999] says that this is indeed the case.

THEOREM 1.6 (FREIMAN-RUZSA THEOREM [RUZSA 1999]). *If $A \subseteq \mathbb{F}_2^n$ has $|A+A| \le K|A|$, then $|\operatorname{span}(A)| \le K^2 2^{K^4}|A|$.*

This theorem was improved in a series of works [Green and Ruzsa 2006; Green and Tao 2009; Sanders 2008], culminating in the recent work [Even-Zohar 2012] which proved an upper bound on the ratio $\frac{|\operatorname{span}(A)|}{|A|}$ of the form $2^{2K}/(2K)$. This bound can be seen to be tight by letting $A = \bigcup_{i=1}^{t}(u_i + V)$, where $u_1, u_2, \ldots, u_t \in \mathbb{F}_2^n$ are linearly independent vectors and $V \subseteq \mathbb{F}_2^n$ is a subspace of dimension d such that $\operatorname{span}(\{u_1, \ldots, u_t\}) \cap V = \{0\}$. Then, in this case, we have $A = t \cdot d$ and $|A+A| \approx \frac{t}{2}|A|$, while $|\operatorname{span}(A)| = 2^t \cdot d = \frac{2^t}{t}|A|$.

This example also shows that the ratio $\frac{|\operatorname{span}(A)|}{|A|}$ must depend exponentially on K. However, it does not rule out the existence of a large subset $A' \subseteq A$ for which the ratio $\frac{|\operatorname{span}(A')|}{|A'|}$ is just polynomial in K, and this is exactly what is suggested by the PFR conjecture.

Conjecture 1.7 (*Polynomial Freiman-Ruzsa* (PFR)). There exists an absolute constant r, such that if $A \subset \mathbb{F}_2^n$ has $|A+A| \le K|A|$, then there exists a subset $A' \subseteq A$ of size at least $K^{-r}|A|$ such that $|\operatorname{span}(A')| \le |A|$.

Note that this conjecture implies that $|\operatorname{span}(A')| \le |A| \le K^r|A'|$. The PFR conjecture has many other interesting equivalent formulations, see the survey of Green [2005] for some of them. It is conjectured to hold for subsets of general groups as well and not only for subsets of the group $\mathbb{F}_2^n$ but we will be interested only in the latter case. Significant progress on this conjecture has been achieved recently by Sanders [2012], using new techniques developed by Croot and Sisask [2010]. Sanders [2012] proved an upper bound on the ratio $\frac{|\operatorname{span}(A')|}{|A'|}$ which is quasi-polynomial in K.

THEOREM 1.8 (QUASI-POLYNOMIAL FREIMAN-RUZSA THEOREM (QFR) [SANDERS 2012]). *Let $A \subset \mathbb{F}_2^n$ be a set such that $|A+A| \le K|A|$. Then, there exists a subset $A' \subseteq A$ of size at least $K^{-O(\log^3 K)}|A|$ such that $|\operatorname{span}(A')| \le |A|$.*

We end this section by mentioning several other recent applications of the PFR conjecture to theoretical computer science. The first application, due to Samorodnitsky [2007], is to the area of low-degree testing, with further results by Lovett [2012] and Green and Tao [2010]. The second application is to the construction of two-source extractors due to Ben-Sasson and Zewi [2011]. The latter paper also introduced the notion of approximate duality which plays a central role in our proof method as well. The PFR conjecture, as well as the approximate duality method, have recently found another application to proving lower bounds on matching vector codes in the subsequent work by Bhowmick et al. [2013]. In the next section, we describe the approximate duality conjecture and our new contributions to its study.

1.4. Approximate Duality

Our main technical contribution (Lemma 1.11) is an improvement of the bounds on approximate duality, assuming the PFR conjecture. The new bound lies at the heart of our proof of Main Theorem 1.1. We believe that Lemma 1.11 and its proof are of independent interest since they improve and simplify the proof of Ben-Sasson and Zewi [2011], and have already found new interesting applications to the study of locally decodable codes [Bhowmick et al. 2013].

For $A, B \subseteq \mathbb{F}_2^n$, we define the *duality measure* of A, B in (4) as an estimate of how "close" this pair is to being dual

$$D(A,B) := \left| \mathbb{E}_{a\in A, b\in B}\left[(-1)^{\langle a,b\rangle_2}\right]\right|, \tag{4}$$

where $\langle a,b\rangle_2$ denotes the binary inner-product of a, b over $\mathbb{F}_2$, defined by $\langle a,b\rangle_2 = \sum_{i=1}^n a_i \cdot b_i$ where all arithmetic operations are in $\mathbb{F}_2$.

It can be verified that, if $D(A,B) = 1$, then A is contained in an affine shift of $B^\perp$ which is the space dual to the linear $\mathbb{F}_2$-span of B. The question is what can be said about the structure of A, B when $D(A,B)$ is sufficiently large, but strictly smaller than 1. The following theorem from Ben-Sasson and Zewi [2011] says that if the duality measure is a constant very close to 1 (though strictly smaller than 1), then there exist relatively large subsets $A' \subseteq A$, $B' \subseteq B$, such that $D(A', B') = 1$.

THEOREM 1.9 (APPROXIMATE DUALITY FOR NEARLY-DUAL SETS, THEOREM 2.10 IN BEN-SASSON AND RON-ZEWI [2012]). *For every $\delta > 0$ there exists a constant $\epsilon > 0$ that depends only on δ, such that if $A, B \subseteq \mathbb{F}_2^n$ satisfy $D(A,B) \geq 1-\epsilon$, then there exist subsets $A' \subseteq A$, $|A'| \geq \frac{1}{4}|A|$ and $B' \subseteq B$, $|B'| \geq 2^{-\delta n}|B|$, such that $D(A', B') = 1$.*

It is conjectured that a similar result holds also when the duality measure is relatively small, and in particular when it tends to zero as n goes to infinity. Furthermore, the following theorem from Ben-Sasson and Zewi [2011], Section 5.5 gives support to this conjecture, by showing that such bounds indeed follow from the PFR conjecture.

THEOREM 1.10 (APPROXIMATE DUALITY ASSUMING PFR, EXPONENTIAL LOSS). *Assuming the PFR Conjecture 1.7, for every pair of constants $\alpha > \delta > 0$ there exists a constant $\zeta > 0$, depending only on α and δ, such that the following holds. If $A, B \subseteq \mathbb{F}_2^n$ satisfy $|A| > 2^{\alpha n}$ and $D(A,B) \geq 2^{-\zeta n}$, then there exist subsets $A' \subseteq A$, $|A'| \geq 2^{-\delta n}|A|$ and $B' \subseteq B$, $|B'| \geq 2^{-\delta n}|B|$ such that $D(A', B') = 1$.*

Our main technical contribution is the following generalization of the previous theorem.

LEMMA 1.11 (MAIN TECHNICAL LEMMA). *Assuming the PFR Conjecture 1.7, there exists a universal integer r such that the following holds. Suppose that $A, B \subseteq \mathbb{F}_2^n$ satisfy $D(A,B) \geq \epsilon$. Then, for every $K \geq 1$ and $t = n/\log K$, there exist subsets A', B' of A, B respectively such that $D(A', B') = 1$, and*

$$|A'| \geq \left(\left(\frac{(\epsilon/2)^{2^t}}{nK}\right)(4n)^{-t}\right)^r |A|, \qquad |B'| \geq \left(\left(\frac{(\epsilon/2)^{2^t}}{nK}\right)2^{-t}\right)^r |B|. \tag{5}$$

The proof of this lemma appears in Section 2. To see that it is indeed a generalization of Theorem 1.10, set $K = 2^{\delta n/(3r)}$, $t = 3r/\delta$, $\zeta = \delta/(3r \cdot 2^t) = \delta/(3r \cdot 2^{3r/\delta})$, $\epsilon = 2^{-\zeta n}$, and note that, in this case, this lemma assures the existence of $|A'| \geq 2^{-\delta n}|A|$, $|B'| \geq 2^{-\delta n}|B|$ such that $D(A', B') = 1$. Note that Lemma 1.11 actually improves on the previous Theorem 1.10 even in this exponential range of parameters in that its parameters do not depend on the size of the set A as was the case in Theorem 1.10.

However, the main significance of Lemma 1.11 is that it allows one to trade off the loss in the sizes of A' and B' with the value of ϵ for a wider range of parameters. More specifically, it allows one to achieve a loss in the sizes of A' and B' which is only subexponential in n by requiring ϵ to be a bit larger.

COROLLARY 1.12 (APPROXIMATE DUALITY ASSUMING PFR, SUBEXPONENTIAL LOSS). *For every constant $\eta > 0$, there exists a constant $c = c(\eta)$ such that the following holds. Suppose that $A, B \subseteq \mathbb{F}_2^n$ satisfy $D(A,B) \geq 2^{-n^{1-\eta}}$. Then assuming the PFR Conjecture* 1.7*, there exist subsets A', B' of A, B respectively such that $D(A', B') = 1$, and $|A'| \geq 2^{-cn/\log n}|A|$, $|B'| \geq 2^{-cn/\log n}|B|$.*

PROOF OF COROLLARY 1.12. Follows from Lemma 1.11 by setting $K = 2^{(2/\eta)n/\log n}$, $t = \frac{\eta \log n}{2}$, $\epsilon = 2^{-n^{1-\eta}}$. □

Note that, in Corollary 1.12, the ratios $|A'|/|A|$, $|B'|/|B|$ are bounded from below by $2^{-cn/\log n}$, whereas, in Theorem 1.10, we only get a smaller bound of the form $2^{-\delta n}$ for some constant $\delta > 0$. However, this improvement comes with a requirement that the duality measure $D(A,B)$ is larger — in this corollary we require that it is at least $2^{-n^{1-\eta}}$ while in Theorem 1.10 we only require it to be at least $2^{-\zeta n} \ll 2^{-n^{1-\eta}}$.

Remark 1.13 ($2^{-O(\sqrt{n})}$ LOSS NECESSARY). Generally speaking, the bound on $\min\left\{\frac{|A'|}{|A|}, \frac{|B'|}{|B|}\right\}$ — which in Corollary 1.12 is $2^{-cn/\log n}$ — cannot be improved beyond $2^{-O(\sqrt{n})}$ even if we assume $D(A,B) > 0.99$. To see this, take $A = B = \binom{n}{c'\sqrt{n}}$ to be the set of all $\{0,1\}$-vectors with exactly $c'\sqrt{n}$ ones, where c' is a sufficiently small positive constant that guarantees $D(A,B) \geq 0.99$. It was shown in Babai et al. [1986] that if $A' \subset A, B' \subset B$ satisfy $D(A', B') = 1$ then $\min\left\{\frac{|A'|}{|A|}, \frac{|B'|}{|B|}\right\}$ is at most $2^{-\Omega(\sqrt{n})}$.

We stress that a benefit of the proof of Lemma 1.11 is that it simplifies the original proof of Theorem 1.10 in Ben-Sasson and Zewi [2011]. Indeed, we believe that the presentation of the proof that appears in this article is clearer and less involved than that in Ben-Sasson and Zewi [2011]. Also, our new proof method allows us to deduce a new equivalence between approximate duality and the PFR Conjecture in the exponential range that was not previously known. We elaborate on this equivalence in Section 4.

1.5. Proof Overview

We briefly sketch the proof of our Main Technical Lemma 1.11. We use the *spectrum* of a set as defined in Tao and Vu [2006, Chap. 4].

Definition 1.14 (SPECTRUM). For a set $B \subseteq \mathbb{F}_2^n$ and $\alpha \in [0,1]$, let the *α-spectrum* of B be the set

$$\mathrm{Spec}_\alpha(B) := \{x \in \mathbb{F}_2^n \mid |\, \mathbb{E}_{b\in B}\left[(-1)^{\langle x,b\rangle_2}\right] | \geq \alpha\}. \tag{6}$$

Notice that $A \subseteq \mathrm{Spec}_\epsilon(B)$ implies $D(A,B) \geq \epsilon$ (cf. (4)). In the other direction, a standard averaging argument (using the fact that $|\ (-1)^{\langle x,b\rangle_2}\ | = 1$ for every $x, b \in \mathbb{F}_2^n$) can be used to deduce that $D(A,B) \geq \epsilon$ implies the existence of $A' \subseteq A$ of relatively large size — $|A'| \geq \frac{\epsilon}{2}|A|$ — such that $A' \subseteq \mathrm{Spec}_{\epsilon/2}(B)$. To prove our lemma we start with $A_1 = A'$ and establish a sequence of sets

$$A_2 \subseteq A_1 + A_1,\ \ A_3 \subseteq A_2 + A_2, \ldots$$

such that $A_i \subseteq \mathrm{Spec}_{\epsilon_i}(B)$ for all i. This holds by construction for A_1 with $\epsilon_1 = \epsilon/2$, and we show that it is maintained throughout the sequence for increasingly smaller values of ϵ_i (we shall use $\epsilon_i = \epsilon_{i-1}^2$).

Each A_i is of size at most 2^n so there must be an index $i \leq n/\log K$ for which $|A_{i+1}| \leq K|A_i|$, let t be the minimal such index. We use the Balog–Szemerédi–Gowers Theorem 2.1 from additive combinatorics to show that our assumption that

$|A_{t+1}| \leq K|A_t|$ implies that a large subset $\tilde{A}_t \subseteq A_t$ satisfies $|\tilde{A}_t + \tilde{A}_t| \leq K'|\tilde{A}_t|$ for some small K' (depending on K, t and ϵ). Applying the PFR conjecture to the set $\tilde{A}_t$, we get that a large subset $A''_t \subseteq \tilde{A}_t \subseteq A_t$ has small span (over $\mathbb{F}_2$).

We now have in hand a set A''_t which is a relatively large fraction of its span and additionally satisfies $D(A''_t, B) \geq \epsilon_t$ because by construction $A''_t \subseteq \mathrm{Spec}_{\epsilon_t}(B)$. We use an approximate duality claim from Ben-Sasson and Zewi [2011] (Lemma 2.2) which applies when one of the sets is a large fraction of its span (in our case the set which is a large fraction of its span is A''_t). This claim says that A''_t and B each contain relatively large subsets A'_t, B'_t satisfying $D(A'_t, B'_t) = 1$. Finally, recalling A'_t is a (carefully chosen) subset of $A_{t-1} + A_{t-1}$, we argue that A_{t-1} contains a relatively large subset A'_{t-1} that is "dual" to a large subset B'_{t-1} of $B'_t \subseteq B$, where by "dual" we mean $D(A'_{t-1}, B'_{t-1}) = 1$ (in other words A'_{t-1} is contained in an affine shift of the space dual to span (B'_{t-1})). We continue in this manner to find pairs of "dual" subsets $A'_i \subseteq A_i, B'_i \subseteq B$ for $i = t-2, t-3, \ldots, 1$ at which point we have found a pair of "dual" subsets of A, B that have relatively large size, thereby completing the proof.

1.6. Discussion and Directions for Future Research

The new connection between additive combinatorics and communication complexity seems to us worthy of further study. In particular, the exciting recent advances in additive combinatorics [Croot and Sisask 2010; Even-Zohar 2012; Sanders 2012] use a rich palette of tools that may yield further insights into problems in communication complexity. We end this section by briefly pointing out a few directions we find interesting.

1.6.1. Improved Unconditional Bounds on Communication Complexity. Given the recent QFR result of Sanders [2012] (Theorem 1.8) which comes very close to proving the PFR conjecture, it is interesting to see if it implies any unconditional improvement on communication complexity of low-rank matrices over $\mathbb{F}_2$ with high discrepancy with respect to uniform distributions over submatrices. Looking at our proof of Lemma 1.11, we apply the PFR conjecture to a subset $\tilde{A}_t$ of A_t which satisfies $|\tilde{A}_t + \tilde{A}_t| \leq K'|\tilde{A}_t|$ for $K' \approx K/\epsilon^{2^t}$. For $\epsilon < \frac{1}{2}$, this gives a nontrivial bound only if $t = O(\log n)$. Since t could be as large as $n/\log K$, we are forced to choose $K = 2^{\Omega(n/\log n)}$ which implies in turn $K' = 2^{\Omega(n/\log n)}$. Thus, Sander's QFR Theorem 1.8 does not yield any nontrivial bounds in our case. However, for the purpose of proving an upper bound of, say, $CC(M) \leq \mathrm{rank}_{\mathbb{F}_2}(M)/4$ in Theorem 1.1, it suffices to improve the loss in the size of A in Theorem 1.8 from $K^{-O(\log^3 K)}$ to $K^{-c\log K}$ for a sufficiently small constant c.

1.6.2. Improved Conditional Bounds. The bounds on approximate duality in Corollary 1.12 can possibly be significantly improved. For all we know, an exponential loss of $2^{-O(\sqrt{n}\log n)}$ obtained by the example shown in Remark 1.13 may be tight even when the duality measure is at least 1/poly(n). This would lead to an improved version of Corollary 1.12 in which the sizes of $|A'|, |B'|$ are a $2^{-O(\sqrt{n}\log n)}$ fraction of $|A|$ and $|B|$, respectively, instead of the $2^{-O(n/\log n)}$ loss we currently have. Such a result would translate directly to an upper bound on communication complexity of the form $\mathrm{CC}(M) \leq O(\sqrt{\mathrm{rank}_{\mathbb{F}_2}(M)}\log(\mathrm{rank}_{\mathbb{F}_2}(M)))$ for a matrix with high discrepancy with respect to uniform distributions on submatrices, matching the result of Lovett [2014] for $\mathbb{R}$-rank, as well as giving a different proof for it.

1.6.3. Does the Log-Rank Conjecture Imply the PFR Conjecture? Alternatively, does it have any other nontrivial consequences in additive combinatorics? We believe the answer to this question is positive and make a step in this direction by showing an equivalence between approximate duality and PFR statements in the exponential range, namely, when the losses in the sizes of sets in both approximate duality and PFR is exponential in n. (See Section 4 for an exact statement and details of the proof.)

1.7. Organization of the Article

The next section contains the proof of the Main Technical Lemma 1.11. Section 3 contains the proofs of Main Theorem 1.1 and Corollary 1.4., assuming Corollary 1.12. In Section 4, we prove a new equivalence between approximate duality and the PFR conjecture in the exponential range.

2. IMPROVED BOUNDS ON APPROXIMATE DUALITY ASSUMING PFR

In this section, we prove our Main Technical Lemma 1.11. We start with some additive combinatorics preliminaries.

2.1. Additive Combinatorics Preliminaries

In what follows, all arithmetic operations are taken over $\mathbb{F}_2$. For the proof of Lemma 1.11 we need two other theorems from additive combinatorics. The first is the well-known Balog–Szemerédi–Gowers Theorem of Balog and Szemerédi [1994] and Gowers [1998].

THEOREM 2.1 (BALOG–SZEMERÉDI–GOWERS). *There exist fixed polynomials $f(x,y)$, $g(x,y)$ such that the following holds for every subset A of an abelian additive group. If A satisfies $\Pr_{a,a'\in A}[a+a'\in S]\geq 1/K$ for $|S|\leq C|A|$, then one can find a subset $A'\subseteq A$ such that $|A'|\geq |A|/f(K,C)$, and $|A'+A'|\leq g(K,C)|A|$.*

The second is a lemma from Ben-Sasson and Zewi [2011] which can be seen as an approximate duality statement which applies when one of the sets has small span.

LEMMA 2.2 (APPROXIMATE-DUALITY FOR SETS WITH SMALL SPAN, LEMMA 5.7 IN BEN-SASSON AND RON-ZEWI [2012]). *If $D(A,B)\geq\epsilon$, then there exist subsets $A'\subseteq A, B'\subseteq B$, $|A'|\geq\frac{\epsilon}{4}|A|$, $|B'|\geq\epsilon^2\frac{|A|}{|\mathrm{span}(A)|}|B|$, such that $D(A',B')=1$. If $A\subseteq\mathrm{Spec}_\epsilon(B)$, then we have $|A'|\geq|A|/2$ and $|B'|\geq\epsilon^2\frac{|A|}{|\mathrm{span}(A)|}|B|$ in this statement.*

Finally, for $S\subset\mathbb{F}_2^n$ and $x\in\mathbb{F}_2^n$, let $\mathrm{rep}_S(x)$ be the number of different representations of x as an element of the form $s+s'$ where $s,s'\in S$. $\mathrm{rep}_S(x)$ can also be written, up to a normalization factor, as $1_S*1_S(x)$ where 1_S is the indicator function of the set S and $*$ denotes convolution.

2.2. The Sequence of Sets

We start by defining the sequence of sets $A_1,A_2,\ldots$ used in our proof. To be able to "pull back" and construct a pair of large sets A'_{i-1},B'_{i-1} from the pair A'_i,B'_i we make sure every element in A_i is the sum of roughly the same number of pairs in $A_{i-1}\times A_{i-1}$.

Let $\epsilon_1:=\epsilon/2$, $A_1:=A\cap\mathrm{Spec}_{\epsilon_1}(B)$. Assuming A_{i-1},ϵ_{i-1} have been defined set $\epsilon_i=\epsilon_{i-1}^2/2$ and let $j_i\in\{0,\ldots,n-1\}$ be an integer index which maximizes the size of

$$\left\{(a,a')\in A_{i-1}^2 \mid a+a'\in\mathrm{Spec}_{\epsilon_i}(B)\text{ and }2^{j_i}\leq\mathrm{rep}_{A_{i-1}}(a+a')\leq 2^{j_i+1}\right\}. \tag{7}$$

and set

$$A_i:=\{a+a'\mid a,a'\in A_{i-1},a+a'\in\mathrm{Spec}_{\epsilon_i}(B)\text{ and }2^{j_i}\leq\mathrm{rep}_{A_{i-1}}(a+a')\leq 2^{j_i+1}\}. \tag{8}$$

CLAIM 2.3. *For $i = 1$, we have $|A_1| \geq (\epsilon/2)|A|$. For $i > 1$, we have*

$$\Pr_{a,a' \in A_{i-1}}[a + a' \in A_i] \geq \epsilon_i/n \tag{9}$$

and additionally

$$|A_i| \geq \frac{\epsilon_i}{2^{j_i+1}n}|A_{i-1}|^2. \tag{10}$$

PROOF. The case of $i = 1$ follows directly from the assumption that $D(A, B) \geq \epsilon$ using a standard averaging argument. For larger i, we argue that

$$\Pr_{a,a' \in A_{i-1}}[a + a' \in \mathrm{Spec}_{\epsilon_i}(B)] \geq \epsilon_i.$$

To see this, use Cauchy-Schwarz to get

$$\begin{aligned}\mathbb{E}_{a,a' \in A_{i-1}}|\mathbb{E}_{b\in B}(-1)^{\langle a+a',b\rangle_2}| &= \mathbb{E}_{b\in B}(\mathbb{E}_{a\in A_{i-1}}[(-1)^{\langle a,b\rangle_2}])^2\\ &\geq (\mathbb{E}_{a\in A_{i-1},b\in B}[(-1)^{\langle a,b\rangle_2}])^2 \geq \epsilon_{i-1}^2\end{aligned}$$

and apply a standard averaging argument to deduce that an ϵ_i-fraction of $(a, a') \in A_{i-1} \times A_{i-1}$ sum to an element of $\mathrm{Spec}_{\epsilon_i}(B)$. Selecting j_i to maximize (7) yields inequality (9). Since every element $x \in A_i$ can be represented as $x = a + a'$ with $a, a' \in A_{i-1}$ in at most 2^{j_i+1} different ways we deduce (10) from (9) and complete the proof. □

2.3. The Inductive Claim

Since each of the sets in the sequence is of size at most 2^n, there must be an index $i \leq n/\log K$ for which

$$|A_{i+1}| \leq K|A_i|. \tag{11}$$

Let t be the minimal such index, $t \leq n/\log K$. We shall prove the following claim by backward induction.

CLAIM 2.4 (INDUCTIVE CLAIM). *For $i = t, t-1, \ldots, 1$, there exist subsets*

$$A'_i \subseteq A_i, \quad B'_i \subseteq B,$$

such that $D(A'_i, B'_i) = 1$ and A'_i, B'_i are not too small:

$$|A'_i| \geq \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)(4n)^{-(t-i)}\left(\prod_{\ell=i}^{t}\epsilon_{\ell+1}\right)|A_i|, \qquad |B'_i| \geq \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)2^{-(t-i)}|B|.$$

We split the proof of the claim into two parts. The base case (Proposition 2.5) is proved using the tools from additive combinatorics listed in the beginning of this section. The inductive step is proved in Proposition 2.6 using a graph construction. Before proving Claim 2.4, we show how it implies Lemma 1.11.

PROOF OF MAIN TECHNICAL LEMMA 1.11. Set $i = 1$ in Claim 2.4. Recall that $\epsilon_{i+1} = \epsilon_i^2/2$ for all i, so

$$\epsilon_{\ell+1} = \epsilon^{2^\ell}/2^{2^\ell - 1} \geq (\epsilon/2)^{2^\ell}.$$

Thus, we have $\epsilon_{t+1} \geq (\epsilon/2)^{2^t}$ and $\prod_{\ell=1}^{t}\epsilon_{\ell+1} \geq (\epsilon/2)^{2^{t+1}}$. This gives the bounds on A', B' stated in (5). □

PROPOSITION 2.5 (BASE CASE OF CLAIM 2.4 ($i = t$)). *There exist subsets $A'_t \subseteq A_t$, $B'_t \subseteq B$ such that $D(A'_t, B'_t) = 1$ and A'_t, B'_t are not too small:*

$$|A'_t| \geq \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)|A_t|, \qquad |B'_t| \geq \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)|B|.$$

PROOF. By assumption $|A_{t+1}| \leq K|A_t|$ and $\Pr_{a,a' \in A_t}[a + a' \in A_{t+1}] \geq \epsilon_{t+1}/n$ by (9). Hence, we can apply the Balog–Szemerédi–Gowers Theorem (Theorem 2.1) to the set A_t to obtain a subset $\tilde{A}_t \subseteq A_t$ such that

$$|\tilde{A}_t| \geq \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)|A_t|,$$

and

$$|\tilde{A}_t + \tilde{A}_t| \leq \mathrm{poly}\left(\frac{nK}{\epsilon_{t+1}}\right)|A_t| = \mathrm{poly}\left(\frac{nK}{\epsilon_{t+1}}\right)|\tilde{A}_t|.$$

Now we can apply the PFR Conjecture 1.7 to the set $\tilde{A}_t$ which gives a subset $A''_t \subseteq \tilde{A}_t$ such that

$$|A''_t| \geq \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)|\tilde{A}_t| = \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)|A_t|,$$

and

$$|\,\mathrm{span}\,(A''_t)\,| \leq |\tilde{A}_t| = \mathrm{poly}\left(\frac{nK}{\epsilon_{t+1}}\right)|A''_t|.$$

Recall that $A''_t \subseteq \mathrm{Spec}_{\epsilon_t}(B)$. Applying Lemma 2.2 to the sets A''_t and B, we conclude that there exist subsets $A'_t \subseteq A''_t$, $B'_t \subseteq B$ such that $D(A'_t, B'_t) = 1$, and which satisfy $|A'_t| \geq \frac{1}{2}|A''_t|$ and

$$|B'_t| \geq \epsilon_t^2 \frac{|A''_t|}{|\,\mathrm{span}\,(A''_t)\,|}|B| = \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)|B|.$$

This completes the proof of the base case. □

PROPOSITION 2.6 (INDUCTIVE STEP OF CLAIM 2.4). *For every $i = t-1, \ldots, 1$, there exist subsets $A'_i \subseteq A_i$, $B'_i \subseteq B$ such that $D(A'_i, B'_i) = 1$ and A'_i, B'_i are not too small:*

$$|A'_i| \geq \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)(4n)^{-(t-i)}\left(\prod_{\ell=i}^{t}\epsilon_{\ell+1}\right)|A_i|, \qquad |B'_i| \geq \mathrm{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)2^{-(t-i)}|B|.$$

PROOF. Suppose that the claim is true for i and argue it holds for index $i-1$. Let $G = (A_{i-1}, E)$ be the graph whose vertices are the elements in A_{i-1}, and (a, a') is an edge if $a + a' \in A'_i$. We bound the number of edges in this graph from below. Recall from (8) that every $a \in A'_i$ (where $A'_i \subseteq A_i$) satisfies $2^{j_i} \leq \mathrm{rep}_{A_{i-1}}(a) \leq 2^{j_i+1}$. Using this we get

$$\begin{aligned}
|E| &\geq 2^{j_i} \cdot |A'_i| && (\mathrm{rep}_{A_{i-1}}(x) \geq 2^{j_i} \text{ for all } x \in A'_i)\\
&\geq 2^{j_i} \cdot \mathrm{poly}\left(\tfrac{\epsilon_{t+1}}{nK}\right)(4n)^{-(t-i)}\left(\textstyle\prod_{\ell=i}^{t}\epsilon_{\ell+1}\right)|A_i| && (\text{induction hypothesis})\\
&\geq 2^{j_i} \cdot \mathrm{poly}\left(\tfrac{\epsilon_{t+1}}{nK}\right)(4n)^{-(t-i)}\left(\textstyle\prod_{\ell=i}^{t}\epsilon_{\ell+1}\right)\tfrac{\epsilon_i}{2^{j_i+1}n}|A_{i-1}|^2 && (\text{by (10)})\\
&= 2 \cdot \mathrm{poly}\left(\tfrac{\epsilon_{t+1}}{nK}\right)(4n)^{-(t-(i-1))}\left(\textstyle\prod_{\ell=i-1}^{t}\epsilon_{\ell+1}\right)|A_{i-1}|^2.
\end{aligned}$$

Let $M := \text{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)(4n)^{-(t-(i-1))}\left(\prod_{\ell=i-1}^{t}\epsilon_{\ell+1}\right)$. Since our graph has at least $2M|A_{i-1}|^2$ edges and $|A_{i-1}|$ vertices, it has a connected component with at least $2M|A_{i-1}|$ vertices and denote by A''_{i-1} the set of vertices in it.

Choose an arbitrary element a in A''_{i-1}. Partition B'_i into two sets $B'_{i,0}$ and $B'_{i,1}$ such that all elements in $B'_{i,0}$ have inner product 0 with a, and all elements in $B'_{i,1}$ have inner product 1 with a. Let B'_{i-1} be the larger of $B'_{i,0}$,$B'_{i,1}$, and note that $|B'_{i-1}| \geq |B'_i|/2$. Recall that our assumption was that $D(A'_i, B'_i) = 1$. Abusing notation, let $\langle A'_i, B'_i\rangle_2$ denote the value of $\langle a', b'\rangle_2$ for some $a' \in A'_i, b' \in B'_i$ (the choice of a', b' does not matter because $D(A'_i, B'_i) = 1$). Next we consider two cases — the case where $\langle A'_i, B'_i\rangle_2 = 0$, and the case where $\langle A'_i, B'_i\rangle_2 = 1$.

In the first case, we have that for every $a, a' \in A''_{i-1}$ which are neighbors in the graph, $a + a' \in A'_i$, and therefore $\langle a + a', b\rangle_2 = 0$ for every $b \in B'_{i-1}$. This implies in turn that $\langle a, b\rangle_2 = \langle a', b\rangle_2$ for all elements $a, a' \in A''_{i-1}$ which are neighbors in the graph, $b \in B'_{i-1}$. Since A''_{i-1} induces a connected component, and due to our choice of B'_{i-1}, this implies that $D(A''_{i-1}, B'_{i-1}) = 1$ so we set $A'_{i-1} = A''_{i-1}$.

In the second case, we have that $\langle a + a', b\rangle_2 = 1$ for every $a, a' \in A''_{i-1}$ which are neighbors in the graph, $b \in B'_{i-1}$. In particular, this implies that $\langle a, b\rangle_2 = \langle a', b\rangle_2 + 1$ for every elements $a, a' \in A''_{i-1}$ which are neighbors in the graph, $b \in B'_{i-1}$. This means that A''_{i-1} can be partitioned into two sets $A'_{i-1,0}$,$A'_{i-1,1}$, where the first one contains all elements in A''_{i-1} that have inner product 0 with all elements in B'_{i-1}, while the second set contains all elements in A'_{i-1} that have inner product 1 with all elements in B'_{i-1}. We set A'_{i-1} to be the larger of these two sets and get $D(A'_{i-1}, B'_{i-1}) = 1$ and $|A'_{i-1}| \geq M|A_{i-1}|$.

Concluding, in both cases we obtained subsets A'_{i-1}, B'_{i-1} of A_{i-1}, B, respectively, such that $D(A'_{i-1}, B'_{i-1}) = 1$ and A'_{i-1}, B'_{i-1} are not too small:

$$|A'_{i-1}| \geq \text{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)(4n)^{-(t-(i-1))}\left(\prod_{\ell=i-1}^{t}\epsilon_{\ell+1}\right)|A_{i-1}|,$$

and

$$|B'_{i-1}| \geq \frac{1}{2}|B'_i| \geq \frac{1}{2}\text{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)2^{-(t-i)}|B| = \text{poly}\left(\frac{\epsilon_{t+1}}{nK}\right)2^{-(t-(i-1))}|B|.$$

This concludes the proof of the inductive claim. □

3. FROM APPROXIMATE DUALITY TO COMMUNICATION COMPLEXITY UPPER BOUNDS

3.1. Proof of Theorem 1.1

In this section, we prove our Main Theorem 1.1, based on Corollary 1.12. The proof of Theorem 1.1 follows the high-level approach of Nisan and Wigderson [1995]. They showed that in order to prove the log-rank conjecture (Conjecture 1.2) it suffices to show that every $\{0, 1\}$-valued matrix of low rank over the reals has a large monochromatic submatrix (we say that a matrix is monochromatic if it is either the all-zeros or the all-ones matrix).

We therefore start with the following lemma which says that assuming the PFR conjecture, every $\{0, 1\}$-valued matrix M of low rank over $\mathbb{F}_2$ and of high $\text{disc}_{U_M}(M)$ has a large monochromatic submatrix, where U_M denotes the uniform distribution over the entries of M.

LEMMA 3.1. *For every constant $\eta > 0$, there exists a constant $c = c(\eta)$ such that the following holds. Let M be a $\{0, 1\}$-valued matrix with no identical rows or columns and of rank at most r over $\mathbb{F}_2$ which satisfies that $\mathrm{disc}_{U_M}(M) \geq 2^{-r^{1-\eta}}$. Then assuming the PFR Conjecture (Conjecture 1.7), there exists a monochromatic submatrix M' of M of size at least $2^{-cr/\log r}|M|$.*

PROOF. Denote the number of rows and columns of M by k, ℓ, respectively. It is well-known that the rank of M over a field $\mathbb{F}$ equals r if and only if M can be written as the sum of r rank one matrices over the field $\mathbb{F}$. Since $\mathrm{rank}_{\mathbb{F}_2}(M) \leq r$ this implies in turn that there exist subsets $A, B \subseteq \mathbb{F}_2^r$, $A = \{a_1, a_2, \ldots, a_k\}$, $B = \{b_1, b_2, \ldots, b_\ell\}$ such that $M_{i,j} = \langle a_i, b_j \rangle_2$ for all $1 \leq i \leq k, 1 \leq j \leq \ell$. Since M has no identical rows or columns we know that $|A| = k$, $|B| = \ell$.

The assumption that $\mathrm{disc}_{U_M}(M) \geq 2^{-r^{1-\eta}}$ implies that there exists a submatrix $\tilde{M}$ of M such that

$$\frac{|\tilde{M}|}{|M|} \cdot \left| \mathbb{E}_{(x,y)\in\tilde{M}} (-1)^{M_{x,y}} \right| = \left| \sum_{(x,y)\in\tilde{M}} (-1)^{M_{x,y}} \cdot \frac{1}{|M|} \right| \geq 2^{-r^{1-\eta}}.$$

In particular, we have that both $|\tilde{M}|/|M| \geq 2^{-r^{1-\eta}}$ and $\left| \mathbb{E}_{(x,y)\in\tilde{M}} (-1)^{M_{x,y}} \right| \geq 2^{-r^{1-\eta}}$. Let $\tilde{A}, \tilde{B}$ be the subsets of A, B, respectively, which correspond to the sets of rows and columns of $\tilde{M}$, respectively. The main observation is that

$$D(\tilde{A}, \tilde{B}) = \left| \mathbb{E}_{(x,y)\in\tilde{M}} (-1)^{M_{x,y}} \right| \geq 2^{-r^{1-\eta}}.$$

Corollary 1.12 then implies the existence of subsets $A' \subseteq \tilde{A}$, $B' \subseteq \tilde{B}$, $|A'| \geq 2^{-cr/\log r}|\tilde{A}|$, $|B'| \geq 2^{-cr/\log r}|\tilde{B}|$ such that $D(A', B') = 1$. Let M' be the submatrix of M whose rows and columns correspond to the indices in A' and B', respectively. The fact that $D(A', B') = 1$ implies that $M_{i,j} = \langle a_i, b_j \rangle_2 \equiv \text{const}$ for all $a_i \in A'$, $b_j \in B'$. So M' is a monochromatic submatrix of M which satisfies

$$|M'| = |A'||B'| \geq 2^{-2cr/\log r}|\tilde{A}||\tilde{B}| \geq 2^{-2cr/\log r} \cdot 2^{-r^{1-\eta}} \cdot |A||B| \geq 2^{-3cr/\log r}|M|. \qquad \square$$

We proceed to the proof of Theorem 1.1. The proof is similar to that of Nisan and Wigderson [1995], with the difference being that they analyzed the case in which M has a monochromatic submatrix of density $2^{-\log^{O(1)}(\mathrm{rank}_{\mathbb{R}}(M))}$ inside M, while we analyze the case in which the density is $2^{-O(\mathrm{rank}_{\mathbb{F}_2}(M)/\log(\mathrm{rank}_{\mathbb{F}_2}(M)))}$.

PROOF OF THEOREM 1.1. We shall show a deterministic protocol with $2^{O(r/\log r)}$ leaves. This will suffice since it is well-known that a protocol with t leaves has communication complexity at most $O(\log t)$ (cf. Kushilevitz and Nisan [1997, Chapter 2, Lemma 2.8]). We may assume, without loss of generality that M has no repeated rows or columns; otherwise, we can eliminate the repeated row or column and the protocol we construct for the "compressed" matrix (with no repeated rows/columns) will also be a protocol for M.

Now we describe the protocol. Let Q be the largest monochromatic submatrix of M. Then Q induces a natural partition of M into four submatrices Q, R, S, T with R sharing the rows of Q and S sharing the columns of Q:

$$M = \begin{pmatrix} Q & R \\ S & T \end{pmatrix}.$$

Let U_1 be a subset of the rows of $(Q|R)$ whose restriction to the columns of R span the rows of R over $\mathbb{F}_2$. Similarly, let U_2 be a subset of the rows of $(S|T)$ whose restriction to the columns of S span the rows of S over $\mathbb{F}_2$. Note that if Q is the all zeros matrix then the rows of U_1 are independent of the rows of U_2. Otherwise, if Q is the all ones matrix, then the rows of U_1 are independent of all the rows of U_2 except possibly for the vector in U_2 whose restriction to the columns of S is the all ones vector (if such vector exists). Thus, since Q is monochromatic, we have that $\operatorname{rank}_{\mathbb{F}_2}(R) + \operatorname{rank}_{\mathbb{F}_2}(S) = |U_1| + |U_2| \leq \operatorname{rank}_{\mathbb{F}_2}(M) + 1$.

If $\operatorname{rank}_{\mathbb{F}_2}(R) \leq \operatorname{rank}_{\mathbb{F}_2}(S)$, then the row player sends a bit saying if his input belongs to the rows of Q or not. The players continue recursively with a protocol for the submatrix $(Q|R)$ or the submatrix $(S|T)$ according to the bit sent. If $\operatorname{rank}_{\mathbb{F}_2}(R) \geq \operatorname{rank}_{\mathbb{F}_2}(S)$, the roles of the row and column players are switched.

Suppose, without loss of generality, that $\operatorname{rank}_{\mathbb{F}_2}(R) \leq \operatorname{rank}_{\mathbb{F}_2}(S)$ and let c' be the constant guaranteed by Lemma 3.1 for the constant $\eta/2$. Then, after sending one bit, we continue with either the matrix $(Q|R)$ which is of rank at most $r/2$ over $\mathbb{F}_2$ or with the matrix $(S|T)$ which - since $\operatorname{disc}_{U_M}(M) \geq 2^{-r^{1-\eta/2}}$ and thanks to Lemma 3.1 — is of size at most $\left(1 - 2^{-c' \cdot r/\log r}\right)|M|$.

Let $L(m, r, \gamma)$ denote the number of leaves in the protocol starting with a matrix of size at most m, rank at most r over $\mathbb{F}_2$ and $\operatorname{disc}_{\mathcal{U}} \geq \gamma$. Then, we get the following recurrence relation:

$$L(m, r, \gamma) \leq \begin{cases} L(m, r/2, \gamma) + L(m(1 - \delta(r)), r, \gamma), & \gamma \geq 2^{-r^{1-\eta/2}} \\ 2^r & \\ 1, & m = 1, \end{cases}$$

where $\delta(r) = 2^{-c'r/\log r}$.

Applying the recurrence iteratively $\log m \cdot \delta^{-1}(r)$ times to the rightmost summand in the top case, we get

$$L(m, r, \gamma) \leq \log m \cdot \delta^{-1}(r) \cdot L(m, r/2, \gamma) + L(1, r, \gamma),$$

assuming that $\gamma \geq 2^{-r^{1-\eta/2}}$.

Using the fact that $L(1, r, \gamma) = 1$ and $m \leq 2^{2r}$ (since we may assume there are no identical rows or columns in the matrix M), we thus have

$$L(m, r, \gamma) \leq 2r \cdot \delta^{-1}(r) \cdot L(m, r/2, \gamma) + 1 \leq 4r \cdot \delta^{-1}(r) \cdot L(m, r/2, \gamma),$$

assuming that $\gamma \geq 2^{-r^{1-\eta/2}}$.

Applying this recursion iteratively $\log \log r$ times and noting that in our case

$$\gamma \geq 2^{-r^{1-\eta}} \geq 2^{-(r')^{1-\eta/2}}$$

for every $r' \geq r/\log r$ gives

$$L(m,r,\gamma) \leq \left[\prod_{i=0}^{\log\log r-1} 4\cdot(r/2^i)\cdot\delta^{-1}(r/2^i)\right]L(m,r/\log r,\gamma)$$
$$\leq (4r)^{\log\log r}\left[\prod_{i=0}^{\log r\log r-1}\delta^{-1}(r/2^i)\right]\cdot 2^{r/\log r}.$$

This implies in turn that the number of leaves in the protocol is at most

$$O(r/\log r) + \sum_{i=0}^{\log\log r-1}\log\delta^{-1}(r/2^i).$$

Plugging $\delta(r) = 2^{-c'r/\log r}$ in this equation, we get that the number of leaves is at most

$$O(r/\log r)+c'\sum_{i=0}^{\log\log r-1}\frac{r}{2^i\cdot\log(r/2^i)} \leq O(r/\log r)+\frac{c'}{\log(r/\log r)}\sum_{i=0}^{\log\log r-1}\frac{r}{2^i} = O(r/\log r),$$

which concludes the proof of the theorem. □

3.2. Proof of Corollary 1.4

Corollary 1.4 is a simple consequence of Theorem 1.1 and the following theorem from Nisan and Wigderson [1995], which says that every $\{0,1\}$-valued matrix M of low rank over the reals has high discrepancy with respect to uniform distributions over submatrices.

THEOREM 3.2 (THEOREM 3 IN NISAN AND WIGDERSON [1995]). *For every* $\{0,1\}$*-valued matrix* M*,*

$$\mathrm{disc}_{\mathcal{U}}(M) = \Omega(\mathrm{rank}_{\mathbb{R}}(M)^{-3/2}).$$

PROOF OF COROLLARY 1.4. Let $r := \mathrm{rank}_{\mathbb{R}}(M)$. Our first observation is that $\mathrm{rank}_{\mathbb{F}_2}(M) \leq \mathrm{rank}_{\mathbb{R}}(M)$ for every $\{0,1\}$-valued matrix M and therefore we also have that $\mathrm{rank}_{\mathbb{F}_2}(M) \leq r$. Furthermore, Theorem 3.2 implies that $\mathrm{disc}_{\mathcal{U}}(M) \geq \Omega(r^{-3/2}) \gg 2^{-r^{1-\eta}}$ for every constant $\eta > 0$. Hence, Theorem 1.1 applies and we have that $\mathrm{CC}(M) = O(r/\log r)$ assuming the PFR conjecture. □

4. EQUIVALENCE BETWEEN APPROXIMATE DUALITY AND THE PFR CONJECTURE IN THE EXPONENTIAL RANGE

In this section, we show a new equivalence between approximate duality and PFR statements in the exponential range which follows from our main technical Lemma 1.11. Before we elaborate on this, we discuss the previously known relations between approximate duality and the PFR conjecture. Recall first that Theorem 1.10 (which was proven in Ben-Sasson and Zewi [2011]) shows that the following version of approximate duality is implied by the PFR conjecture.

Conjecture 4.1 (*Approximate Duality Conjecture, Exponential Loss*). For every pair of constants $\alpha > \delta > 0$, there exists a constant $\zeta > 0$, depending only on α and δ, such that the following holds. If $A, B \subseteq \mathbb{F}_2^n$ satisfy $|A| > 2^{\alpha n}$ and $D(A,B) \geq 2^{-\zeta n}$, then there exist subsets $A' \subseteq A$, $|A'| \geq 2^{-\delta n}|A|$ and $B' \subseteq B$, $|B'| \geq 2^{-\delta n}|B|$ such that $D(A',B') = 1$.

As to the converse direction, it was shown in Ben-Sasson and Zewi [2011] that this conjecture implies the following weakening of the PFR conjecture.

THEOREM 4.2 (SECTION 5.4 IN BEN-SASSON AND RON-ZEWI [2012]). *Assuming Conjecture* 4.1*, for every constant $\delta > 0$, there exists an integer r which depends only on δ, such that if $A \subset \mathbb{F}_2^n$ has $|A+A| \leq K|A|$, then there exists a subset A' of A of size at least $2^{-\delta n}K^{-r}|A|$ such that* $|\operatorname{span}(A')| \leq K|A|$.

Note that the conclusion in this theorem differs from the standard PFR conjecture in that the loss in the size of A is multiplied by an exponential factor (however, this exponential factor can be made arbitrarily small at the cost of enlarging r). An interesting problem raised by the work of Ben-Sasson and Zewi [2011] was whether one could find an approximate duality type conjecture which is equivalent to some PFR type conjecture. In what follows, we give an example of a pair of such conjectures.

The approximate duality type conjecture that we shall work with is similar to Conjecture 4.1 and the only difference is that the parameters in this conjecture do not depend on the sizes of A and B. Given our main technical Lemma 1.11, this seems like a reasonable conjecture.

Conjecture 4.3. For every constant $\delta > 0$, there exists a constant $\zeta > 0$, depending only on δ, such that the following holds. If $A, B \subseteq \mathbb{F}_2^n$ satisfy $D(A,B) \geq 2^{-\zeta n}$, then there exist subsets $A' \subseteq A$, $|A'| \geq 2^{-\delta n}|A|$ and $B' \subseteq B$, $|B'| \geq 2^{-\delta n}|B|$ such that $D(A', B') = 1$.

We show that this conjecture is equivalent to the following weakening of the PFR conjecture.

Conjecture 4.4 (*PFR Conjecture, Exponential Range*). For every constant δ', there exists a constant ζ', depending only on δ', such that, if $A \subseteq \mathbb{F}_2^n$ has $|A+A| \leq 2^{\zeta' n}|A|$, then there exists a subset $A' \subseteq A$ of size at least $2^{-\delta' n}|A|$ such that $|\operatorname{span}(A')| \leq |A|$.

Note that the PFR Conjecture 1.7 implies this conjecture with $\zeta' = \delta'/r$ for some universal integer r. This conjecture is weaker than the PFR conjecture since we allow ζ' to be an arbitrary function of δ'. Our main result in this section is that Conjectures 4.3 and 4.4 are equivalent.

THEOREM 4.5. *Conjecture* 4.3 *is equivalent to Conjecture* 4.4*.*

The fact that Conjecture 4.4 implies Conjecture 4.3 follows from our proof of the main technical Lemma 1.11. We have already noted in Section 1.4 that Lemma 1.11 implies that Conjecture 4.3 holds assuming the PFR conjecture (by setting $K = 2^{\delta n/(3r)}$, $t = 3r/\delta$, $\zeta = \delta/(3r \cdot 2^t) = \delta/(3r \cdot 2^{3r/\delta})$, $\epsilon = 2^{-\zeta n}$ in Lemma 1.11). Inspecting the proof of Lemma 1.11, it turns out that plugging the weaker Conjecture 4.4 instead of the PFR conjecture in the proof of Lemma 1.11 suffices for obtaining Conjecture 4.3.

In the remainder of the section, we show that Conjecture 4.3 implies Conjecture 4.4. For the proof of this implication, we follow the approach of Ben-Sasson and Zewi [2011]. In particular, we use the following lemma from Tao and Vu [2006] (appearing there as Lemma 4.38) which shows that a set having a small sumset must have large spectrum.

LEMMA 4.6 (SMALL SUMSET FORCES LARGE SPECTRUM). *Let A be a subset of a finite Abelian group Z, and let $0 < \epsilon \leq 1$. Then, we have the following lower bound on the sumset:*

$$|A - A| \geq \frac{|A||Z|}{|A||\operatorname{Spec}_\epsilon(A)| + |Z|\epsilon^2}$$

Note that in $\mathbb{F}_2^n$ we have that $A - A = A + A$.

Proof of (Conjecture 4.3 ⇒ Conjecture 4.4). The idea of the proof is as follows. Suppose that A has a small sumset. Then, Lemma 4.6 implies that A has large spectrum, denote the spectrum set by B. Assuming Conjecture 4.3, we have that A and B contain large subsets A', B' respectively which lie in affine shifts of dual subspaces. But this implies in turn that $\dim(A') \leq n - \dim(B')$, that is, A' has a small span, and setting the parameters correctly we arrive at the desired result. Details follow.

Let ζ be the constant guaranteed by Conjecture 4.3 for the constant $\delta = \delta'/3$. Also, let $\zeta' = \min\{\delta'/6, \zeta\}$, and suppose that $|A + A| \leq 2^{\zeta' n}|A|$. In Lemma 4.6, set $\epsilon = 2^{-\zeta n}$. Then, from the lemma and the assumption that $|A + A| \leq 2^{\zeta' n}|A|$, we have

$$2^{\zeta' n}|A| \geq |A - A| \geq \frac{|A|2^n}{|A||\mathrm{Spec}_\epsilon(A)| + 2^n \epsilon^2}.$$

Rearranging, we obtain

$$|\mathrm{Spec}_\epsilon(A)| \geq \frac{2^n(1 - 2^{\zeta' n}\epsilon^2)}{2^{\zeta' n}|A|} \geq \frac{2^n(1 - 2^{-\zeta' n})}{2^{\zeta' n}|A|} \geq \frac{2^n}{2^{2\zeta' n}|A|},$$

where the second inequality is due to our choice of $\epsilon = 2^{-\zeta n} \leq 2^{-\zeta' n}$.

Conjecture 4.3 then implies (noting that $\epsilon = 2^{-\zeta n}$) the existence of subsets $A' \subseteq A$, $B' \subseteq \mathrm{Spec}_\epsilon(A)$ which lie in affine shifts of dual spaces such that $|A'| \geq 2^{-(\delta'/3)n}|A|$, $|B'| \geq 2^{-(\delta'/3)n}|\mathrm{Spec}_\epsilon(A)|$.

But this implies in turn that $\dim(A') + \dim(B') \leq n$, and consequently

$$|\mathrm{span}\left(A'\right)| \leq \frac{2^n}{|B'|} \leq \frac{2^{(\delta'/3)n} \cdot 2^n}{|\mathrm{Spec}_\epsilon(A)|} \leq 2^{(\delta'/3)n} 2^{2\zeta' n}|A| \leq 2^{2\delta' n/3}|A|,$$

where the last inequality is due to our choice of $\zeta' \leq \delta'/6$.

Concluding, we have that $|\mathrm{span}\left(A'\right)| \leq 2^{2\delta' n/3}|A|$ where A' is a subset of A of size at least $2^{-(\delta'/3)n}|A|$. Write $\mathrm{span}\left(A'\right)$ as a direct sum of subspaces L_1 and L_2, where L_2 is a subspace of size $2^{2\delta' n/3}$, and L_1 is a subspace of size at most $|A|$ which maximizes the size of $A'' = A' \cap L_1$. We have that A'' is a subset of A of size at least $2^{-\delta' n}|A|$ such that $|\mathrm{span}\left(A''\right)| \leq |L_1| \leq |A|$ which concludes the proof that Conjecture 4.3 ⇒ Conjecture 4.4. □

ACKNOWLEDGMENTS

We thank Nati Linial and Eyal Kushilevitz for drawing our attention, independently, to the similarities between the notions of discrepancy and approximate duality, which led us to consider the question addressed in this paper.

REFERENCES

László Babai, Peter Frankl, and Janos Simon. 1986. Complexity classes in communication complexity theory (preliminary version). In *Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 337–347.

Antal Balog and Endre Szemerédi. 1994. A statistical theorem of set addition. *Combinatorica 14*, 3, 263–268.

Eli Ben-Sasson and Noga Ron-Zewi. 2012. From affine to two-source extractors via approximate duality. In *Electronic Colloquium on Computational Complexity (ECCC)*. http://eccc.hpi-web.de/report/2010/144/ (Revision 1 (2012)).

Eli Ben-Sasson and Noga Zewi. 2011. From affine to two-source extractors via approximate duality. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC)*. ACM, 177–186.

Abhishek Bhowmick, Zeev Dvir, and Shachar Lovett. 2013. Lower bounds on vector matching codes. In *Proceedings of the 47rd ACM Symposium on Theory of Computing (STOC)*. ACM, 823–832.

Benny Chor and Oded Goldreich. 1988. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM J. Comput. 17*, 2, 230–261.

Ernie Croot and Olof Sisask. 2010. A probabilistic technique for finding almost-periods of convolutions. *Geomet. Funct. Anal. 20*, 6, 1367–1396.

Chaim Even-Zohar. 2012. On sums of generating sets in $(z_2)^n$. *Combinat. Probab. Comput. 21*, 6, 916–941.

Siemion Fajtlowicz. 1988. On conjectures of graffiti. *Disc. Math. 72*, 1–3, 113–118. DOI:http://dx.doi.org/10.1016/0012-365X(88)90199-9.

William Timothy Gowers. 1998. A new proof of Szemerèdi's theorem for arithmetic progressions of length four. *Geomet. Funct. Anal. 8*, 3, 529–551.

Ben Green. 2005. Finite field models in additive combinatorics. In *London Mathematical Society Lecture Note Series*, Vol. 324. Cambridge University Press.

Ben Green and Imre Z. Ruzsa. 2006. Sets with small sumset and rectification. *Bull. Lond. Math. Soc. 1*, 38, 43–52.

Ben Green and Terence Tao. 2009. Freiman's theorem in finite fields via extremal set theory. *Combinat. Probab. Comput. 18*, 3, 335–355. DOI:http://dx.doi.org/10.1017/S0963548309009821.

Ben Green and Terence Tao. 2010. An equivalence between inverse sumset theorems and inverse conjectures for the U^3 norm. *Math. Proc. Cambridge Philos. Soc. 149*, 1, 1–19.

Andrew Kotlov. 1997. Rank and chromatic number of a graph. *J. Graph Theory 26*, 1, 1–8.

Andrew Kotlov and László Lovász. 1996. The rank and size of graphs. *J. Graph Theory 23*, 2, 185–189.

Eyal Kushilevitz and Noam Nisan. 1997. *Communication Complexity*. Cambridge University Press, New York.

Nati Linial, Shahar Mendelson, Gideon Schechtman, and Adi Shraibman. 2007. Complexity measures of sign matrices. *Combinatorica 27*, 4, 439–463.

Nathan Linial and Adi Shraibman. 2009. Learning complexity vs communication complexity. *Combinat. Probab. Comput. 18*, 1–2, 227–245.

László Lovász and Michael E. Saks. 1988. Lattices, Möbius functions and communication complexity. In *Proceedings of the 29th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 81–90.

Shachar Lovett. 2012. Equivalence of polynomial conjectures in additive combinatorics. *Combinatorica 32*, 5, 607–618.

Shachar Lovett. 2013. Additive combinatorics and its applications in theoretical computer science. http://cseweb.ucsd.edu/~slovett/files/addcomb-survey.pdf.

Shachar Lovett. 2014. Communication is bounded by root of rank. In *Proceedings of the 46th ACM Symposium on Theory of Computing (STOC'14)*.

Kurt Mehlhorn and Erik M. Schmidt. 1982. Las Vegas is better than determinism in VLSI and distributed computing (Extended Abstract). In *Proceedings of the 14th Annual ACM Symposium on Theory of Computing (STOC)*. ACM Press, 330–337. DOI:http://dx.doi.org/10.1145/800070.802208.

Noam Nisan and Avi Wigderson. 1995. On rank vs. communication complexity. *Combinatorica 15*, 4, 557–565.

Imre Z. Ruzsa. 1999. An analog of Freiman's theorem in groups. *Astèrique* 258, 323–326.

Alex Samorodnitsky. 2007. Low-degree tests at large distances. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC)*. ACM, 506–515. DOI:http://doi.acm.org/10.1145/1250790.1250864.

Tom Sanders. 2008. A note on Freiman's theorem in vector spaces. *Combinat. Probab. Comput. 17*, 2, 297–305. DOI:http://dx.doi.org/10.1017/S0963548307008644.

Tom Sanders. 2012. On the Bogolyubov-Ruzsa Lemma. *Anal. PDE 5*, 3, 627–655. DOI:http://arxiv.org/abs/1011.0107.

Terence Tao and Van Vu. 2006. *Additive Combinatorics*. Cambridge University Press, Cambridge.

C. Van Nuffelen. 1976. A bound for the chromatic number of a graph. *Amer. Math. Monthly 83*, 265–266.

Received November 2012; revised June 2013 and April 2014; accepted April 2014