Extracting Mergers and Projections of Partitions

Swastik Kopparty
Department of Computer Science and Department of Mathematics, University of Toronto, Canada

Vishvajeet N
School of Informatics, University of Edinburgh,UK

Abstract

We study the problem of extracting randomness from somewhere-random sources, and related combinatorial phenomena: partition analogues of Shearer's lemma on projections.

A somewhere-random source is a tuple $(X_1, \ldots, X_t)$ of (possibly correlated) $\{0,1\}^n$-valued random variables X_i where for some unknown $i \in [t]$, X_i is guaranteed to be uniformly distributed. An *extracting merger* is a seeded device that takes a somewhere-random source as input and outputs nearly uniform random bits. We study the seed-length needed for extracting mergers with constant t and constant error.

Since a somewhere-random source has min-entropy at least n, a standard extractor can also serve as an extracting merger. Our goal is to understand whether the further structure of being somewhere-random rather than just having high entropy enables smaller seed-length, and towards this we show:

- Just like in the case of standard extractors, seedless extracting mergers with even just one output bit do not exist.
- Unlike the case of standard extractors, it *is* possible to have extracting mergers that output a constant number of bits using only constant seed. Furthermore, a random choice of merger does not work for this purpose!
- Nevertheless, just like in the case of standard extractors, an extracting merger which gets most of the entropy out (namely, having $\Omega(n)$ output bits) must have $\Omega(\log n)$ seed. This is the main technical result of our work, and is proved by a second-moment strengthening of the graph-theoretic approach of Radhakrishnan and Ta-Shma to extractors.

All this is in contrast to the status for condensing mergers (where the output is only required to have high min-entropy), whose seed-length/output-length tradeoffs can all be fully explained by using standard condensers.

Inspired by such considerations, we also formulate a new and basic class of problems in combinatorics: partition analogues of Shearer's lemma. We show basic results in this direction; in particular, we prove that in any partition of the 3-dimensional cube $[0,1]^3$ into two parts, one of the parts has an axis parallel 2-dimensional projection of area at least $3/4$.

2012 ACM Subject Classification Theory of computation → Expander graphs and randomness extractors; Mathematics of computing → Combinatorics; Theory of computation → Complexity theory and logic; Mathematics of computing → Discrete mathematics

Keywords and phrases randomness extractors, randomness mergers, extracting mergers, partitions, projections of partitions, covers, projections of covers

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2023.52

Category RANDOM

Related Version *Full Version*: https://arxiv.org/abs/2306.16915 [13]

Funding *Swastik Kopparty*: Research supported by an NSERC Discovery Grant.
Vishvajeet N: Research supported by the ERC (grant agreement No. 947778).

1 Introduction

We study the problem of extracting randomness from somewhere-random sources, and related combinatorial phenomena: partition analogues of Shearer's lemma on projections. For the (completely self-contained) combinatorics, see Section 1.2, Section 6 and Section 7.

A t-part somewhere-random source is a tuple $(X_1, \ldots, X_t)$ of (possibly correlated) $\{0,1\}^n$-valued random variables X_i, where some unknown X_i is guaranteed to be uniformly distributed. We will take t to be constant and n growing throughout this paper. A *merger* is a seeded device that takes a somewhere-random source and purifies its randomness. Mergers have been extensively studied in the theory of extractors, and have played an important role in their development. In fact, there were at least 3 distinct points in the history of extractors [19, 15, 7] when the best known explicit extractor constructions were based on new advances in explicit merger constructions.

An important observation is that t-part somewhere-random sources are special cases of sources with (min) entropy rate $1/t$. Thus any randomness purifying device (such as an extractor, condenser or disperser) that can give guarantees when fed a source with entropy rate at least $1/t$ is automatically some kind of merger for t-part somewhere-random sources.

In the literature, mergers have only been studied in the *condensing* regime: where their output is required to have high entropy rate (rather than requiring the output to be near-uniform). It turns out that information-theoretically, condensing mergers are completely overshadowed by classical condensers. A condenser is a seeded device that takes in a source with sufficient entropy rate and outputs a random variable with high entropy rate. Thus a condenser that can operate on sources with entropy rate $1/t$ is automatically a condensing merger for t-part somewhere-random sources. It turns out that whatever parameter ranges are achievable by condensing mergers can be completely explained by condensers.

In this paper, we study mergers in the *extracting* regime: where their output is required to be near-uniform. Our main result is a characterization of the seed-length needed for such extracting mergers. Unlike the tragic case of condensing mergers and their relationship with condensers, extracting mergers are able to step out of the shadow of extractors, and carve a niche, albeit small, for themselves.

We also study extracting multimergers, where more random variables out of the given tuple of random variables are required to be uniform and independent. This leads us to a number of interesting combinatorial / geometric questions, for which we give some new and basic combinatorial theorems (such as a partition analogue of Shearer's lemma on projections of a set in a product space).

1.1 Overview of results

Our results are best viewed in contrast to the situation with classical extractors and condensers. An extractor takes a source with some min-entropy and an independent uniform seed, and outputs a nearly-uniform distributed random variable. A condenser takes a source with some min-entropy and an independent uniform seed, and outputs a source with higher min-entropy-rate.

Both extractors and condensers are functions of the form:

$$F : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m,$$

where d is the "seed-length" and m is the "output-length".

Consider a random source $\mathbf{X}$ that is $\{0,1\}^n$-valued and has entropy rate $1/t$ (which means that its min-entropy is $\geq n/t$).

In the case of extractors, for $(1-\epsilon)$-fraction of $j \in \{0,1\}^d$, the output $F(\mathbf{X}, j)$ is required to be ϵ-close in statistical distance to the uniform distribution over $\{0,1\}^m$. In the case of condensers, for $(1-\epsilon)$-fraction of $j \in \{0,1\}^d$, the output $F(\mathbf{X}, j)$ is required to be ϵ-close in statistical distance to some $\{0,1\}^m$-valued random variable with min-entropy $\geq k'$.

Extractors and condensers are qualitatively very different from the point of view of seed-length. We summarize their salient features below:

- There are no seedless extractors or condensers.
- There are condensers with **constant** seed-length $d = O(\log \frac{1}{\epsilon})$ which are **lossless** (we can take k' as large as $\frac{n}{t} + d$), provided $m > k' + \Omega(\log \frac{1}{\epsilon})$.
- The seed-length required for an extractor to extract one bit of entropy from a random source $(\{0,1\}^n)^t$ is $\log n + 2\log \frac{1}{\epsilon} + O(1)$. Furthermore, this seed-length suffices to extract almost all the entropy out of the source.

A merger takes in a t-part somewhere-random source (which is a special case of a source with entropy rate $\frac{1}{t}$) and an independent uniform seed, and outputs a source with purer randomness. This naturally creates two kinds of mergers - condensing mergers and extracting mergers. To the best of our knowledge, only condensing mergers have been studied in the literature, and the (non-constructive) existence results for condensing mergers all follow from the existence results for condensers mentioned above.

Let $E : (\{0,1\}^n)^t \times \{0,1\}^d \to \{0,1\}^m$ be an extracting merger, namely its output is guaranteed to be ϵ-close to uniform on $\{0,1\}^m$ whenever given a t-part somewhere-random source as input.

▶ **Theorem A** (Informal). *We have the following:*

- *There are no seedless extracting mergers, even with output length* 1.
- *There are extracting mergers with* **constant** *seed length* $O(\log \frac{1}{\epsilon})$*, which can output a constant number of nearly-uniform bits.*
- *Nevertheless, if the seed length required for an extracting merger to extract almost all (or even a constant fraction) the entropy out of a somewhere-random source is* $\Theta(\log n)$*.*

The first item is trivial. The second item is also not difficult, but it already gives a taste of why things are different with extracting mergers. Indeed, randomly-chosen functions are not extracting mergers. The third item in the above theorem is our main technical result. It is proved by a second-moment strengthening of the graph-theoretic approach of Radhakrishnan and Ta-Shma to extractors.

1.2 Projections of partitions

Our study of these questions about randomness extraction leads us to formulate and make progress on a new and natural combinatorial question: the partition analogue of the Shearer/Loomis-Whitney inequalities on volumes of projections. These questions arise when we consider the problem of extracting randomness from t-part s-where random sources (where s out of the t parts of the source are uniform and independent). We call devices that do this *extracting multimergers*. For the rest of this subsection we only focus on the combinatorial aspect.

Let A be an "nice" subset of the solid cube $[0,1]^3$ with (Lebesgue) volume α. Consider the three axis-parallel 2-dimensional projections: $\Pi_{XY}(A)$, $\Pi_{YZ}(A)$, $\Pi_{XZ}(A)$. The Shearer/ Loomis-Whitney inequality [5, 14] implies that at least one of these three projections has area at least $\alpha^{2/3}$. This is tight, as witnessed by the case where A is a cube of side-length $\alpha^{1/3}$ (and this is roughly the only such example).

Now consider the following partition variant: Let A, B be "nice" subsets of $[0,1]^3$ that partition $[0,1]^3$. Consider the six axis-parallel 2-dimensional projections of these two sets: $\Pi_{XY}(A)$, $\Pi_{YZ}(A)$, $\Pi_{XZ}(A)$ and $\Pi_{XY}(B)$, $\Pi_{YZ}(B)$, $\Pi_{XZ}(B)$. How large can we guarantee that one of them is?

Using the previous inequality and the fact that at least one of A, B has volume at least $1/2$, we get that one of these six 2-dimensional projections has area at least $(1/2)^{2/3} \geq 0.6299$. For this bound to be tight, we would need both A and B to have volume $1/2$, and both A and B to be tight examples for the Shearer/Loomis-Whitney inequality. This would require us to be able to cover $[0,1]^3$ by two cubes of volume $1/2$ – which is clearly impossible. This suggests that there should be a better bound!

We show, using a delicate study of the sections of the cube and some seemingly lucky inequalities, a tight bound for this problem.

▶ **Theorem B** (Informal). *Let A, B be "nice" subsets of $[0,1]^3$ that partition $[0,1]^3$. Then at least one of the six 2-dimensional projections*

$$\Pi_{XY}(A), \Pi_{YZ}(A), \Pi_{XZ}(A), \Pi_{XY}(B), \Pi_{YZ}(B), \Pi_{XZ}(B),$$

has area at least $3/4$.

Such "projections of partitions" questions can be formulated in great generality, and apart from Theorem B (whose proof we find very interesting), we also make some general observations and make some slightly non-trivial progress. We think these are very natural combinatorial questions worthy of further study. Beyond having connections to mergers, these questions turn out to be related to the KKL and BKKKL theorems/conjectures [12, 2, 10, 9] on influences of Boolean functions on the solid cube $[0,1]^n$. For example, Theorem B implies that any 3-variable Boolean function $f : [0,1]^3 \to \{0,1\}$ has some variable and some bit b such that the "influence towards b" of that variable is at least $1/4$, and this is tight.

Another application of such results is to partition analogues of the Kruskal-Katona theorem. For example, Theorem B implies that for any partition of $\binom{[n]}{3}$ into two parts, one of the two parts has shadow with size at least $\left(\frac{3}{4} - o(1)\right)\binom{n}{2}$.

1.3 Related work

Mergers were introduced by Ta-Shma [19] in his thesis, and were used to construct state-of-the-art extractors at the time (these were condensing mergers). Later, [15] proposed a new condensing merger construction based on taking random linear combinations of vectors over finite fields, and used it in their construction of the first extractors optimal upto constant factors. This analysis was greatly improved by Dvir [6] through his solution to the finite field Kakeya conjecture. Subsequently, [8, 7] defined a higher degree polynomial variant of the [15] merger, and by developing the ideas from [6], were able to construct improved (constant seed) mergers and state-of-the-art extractors. Subsequently [20] showed how to get analogous explicit constructions of condensers (subsuming the [7] condensing mergers) by improving the [11] condensers.

Another interesting constant seed condensing merger is by [18], which was constructed on the way to multi-source extractors.

Our lower bounds for the seed length of extracting mergers are proved by developing ideas from the paper of Radhakrishnan and Ta-Shma [17]. A recent beautiful proof of [1] also achieved a similar result to [17] in a much cleaner way, but we were not able to adapt this approach to our setting.

Other papers relevant to the study of multimergers are related to resilient functions [3, 4, 16].

Finally, our combinatorial results are related to the KKL and BKKKL theorems/conjectures [12, 2, 10, 9] on influences of Boolean functions on the solid cube $[0,1]^n$.

1.4 Organization

We give the basic definitions of extracting mergers and extracting multimergers in Section 2. In Section 3 we start with a simple proof that seedless mergers do not exist. This is followed by showing the existence of mergers and multimergers in the extracting regime with constant seed-length. We prove our lower bound on the seed length of extracting mergers in Section 4, which culminates in Theorem 9. In Section 5 we explore the connection between *seedless* extracting mergers and projections of partition questions. Section 6 is devoted to proving Theorem 17, our (optimal) lower bound on partitioning the unit cube into 2 parts, and Section 7 is devoted to partitions of the cube into 3 parts.

2 Sources and Mergers

▶ **Definition 1** (k-source). *For any k, we say that a random variable X is a k-source if for all x, $\Pr[X = x] \leq 2^{-k}$*

2.1 Somewhere and s-where Random Sources

▶ **Definition 2** (Somewhere-Random Source). *For a domain D, a tuple $\mathbf{X} = (X_1, \ldots, X_t)$ of jointly distributed D-valued random variables is called a t-part somewhere random source if for some $i \in [t]$, the distribution of X_i is uniform over D.*

▶ **Definition 3** (s-where Random Source). *For a domain D and an integer $s > 0$, a tuple $\mathbf{X} = (X_1, \ldots, X_t)$ of jointly distributed D-valued random variables is called a t-part s-where random source if for some distinct $i_1, \ldots, i_s \in [t]$, the joint distribution of $(X_{i_1}, X_{i_2}, \ldots, X_{i_s})$ is uniform over D^s.*

2.2 Extracting Mergers and Multimergers

▶ **Definition 4** (Extracting Mergers). *Let n, t, d, m be integers, and let $\epsilon > 0$.*

A function $E : (\{0,1\}^n)^t \times \{0,1\}^d \to \{0,1\}^m$ is called an ***(n, t, d, m, ϵ)-extracting merger*** *if the following holds.*

Suppose $\mathbf{X} = (X_1, \ldots, X_t)$ is a somewhere-random source where each X_i is $\{0,1\}^n$-valued. Then for at least $(1-\epsilon)$-fraction of $j \in \{0,1\}^d$, the distribution of:

$$Z = E(\mathbf{X}, j),$$

is ϵ-close to the uniform distribution on $\{0,1\}^m$.

We will sometimes refer to these as ϵ-extracting mergers (since n, d, t, m are related to the shape of E).

▶ **Definition 5** (Extracting Multimergers). *Let n, t, s, d, m be integers, and let $\epsilon > 0$.*

A function $E : (\{0,1\}^n)^t \times \{0,1\}^d \to \{0,1\}^m$ is called an ***$(n, d, t, m, \epsilon, s)$-extracting multimerger*** *if the following holds.*

Suppose $\mathbf{X} = (X_1, \ldots, X_t)$ *is an* s*-where random source where each* X_i *is* $\{0,1\}^n$*-valued. Then for at least* $(1-\epsilon)$*-fraction of* $j \in \{0,1\}^d$*, the distribution of:*

$$Z = E(\mathbf{X}, j),$$

is ϵ*-close to the uniform distribution on* $\{0,1\}^m$*.*

We will sometimes refer to these as (ϵ, s)-extracting multimergers (since n, d, t, m are related to the shape of E).

Observe that the $s = 1$ case in the above definition corresponds to extracting mergers.

Note on the definitions

In all our definitions, we chose to define the "strong" versions (where the output bits are required to be independent of the seed) for simplicity. In fact, our existence result for mergers is for the strong version, and our impossibility result is for the weak version.

3 Simple results about extracting mergers

For the rest of this paper, we only talk about *extracting* (not condensing) mergers and multimergers.

3.1 Seedless Mergers do not exist

We begin with the simple observation that there are no seedless extracting mergers.

▶ **Theorem 6** (There are no seedless mergers)**.** *Let* n *be an integer and* $\varepsilon < 1/2$*. There does not exist a function* $M : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *that is an* ε*-merger.*

Proof. Fix an $\varepsilon < 1/2$. Assume for the sake of contradiction there exists an ε-merger $M : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.

In particular, this means for *every* function $f : \{0,1\}^n \to \{0,1\}^n$, when X is distributed uniformly over $\{0,1\}^n$, the distribution of $M(X, f(X))$ is ε-close to uniform on $\{0,1\}$ – and in particular, it has full support on $\{0,1\}$. We will now demonstrate a function $g : \{0,1\}^n \to \{0,1\}^n$ such that $M(g(Y), Y)$ is constant for uniformly distributed Y, thus contradicting the merger assumption.

Fix any $y \in \{0,1\}^n$. Consider the constant function $f_y : \{0,1\}^n \to \{0,1\}^n$ given by $f_y(x) = y$ for all x. By our hypothesis above, the distribution of $M(X, f_y(X))$ has full support $\{0,1\}$. Thus there exists $x \in \{0,1\}^n$ such that $M(x, y) = 0$. Pick one such x and call it $g(x)$.

Thus we have $M(g(y), y) = 0$ for all $y \in \{0,1\}^n$. We conclude that for uniform $Y \in \{0,1\}^n$, $M(g(Y), Y) = 0$, which is the desired contradiction. ◀

3.2 Extracting mergers with constant seed exist

We now show that constant seed extracting mergers with constant output length exist. While the proof is quite simple, it is interesting because (1) constant seed extractors do not exist, (2) a random choice of $E : (\{0,1\}^n)^t \times \{0,1\}^d \to \{0,1\}^m$ does not give a constant seed extracting mergers, and most importantly (3) as we will later see, the seed length still needs to be superconstant to produce a superconstant number of output bits, as we will see in the next section.

▶ **Theorem 7.** *Let n, t be integers and $\epsilon > 0$.*
Then for any integer $m \leq n$, setting:

$$d = \log m + \log(t-1) + 2\log\frac{1}{\epsilon} + O(1),$$

there exists a function $E : (\{0,1\}^n)^t \times \{0,1\}^d \to \{0,1\}^m$ that is an ε-extracting merger.

Thus with $O(\log t + \log \frac{1}{\epsilon})$ bits of seed, we can extract $\text{poly}(\frac{1}{\epsilon})$ bits out.

Proof. We want to get an extracting merger $E((x_1, \ldots, x_t), j)$, where the $x_i \in \{0,1\}^n$ and $j \in \{0,1\}^d$.

The nature of a somewhere-random source is that applying a truncation to each element of the source yields a smaller somewhere-random source. The idea of our extracting merger is to truncate our somewhere-random source, and to then apply a standard seeded extractor to the entire truncated source. The truncation makes the instance size smaller, enabling us to use a reduced seed length in the extractor.

We truncate each x_i to the first m bits, thus obtaining $x'_1, \ldots, x'_t \in \{0,1\}^m$.

We can verify that our truncation to the first m bits produces a source $(X'_1, \ldots, X'_t)$ of length mt and min-entropy m. By the standard result on existence of extractors (See Theorem 6.14 in [21]), there exists a strong (m, ϵ)-extractor $Ext_0 : \{0,1\}^{mt} \times \{0,1\}^d \to \{0,1\}^m$ with seed length $d = \log m + \log(t-1) + 2\log\frac{1}{\epsilon} + O(1)$.

We can thus define the function $E : (\{0,1\}^n)^t \times \{0,1\}^d \to \{0,1\}^m$:

$$E((x_1, \ldots, x_t), j) = Ext_0((x'_1, \ldots, x'_t), j).$$

Observe that the function E is an ϵ-extracting merger that uses a seed j of length d and outputs m bits as required. ◀

In contrast, a random $E : (\{0,1\}^n)^t \times \{0,1\}^d \to \{0,1\}$ is not an extracting merger at all! To see this, it suffices to fix $t = 2$. If E is chosen at random, then for every $j \in \{0,1\}^d$ and $x \in \{0,1\}^n$, it is very likely that there exists a $y \in \{0,1\}^n$ such that $E((x,y),j) = 0$. Define $f_j : \{0,1\}^n \to \{0,1\}^n$ by $f_j(x) =$ any such y. Then for every $j \in \{0,1\}^d$, $E(X, f_j(X), j)$ is constant when X is picked uniformly at random, showing that E is not a merger.

3.3 Extracting Multimergers

Using the same idea, we also get interesting multimergers.

▶ **Theorem 8.** *Let n, t, s be integers with $s < t$, and $\epsilon > 0$. Then for any integer $a \leq n$, setting $m = s \cdot a$ and:*

$$d = \log a + \ 2\log\frac{1}{\epsilon} + \log(t-s) + \Omega(1),$$

there exists a function $E : (\{0,1\}^n)^t \times \{0,1\}^d \to \{0,1\}^m$ that is an (ε, s)-extracting multimerger.

Taking for example $s = t - 1$ and $a = \text{poly}\left(\frac{1}{\epsilon}\right) \ll n$, we get that by investing $O(\log \frac{1}{\epsilon})$ bits of seed, we can extract $\text{poly}\left(\frac{1}{\epsilon}\right) \cdot t$ bits of randomness from any t-part $(t-1)$-where random source $\mathbf{X} \in (\{0,1\}^n)^t$.

In this setting of parameters, the seed length does not even depend on t, and we could take t to be growing superconstantly while preserving constant seed-length.

3.4 Seedless Multimergers

Our final observation of this section is that for multimergers with large t and where s is a large fraction of t, seedless multimergers with small error *do* exist. Indeed, if $s = t - 1$, and we define $E : (\{0,1\}^n)^t \to \{0,1\}$ by

$$E(x_1, \ldots, x_t) = Maj(x_{11}, x_{21}, \ldots, x_{t1}),$$

it is easy to see that E is a seedless $(\epsilon, t-1)$-multimerger for $\epsilon = O(\frac{1}{\sqrt{t}})$. Replacing E with any resilient function gives other examples of seedless multimergers (including with larger output size).

Investigation of this phenomenon leads us to the projections of partitions question, and we explicitly give the connection and some results about it in a later section. Nevertheless, this seems like the tip of an iceberg.

4 Mergers with large output need large seed

In this section we show a lower bound on the seed-length for 2-source extracting mergers, essentially showing that the dependence of the seed-length for extracting mergers in Theorem 7 on m and ϵ is tight.

▶ **Theorem 9.** *Let $\epsilon < 1/40$. Let $E : (\{0,1\}^n)^2 \times \{0,1\}^d \to \{0,1\}^m$ be a ε-extracting merger. Then for $\epsilon \geq 2^{-\Omega(m)}$, we have:*

$$d \geq \log m + \log \frac{1}{\epsilon} - O(1).$$

and for $\epsilon < 2^{-\Omega(m)}$, we have:

$$d \geq \Omega(m).$$

For the proof of this theorem, the representation of the inputs and output of E in terms of bits is a distraction. So, letting $N = 2^n$, $D = 2^d$, $M = 2^m$ and identifying $\{0,1\}^n, \{0,1\}^d, \{0,1\}^m$ with $[N], [D], [M]$ respectively, we will view E as a function $E : [N]^2 \times [D] \to [M]$.

Recalling the ϵ-extracting merger property, we have that E is such that whenever X, Y are jointly distributed $[N]$-valued random variables, with at least one of them uniformly distributed, and J is picked uniformly from $[D]$ and independently of (X, Y), then the distribution of $E((X, Y), J)$ is ϵ-close to the uniform distribution on $[M]$.

We will show that for $\epsilon \geq M^{-\Omega(1)}$, we have:

$$D \geq \Omega\left(\frac{1}{\epsilon} \log M\right),$$

and for $\epsilon < M^{-\Omega(1)}$, we have:

$$D \geq \Omega\left(M^{\Omega(1)}\right).$$

Our proof is based on the following idea. Consider a uniformly random subset $S \subseteq [M]$ of size λM. For each $y \in [N]$, we look for an x such that for all $j \in [D]$, $E(x, y, j) \notin S$. If there is such an x, then we define $g(y) = x$. If such an x exists for most y, then for uniformly chosen $Y \in [N], J \in [D]$, we have $\Pr_{Y,J}[E(g(Y), Y, J) \in S] \ll \lambda - \epsilon$, contradicting the merger property. Thus for most S, for many y there is no such x; namely, for most S, for many y,

for all x, there is some j, such that $E(x, y, j) \in S$. For this to happen for even one y turns out to be very abnormal, and we derive our lower bound on D by digging into its structure. This part uses a second moment variation of the Radhakrishnan-TaShma [17] approach to extractor lower bounds.

4.1 Abnormal conductors

A map $C : [N] \times [D] \to [M]$ is called a conductor (this is a general term capturing the shape of seeded extractors and seeded condensers). We will also view this as a bipartite multigraph with $[N]$ on the left, $[M]$ on the right and D labelled edges coming out of every left vertex.

If C is chosen at random, then for most $S \subseteq [M]$ of size λM and most $x \in [N]$, we expect about λ fraction of the edges coming out of x to land in S. But we do not expect that this will happen for *all* x! When C is chosen at random, then for most S there will be some $x \in [N]$ for which a very small ($\ll \lambda$) fraction of edges coming out of x lie in S. We capture this with the following definition.

▶ **Definition 10.** *Let $C : [N] \times [D] \to [M]$ be a conductor. Let S be a subset of $[M]$. We say the vertex $x \in [N]$* totally misses *S (under C) if*

$$|\{j \in [D] \mid C(x, j) \in S\}| = 0.$$

We say the vertex $x \in [N]$ mostly misses *S (under C) if*

$$|\{j \in [D] \mid C(x, j) \in S\}| < \frac{1}{2}\frac{|S|}{M}D.$$

▶ **Definition 11** (Abnormal conductors)**.** *Let $C : [N] \times [D] \to [M]$ be a conductor. We say that C is (γ, λ)-abnormal if*

$$\Pr_{S \in \binom{[M]}{\lambda M}}[\exists x \in [N] \text{ s.t. } x \text{ mostly misses } S] < 1 - \gamma.$$

▶ **Lemma 12** (Extracting mergers contain abnormal conductors)**.** *Suppose $0 < \gamma < \frac{\lambda}{2} - \epsilon$. Suppose $E : [N]^2 \times [D] \to [M]$ is an ϵ-extracting merger. For $y \in [N]$, let $E_y : [N] \times [D] \to [M]$ be the function $E(\cdot, y, \cdot)$. Then for some $y \in [N]$, E_y is (γ, λ)-abnormal.*

Proof. Suppose not; namely that for all $y \in [N]$, we have that E_y is not (γ, λ)-abnormal.

Pick $S \in \binom{[M]}{\lambda M}$ uniformly at random.

Let B_y be the event that there exists some $x \in [N]$ that mostly misses S under E_y.

By our assumption, $\Pr[B_y] \geq 1 - \gamma$. So the expected number of y for which B_y happens is at least $(1 - \gamma)N$.

Thus there exists some particular choice of S for which B_y happens for at least $(1 - \gamma)N$ many ys. Call this choice S_0. Define $f : [N] \to [N]$ by defining $f(y)$ as follows:

$$f(y) = \begin{cases} \text{any } x \text{ that mostly misses } S_0 \text{ under } E_y & B_y \text{ happened,} \\ \text{arbitrary} & B_y \text{ did not happen.} \end{cases}$$

Then

$$\Pr_{Y \in [N], J \in [D]}[E(f(Y), Y, J) \in S_0] < \frac{\lambda}{2}(1 - \gamma) + \gamma < \lambda - \epsilon.$$

But $|S_0| = \lambda M$, and thus we get a contradiction to the ϵ-extracting merger property of E. This completes the proof. ◀

4.2 The structure of abnormal conductors

The previous lemma gave us a y for which E_y is abnormal. We now use show that abnormal conductors are very structured, and thus get a lower bound on D.

▶ **Lemma 13.** *Let $C : [N] \times [D] \to [M]$ be a (γ, λ)-abnormal conductor. Suppose $10\epsilon < \lambda < \frac{1}{2}$.*

Suppose that for $X \in [N]$ and $J \in [D]$ picked uniformly and independently, $C(X, J)$ is ϵ-close to the uniform distribution on $[M]$. Then

$$D \geq \min\left\{\Omega\left(\frac{1}{\lambda}\log(\lambda\gamma M)\right), \Omega\left((\lambda\gamma M)^{1/4}\right)\right\}.$$

Proof. We begin with a pruning phase to remove the high degree vertices from the right side. At first reading, it will be helpful to consider the case where $B = \emptyset$.

Let $\beta = \frac{\lambda}{5} - \epsilon$. Note that the average right degree is ND/M. Define the set of high-degree right vertices by:

$$B = \{z \in [M] \mid \text{ there are at least } \frac{1}{\beta}\frac{ND}{M} \text{ edges to } z\}.$$

Thus $|B| \leq \beta M$. By the hypothesis on $C(X, J)$, we have

$$\Pr_{X\in[N],J\in[D]}[C(X, J) \in B] \leq \beta + \epsilon.$$

Let G be the set of all vertices on the left that do not have too many edges to B; namely:

$$G = \{x \in [N] \mid x \text{ has at most } 2(\beta + \epsilon)D \text{ edges to } B\ \}.$$

Then $|G| \geq N/2$.

Now pick $S \in \binom{[M]}{\lambda M}$ uniformly at random. If there is a vertex $x \in G$ that totally misses $S \setminus B$, then by choice of G:

$$|\{j \mid C(x, j) \in S\}| \leq 2(\beta + \epsilon)D < \frac{1}{2}\lambda D,$$

namely, x mostly misses S.

By our hypothesis on the abnormality of C, the existence of such an x cannot happen too often. Thus:

$$\Pr_S[\exists x \in G \mid x \text{ totally misses } S \setminus B] < 1 - \gamma. \tag{1}$$

For each $x \in G$, let A_x be the event that x totally misses $S \setminus B$ under C.

We are interested in the event that some $x \in G$ totally misses $S \setminus B$, namely, the event $\bigvee_{x\in G} A_x$.

Observe that[1]

$$\Pr[A_x] \geq \frac{\binom{M-D}{\lambda M}}{\binom{M}{\lambda M}} \geq e^{-4\lambda D} =: p.$$

Define $A = \sum_{x\in G} A_x$. Then $\mathbf{E}[A] \geq |G|p$.

---

[1] Here we use the observation that $(1 - \frac{D}{(1-\lambda)M}) < e^{-\frac{2D}{(1-\lambda)M}} < e^{-4D/M}$, which follows from the fact that $1 - x < e^{-2x}$ for $x < 1/2$.

By the second moment method, we have:

$$\Pr[A = 0] \leq \frac{\mathbf{Var}[A]}{\mathbf{E}[A]^2}.$$

But Equation (1) tells us that $\Pr[A = 0] > \gamma$.
Thus $\mathbf{Var}[A] \geq \gamma \mathbf{E}[A]^2 \geq \gamma \cdot p^2 |G|^2$.
We now extract some structure from this.
We have:

$$\mathbf{Var}[A] = \sum_{x,x' \in G} \left(\Pr[A_x \wedge A_{x'}] - \Pr[A_x] \Pr[A_{x'}] \right).$$

Two simple observations about this expression:

- Each term in the sum above is at most 1.
- Furthermore, if x, x' have no common neighbors in $[M] \setminus B$, then the corresponding term of the sum above is ≤ 0. Indeed, if $U_x, U_{x'} \subseteq [M] \setminus B$ are the neighborhoods of x and x' in $[M] \setminus B$, and if they are disjoint, then:

$$\Pr[A_x] = \frac{\binom{M - |U_x|}{\lambda M}}{\binom{M}{\lambda M}},$$

$$\Pr[A_{x'}] = \frac{\binom{M - |U_{x'}|}{\lambda M}}{\binom{M}{\lambda M}},$$

$$\Pr[A_x \wedge A_{x'}] = \frac{\binom{M - |U_x \cup U_{x'}|}{\lambda M}}{\binom{M}{\lambda M}} = \frac{\binom{M - |U_x| - |U_{x'}|}{\lambda M}}{\binom{M}{\lambda M}}.$$

So

$$\frac{\Pr[A_x \wedge A_{x'}]}{\Pr[A_x] \Pr[A_{x'}]} = \prod_{i=0}^{\lambda M - 1} \frac{(M - i) \cdot (M - |U_x| - |U_{x'}| - i)}{(M - |U_x| - i) \cdot (M - |U_{x'}| - i)} \leq 1.$$

Combining the largeness of $\mathbf{Var}[A]$ with these two observations tells us that there are many $x, x' \in G$ which have a common neighbor in $[M] \setminus B$. Specifically:

$$\gamma p^2 |G|^2 \leq \mathbf{Var}[A] \leq \sum_{x,x' \in G} \mathbf{1}[x, x' \text{ have a common neighbor in } [M] \setminus B].$$

Thus there are at least $\gamma p^2 |G|^2 \geq \frac{1}{4} \gamma p^2 N^2$ pairs x, x' from G that have a common neighbor in $[M] \setminus B$.

Now the initial pruning we did will help us. Since all the vertices in $[M] \setminus B$ have degree at most $\frac{1}{\beta} \frac{ND}{M}$, we can bound the number of such pairs x, x'. For every vertex $x \in G$, there are at most $D \cdot \frac{1}{\beta} \frac{ND}{M}$ vertices x' such that x and x' share a common neighbor in $[M] \setminus B$. Thus the total number of pairs x, x' from G that have a common neighbor in $[M] \setminus B$ is at most

$$N \cdot D \cdot \frac{1}{\beta} \frac{ND}{M} = \frac{1}{\beta} \frac{D^2}{M} N^2.$$

Thus $\frac{1}{4} \gamma p^2 \leq \frac{1}{\beta} \frac{D^2}{M}$. Since $p = e^{-4\lambda D}$, we get:

$$M \leq \frac{4}{\gamma \beta} D^2 e^{8\lambda D}.$$

This means that either $D \geq \Omega\left((\gamma \beta M)^{1/4} \right) = \Omega\left((\gamma \lambda M)^{1/4} \right)$, or else:

$$D \geq \Omega\left(\frac{1}{\lambda} \log(\gamma \beta M) \right) \geq \Omega\left(\frac{1}{\lambda} \log(\gamma \lambda M) \right).$$

◀

4.3 Putting everything together

We now prove Theorem 9.

Proof. Let $E : [N]^2 \times [D] \to [M]$ be an ϵ-extracting merger.

Set $\lambda = 20\epsilon$ and $\gamma = \epsilon$. Lemma 12 tells us that there is some $y := y_0$ for which E_y is (λ, γ)-abnormal.

Now, since E is ϵ-extracting, we have that $E_y(X, J) = E(X, y, J)$ is ϵ-close to the uniform distribution on $[M]$ for uniform and independent $X \in [N]$ and $J \in [D]$. Thus Lemma 13 tells us that

$$D \geq \min\left\{\Omega\left(\frac{1}{\epsilon}\log(\epsilon^2 M)\right), \Omega\left((\epsilon^2 M)^{1/4}\right)\right\}$$

.

If $\epsilon \geq \frac{1}{M^{1/10}}$, then the first expression is smaller and

$$D \geq \Omega(\frac{1}{\epsilon}\log M),$$

and if $\epsilon < \frac{1}{M^{1/10}}$, then E is also a $\frac{1}{M^{1/10}}$-extracting merger, and thus using the above lower bound for $\frac{1}{M^{1/10}}$ in place of ϵ, we get that:

$$D \geq M^{\Omega(1)}.$$ ◀

5 Seedless Extracting Multimergers and Projections of Partitions

In this section, we study seedless multimergers. Here our understanding is far from complete, and we suggest many directions for research.

We begin by observing a connection between seedless multimergers and a very natural and clean geometric question: how do we partition the unit cube $[0, 1]^t$ into c parts to ensure that all s-dimensional axis-parallel projections of all parts are small? We then prove some interesting positive and negative results about special cases of this general question. We conclude by collecting a number of observations and questions about this natural partitioning problem.

5.1 Seedless Multimergers with 1 bit output

In Section 3.1 we have already seen that there are no seedless mergers (i.e., with $s = 1$). We now look into seedless multimergers.

Let us consider the simplest nontrivial situation: $t = 3$ and $s = 2$, and $m = 1$ (we only try to extract 1 bit of randomness), with n big. Suppose a given function $E : (\{0, 1\}^n)^3 \to \{0, 1\}$ is known to be a (ϵ, s)-multimerger. For convenience, we identify $\{0, 1\}^n$ with $[N]$, for $N = 2^n$.

By the multimerger property, for every function $f : [N]^2 \to [N]$, the distribution of $E(X, Y, f(X, Y))$ should be ϵ-close to uniform. Let

$$P_{XY,0} = \{(x, y) \in [N]^2 : \exists z \mid E(x, y, z) = 0\}.$$

Notice that this is the projection of $E^{-1}(0)$ to two coordinates.

If $P_{XY,0}$ is bigger than $\frac{1+\epsilon}{2}N^2$, then we can violate the multimerger property: we define $f : [N]^2 \to [N]$ by $f(x, y) = z$, if any, such that $E(x, y, z) = 0$". Then $E(X, Y, f(X, Y))$ for uniform and independent $X, Y \in [N]$ is ϵ-far from uniform.

We have a similar observation for all the other two dimensional projections, and also for the set $E^{-1}(1)$. Thus if a seedless one-bit output multimerger for 3-part 2-where random sources exists, then there is a partition of $[N]^3$ into 2 parts such that each part has all its 2-dimensional axis parallel projections have size at most $\frac{1+\epsilon}{2}N^2$.

The connection also goes in reverse. Suppose we have a partition A, B of $[N]^3$ for which each part has all its 2-dimensional axis parallel projections with size at most $\frac{1+\epsilon}{2}N^2$. Let $E : [N]^3 \to \{0,1\}$ be the unique function with $E^{-1}(0) = A$ and $E^{-1}(1) = B$. Suppose (X, Y, Z) is an $[N]^3$-valued random variable that is 2-where random. Then we claim that $E(X, Y, Z)$ is ϵ-close to the uniform distribution. Indeed, if (X, Y) is uniformly distributed over $[N]^2$ (the cases of (Y, Z) and (X, Z) being uniformly distributed are similar), then:

$$\begin{aligned}
\Pr[E(X,Y,Z)=0] &\leq \Pr_{X,Y}[\exists z \in [N] \text{ s.t. } E(X,Y,z)=0] \\
&\leq \Pr_{X,Y}[\exists z \in [N] \text{ s.t. } (X,Y,z) \in A] \\
&\leq \frac{|\Pi_{XY}(A)|}{N^2} \\
&\leq \frac{1+\epsilon}{2}, \\
\Pr[E(X,Y,Z)=1] &\leq \Pr_{X,Y}[\exists z \in [N] \text{ s.t. } E(X,Y,z)=1] \\
&\leq \Pr_{X,Y}[\exists z \in [N] \text{ s.t. } (X,Y,z) \in B] \\
&\leq \frac{|\Pi_{XY}(B)|}{N^2} \\
&\leq \frac{1+\epsilon}{2},
\end{aligned}$$

which implies the desired ϵ-closeness to uniform of $E(X, Y, Z)$.

The exact same argument applies to general t, s. We record this below.

▶ **Theorem 14.** *Let $N = 2^n$. There exists a seedless $(n, d, t, m, \epsilon, s)$-multimerger if and only if there is a partition of $[N]^t$ into two sets A, B such that for every subset $U \subseteq [t]$ of size s, the projections $\Pi_U(A)$ and $\Pi_U(B)$ onto the coordinates U are of size at most $\frac{1+\epsilon}{2}N^s$.*

Motivated by this, we consider general projections of partitions questions, where the set $[N]^t$ is partitioned into c parts, and we seek to minimize the maximum s-dimensional axis parallel projection of all the parts[2].

As noted in the introduction, there is a basic bound for this problem that comes from Shearer's lemma. It says that there is a lower bound of $\left(\frac{1}{c}\right)^{s/t} N^s$ on the size of some projection. This bound is usually not tight – but it sometimes is! Whenever c is a perfect t'th power, then this bound is tight, and is realized by a partition into product sets. But for other c this kind of partition does not work, and very interesting questions ensue. In particular, we would like to highlight the case of N gigantic, and $c = \text{poly}(t)$ (so that c is clearly not a perfect t'th power).

Here is one observation that gives a flavor of what happens for large t and s. When c is a constant, and $s = t - o(\sqrt{t})$, there is a partition so that all s-dimensional projections of size $\frac{1}{c} + o(1)$. This comes by considering suitable threshold partitions. Extensions of this are related to the BKKKL [2, 10] conjectures on low influence functions.

[2] For $c > 2$, the problem of getting such partitions with c parts is somewhat related to the problem of multimergers with $\log_2(c)$ bit output, but the connection is not as tight as for the case of $c = 2$

This question is also equivalent to a problem in the continuous domain about open covers of $[0,1]^t$. Here we want to minimize the maximum s-dimensional projection size when we cover $[0,1]^t$ by c open sets.

In the following sections, we discuss two results on partitioning in three dimensions. For the first result, we get (to our surprise!) the tight bound for partitioning the cube into two parts. For the second result, we get nontrivial bounds (both upper and lower) for partitioning the cube into three parts.

Apology

These questions are more naturally phrased as questions about covers rather than partitions. However we stick to the partition language because of the particular sequence of events that led us to these problems.

6 Partitioning the 3-dimensional cube into two parts

In this section, we prove a tight bound on the largest 2 dimensional axis parallel projection of a part when partitioning $[0,1]^3$ into 2 parts.

Let $\pi_{XY}, \pi_{YZ}, \pi_{XZ} : [0,1]^3 \to [0,1]^2$ be the 2-dimensional projection maps.

The following example gives a nice partitioning with small projections.

▶ **Definition 15** (Majority Partitioning Scheme). *We define the function $MAJ_3 : [0,1]^3 \to \{0,1\}$ as*

$$MAJ_3(x,y,z) = Maj(x_1, y_1, z_1)$$

where Maj denotes the Majority function on 3 bits, and where x_1, y_1, z_1 denote the indicator variables for whether $x > 1/2$, $y > 1/2$, $z > 1/2$ respectively.

We refer to the partition naturally induced by the output of MAJ_3 on the input space $[0,1]^3$ i.e. $\{MAJ_3^{-1}(0), MAJ_3^{-1}(1)\}$, as the Majority Partitioning Scheme.

We next record the observation tha all 2-dimensional axis-parallel projections of all parts in the majority partitioning scheme on $[N]^3$ are of size at most $\frac{3}{4}N^2$, which is stated in the following lemma:

▶ **Lemma 16** (Majority Partitions Optimally). *Every 2-dimensional projection of every partition in the majority partitioning scheme MAJ_3 on $[0,1]^3$ is of size at most $\frac{3}{4}$.*

In the other direction, we first prove a lower bound on projection sizes for a discrete version of the problem.

Let N be a large positive integer. We reuse notation and let $\pi_{XY}, \pi_{YZ}, \pi_{XZ} : [N]^3 \to [N]^2$ be the 2-dimensional projection maps.

▶ **Theorem 17.** *Let $A, B \subseteq [N]^3$ be a partition.*

Then one of the six 2-dimensional projections of A and B

$$\pi_{XY}(A), \pi_{YZ}(A), \pi_{XZ}(A), \pi_{XY}(B), \pi_{YZ}(B), \pi_{XZ}(B)$$

has size at least $\frac{3}{4}N^2$.

Proof of Theorem 17 can be found in the appendix.

By a simple discretization argument, we get the following corollary:

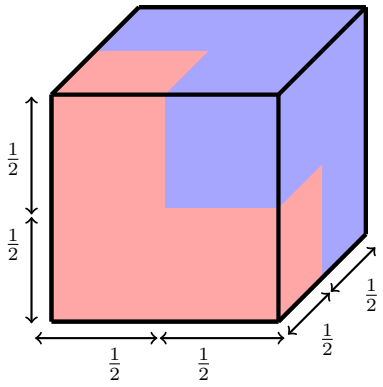

Figure 1 Majority Partitioning of the cube into 2 parts, where the partitioned sets are coloured in red and blue. Observe that *all* projections of the red set and the blue set are of equal size $\frac{3}{4}$, and Theorem 17 implies this partitioning is optimal.

▶ **Corollary 18.** *Any cover of* $[0,1]^3$ *by two open sets* A, B *has one of the following 6 sets:*

$$\Pi_{XY}(A), \Pi_{YZ}(A), \Pi_{XZ}(A), \Pi_{XY}(B), \Pi_{YZ}(B), \Pi_{XZ}(B)$$

having area at least $3/4$.

Thus we get that MAJ_3 is an *optimal* partition for partitioning $[N]^3$ into two parts.

7 Partitioning the 3-dimensional cube into three parts

In this section we study the case of partitioning the 3 dimensional cube $[0,1]^3$ into 3 parts.

We begin with a nice partition of $[0,1]^3$ into 3 parts so that each part has small 2-dimensional axis-parallel projections.

▶ **Definition 19** (Golden Ratio Partitioning Scheme)**.** *Let* u *be the positive root of* $x^2 + x = 1$. *We define the function* $GR_3 : [0,1]^3 \to \{0,1,2\}$ *as*

$$GR_3(x,y,z) = \begin{cases} 0, & |x| > u, |y| > u \\ 1, & |x| \le u, |y| \le u, |z| \le \frac{1}{2} \\ 2, & \textit{otherwise.} \end{cases}$$

We refer to the partition into 3 parts naturally induced by the output of GR_3 *on the input space* $[0,1]^3$ *i.e.* $\{GR_3^{-1}(0), GR_3^{-1}(1), GR_3^{-1}(2)\}$, *as the golden ratio partitioning scheme.*

▶ **Lemma 20** (Golden Ratio Partitioning Bound)**.** *Every 2-dimensional projection of every partition in the golden ratio partitioning scheme* GR_3 *on* $[0,1]^3$ *is of size* $u \le 0.619$.

We do not know if this is the optimal partition into 3 parts. For the rest of this section, we prove the best lower bound that we know. As in the previous section, we do this via an analogous discrete problem.

Let $\eta_0 \approx 0.5264$ be the real number $\in [0.5, 1.0]$ satisfying:

$$(2 - 3\eta_0) \cdot \left(2 - 2\sqrt{1 - \eta_0}\right) + (3\eta_0 - 1) = \frac{1}{6}(4 - \eta_0).$$

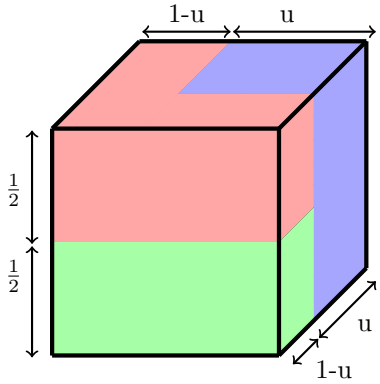

Figure 2 Golden Ratio Partitioning of the cube into 3 parts, where the partitioned sets are coloured in red, green and blue. The green and red parts are just translates of each other. Here u is the positive root of $x^2 + x = 1$.

▶ **Theorem 21.** *Let $A, B, C \subseteq [N]^3$ be a 3-partition of $[N]^3$. Then one of the nine 2-dimensional projections of A, B and C, i.e.,*

$\Pi_{XY}(A), \Pi_{XY}(B), \Pi_{XY}(C), \Pi_{YZ}(A), \Pi_{YZ}(B), \Pi_{YZ}(C), \Pi_{XZ}(A), \Pi_{XZ}(B), \Pi_{XZ}(C)$ *has size at least $\eta_0 N^2$.*

Proof of Theorem 21 can be found in the appendix.

This gives us a corresponding result about covers of $[0,1]^3$ with 3 open sets.

▶ **Corollary 22.** *Any cover of $[0,1]^3$ by three open sets A, B, C has one of the following 9 sets:*

$$\Pi_{XY}(A), \Pi_{YZ}(A), \Pi_{XZ}(A), \Pi_{XY}(B), \Pi_{YZ}(B), \Pi_{XZ}(B), \Pi_{XY}(C), \Pi_{YZ}(C), \Pi_{XZ}(C)$$

having area at least η_0.

References

1. Divesh Aggarwal, Siyao Guo, Maciej Obremski, João Ribeiro, and Noah Stephens-Davidowitz. Extractor Lower Bounds, Revisited. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*, 2020.
2. Jean Bourgain, Jeff Kahn, Gil Kalai, Yitzhak Katznelson, and Nathan Linial. The Influence of Variables in Product Spaces. In *Israel Journal of Mathematics*, 1992.
3. Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, and Xin Li. Extractors for Adversarial Sources via Extremal Hypergraphs. In *Proceedings of the 52nd Annual ACM Symposium on Theory of Computing (STOC)*, 2020.
4. Eshan Chattopadhyay and David Zuckerman. Explicit Two-Source Extractors and Resilient Functions. In *Annals of Mathematics*, 2019.
5. F.R.K Chung, R.L Graham, P Frankl, and J.B Shearer. Some Intersection Theorems for Ordered Sets and Graphs. *Journal of Combinatorial Theory, Series A*, 1986.
6. Zeev Dvir. On The Size of Kakeya Sets in Finite Fields. In *Journal of the American Mathematical Society*, 2009.
7. Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the Method of Multiplicities, with Applications to Kakeya Sets and Mergers. In *SIAM Journal on Computing*, 2013.
8. Zeev Dvir and Avi Wigderson. Kakeya Sets, New Mergers and Old Extractors. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2008.

9 Yuval Filmus, Lianna Hambardzumyan, Hamed Hatami, Pooya Hatami, and David Zuckerman. Biasing Boolean Functions and Collective Coin-Flipping Protocols over Arbitrary Product Distributions. In *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming (ICALP)*, 2019.

10 Ehud Friedgut. Influences in Product Spaces: KKL and BKKKL Revisited. *Comb. Probab. Comput*, 2004.

11 Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced Expanders and Randomness Extractors from Parvaresh–Vardy Codes*. In *Journal of the Association for Computing Machinery*, 2009.

12 J. Kahn, G. Kalai, and N. Linial. The influence of variables on Boolean functions. In *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science, (FOCS)*, 1988.

13 Swastik Kopparty and Vishvajeet N. Extracting mergers and projections of partitions, 2023. `arXiv:2306.16915`.

14 Lynn Harold Loomis and Hassler Whitney. An Inequality Related to the Isoperimetric Inequality. *Bull. AMS*, 1949.

15 Chi-Jen Lu, Omer Reingold, Salil Vadhan, and Avi Wigderson. Extractors: Optimal up to Constant Factors. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing (STOC)*, 2003.

16 Raghu Meka. Explicit Resilient Functions Matching Ajtai-Linial. In *Proceedings of the 2017 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2017.

17 Jaikumar Radhakrishnan and Amnon Ta-Shma. Bounds for Dispersers, Extractors, and Depth-Two Superconcentrators. In *SIAM Journal on Discrete Mathematics*, 2000.

18 Ran Raz. Extractors with Weak Random Seeds. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC)*, 2005.

19 Amnon Ta-Shma. Refining Randomness. In *Thesis Submitted to the Hebrew University of Jerusalem*, 2000.

20 Amnon Ta-Shma and Christopher Umans. Better Condensers and New Extractors from Parvaresh-Vardy Codes. In *Proceedings of the 27th Conference on Computational Complexity (CCC)*, 2012.

21 Salil P. Vadhan. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science*, 2012.

A Appendix

▶ **Theorem 23** (Restatement of Theorem 17). *Let $A, B \subseteq [N]^3$ be a partition. Then one of the six 2-dimensional projections of A and B*

$$\pi_{XY}(A), \pi_{YZ}(A), \pi_{XZ}(A), \pi_{XY}(B), \pi_{YZ}(B), \pi_{XZ}(B)$$

has size at least $\frac{3}{4}N^2$.

Proof. Suppose $\pi_{XY}(A)$ and $\pi_{XY}(B)$ are both at most $\frac{3}{4}N^2$.

Fix $z \in [N]$. Let us consider the slice $S_z = [N]^2 \times \{z\}$, and focus on the X and Y projections of the sets $A \cap S_z$ and $B \cap S_z$ (so four projections in all, each being a subset of $[N]$).

Define[3]:

$$A_{Xz} = \{x \mid \forall y \in [N], (x, y, z) \in A\}.$$

[3] If A, B was merely a cover of $[N]^3$ rather than a partition, the correct definition would be

$$A_{Xz} = \{x \mid \nexists y \in [N] \text{ s.t. } (x, y, z) \in B\},$$

etc, and the rest of the proof would remain the same.

$B_{Xz} = \{x \mid \forall y \in [N], (x, y, z) \in B\}$.

$A_{Yz} = \{y \mid \forall x \in [N], (x, y, z) \in A\}$.

$B_{Yz} = \{y \mid \forall x \in [N], (x, y, z) \in B\}$.

Let $\alpha_{Xz}, \beta_{Xz}, \alpha_{Yz}, \beta_{Yz} \in [0, 1]$ be their fractional sizes (= size divided by N).

Then we have the following:

- $A_{Xz} \cap B_{Xz} = \emptyset$ and $A_{Yz} \cap B_{Yz} = \emptyset$. Thus:

$$\alpha_{Xz} + \beta_{Xz} \leq 1, \tag{2}$$

$$\alpha_{Yz} + \beta_{Yz} \leq 1. \tag{3}$$

- $((A_{Xz} \times [N]) \cup ([N] \times A_{Yz})) \subseteq \pi_{XY}(A)$.
  This is because any $(x, y) \in (A_{Xz} \times [N])$ has $(x, y, z) \in A$, and thus $(x, y) \in \pi_{XY}(A)$.
  The fractional size of the left hand side is $1 - (1 - \alpha_{Xz})(1 - \alpha_{Yz})$, and the fractional size of the right hand side is $\leq 3/4$.
  This gives us (after applying the AM-GM inequality[4]):

$$\alpha_{Xz} + \alpha_{Yz} \leq 1. \tag{4}$$

- Similarly,

$$((B_{Xz} \times [N]) \cup ([N] \times B_{Yz})) \subseteq \pi_{XY}(B),$$

$$\beta_{Xz} + \beta_{Yz} \leq 1. \tag{5}$$

- At most one of A_{Xz}, B_{Yz} can be nonempty, and at most one of $A_{Yz}, B_{X,z}$ can be nonempty.
  This is because $x \in A_{Xz}$ and $y \in B_{Yz}$ imply that $(x, y, z) \in A$ and $(x, y, z) \in B$ respectively. Thus at most one of α_{Xz}, β_{Yz}, and at most one of α_{Yz}, β_{Xz} can be nonzero.

Putting everything together, we get that only two of the four numbers $\alpha_{Xz}, \beta_{Xz}, \alpha_{Yz}, \beta_{Yz}$ can be nonzero, and furthermore, the sum of those two is bounded above by 1.

Therefore, for each $z \in [N]$,

$$\alpha_{Xz} + \beta_{Xz} + \alpha_{Yz} + \beta_{Yz} \leq 1.$$

Averaging in z, we get that

$$\mathbf{E}_z[\alpha_{Xz} + \beta_{Xz} + \alpha_{Yz} + \beta_{Yz}] \leq 1,$$

and thus one of the four numbers:

$$\mathbf{E}_z[\alpha_{Xz}], \mathbf{E}_z[\beta_{Xz}], \mathbf{E}_z[\alpha_{Yz}], \mathbf{E}_z[\beta_{Yz}]$$

is at most 1/4.

Finally, observe that $(1 - \mathbf{E}_z[\alpha_{Xz}])$ is the fractional size of $\pi_{XZ}(B)$ (and similarly for the other three numbers), and so one of the four projections

$$\pi_{XZ}(B), \pi_{XZ}(A), \pi_{YZ}(B), \pi_{YZ}(A)$$

has size at least $\frac{3}{4}N^2$. ◀

[4] For any non-negative real numbers x and y, $\sqrt{x \cdot y} \leq \frac{x+y}{2}$

▶ **Theorem 24** (Restatement of Theorem 21). *Let $A, B, C \subseteq [N]^3$ be a 3-partition of $[N]^3$. Then one of the nine 2-dimensional projections of A, B and C, i.e.,*

$\Pi_{XY}(A), \Pi_{XY}(B), \Pi_{XY}(C), \Pi_{YZ}(A), \Pi_{YZ}(B), \Pi_{YZ}(C), \Pi_{XZ}(A), \Pi_{XZ}(B), \Pi_{XZ}(C)$ has size at least $\eta_0 N^2$.

Before embarking on the proof of Theorem 21, we note down a simple set intersection lemma that will be useful.

▶ **Lemma 25** (Set intersection inequality). *Suppose U, V, W be arbitrary sets which have union equal to T.*

Then

$$|U| + |V| + |W| \geq 2|T| - (|U \setminus (V \cup W)| + |V \setminus (W \cup U)| + |W \setminus (U \cup V)|) + |U \cap V \cap W|.$$

This lemma gives a way to get a lower bound on the average size of three sets U, V, W that cover a set T by first proving an upper bound on the sizes of the "unique" parts $U \setminus (V \cup W), V \setminus (U \cup W), W \setminus (U \cup V)$. The proof is simple and omitted.

We now prove Theorem 21.

Proof. Consider any partition A, B and C of $[N]^3$ into 3 parts. Suppose $\Pi_{XY}(A)$, $\Pi_{XY}(B)$ and $\Pi_{XY}(C)$ are at most η_0. (If not we are done).

Fix $z \in [N]$.

Our first step is to consider the slice $S_z = [N]^2 \times \{z\}$, and focus on the X and Y projections of the 3 sets $A \cap S_z, B \cap S_z, C \cap S_z$ (so six projections in all, each being a subset of $[N]$).

Define:

$$A_{Xz} = \{x \in [N] \mid \exists y \in [N] \text{ s.t. } (x, y, z) \in A\}.$$

$$B_{Xz} = \{x \in [N] \mid \exists y \in [N] \text{ s.t. } (x, y, z) \in B\}.$$

$$C_{Xz} = \{x \in [N] \mid \exists y \in [N] \text{ s.t. } (x, y, z) \in C\}.$$

$$A_{Yz} = \{y \in [N] \mid \exists x \in [N] \text{ s.t. } (x, y, z) \in A\}.$$

$$B_{Yz} = \{y \in [N] \mid \exists x \in [N] \text{ s.t. } (x, y, z) \in B\}.$$

$$C_{Yz} = \{y \in [N] \mid \exists x \in [N] \text{ s.t. } (x, y, z) \in C\}.$$

Note that:

$$A_{Xz} \cup B_{Xz} \cup C_{Xz} = [N]$$

$$A_{Yz} \cup B_{Yz} \cup C_{Yz} = [N]$$

since A, B, C is a partition of $[N]^3$.

Next we identify the "pure" parts of these projections, defined below:

$$\widetilde{A}_{Xz} = A_{Xz} \setminus (B_{Xz} \cup C_{Xz})$$

$$\widetilde{B}_{Xz} = B_{Xz} \setminus (C_{Xz} \cup A_{Xz})$$

$$\widetilde{C}_{Xz} = C_{Xz} \setminus (A_{Xz} \cup B_{Xz})$$

$$\widetilde{A}_{Yz} = A_{Yz} \setminus (B_{Yz} \cup C_{Yz})$$

$$\widetilde{B}_{Yz} = B_{Yz} \setminus (C_{Yz} \cup A_{Yz})$$

$$\widetilde{C}_{Yz} = C_{Yz} \setminus (A_{Yz} \cup B_{Yz})$$

Furthermore, we have:

$$\{x \mid \Pi_{XZ}^{-1}(x,z) \subseteq A\} \subseteq \widetilde{A}_{Xz}$$

and five similar containments for $\widetilde{B}_{Xz}, \widetilde{C}_{Xz}, \widetilde{A}_{Yz}, \widetilde{B}_{Yz}, \widetilde{C}_{Yz}$.

Let $\widetilde{\alpha}_{Xz}, \widetilde{\beta}_{Xz}, \widetilde{\gamma}_{Xz}, \widetilde{\alpha}_{Yz}, \widetilde{\beta}_{Yz}, \widetilde{\gamma}_{Yz} \in [0,1]$ be their fractional sizes.

Note that since the corresponding sets are disjoint, we have:

$$\widetilde{\alpha}_{Xz} + \widetilde{\beta}_{Xz} + \widetilde{\gamma}_{Xz} \leq 1 \tag{6}$$

$$\widetilde{\alpha}_{Yz} + \widetilde{\beta}_{Yz} + \widetilde{\gamma}_{Zz} \leq 1 \tag{7}$$

▶ **Lemma 26.** *For any $z \in [N]$, out of the 6 variables $\widetilde{\alpha}_{Xz}, \widetilde{\beta}_{Xz}, \widetilde{\gamma}_{Xz}, \widetilde{\alpha}_{Yz}, \widetilde{\beta}_{Yz}, \widetilde{\gamma}_{Yz}$, let H be the set of those variables that are nonzero. Then H is a subset of at least one of the following sets of variables:*

$$\{\widetilde{\alpha}_{Xz}, \widetilde{\alpha}_{Yz}\}, \{\widetilde{\beta}_{Xz}, \widetilde{\beta}_{Yz}\}, \{\widetilde{\gamma}_{Xz}, \widetilde{\gamma}_{Yz}\}, \{\widetilde{\alpha}_{Xz}, \widetilde{\beta}_{Xz}, \widetilde{\gamma}_{Xz}\}, \{\widetilde{\alpha}_{Yz}, \widetilde{\beta}_{Yz}, \widetilde{\gamma}_{Yz}\}$$

Proof. It is a consequence of the easy observation that $\widetilde{\alpha}_{Xz}$ and $\widetilde{\beta}_{Yz}$ cannot both be nonzero (and 5 similar easy observations). ◀

Let

$$\delta_{Xz} = \begin{cases} 1 & \widetilde{\alpha}_{Yz}, \widetilde{\beta}_{Yz}, \widetilde{\gamma}_{Yz} > 0 \\ 0 & \text{otherwise} \end{cases}.$$

$$\delta_{Yz} = \begin{cases} 1 & \widetilde{\alpha}_{Xz}, \widetilde{\beta}_{Xz}, \widetilde{\gamma}_{Xz} > 0 \\ 0 & \text{otherwise} \end{cases}.$$

Note that δ_{Xz} depends on the projections in the Y direction (and vice versa). The reason for this definition is the following observation: if $\delta_{Xz} = 1$, then we have

$$A_{Xz} \cap B_{Xz} \cap C_{Xz} = A_{Xz} = B_{Xz} = C_{Xz} = [N], \tag{8}$$

and similarly, if $\delta_{Yz} = 1$, then we have

$$A_{Yz} \cap B_{Yz} \cap C_{Yz} = A_{Yz} = B_{Yz} = C_{Yz} = [N], \tag{9}$$

which is something that our set intersection lemma can exploit.

Define

$$\lambda_{Xz} = \widetilde{\alpha}_{Xz} + \widetilde{\beta}_{Xz} + \widetilde{\gamma}_{Xz} - \delta_{Xz},$$

$$\lambda_{Yz} = \widetilde{\alpha}_{Yz} + \widetilde{\beta}_{Yz} + \widetilde{\gamma}_{Yz} - \delta_{Yz}.$$

$$\lambda_z = \lambda_{Xz} + \lambda_{Yz}.$$

Note that by Equations (6), (7), for all z,

$$\lambda_{Xz} \leq 1. \tag{10}$$

$$\lambda_{Yz} \leq 1. \tag{11}$$

By the set intersection lemma,

$$|A_{Xz}| + |B_{Xz}| + |C_{Xz}| \geq 2N - \left(|\widetilde{A}_{Xz}| + |\widetilde{B}_{Xz}| + |\widetilde{C}_{Xz}|\right) + |A_{Xz} \cap B_{Xz} \cap C_{Xz}|$$
$$\geq (2 - \lambda_{Xz})N$$

Similarly,

$$|A_{Yz}| + |B_{Yz}| + |C_{Yz}| \geq (2 - \lambda_{Yz})N$$

Summing over $z \in [N]$ and adding these two equations, we get:

$$\Pi_{XZ}(A) + \Pi_{XZ}(B) + \Pi_{XZ}(C) \geq (2 - \mathbf{E}_z[\lambda_{Xz}])\, N^2, \tag{12}$$
$$\Pi_{YZ}(A) + \Pi_{YZ}(B) + \Pi_{YZ}(C) \geq (2 - \mathbf{E}_z[\lambda_{Yz}])\, N^2, \tag{13}$$
$$\Pi_{XZ}(A) + \Pi_{XZ}(B) + \Pi_{XZ}(C) + \Pi_{YZ}(A) + \Pi_{YZ}(B) + \Pi_{YZ}(C) \geq (4 - \mathbf{E}_z[\lambda_z])\, N^2. \tag{14}$$

Our goal is now to get an upper bound on $\mathbf{E}_z[\lambda_z]$.

To get our main result, we will show that $\mathbf{E}_z[\lambda_z] \leq \lambda^* := 4 - 6\eta_0 \approx 0.856$ (or else we find a large projection in some other way). This will show that one of the 6 projections on the left hand side is at least $\eta_0 N^2$, as desired.

If we just want to get a projection of size $\geq \frac{1}{2}N^2$, then it suffices to show that $\lambda^* \leq 1$, and this turns out to be simpler.

Towards that end, we define α_X to be the fraction of x for which $\{x\} \times [N] \subseteq \Pi_{XY}(A)$. Similarly define $\alpha_Y, \beta_X, \beta_Y, \gamma_X, \gamma_Y$.

Note that since $\widetilde{A}_{Xz} \times [N] \times \{z\} \subseteq A$, we have:

$$\alpha_{Xz} \leq \alpha_X,$$

and 5 similar inequalities.

Note that $\alpha_X \leq \eta$, and 5 similar inequalities.

Define $u : [0,1] \to [0,2]$ by:

$$u(a) = 2 - 2\sqrt{1-a}.$$

Using the argument used to arrive at Equation (4) (by the AM-GM inequality), we have

$$\widetilde{\alpha}_{Xz} + \widetilde{\alpha}_{Yz} \leq u(\eta_0) \qquad (\text{ and thus } \alpha_X + \alpha_Y \leq u(\eta_0)\ ).$$

and 2 similar pairs of inequalities.

Let $g_X = \max\{\alpha_X + \beta_X, \beta_X + \gamma_X, \alpha_X + \gamma_X\}$., similarly q_Y.

By the inequalities above, we have: $g_X + g_Y \leq 2\eta_0 + u(\eta_0)$.

Now let $q_X = \Pr_{z\in[n]}[\text{exactly two of } \alpha_{Xz}, \beta_{Xz}, \gamma_{Xz} \text{ are nonzero}]$, similarly define q_Y.

$$q = \Pr_{z\in[n]}[\text{at most one of } \alpha_{Xz}, \beta_{Xz}, \gamma_{Xz} \text{ and at most one of } \alpha_{Yz}, \beta_{Yz}, \gamma_{Yz} \text{ is nonzero}]$$

We are now in a position to state a key lemma which will prove our lower bound:

▶ **Lemma 27.**

$$\mathbf{E}_z[\lambda_z] \leq q \cdot u(\eta_0) + q_X \cdot \min(g_X, 1) + q_Y \cdot \min(g_Y, 1)).$$

Proof. Let $z \in [N]$. We take cases on which of the 6 numbers $\widetilde{\alpha}_{Xz}, \widetilde{\beta}_{Xz}, \widetilde{\gamma}_{Xz}, \widetilde{\alpha}_{Yz}, \widetilde{\beta}_{Yz}, \widetilde{\gamma}_{Yz}$ are nonzero. By Lemma 26, there only a few cases to consider.

- If the first three numbers are nonzero or the second three numbers are nonzero, then λ_z is nonpositive because the sum of those three is at most 1 (by Equations (6), (7), and $\delta_{Xz} = 1$ or $\delta_{Yz} = 1$.
- If exactly two of the first three numbers are nonzero, then λ_z is at most $\min(g_X, 1)$. This happens for q_X fraction of the z's.
- If exactly two of the second three numbers are nonzero, then λ_z is at most $\min(g_Y, 1)$. This happens for q_Y fraction of the z's
- If at most one of the first three numbers and at most one of the second three numbers is nonzero, then λ_z is at most $2 - 2\sqrt{1-\eta_0}$. This happens for q fraction of the z's. ◀

Now $q+q_X+q_Y \leq 1$. At this point, we already see that $\mathbf{E}_z[\lambda_z] \leq 1$ (since $u(\eta_0) \approx 0.6237 \leq 1$), and this gives us the result that some projection has size at least $\frac{1}{2}N^2$.

To get our improved bound of $\eta_0 N^2$, we need one more idea.

▶ **Lemma 28.** *$q_X + \mathbf{E}_z[\lambda_{Yz}] \leq 1$ and $q_Y + \mathbf{E}_z[\lambda_{Xz}] \leq 1$*

Proof. We prove the first inequality, the second being similar. q_X is the fraction of z for which exactly two of $\{\widetilde{\alpha}_{Xz}, \widetilde{\beta}_{Xz}, \widetilde{\gamma}_{Xz}\}$ are nonzero. For such a z, we have $\widetilde{\alpha}_{Yz} = \widetilde{\beta}_{Yz} = \widetilde{\gamma}_{Yz} = \delta_{Yz} = 0$, and thus $\lambda_{Yz} = 0$. Along with Equations (10), (11), this completes the proof. ◀

By Equation (12), if $\mathbf{E}_z[\lambda_{Xz}]$ is at most $2 - 3\eta_0$, then we get a projection onto the XZ plane of size at least $\eta_0 N^2$, and we are done. Similarly, by Equation (13), if $\mathbf{E}_z[\lambda_{Yz}]$ is at most $2 - 3\eta_0$, then we get a projection onto the YZ plane of size at least $\eta_0 N^2$, and we are done. Thus we may assume that both $\mathbf{E}_z[\lambda_{Xz}]$ and $\mathbf{E}_z[\lambda_{Yz}]$ are at least $2 - 3\eta_0$.

By the previous lemma, we thus get that $q_X, q_Y \leq 3\eta_0 - 1$. Summarizing everything we know: $g_X + g_Y \leq 2\eta_0 + u(\eta_0)$, $q_X, q_Y \leq 3\eta_0 - 1$. and $q + q_X + q_Y \leq 1$. Under these constraints, we claim that: $q \cdot u(\eta_0) + q_X \cdot \min(g_X, 1) + q_Y \cdot \min(g_Y, 1) \leq \lambda^*$. By inspection, we see that the LHS is maximized when:

$$g_X = 1, q_X = 3\eta_0 - 1, q = 1 - q_X = 2 - 3\eta_0,$$

which makes it evaluate to:

$$(2 - 3\eta_0) \cdot u(\eta_0) + (3\eta_0 - 1) = \frac{1}{6}(4 - \eta_0) = \lambda^*,$$

where the first equality is the defining equation of η_0, and the second equality is the definition of λ^*. This completes the proof. ◀