Mathematika 65 (2019) 950–957 © 2019 University College London
doi:10.1112/S0025579319000238

AN EXPLICIT TWO-SOURCE EXTRACTOR WITH MIN-ENTROPY RATE NEAR 4/9

MARK LEWKO

Abstract. In 2005 Bourgain gave the first explicit construction of a two-source extractor family with min-entropy rate less than $1/2$. His approach combined Fourier analysis with innovative but inefficient tools from arithmetic combinatorics and yielded an unspecified min-entropy rate which was greater than 0.499. This remained essentially the state of the art until a 2015 breakthrough by Chattopadhyay and Zuckerman in which they gave an alternative approach which produced extractors with arbitrarily small min-entropy rate. In the current work, we revisit the Fourier analytic approach. We give an improved analysis of one of Bourgain's extractors which shows that it in fact extracts from sources with min-entropy rate near $\frac{21}{44} = 0.477\ldots$. Moreover, we construct a variant of this extractor which we show extracts from sources with min-entropy rate near $4/9 = 0.444\ldots$. While this min-entropy rate is inferior to Chattopadhyay and Zuckerman's construction, our extractors have the advantage of exponential small error, which is important in some applications. The key ingredient in these arguments is recent progress connected to the restriction theory of the finite field paraboloid by Rudnev and Shkredov. This in turn relies on a Rudnev's point–plane incidence estimate, which in turn relies on Kollár's generalization of the Guth–Katz incidence theorem.

§1. *Introduction.* A well-known probability puzzle asks how to simulate a fair coin toss given a coin with unknown bias. A solution, due to von Neumann [**21**], is to flip the coin twice and if the flips disagree use the first, otherwise flip twice again and repeat. We leave it to the reader to verify that this algorithm does in fact solve the problem. The purpose of extractors in theoretical science is to address a similar problem: given the output of a random variable/source with unknown biases, subject to only some weak assumptions, use these outputs to simulate a random variable with much stronger (more uniform) randomness properties.

We say that a real-valued random variable $X : \Omega \to R$ has min-entropy k if $\sup_{r\in R} \mathbb{P}[X = r] \leqslant 2^{-k}$. Given random variables X and Y, we define the statistical distance between them as

$$\mathrm{SD}(X, Y) := \frac{1}{2}\sum_{r\in R} |\mathbb{P}[X = r] - \mathbb{P}[Y = r]|.$$

We call a family of maps $\mathrm{Ext}_N : [N] \times [N] \to \{0, 1\}$ an extractor family with min-entropy ρ if there exists a fixed $\delta > 0$ such that for any independent random

Received 24 April 2018, published online 24 July 2019.
MSC (2010): 65T50, 97K20, 97P20 (primary).

https://doi.org/10.1112/S0025579319000238 Published online by Cambridge University Press

variables $X, Y : \Omega \to [N]$ with min-entropy rate $\rho \log_2 N$ one has

$$\mathrm{SD}(\mathrm{Ext}_N(X, Y), U) \lesssim \log^{-\delta} N,$$

where U is the uniform distribution on $\{0, 1\}$. To ease notation, we will say that Ext_N is an extractor family with min-entropy rate *near* ρ if it extracts from all sources with min-entropy rate $\rho' > \rho$. We will say that Ext_N has exponentially small error if one has the stronger estimate

$$\mathrm{SD}(\mathrm{Ext}_N(X, Y), U) \lesssim N^{-\delta}$$

for some fixed $\delta > 0$.

Remark 1. The computer science literature typically considers maps from $\{0, 1\}^\ell \times \{0, 1\}^\ell \to \{0, 1\}$ when defining extractors. One can convert to this regime by taking $\ell = \lceil 2 \log p \rceil$.

There are a number of elementary constructions of extractor families with min-entropy rate greater than $1/2$. In 2005, Bourgain [1] gave the first explicit constructions of an extractor with min-entropy rate less than $1/2$. His proof depended on the finite field Szemerédi–Trotter theorem [2] and gave an unspecified min-entropy rate. An optimization of the key ingredient, the Szemerédi–Trotter incidence theorem, by Helfgott and Rudnev [7] in 2010 gave an exponent $\frac{3}{2} - \frac{1}{10\,678}$ in that result. Combined with Bourgain's method in the form below, this gives a min-entropy rate estimate of $\frac{16\,017}{32\,036} = 0.49996\ldots$. The incidence estimate was further refined by Jones in 2011 who gave an incidence estimate with exponent of $\frac{3}{2} - \frac{1}{622} = \frac{496}{331}$ which gives a min-entropy rate of around $\frac{2647}{5296} = 0.4998\ldots$. More recently, Stevens and de Zeeuw [19] introduced several new ideas which allowed them to improve the exponent in the incidence theorem to $\frac{3}{2} - \frac{1}{30} = \frac{22}{15}$. This yields an extractor with min-entropy rate near $\frac{45}{92} = 0.489\ldots$. Lastly, we note that an optimal Szemerédi–Trotter theorem in finite fields with exponent $4/3$ would imply Bourgain's extractor has min-entropy rate near $\frac{9}{20} = 0.45$, following the initial approach of [1]. See also [6] for generalizations of Bourgain's work.

In a 2015 breakthrough paper, Chattopadhyay and Zuckerman [4] gave an alternative approach which produced explicit extractors which extract from sources with arbitrarily small (in fact poly-logarithmic) min-entropy rate. One advantage to Bourgain's Fourier analytic constructions is that these extractors have exponentially small error, where Chattopadhyay and Zuckerman's only have poly-logarithmically small error. Finding explicit constructions with both an arbitrarily small min-entropy rate and exponentially small error remains an important open problem in the field. Our interest here is in showing how one can push Bourgain's Fourier analytic approach further using recent advances in finite field incidence geometry. This allows us to produce explicit constructions with exponentially small error and a lower min-entropy rate than available in the prior literature.

https://doi.org/10.1112/S0025579319000238 Published online by Cambridge University Press

We start by recalling one of Bourgain's constructions. Let F be a prime order finite field. Given an element $x \in F$, we let $\sigma(x) \in [0, (p-1)/p]$ denote the real numbers in the interval $[0, 1]$ given by considering the integer representation of x between 0 and $p-1$ and dividing that number by p. Moreover, we let $\rho : F \to \{0, 1\}$ be defined by $\rho(x) := \operatorname{sign} \sin(2\pi\sigma(x))$, where we adopt the convention that $\operatorname{sign}(0) = 1$. We take $N = p^2$ and consider the maps Ext_{p^2} from $F^2 \times F^2 \to \{0, 1\}$ given by

$$(x, y) \to \rho(x \cdot y + x \cdot x \times y \cdot y).$$

If p is chosen so that there does not exist an element $i \in F$ such that $i^2 = -1$, then the map just defined is a Bourgain extractor. Our first result is a refined analysis of one of Bourgain's extractors.

THEOREM 2. *Bourgain's extractor (for F a prime order finite field in which -1 is not a square) defined above extracts from two independent sources with min-entropy rate near $\frac{21}{44} = 0.477\ldots$ and has exponentially small error.*

Next we show that one can construct extractors with lower min-entropy rate by replacing F^2 in Bourgain's construction with F^3.

THEOREM 3. *Let F be finite field of order p and identify $[N] = F^3$. Then the map $\operatorname{Ext}_{p^3}(x, y) \to \rho(x \cdot y + x \cdot x \times y \cdot y)$ from $F^3 \times F^3 \to \{0, 1\}$ is a two-source extractor with min-entropy rate near $\frac{4}{9} = 0.444\ldots$ and has exponentially small error.*

We note that Bourgain's extractor requires one to restrict to prime order fields in which -1 is not a square, while this hypothesis on the prime order field in Theorem 3. In Bourgain's case, if F is such that there exists an $i \in F$ such that $i^2 = -1$ then the the zero set of $z := \{x \in F^2 : \sigma(x) = 0\}$ contains the line $\{(t, it) : t \in F\} \subset F^2$ and the required additive energy will not hold for certain subsets of this line. In the second case, the analogous level set will contain a line regardless of the field. However, to prove Theorem 3 one only needs control of the additive energy for sets substantially larger than that of a line. This phenomenon is explained by the theory of quadratic forms in finite fields, and is discussed in detail in [**12**] and also is connected to the recent observation that one can obtain sharp L^2 restriction theorems for the finite field paraboloid in high dimensions while the analogous problem remains open in three dimensions. See [**8**] and [**18**].

The proofs proceed by observing that Bourgain's argument can be extended to a rather general statement relating extraction properties of certain maps to the additive energy of certain subsets in finite fields. Lemmas 4 and 6 below articulate this generalization. The second step is to observe that these statements reduce the maps above to additive energy estimates for subsets of the paraboloid obtained by Rudnev and Shkredov [**18**] in their recent work on the finite field restriction problem. See [**8**, **11**–**13**], and [**15**] for a discussion of this problem.

https://doi.org/10.1112/S0025579319000238 Published online by Cambridge University Press

Finally we remark that inserting an optimal finite field Szemerédi–Trotter theorem into the Rudnev–Shkredov [18] machinery yields an additive energy estimate which when inserted into the machinery below shows that Bourgain's extractor defined above extracts from sources with min-entropy rate near $3/8 = 0.375$.

§2. *Notation and preliminaries.* We will use R and C to denote the fields of real and complex numbers, respectively. We will use F to denote a finite field, which will always be of prime order. We denote the non-zero elements of F by F_*. As usual, we write the additive character on F as $e(x) := \mathrm{e}^{2\pi \mathrm{i} x/p}$. Given $x, y \in F^n$, we write $x \cdot y := x_1 y_1 + \cdots + x_n y_n$. Given a subset $A \in F^n$, we define the additive energy

$$\Lambda(A) := \sum_{\substack{a+b=c+d \\ a,b,c,d \in A}} 1 = \sum_{x \in F^n} \Big(\sum_{\substack{a+b=x \\ a,b \in A}} 1 \Big)^2.$$

Parseval's identity is the equality

$$\sum_{x \in F^n} \Big| \sum_{\xi \in F^n} f(\xi) e(x \cdot \xi) \Big|^2 = |F| \sum_{\xi \in F^n} |f(\xi)|^2.$$

If f is a real- or complex-valued function on a domain D we define $\|f\|_{\ell^\infty} := \sup_{x \in D} |f(x)|$. We will write $X \sim Y$ to indicate that $Y/2 \leqslant X \leqslant 2Y$. Typically we use this to select a level set of a function. For example $D_\lambda := \{x \in D : f(x) \sim \lambda\}$ would denote the elements of the domain, D, of f where $\lambda/2 \leqslant f(x) \leqslant 2\lambda$. We will also use the notation $a \lesssim b$ to indicate that the inequality $a \leqslant cb$ holds with some universal constant c. Let F^d denote the d-dimensional vector space over F. We define the d-dimensional paraboloid $P_d \subset F^d$ by $P_d := \{(\underline{x}, \underline{x} \cdot \underline{x}), \underline{x} : F^{d-1}\}$.

§3. *Estimates.* We start by showing how Fourier analytic estimates imply extractor-type properties. Recall that the Fourier coefficients in the expansion $\operatorname{sign} \sin(x) = \sum_{\xi \in F} c(\xi) e(\xi x)$ satisfy

$$\sum_{\xi \in F} |c(\xi)| \lesssim \log |F|. \tag{1}$$

This can be seen from a simple and direct computation with the Dirichlet kernel; see [1, Remark 3.3].

LEMMA 4. *Let $f : F^n \times F^n \to F$ be a family of maps indexed by F, such that the following holds. For some fixed $\delta > 0$, one has for all functions $a, b : F^n \to F$ with $\|a\|_{\ell^\infty}, \|b\|_{\ell^\infty} \leqslant 1$ with respective supports $A, B \in F^n$ satisfying $|A|, |B| \geqslant |F|^{n\rho}$ that*

$$\max_{\lambda \in F_*} \Big| \sum_{x \in A, y \in B} a(x) b(y) e(\lambda f(x, y)) \Big| \lesssim |F|^{-\delta} |A||B|.$$

https://doi.org/10.1112/S0025579319000238 Published online by Cambridge University Press

Then the family of maps $\rho(f(x,y))$ from $F^n \times F^n \to \{0,1\}$ is a two-source extractor family with min-entropy rate near ρ.

Proof. Let U denote the uniform distribution on $\{0,1\}$. Our goal is to show $\mathrm{SD}(\rho(f(x,y)),U) \leqslant |F|^{-\delta}$ for some $\delta > 0$. Let X and Y denote independent random variables with min-entropy k and probability mass functions A and B, respectively. Let $J' : F \times F \to \{0,1\}$ denote the probability mass function of $\rho(f(x,y))$, that is, $J'(x) := \mathbb{P}[\rho(f(x,y)) = x]$ and $J(x) = J'(x) - 2^{-1}$. We then have

$$\mathrm{SD}(\rho(f(x,y)),U) = \frac{1}{2}\sum_{x\in\{0,1\}} |J(x)|.$$

Expanding in a Fourier series $\operatorname{sign}\sin x = \sum_{\lambda\in F} c(\lambda)e(\lambda x)$, and applying the estimate (1), we have that the above is

$$\begin{aligned}\lesssim |\mathbb{E}\rho(f(x,y))| &= \left|\sum_{x\in F^n}\sum_{y\in F^n}\sum_{\lambda\in F} A(x)B(y)c(n)e(\lambda f(x,y))\right| \\ &\lesssim \log|F| \max_{\lambda\in F_*}\left|\sum_{y\in F^n}\sum_{x\in F} A(x)B(y)e(\lambda f(x,y))\right|.\end{aligned}$$

The min-entropy assumption implies that $A(x), B(x) \leqslant |F|^{-\eta}$. Let $S_\theta := \{x \in F^n : A(x) \sim \theta\}$, and similarly $W_\theta := \{x \in F^n : B(x) \sim \theta\}$. Now we split $A(x)$ and $B(y)$ into $O(\log|F|)$ level sets such that $A_\ell(x) = A(x) \sim 2^{-\ell}$ and $B_\ell(x) = B(x) \sim 2^{-\ell}$ on their support which is at most 2^ℓ. From the hypotheses we may assume that $\ell \geqslant k$ and have

$$\begin{aligned}&\max_{\lambda\in F_*}\left|\sum_{x\in A, y\in B} A(x)B(y)e(\lambda f(x,y))\right| \\ &\quad\leqslant \sum_{i,j=k}^{\log|F|}\max_{\lambda\in F_*}|A_i(x)B_j(y)e(\lambda f(x,y))| \\ &\quad\lesssim |F|^{-\delta}\sum_{i,j=k}^{\log|F|} 2^{-i-j}|\mathrm{supp}(A_i)||\mathrm{supp}(B_j)| \lesssim |F|^{-\delta}\log|F|.\end{aligned}$$

This completes the proof. □

Remark 5. The above argument is a special case of what is called Vazirani's XOR lemma in the computer science literature. See [**16**, Lemma 4.1]. This lemma, which considers the more general case where the function ρ is replaced by a map into other finite abelian groups larger than $\{0,1\}$, allows one to use the methods presented here to obtain extractors that output more than one bit. We refer the reader to [**16**] and omit the routine details.

Next we show how to obtain estimates on exponential sums of the form appearing in the statement of Lemma 4.

https://doi.org/10.1112/S0025579319000238 Published online by Cambridge University Press

LEMMA 6. *Let $A, B \subseteq F^n$ and a, b be functions on A and B, respectively, such that $\|a\|_{\ell^\infty}, \|b\|_{\ell^\infty} \leqslant 1$. Then*

$$\max_{\lambda \in F_*} \left| \sum_{x \in A, b \in B} a(x)b(y)e(\lambda x \cdot y) \right| \leqslant |A|^{1/2}|B|^{1/2}|F|^{n/8}(\Lambda(A)\Lambda(B))^{1/8}.$$

Proof. By Cauchy–Schwarz,

$$\begin{aligned}
&\max_{\lambda \in F_*} \left| \sum_{x \in A, y \in B} a(x)b(y)e(\lambda x \cdot y) \right| \\
&\quad \leqslant |A|^{1/2} \max_{\lambda \in F_*} \left(\sum_{x \in A} \left| \sum_{y \in B} a(x)b(y)e(\lambda x \cdot y) \right|^2 \right)^{1/2} \\
&\quad = |A|^{1/2} \max_{\lambda \in F_*} \left(\sum_{x \in A} \sum_{y_1, y_2 \in B} a(x)b(y_1)b(y_2)e(\lambda x \cdot (y_1 - y_2)) \right)^{1/2} \\
&\quad \leqslant |A|^{1/2}|B|^{1/2} \\
&\qquad \times \max_{\lambda \in F_*} \left(\sum_{x_1, x_2 \in A} \sum_{y_1, y_2 \in B} a(x_1)a(x_2)b(y_1)b(y_2)e(\lambda(x_1 - x_2) \cdot (y_1 - y_2)) \right)^{1/4}.
\end{aligned}$$

Now, for $\xi, \eta \in F^n$, let

$$\begin{aligned}
\mathcal{A}_\lambda(\xi) &= \sum_{\substack{x_1, x_2 \in A \\ x_1 - x_2 = \lambda^{-1}\xi}} a(x_1)a(x_2), \\
\mathcal{B}(\eta) &= \sum_{\substack{y_1, y_2 \in B \\ y_1 - y_2 = \eta}} a(x_1)a(x_2),
\end{aligned}$$

where we let $\mathcal{A}(\xi) := \mathcal{A}_1(\xi)$. With this notation, we may rewrite the above as

$$\begin{aligned}
&\leqslant |A|^{1/2}|B|^{1/2} \max_{\lambda} \left(\sum_{\xi, \eta \in F^n} \mathcal{A}_\lambda(\xi)\mathcal{B}(\eta)e(\xi \cdot \eta) \right)^{1/4} \\
&\leqslant |A|^{1/2}|B|^{1/2} \left(\left(\sum_{\xi \in F^n} |\mathcal{A}(\xi)|^2 \right)^{1/2} \left(\sum_{\xi \in F^n} \left| \sum_{\eta \in F^n} \mathcal{B}(\eta)e\left(\xi \cdot \eta\right) \right|^2 \right)^{1/2} \right)^{1/4}.
\end{aligned}$$

Applying Parseval and noting that $\sum_{\xi \in F^n} |\mathcal{A}(\xi)|^2 \leqslant \Lambda(A)$ gives

$$\leqslant |A|^{1/2}|B|^{1/2}|F|^{n/8}(\Lambda(A)\Lambda(B))^{1/8}.$$

This completes the proof. □

Remark 7. The referee has pointed out that nearly the same lemma appears in [3].

https://doi.org/10.1112/S0025579319000238 Published online by Cambridge University Press

Combining Lemmas 4 and 6 gives us the following proposition.

PROPOSITION 8. *Let $n > d$ and $M : F^d \to F^n$. Let $\eta > 0$ and assume that for every subset $A \subseteq F^d$ with $|A| \sim |F|^{n/(8-2\alpha)}$ one has the energy estimate $\Lambda(M(A)) \lesssim |A|^\alpha$. Then the map $(x, y) \to \rho(M(x) \times M(y))$ is an extractor with min-entropy rate near $n/d(8 - d\alpha)$.*

At this point we state the following additive energy estimates of Rudnev and Shkredov [**18**] for subsets of the three-dimensional and four-dimensional paraboloids, P_3 and P_4.

THEOREM 9. *We have the following additive energy estimates. Let F be a prime order field in which -1 is not a square. Let $A \subset P_3$ with $|A| \leqslant |F|^{26/21}$. Then*

$$\Lambda(A) \lesssim |A|^{17/7}.$$

Let F be an arbitrary prime order finite field. Let $B \subset P_4$ with $p^{4/3} \leqslant |B| \leqslant p^2$. Then

$$\Lambda(B) \lesssim |B|^{5/2}.$$

Inserting these estimates into Proposition 8 proves Theorems 2 and 3.

Note added. Recently the author has slightly improved the exponent in the first energy estimate above from $17/7$ to $99/41 + \epsilon$ for any $\epsilon > 0$. This improves the min-entropy rate of the respective extractor to near $123/260$ from $21/41$. See [**14**].

Acknowledgement. We thank David Zuckerman for comments on an earlier draft of this note.

References

1. J. Bourgain, More on the sum-product phenomenon in prime fields and its applications. *Int. J. Number Theory* **1**(1) (2005), 1–32.
2. J. Bourgain, N. Katz and T. Tao, A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.* **14**(1) (2004), 27–57.
3. J. Bourgain and M. Z. Garaev, On a variant of sum-product estimates and explicit exponential sum bounds in prime fields. *Math. Proc. Cambridge Philos. Soc.* **146** (2009), 1–21.
4. E. Chattopadhyay and D. Zuckerman, Explicit two-source extractors and resilient functions. *Proc. Symp. on the Theory of Computing (STOC 2016)*, ACM (2016), 670–683.
5. L. Guth and N. H. Katz, On the Erdös distinct distance problem in the plane. *Ann. of Math.* (2) **181**(1) (2015), 155–190.
6. N. Hegyvari and F. Hennecart, Explicit constructions of extractors and expanders. *Acta Arith.* **140** (2009), 233–249.
7. H. Helfgott and M. Rudnev, An explicit incidence theorem in F_p. *Mathematika* **57** (2011), 135–156.
8. A. Iosevich, D. Koh and M. Lewko, Finite field restriction estimates for the paraboloid in high even dimensions. *Preprint*, 2017, arXiv:1712.05549v1.
9. T. Jones, Further improvements to incidence and Beck-type bounds over prime finite fields. *Preprint*, 2012, arXiv:1206.4517.
10. J. Kollár, Szemerédi–Trotter-type theorems in dimension 3. *Adv. Math.* **271** (2015), 30–61.
11. A. Lewko and M. Lewko, Endpoint restriction estimates for the paraboloid over finite fields. *Proc. Amer. Math. Soc.* **140** (2012), 2013–2028.

https://doi.org/10.1112/S0025579319000238 Published online by Cambridge University Press

12. M. Lewko, Finite field restriction estimates based on Kakeya maximal operator estimates. *J. Eur. Math. Soc. (JEMS)*, to appear. Preprint, 2014, arXiv:1401.8011v5.
13. M. Lewko, New restriction estimates for the 3-d paraboloid over finite fields. *Adv. Math.* **270** (2015), 457–479.
14. M. Lewko, Counting rectangles and an improved restriction estimate for the paraboloid in F_p^3. *Preprint*, 2019, arXiv:1901.10085.
15. G. Mockenhaupt and T. Tao, Restriction and Kakeya phenomena for finite fields. *Duke Math. J.* **121**(1) (2004), 35–74.
16. A. Rao, An exposition of Bourgain's 2-source extractor, http://homes.cs.washington.edu/∼anuprao/pubs/bourgain.pdf.
17. M. Rudnev, On the number of incidences between planes and points in three dimensions. *Combinatorica* **38**(1) (2018), 219–254.
18. M. Rudnev and I. Shkredov, On the restriction problem for the discrete paraboloid in lower dimension. *Preprint*, 2018, arXiv:1803.11035.
19. S. Stevens and F. de Zeeuw, An improved point-line incidence bound over arbitrary fields. *Bull. Lond. Math. Soc.* **49** (2017), 842–858.
20. T. Tao and V. Vu, *Additive Combinatorics*, Cambridge University Press (Cambridge, 2006).
21. J. von Neumann, Various techniques used in connection with random digits. In *Monte Carlo Method* (*National Bureau of Standards Applied Mathematics Series* **12**) (eds A. S. Householder, G. E. Forsythe and H. H. Germond), U.S. Government Printing Office (Washington, DC, 1951), 36–38.

Mark Lewko,
New York,
NY 10017,
U.S.A.
E-mail: mlewko@gmail.com

https://doi.org/10.1112/S0025579319000238 Published online by Cambridge University Press