POLYNOMIAL CONFIGURATIONS IN SUBSETS OF RANDOM AND PSEUDO-RANDOM SETS

ELAD AIGNER-HOREV AND HIỆP HÀN

Abstract. We prove transference results for sparse random and pseudo-random subsets of $\mathbb{Z}_N$, which are analogous to the quantitative version of the well-known Furstenberg-Sárközy theorem due to Balog, Pintz, Pelikán, and Szemerédi.

In the dense case, Balog et al showed that there is a constant $C > 0$ such that for all integer $k \geq 2$ any subset of the first N integers of density at least $C(\log N)^{-\frac{1}{4}\log\log\log\log N}$ contains a configuration of the form $\{x, x+d^k\}$ for some integer $d > 0$.

Let $[\mathbb{Z}_N]_p$ denote the random set obtained by choosing each element from $\mathbb{Z}_N$ with probability p independently. Our first result shows that for $p > N^{-1/k+o(1)}$ asymptotically almost surely any subset $A \subset [\mathbb{Z}_N]_p$ (N prime) of density $|A|/pN \geq (\log N)^{-\frac{1}{5}\log\log\log\log N}$ contains the polynomial configuration $\{x, x+d^k\}$, $0 < d \leq N^{1/k}$. This improves on a result of Nguyen in the setting of $\mathbb{Z}_N$.

Moreover, let $k \geq 2$ be an integer and let $\gamma > \beta > 0$ be real numbers satisfying

$$\gamma + (\gamma - \beta)/(2^{k+1} - 3) > 1.$$

Let $\Gamma \subset \mathbb{Z}_N$ (N prime) be a set of size at least N^γ and linear bias at most N^β. Then our second result implies that every $A \subset \Gamma$ with positive relative density contains the polynomial configuration $\{x, x+d^k\}$, $0 < d \leq N^{1/k}$.

For instance, for squares, i.e., $k = 2$, and assuming the best possible pseudo-randomness $\beta = \gamma/2$ our result applies as soon as $\gamma > 10/11$.

1. Introduction

A classical result in additive combinatorics, proved independently by Sárközy [20] and Furstenberg [5], states in its qualitatively form that subsets of the first N integers with positive density contains a pair which differ by a perfect k-th power, i.e., a pair $\{x, x+d^k\}$ for some $d > 0$. Improving on [20, 5] it is shown by Pintz, Steiger, Szemerédi [18] and by Balog, Pintz, Pelikán, Szemerédi [1] that this conclusion already holds for sets of much smaller density.

Theorem 1. *There exists a constant $C > 0$ such that for all integer $k \geq 2$ and all sets $A \subset \{1, \ldots, N\}$ with density*

$$|A|/N \geq C(\log N)^{-\frac{1}{4}\log\log\log\log N}$$

there exist integers $x, d > 0$, such that $\{x, x+d^k\} \subset A$. □

To appreciate the bound in Theorem 1 we note it is conjectured the bound is not far from best possible and that the largest set without the configuration $x, x+d^k$ has size $\Omega(N^{1-\varepsilon})$ for all $\varepsilon > 0$. A construction due to Ruzsa [19] shows that this is

The second author was supported by FAPESP (Proc. 2010/16526-3).

true for $\varepsilon > 0.267$. Moreover, it is of interest to improve upon the constant $1/4$ in Theorem 1 (see [10]).

Of course the result also holds for the setting $\mathbb{Z}_N$ instead of $\{1, \dots, N\}$ and in this note we prove results analogous to Theorem 1 for $\mathbb{Z}_N$ with prime N. More precisely, we will study the case when the dense host $\{1, \dots, N\}$ or $\mathbb{Z}_N$ is replaced by sparse random subsets or by pseudo-random subsets of $\mathbb{Z}_N$ defined via small linear bias. These types of results are commonly called *transference* in which extremal results known for dense hosts are transferred or carried over to sparse hosts taken from a well-behaved universe like random or pseudo-random subsets of the original dense host.

For sparse random hosts transference has been studied extensively in the last decades and the recent breakthroughs [22, 3] (see also [12, 21]) led to a much better understanding of the subject.

First to extend Theorem 1 to random hosts were Hamel and Łaba [14]. Their result was improved by Nguyen [17] later on. Let $[\mathbb{Z}_N]_p$ denote the random set obtained by choosing each element from $\mathbb{Z}_N$ with probability p independently. Nguyen [17] proved that asymptotically almost surely (i.e. with probability tending to one as $N \to \infty$) every relatively dense subset of $[\mathbb{Z}_N]_p$ contains a configuration $\{x, x + d^k\}$ provided that $p > CN^{-1/k}$ for some constant $C = C(k)$. Up to the multiplicative constant C the bound on p is best possible. Again, the result in [17] is stated for $\{1, \dots, N\}$ instead of $\mathbb{Z}_N$. Concerning transference to random host we show the following.

Theorem 2. *N is prime For all integer $k \geq 2$ following holds asymptotically almost surely. Let $p > N^{-1/k} \exp\left((\log N)^{9/10}\right)$ and let $A \subset [\mathbb{Z}_N]_p$, N prime, be such that*

$$|A|/pN \geq (\log N)^{-\frac{1}{5}\log\log\log\log N}.$$

Then there exist $x \in \mathbb{Z}_N$ and an integer $0 < d \leq N^{1/k}$ such that $\{x, x + d^k\} \subset A$.

The proof of Theorem 2 relies on a result of the second author in [6] and is given in Section 2. Note that for $p = 1$ Theorem 2 essentially recovers the quantitative dense case, i.e., Theorem 1 [1]. Further, as $\exp\left((\log N)^{9/10}\right) \ll N^{\varepsilon}$ for all $\varepsilon > 0$ Theorem 2 shows that for essentially the same range of probability as in Nguyen's result [17], subsets of $[\mathbb{Z}_N]_p$ of quite smaller density than in [17] already span the desired polynomial configuration. Lastly, we note that for the density $(\log N)^{-\frac{1}{5}\log\log\log\log N} = 1/\omega(N)$ as in Theorem 2 the term $\exp\left((\log N)^{9/10}\right)$ cannot be improved to any function of the form $o(\omega(N))$. In particular, the condition on p in Theorem 2 cannot be improved to $p \gg N^{-1/k}$ as in Nguyen's result.

To see this suppose that Theorem 2 holds for $p = \gamma(N)N^{-1/k}\omega(N)$ with $\gamma(N) = o(1)$. Consider the two round exposure $[\mathbb{Z}_N]_{p_1} \cup [\mathbb{Z}_N]_{p_2} = [\mathbb{Z}_N]_p$ with $p_1 = \beta(N)N^{-1/k}$ for some function $o(1) = \beta(N) \gg \gamma(N)$. By Chernoff's bound asymptotically almost surely $[\mathbb{Z}_N]_{p_1}$ has size at least $p_1 N/2$. Further, by Markov's inequality asymptotically almost surely the number of configurations $\{x, x + d^k\}$, $0 < d \leq N^{1/k}$, in $[\mathbb{Z}_N]_{p_1}$ is $o(p_1 N)$. Thus by deleting at most one element for each configuration $\{x, x + d^k\}$ we obtain a subset of $[\mathbb{Z}_N]_{p_1} \subset [\mathbb{Z}_N]_p$ which does not contain the configuration $\{x, x + d^k\}$ and which has size at least $p_1 N/4 = \beta(N)N^{1-1/k}/4 \gg$

[1] Indeed, the constant $1/5$ can be improved to $1/4 + o(1)$ at the cost of $\exp\left((\log N)^{9/10}\right)$ changing to $\exp\left((\log N)^{1-o(1)}\right)$, but we state this version for simplicity.

$2\gamma(N)N^{1-1/k} = 2pN/\omega(N)$. As $[\mathbb{Z}_N]_p$ has size at most $2pN$ asymptotically almost surely we obtain a contradiction to the fact that Theorem 2 holds for $p = \gamma(N)N^{-1/k}\omega(N)$.

As the second part, and the main objective of this paper, we show a transference result of Theorem 1 for pseudo-random host. It is interesting to note that Tao and Ziegler [24] proved that the polynomial Szemerédi theorem also holds in the primes. Their proof relies heavily on pseudo-random properties of the primes, thus, can be seen in the scheme mentioned above.

The notion of pseudo-randomness we shall rely on in this paper is a traditional one defined through small non-trivial Fourier coefficients. Transference problems with this notion of pseudo-randomness have been studied previously for Roth's theorem [9, 13, 4]. To our best knowledge, however, there is no result known concerning transference of the Furstenberg-Sarközy theorem to this pseudo-random setting and our next result, Theorem 3, shall give the first non-trivial bound.

Given a function $f : \mathbb{Z}_N \to \mathbb{C}$ the Fourier transform of f is defined to be the function

$$\widehat{f} : \widehat{\mathbb{Z}}_N \to \mathbb{C} \text{ given by } \widehat{f}(\xi) = \sum_{x\in\mathbb{Z}} f(x)e(-\xi x)$$

where $e(x) = e^{2\pi ix/N}$. The *linear bias* of f, denoted by $\|f\|_u$, is then given by

$$\|f\|_u = \sup_{\widehat{0}\neq\xi\in\widehat{\mathbb{Z}}_N} |\widehat{f}(\xi)|.$$

The result then reads as follows.

Theorem 3. *Let $k \geq 2$ be an integer and let $\gamma > \beta > 0$ be reals with*

$$\gamma + \frac{\gamma - \beta}{(2^{k+1} - 3)} > 1.$$

Then there is a function $\omega(N)$ with $\lim_{N\to\infty} \omega(N) = \infty$ such that the following holds. Let $\Gamma \subset \mathbb{Z}_N$ be such that

$$|\Gamma| \geq N^{\gamma} \quad \text{and} \quad \|\Gamma\|_u \leq N^{\beta},$$

and let $\alpha = \alpha(N) \geq (\log\log N)^{-\omega(N)}$. Then, every subset $A \subset \Gamma$ satisfying $|A| \geq \alpha|\Gamma|$ contains a pair $x, x + d^k$ for an integer $0 < d \leq N^{1/k}$.

Due to Parseval's equality the the parameter β in Theorem 3 controlling the pseudo-randomness of Γ satisfies $\beta \geq \gamma/2$. One may think of $\beta = \gamma/2$ as though Γ is "as pseudo-random as possible". In this case, i.e., $\beta = \gamma/2$, we have that Theorem 3 is applicable as long as $\gamma > 1 - \frac{1}{2^{k+2}-5}$.

The proof of Theorem 3 combines the techniques in [8] and an unpublished note of Green which investigates transference for Roth's theorem for pseudo-random setting. The latter is in flavor similar to Green's proof of Roth's theorem in the primes [9] and an important part of the argument relies on a discrete version of a restriction type result due to Tomas [25] (see Theorem 4).

Sketch of the proof of Theorem 3 and a restriction type theorem. For notational convenience we identify a set with its characteristic function, i.e., if $A \subset \mathbb{Z}_N$ then A also denotes a 0, 1-function with $A(x) = 1$ if and only if $x \in A$. Moreover, let $Q_k = \{x^k : 0 < x \leq N^{1/k}, x \text{ is integer }\}$ denote the set of kth powers. Given a sparse pseudo-random set $\Gamma \subset \mathbb{Z}_N$ and a subset $A \subset \Gamma$ with relative density

α (with respect to Γ) as in Theorem 3 we will bound $\sum_{x,d\in\mathbb{Z}_N} A(x)A(x+d)Q_k(d)$ from below as follows.

Using the "large" Fourier coefficients of A and Bohr sets we will construct a function $a : \mathbb{Z}_N \to \mathbb{R}^+$ which satisfies $\|a\|_1 \geq \alpha N$ and which is bounded from above, $\|a\|_\infty \leq 3$ (Lemma 11). Hence, the function a "resembles" a set in the dense setting and by a Varnavides' argument and Theorem 1 we then establish a lower bound on the of number of polynomial configurations "contained in a", i.e. a lower bound for $\sum_{x,d\in\mathbb{Z}_N} a(x)a(x+d)Q_k(d)$, (Lemma 7).

Under the assumption that $A \subset \Gamma$ does not satisfy the conclusion of the Theorems 3, we will exploit the close relationship of A and the function a to obtain an upper bound for the number of configurations "contained in a" which contradicts the lower bound mentioned above. The contribution of the large Fourier coefficients of A can be controlled by the properties of Bohr sets and the contribution of the remaining "small" Fourier coefficients will be controlled using the following restriction type theorem which is at heart of the approach.

Theorem 4. *Let $\gamma > \beta > 0$ and $p = \frac{2-2\beta}{\gamma-\beta}$ be fixed real numbers. Let $\Gamma \subset \mathbb{Z}_N$ with size $|\Gamma| \geq N^\gamma$ and linear bias $\|\Gamma\|_u \leq N^\beta$. Then for every $A \subset \Gamma$ we have*

$$\sum_{\xi\in\widehat{\mathbb{Z}}_N} |\widehat{A}(\xi)|^p \leq 2^p |A|^{p/2}|\Gamma|^{p/2}. \tag{1}$$

Theorem 4 is from an unpublished note of Green (see also [9] and [7]) and will be given in Section 7. It is a discrete version and a close adaptation of the restriction theorem due to Tomas [25]. It is even more closely related to the work of Mockenhaupt and Tao [15] and we refer to this work for further applications of restriction results.

2. Transference for random host – Proof of Theorem 2

In this section we prove Theorem 2. For an integer $k \geq 2$ recall that $Q_k = \{x^k \colon 0 < x \leq N^{1/k}, x \text{ is integer}\}$. Consider the graph $G = (\mathbb{Z}_N, E_k)$ with the vertex set $\mathbb{Z}_N$ in which we connect each $x \in \mathbb{Z}_N$ to $x + d$ for any $d \in Q_k$. Then a set $A \subset \mathbb{Z}_N$, which does not span the polynomial configuration $\{x, x + d\}$ with $d \in Q_k$, corresponds to an independent set in G. Theorem 1 then gives an upper bound on the size of the largest independent set in G and the proof of Theorem 2 will rely on the following related notion of largest almost independent set.

Definition 5. *Given constants $\alpha \in [0, 1]$, $\gamma \in [0, 1]$, and a graph G on N vertices. We say that G is a* (α, γ)-supersaturated *graph if for any subset $S \subset V(G)$ with*

$$e(S) \leq \gamma \left(\frac{|S|}{N}\right)^2 \cdot e(G),$$

we have $|S| \leq \alpha N$.

In addition, let $\alpha = \alpha(n) > 0$ and $\gamma = \gamma(n) > 0$. For a sequence of graphs $\mathbf{G} = \{G_n\}_{n\in\mathbb{N}}$, we say that $\mathbf{G}$ is (α, γ)-supersaturated *if there exists a constant $n_0 \in \mathbb{N}$ such that for every $n \geq n_0$, G_n is* $(\alpha(n), \gamma(n))$-supersaturated.

The following result is a direct consequence of Proposition 2.6 from [6].

Proposition 6 (Proposition 2.6 from [6])**.** *Let $\alpha = \alpha(n)$ and $\gamma = \gamma(n)$ be $(0, 1)$-valued functions, and let $\mathbf{G} = \{G_n\}_{n\in\mathbb{N}}$ be a sequence of (α, γ)-supersaturated*

graphs, in which each G_n has $N = N(n)$ vertices (with $\lim_{n\to\infty} N(n) = \infty$) and average degree $D = D(n)$. Further, let V_p denote the random vertex set obtained by choosing each vertex from $V = V(G_n)$ with probability p independently at random and let $H_n = G_n[V_p]$ denote the subgraph of G_n induced by the vertex set V_p. Then for $p = p(n) \gg (\alpha\gamma D)^{-1}\log^2(e/\alpha)$ asymptotically almost surely $\alpha(H_n) \le 2\alpha pN$ holds.

Proposition 2.6 from [6] is actually more precise but this is insignificant in our setting. We want to apply this proposition and by using Theorem 1 combined with a Varnavides type argument [26] we derive that the the graph $(\mathbb{Z}_N, E_k)$ is indeed supersaturated for suitable choice of parameters. We also establish the functional version which is needed for the proof of Theorem 3.

Lemma 7. *There exists a $c > 0$ such that for all $k \ge 2$, the following holds for sufficiently large N. Let $\omega(n) = \log\log\log\log n$ and let*

$$M : \mathbb{R} \to \mathbb{R} \text{ be given by } M(x) = \exp\left(x^{4.1/\log\log\log(x)}\right).$$

Suppose that $\alpha = \alpha(N)$ satisfies $c > \alpha \ge \frac{1}{2}(\log N)^{-\omega(N)/5}$. Then $M(1/\alpha) < \exp\left(\frac{1}{3}(\log N)^{9/10}\right)$ and for any set $A \subset \mathbb{Z}_N$ of size $|A| \ge \alpha N$ we have

$$\sum_{x,d\in\mathbb{Z}_N} A(x)A(x+d)Q_k(d) \ge \frac{\alpha}{2M(1/\alpha)^2} N|Q_k|. \tag{2}$$

In particular, if $c > \alpha \ge 3(\log N)^{-\omega(N)/5}$ and $a : \mathbb{Z}_N \to \mathbb{R}$ is a function with $\|a\|_1 \ge \alpha N$ and $\|a\|_\infty \le 3$ then

$$\sum_{x,d\in\mathbb{Z}_N} a(x)a(x+d)Q_k(d) \ge \frac{\alpha^3}{48M(6/\alpha)^2} N|Q_k|. \tag{3}$$

Moreover, let $N = N(n)$ be a sequence of increasing primes, then the graph sequence $\mathbf{G} = (G_n)_{n\in\mathbb{N}}$ with $G_n = (\mathbb{Z}_N, E_k)$ is $\big(\alpha, M(1/\alpha)^{-2}\big)$-supersaturated.

Proof. We first note that (3) and the last part of the lemma follow from (2). Indeed, from Definition 5 and (2) it is immediately seen that for $\alpha < 1/2$ we have that $\mathbf{G} = (G_n)_{n\in\mathbb{N}}$ is $\big(\alpha, M(1/\alpha)^{-2}\big)$-supersaturated. Moreover, for a function $a : \mathbb{Z}_N \to \mathbb{R}$ with $\|a\|_1 \ge \alpha N$ and $\|a\|_\infty \le 3$ consider the set $A = \{x\colon a(x) \ge \alpha/2\}$. Then we have $|A| \ge \alpha N/6$ since otherwise $\|a\|_1 < \|a\|_\infty \alpha N/6 + N\alpha/2 \le \alpha N$. With the just defined set A we then have

$$\sum_{x,d\in\mathbb{Z}_N} a(x)a(x+d)Q_k(d) \ge \frac{\alpha^2}{4} \sum_{x,d\in\mathbb{Z}_N} A(x)A(x+d)Q_k(d)$$

and (3) follows from (2).

To establish (2) we first apply Theorem 1 to obtain a constant C. Let $c > 0$ be sufficiently small and let N be sufficiently large for the calculations to hold. For a given α define $M = M_\alpha = M(1/\alpha)$ which is increasing in $1/\alpha$ if α is sufficiently small. Moreover,

$$\omega(M) = \log\log\log\log M = \log\log\left(\frac{4.1}{\log\log\log(1/\alpha)}\log\frac{1}{\alpha}\right) > 0.99\log\log\log\frac{1}{\alpha}.$$

For sufficiently α this implies

$$(\log M)^{\omega(M)/4} = \left(\left(\frac{1}{\alpha}\right)^{4.1/\log\log\log(1/\alpha)}\right)^{\omega(M)/4} \geq \left(\frac{1}{\alpha}\right)^{1.01} \geq \frac{3C}{\alpha}.$$

Consequently from the choice of the function ω and from Theorem 1 any subset of $[M] = \{1, 2, \ldots, M\}$ of density at least $\alpha/3 \geq C(\log M)^{-\omega(M)/4}$ contains a configuration $\{x, x+d\}$, $d \in Q_k$. We will use this to establish (2).

Let $A \subset \mathbb{Z}_N$ of size $|A| \geq \alpha N$ be given. Consider the $N|Q_k|$ progressions in $\mathbb{Z}_N$ given by $P(x,d) = \{x, x+d, \ldots, x+(M-1)d\}$ with $x \in \mathbb{Z}_N$ and $d \in Q_k$. Each progression has M elements since N is prime and we call such a progression good (with respect to A) if $|A \cap P(x,d)| \geq \alpha M/2$. For a fixed d note that $\sum_{x\in\mathbb{Z}_N} |A \cap P(x,d)| = |A|M$ and for fixed x and d we have $|A \cap P(x,d)| \leq M$. Hence, for a fixed d there are at least $|A|/2$ elements $x \in \mathbb{Z}_N$ such that $P(x,d)$ is a good progression. Consequently, with $|A| \geq \alpha N$ we conclude that there are at least $\alpha N|Q_k|/2$ good progressions in total.

We identify a good progression $P(x,d)$ with the interval $\{1, \ldots, M\}$ and recall that $\alpha M/2 > MC(\log M)^{-\omega(M)/4}$. By Theorem 1 we conclude that that each good progression contains a pair $\{x, x+d\} \subset A$, $d \in Q_k$. Moreover, each such pair $\{x, x+d\}$ is contained in at most M^2 progressions as a progression is determined after choosing the positions of $\{x, x+d\}$ in the progression. We obtain

$$\sum_{x,d\in\mathbb{Z}_N} A(x)A(x+d)Q_k(d) \geq \alpha N|Q_k|/2M^2,$$

as claimed.

It is left to show that $M = M(1/\alpha) < \exp\left(\frac{1}{3}(\log N)^{9/10}\right)$. Let $\alpha_0 = \frac{1}{2}(\log N)^{-\omega(N)/5}$ and let $M_0 = M(1/\alpha_0)$. As $M(1/\alpha)$ is increasing in $1/\alpha$ for small enough α, it suffices show that $M_0 \leq \exp\left(\frac{1}{3}(\log N)^{9/10}\right)$, equivalently, $\log M_0 \leq \frac{1}{3}(\log N)^{9/10}$. For sufficiently large N we have

$$\log M_0 = \left(\frac{1}{\alpha_0}\right)^{4.1/\log\log\log(1/\alpha_0)} = \left(2(\log N)^{\omega(N)/5}\right)^{4.1/\log\log\log(1/\alpha_0)}.$$

As $\log\log\log 1/\alpha_0 > \log\log\log\log N = \omega(N)$ we obtain $\log M_0 < 2(\log N)^{4.1/5} < \frac{1}{3}(\log N)^{9/10}$ for sufficiently large N. This finishes the proof. □

With Lemma 7 at hand we now prove Theorem 2.

Proof of Theorem 2. Let $N = N(n)$ be an increasing sequence of primes. Let $\mathbf{G} = \{G_n\}_{n\in\mathbb{N}}$ be a sequence of graphs with each $G_n = (\mathbb{Z}_N, E_k)$ be defined as above. In particular, G_n has $N = N(n)$ vertices and degrees $D = D(n) = |Q_k|$.

We apply Lemma 7 we obtain the constant $c > 0$. Let $\alpha > (\log N)^{-\frac{1}{5}\log\log\log\log N}$ be given. Due to monotonicity we may assume that $c > \alpha$ and let $\beta = \alpha/2 > \frac{1}{2}(\log N)^{-\log\log\log\log(N)/5}$. Lemma 7 then guarantees that the graph sequence $\mathbf{G}$ is (β, γ)-supersaturated with $\gamma = M_\beta^{-2} = \exp\left(-2(1/\beta)^{1/\log\log\log 1/\beta}\right)$.

By Proposition 6 we then derive that for any $p \gg (\beta\gamma D)^{-1}\log^2(e/\beta)$ asymptotically almost surely the largest independent set in $H_n = G_n[V_p]$ has size at most $2\beta pN = \alpha pN$.

Further, we have $\beta^{-1}\log^2 e/\beta \leq M_\beta$ and by Lemma 7 we also have $M < \exp\{\frac{1}{3}(\log N)^{9/10}\}$. Hence $(\beta\gamma D)^{-1}\log^2(e/\beta) \ll N^{-1/k}\exp\{(\log N)^{9/10}\}$. The theorem follows. □

3. Transference for pseudo-random host – Preliminaries

In this section we introduce the definitions and basic properties of discrete Fourier analysis and Bohr sets as well as the theorem of Hardy-Littlewood.

3.1. **Fourier analysis.** As shown in the introduction, for the purposes of Fourier analysis we endow $\mathbb{Z}_N$ with the counting measure and, consequently, endow its dual group $\widehat{\mathbb{Z}}_N$ with the uniform measure. As a result, the Fourier transform of a function $f : \mathbb{Z}_N \to \mathbb{C}$ is the function

$$\widehat{f} : \widehat{\mathbb{Z}}_N \to \mathbb{C} \text{ given by } \widehat{f}(\xi) = \sum_{x\in\mathbb{Z}} f(x)e(-\xi x)$$

where $e(x) = e^{2\pi ix/N}$.

Further, given $g : \mathbb{Z}_N \to \mathbb{C}$, let $f * g$ be the *convolution* of f and g defined by $f * g(x) = \sum_{y\in\mathbb{Z}_N} f(y)g(x-y)$. The basic properties of the Fourier transform then read as follows

- $f(x) = \frac{1}{N}\sum_{\xi\in\widehat{\mathbb{Z}}_N} \widehat{f}(\xi)e(\xi x)$ for all $x \in \mathbb{Z}_N$ (Inversion),
- $\sum_{x\in\mathbb{Z}_N} f(x)^2 = \frac{1}{N}\sum_{\xi\in\widehat{\mathbb{Z}}_N} \widehat{f}(\xi)^2$ (Parseval),
- $\widehat{f * g}(\xi) = \widehat{f}(\xi)\widehat{g}(\xi)$ (Convolution).

3.2. **Bohr sets.** Given a set $S \subset \widehat{\mathbb{Z}}_N$ and a real $0 \le \varrho \le 1$, let

$$B(S, \varrho) = \{y \in \widehat{\mathbb{Z}}_N : |\xi(y) - 1| \le \varrho, \text{for all } \xi \in S\}$$

denote the *Bohr set* with *frequency set* S, *rank* $|S|$, and *radius* ϱ. Then,

$$|B(S, \varrho)| \ge \varrho^{|S|}N \tag{4}$$

see, e.g. [23, Lemma 4.20].

A Bohr set $B(S, \varrho)$ is called *regular* provided

$$(1 - 100|S||\kappa|)|B(S, \varrho)| \le |B(S, (1 + \kappa)\varrho| \le (1 + 100|S||\kappa|)|B(S, \varrho)| \tag{5}$$

for all $|\kappa| \le 1/100|S|$.

Regular Bohr sets are "easily" found as suggested by the following.

Theorem 8. (see [2] or, e.g., [23, Lemma 4.25])
Let $S \subset \widehat{\mathbb{Z}}_N$ be nonempty and let $0 < \varepsilon < 1$. Then there exists a $\varrho \in [\varepsilon/2, \varepsilon]$ such that $B(S, \varrho)$ is regular. □

The following standard property of Bohr sets will be useful to us.

Proposition 9. *If $B = B(S, \varrho)$ and $\xi \in S$ then*

$$\left|1 - \frac{|\widehat{B}(\xi)|}{|B|}\right| \le \varrho.$$

Proof.

$$\begin{aligned}\left|1-\frac{|\widehat{B}(\xi)|}{|B|}\right| &= \left|\frac{|B|}{|B|}-\frac{1}{|B|}\sum_{x\in B}\xi(x)\right| \\ &= \frac{1}{|B|}\left||B|-\sum_{x\in B}\xi(x)\right| \\ &= \frac{1}{|B|}\left|\sum_{x\in B}(1-\xi(x))\right| \\ &\leq \frac{1}{|B|}\sum_{x\in B}|1-\xi(x)|\,.\end{aligned}$$

As $\xi \in S$ we have $|1-\xi(x)| \leq \varrho$ and the proposition follows. □

3.3. **Waring's problem.** Given positive integers s, k and n, let $r_{s,k}(n)$ to denote the number of solutions (in the integers) to the equation

$$x_1^k + \cdots x_s^k = n.$$

Then $r_{s,k}(n)$ can be expressed as an s-fold convolution of $Q_k = \{x^k \colon x \leq N^{1/k}, x \in \mathbb{Z}_N\}$ as follows

$$r_{s,k}(n) = \underbrace{Q_k * \cdots * Q_k}_{s-\text{times}}(n).$$

The following is a well-known result of Hardy and Littlewood [11] (see also [16], Theorem 5.7) solving a well-known problem of Waring.

Theorem 10. (Hardy-Littlewood [11]) *For every $s \geq 2^k - 1$ we have*

$$r_{s,k}(n) = \Theta(n^{s/k-1}).$$

4. Transference for pseudo-random host – A "dense" set model

As mentioned in the introduction we will construct a model for a given a subset $A \subset \Gamma$. This is established by the following lemma.

Lemma 11. *Let $\Gamma \subset \mathbb{Z}_N$ and for $\alpha = \alpha(N) > 0$, $\varepsilon = \varepsilon(N) > 0$ let $A \subset \Gamma$ with $|A| \geq \alpha|\Gamma|$ and let $\emptyset \neq S \subset \widehat{\mathbb{Z}}_N$ and $\varrho = \varrho(N) \in [\varepsilon/2, \varepsilon]$ be such that $B = B(S, \varrho)$ is a regular Bohr set. Then the function $a : \mathbb{Z}_N \to \mathbb{R}$ given by*

$$a(x) = \frac{N}{|\Gamma||B|}(A * B)(x)$$

satisfies:

1. *$\|a\|_1 \geq \alpha N$, and*
2. *if $|\Gamma|\|\Gamma\|_u^{-1} > 2(20|S|^{1/2}/\varepsilon)^{|S|}$, then $\|a\|_\infty \leq 3$.*

Proof. The property $\|a\|_1 \geq \alpha N$ is clear and we focus on proving $\|a\|_\infty \leq 3$. For given $S \subset \widehat{\mathbb{Z}_N}$ choose $\kappa = 1/(100|S|)$ and let $B_1 = B(S, (1+\kappa)\varrho)$ and $B_2 = B(S, \kappa\varrho)$, so that $B_2 \subset B \subset B_1$. Since $(B_1 * B_2)(x) \geq |B_2|$ for all $x \in B$ and $B \subset B_1$ the function $f(x) = (B_1 * B_2)(x)/|B_2|$ satisfies $f(x) \geq B(x)$ for all $x \in \mathbb{Z}_N$. Hence,

$A*B(x) \leq \Gamma * f(x)$, for every $x \in \mathbb{Z}_N$, and by Fourier-inversion and the convolution property we have

$$\begin{aligned} a(x) &\leq \frac{N}{|\Gamma||B|}(\Gamma * f)(x) = \frac{1}{|\Gamma||B|}\sum_{\xi\in\widehat{\mathbb{Z}_N}} \widehat{\Gamma}(\xi)\widehat{f}(\xi) \\ &= \frac{\widehat{\Gamma}(0)\widehat{f}(0)}{|B||\Gamma|} + \frac{1}{|\Gamma||B|}\sum_{\xi\in\widehat{\mathbb{Z}_N}\setminus\{0\}} \widehat{\Gamma}(\xi)\widehat{f}(\xi). \end{aligned}$$

By the convolution property $\widehat{f}(\xi) = \frac{|\widehat{B_1}(\xi)||\widehat{B_2}(\xi)|}{|B_2|}$, hence, using Cauchy-Schwarz and Parseval, we derive

$$\begin{aligned} a(x) \ &\leq \frac{|B_1|}{|B|} + \frac{\|\Gamma\|_u}{|\Gamma||B||B_2|}\sum_{\xi\in\widehat{\mathbb{Z}_N}} |\widehat{B_1}(\xi)||\widehat{B_2}(\xi)| \\ &\leq \frac{|B_1|}{|B|} + \frac{\|\Gamma\|_u}{|\Gamma||B||B_2|}\|\widehat{B_1}\|_2\|\widehat{B_2}\|_2 \\ &= \frac{|B_1|}{|B|} + N\frac{\|\Gamma\|_u}{|\Gamma|}\frac{|B_1|^{1/2}}{|B||B_2|^{1/2}} \end{aligned} \tag{6}$$

Using (5) and $|B_1|/|B| \leq 2$, which follows from the choice of κ, we obtain

$$a(x) \leq 2 + N\frac{\|\Gamma\|_u\sqrt{2}}{|\Gamma|(|B||B_2|)^{1/2}},$$

By (4) we conclude

$$(|B||B_2|)^{1/2} \geq N(\varrho\kappa^{1/2})^{|S|} \geq N(\varepsilon/(20|S|^{1/2}))^{|S|} > 2N\|\Gamma\|_u\|\Gamma|^{-1}.$$

Hence, $\|a\|_\infty \leq 3$, as required. □

We just showed that a sparse set A can be associated to a function a which behaves like a characteristic function of a dense set.

By (3) of Lemma 7 this function a "contains" many of the desired polynomial configurations, i.e. $\sum a(x)a(x+d)Q_k(d)$ is large. In the next section we shall work towards an upper bound for $\sum a(x)a(x+d)Q_k(d)$. Under the assumption that the sparse set A does not contain the desired configuration this upper bound will then yield a contradiction with (3).

5. Transference for pseudo-random host – An upper bound

In this section we use Theorem 4 and Theorem 10 to derive an upper bound for the contribution of the "small" Fourier coefficients. The method of using Theorem 10 to deal with the Fourier coefficients of Q_k was introduced in [8].

Lemma 12. *For all $k \geq 2$ there is a W such that for all $\gamma > 0$ and $\beta > 0$ satisfying*

$$1 + \frac{1}{(2^{k+1}-3)} \geq \frac{(1-\beta)}{(\gamma-\beta)}$$

the following holds. Let $\Gamma \subset \mathbb{Z}_N$ with be a set of size $|\Gamma| \geq N^\gamma$ with linear bias $\|\Gamma\|_u \leq N^\beta$. Let $\delta = \delta(N)$, $A \subset \Gamma$ and $S \subset \widehat{\mathbb{Z}}_N$ such that $\sup_{\xi\notin S}|\widehat{A}(\xi)| \leq \delta|\Gamma|$.

Then we have

$$\sum_{\xi\notin S}|\widehat{A}(\xi)|^2\widehat{Q}_k(\xi)\leq W\delta^{(2t-p)/t}N^{1/k}|\Gamma|^2. \tag{7}$$

Proof. Choose W such that $r_{t/2,k}(n)\leq (W/4)^{t/2}n^{t/2k-1}$; this is possible due to Theorem 10. Let $t=1+1/(2^{k+1}-3)$ and let $t'=t/(t-1)=2(2^k-1)$ be the dual index of t. By Hölder inequality applied with t and t' we have:

$$\sum_{\xi\notin S}|\widehat{A}(\xi)|^2\widehat{Q}_k(\xi)\leq\left(\sum_{\xi\notin S}|\widehat{A}(\xi)|^{2t}\right)^{1/t}\|\widehat{Q}_k\|_{t'}.$$

By Theorem 4 with $p=(2-2\beta)/(\gamma-\beta)$ and by the choice of t we have $2t>p$ and hence

$$\sum_{\xi\notin S}|\widehat{A}(\xi)|^{2t}\leq\sup_{\xi\notin S}|\widehat{A}(\xi)|^{2t-p}\sum_{\xi\notin S}|\widehat{A}(\xi)|^p\leq(\delta|\Gamma|)^{2t-p}(2|\Gamma|)^p.$$

Consequently, it suffices to show that

$$\|\widehat{Q}_k\|_{t'}\leq WN^{1/k}/4. \tag{8}$$

To this end, recall that the $(t'/2)$-fold convolution of Q_k coincide with $r_{t/2,k}$. Hence, by appealing to the convolution property, Parseval and Theorem 10 we obtain

$$\begin{aligned}\sum_{\xi\in\widehat{\mathbb{Z}_N}}|\widehat{Q}_k(\xi)|^{t'}&=\sum_{\xi\in\widehat{\mathbb{Z}_N}}\left(\widehat{Q}_k(\xi)^{t'/2}\right)^2\\&=\sum_{\xi\in\widehat{\mathbb{Z}_N}}\left(\widehat{Q}_k*\cdots*\widehat{Q}_k(\xi)\right)^2\\&\leq N\sum_{n\in\mathbb{Z}_N}\left(Q_k*\cdots*Q_k(n)\right)^2\\&\leq N^2(W/4)^{t'}N^{t'/k-2}\leq(W/4)^{t'}N^{t'/k}.\end{aligned}$$

□

6. Transference for pseudo-random host – Proof of Theorem 3

We are now in the position to prove Theorem 3.

Proof of Theorem 3. For given $k\geq 2$ let W be the constant obtained by applying Lemma 12 with k. Let $\gamma>\beta>0$ be such that

$$\gamma+\frac{\gamma-\beta}{2^{k+1}-3}>1\qquad\text{and let}\qquad t=1+\frac{1}{(2^{k+1}-3)}\qquad\text{and}\qquad p=\frac{2-2\beta}{\gamma-\beta}.$$

Then $p<2t$, thus, $p<4$ and $t/(2t-p)$ is a constant depending on γ,β and k but independent of N.

For $\omega(N)=\frac{1}{10}\log\log\log\log\log N$ let $\alpha=\alpha(N)>(\log\log N)^{-\omega(N)}$. We may further assume that α is sufficiently small for the calculations to hold (say $\alpha<c$ for some constant $c>0$). Let

$$M(1/\alpha)=\exp\{(1/\alpha)^{4.1/\log\log\log(1/\alpha)}\}$$

and recall from (3) of Lemma 7 that any function $a : \mathbb{Z}_N \to \mathbb{R}$ with $\|a\|_1 \geq \alpha N$ and $\|a\|_\infty \leq 3$ satisfies

$$\sum_{x,d\in\mathbb{Z}_N} a(x)a(x+d)Q_k(d) \geq \frac{\alpha^3}{48M(6/\alpha)^2}N|Q_k|.$$

Let

$$\eta = \frac{\alpha^3}{48}M(6/\alpha)^{-2} \quad \text{and} \quad \delta = \Big(\frac{\eta}{10W}\Big)^{t/(2t-p)} \quad \text{and} \quad \varepsilon = \frac{\eta\cdot\delta^p}{10\cdot 2^p}.$$

For a sufficiently small $\alpha > (\log\log N)^{-\omega(N)}$ and sufficiently large N a straightforward computation shows that

$$|\Gamma|\|\Gamma\|_u^{-1} = N^{\gamma-\beta} > 2\left(\frac{(2^p 20)}{\varepsilon\delta^p}\right)^{(2/\delta)^p}. \tag{9}$$

This puts us in the position to apply Lemma 11 as argued in the following.

Given a set $A \subset \Gamma$ with $|A| \geq \alpha|\Gamma|$ let

$$S = Spec_\delta(A) = \{\xi \in \widehat{\mathbb{Z}}_N : |\widehat{A}(\xi)| \geq \delta|\Gamma|\}$$

denote the δ-*spectrum* of A. Due to Theorem 4 we have

$$|Spec_\delta(A)| \leq (2/\delta)^p. \tag{10}$$

By Theorem 8 there is a $\varrho \in [\varepsilon/2, \varepsilon]$ such that the Bohr set $B = B(S,\varrho) = \{y \in \widehat{\mathbb{Z}}_N \colon |\xi(y)-1| \leq \varrho \text{ for all } \xi \in S\}$ is regular. Hence, we can apply Lemma 11 with S and ε to conclude that the function $a = \frac{N}{|\Gamma||B|}(A*B)$ satisfies $\|a\|_1 \geq \alpha N$ and $\|a\|_\infty \leq 3$. From (3) of Lemma 7 we obtain

$$\sum_{x,d\in\mathbb{Z}_N} a(x)a(x+d)Q_k(d) \geq \eta N|Q_k|. \tag{11}$$

Assume that A does not satisfy the conclusion of Theorem 3, (actually we will even work under the following weaker assumption that A contains only "few" desired configuration)

$$\sum_{x,d\in\mathbb{Z}_N} A(x)A(x+d)Q_k(d) < \frac{\eta}{2}|\Gamma|^2\frac{|Q_k|}{N}. \tag{12}$$

We will derive an upper bound contradicting (11) as follows.

Due to inversion and orthogonality of characters we have

$$\begin{aligned}\sum_{x,d\in\mathbb{Z}_N} & A(x)A(x+d)Q_k(d) \\ &= \frac{1}{N^3}\sum_{x,d\in\mathbb{Z}_N}\sum_{\xi_1,\xi_2,\xi_3\in\widehat{\mathbb{Z}}_N}\widehat{A}(\xi_1)\widehat{A}(\xi_2)\widehat{Q}_k(\xi_3)e(x(\xi_1+\xi_2))e(d(\xi_1+\xi_3)) \\ &= \frac{1}{N}\sum_{\xi\in\widehat{\mathbb{Z}}_N}\widehat{A}(\xi)\widehat{A}(-\xi)\widehat{Q}_k(\xi). \end{aligned}\tag{13}$$

Hence, (12) translates to

$$\frac{\eta}{2}N|Q_k| - \frac{N}{|\Gamma|^2}\sum_{\xi\in\widehat{\mathbb{Z}}_N}\widehat{A}(\xi)\widehat{A}(-\xi)\widehat{Q}_k(\xi) > 0. \tag{14}$$

Further, by the definition of a we obtain due to the convolution property that

$$\sum_{x,d\in\mathbb{Z}_N} a(x)a(x+d)Q_k(d) = \frac{1}{N}\sum_{\xi\in\widehat{\mathbb{Z}}_N} \widehat{a}(\xi)\widehat{a}(-\xi)\widehat{Q}_k(\xi)$$
$$= \frac{N}{|\Gamma|^2}\sum_{\xi\in\widehat{\mathbb{Z}}_N} \widehat{A}(\xi)\widehat{A}(-\xi)\widehat{Q}_k(\xi)\frac{\widehat{B}(\xi)\widehat{B}(-\xi)}{|B|^2}. \tag{15}$$

Hence, adding the left hand side of (14) to the right hand side of (15) we obtain

$$\sum_{x,d\in\mathbb{Z}_N} a(x)a(x+d)Q_k(d) < \frac{N}{|\Gamma|^2}\sum_{\xi\in\widehat{\mathbb{Z}}_N} |\widehat{A}(\xi)|^2|\widehat{Q}_k(\xi)|\left|\frac{|\widehat{B}(\xi)|^2}{|B|^2}-1\right| + \frac{\eta}{2}N|Q_k|.$$

To derive a contradiction to (11) it is now sufficient to show that

$$\sum_{\xi\in\widehat{\mathbb{Z}}_N} |\widehat{A}(\xi)|^2|\widehat{Q}_k(\xi)|\left|\frac{|\widehat{B}(\xi)|^2}{|B|^2}-1\right| \le \eta|\Gamma|^2|Q_k|/2.$$

To this end, we split the sum on the left hand into one over $\xi\in S = Spec_\delta(A)$ and another over $\xi\notin S$. To estimate the first sum, recall from (10) that $|S|\le(2/\delta)^p$ and from Proposition 9 we know for all $\xi\in S$

$$\left|\frac{|\widehat{B}(\xi)|}{|B|}-1\right|\le\varrho \quad \text{hence} \quad \left|\frac{|\widehat{B}(\xi)|^2}{|B|^2}-1\right|\le 2\varrho.$$

We now conclude that

$$\sum_{\xi\in S} |\widehat{A}(\xi)|^2|\widehat{Q}_k(\xi)|\left|\frac{|\widehat{B}(\xi)|^2}{|B|^2}-1\right| \le 2\varrho|S||\widehat{A}(0)|^2|\widehat{Q}_k(0)| \le \eta|\Gamma|^2|Q_k|/4$$

due to the choice of ε and $\varrho\in[\varepsilon/2,\varepsilon]$.

Using (7) of Lemma 12 we derive that the sum over $\xi\notin S$ is at most

$$2\sum_{\xi\in\widehat{\mathbb{Z}}_N\setminus S} |\widehat{A}(\xi)|^2|\widehat{Q}_k(\xi)| \le 2W\delta^{(2t-p)/t}|\Gamma|^2|Q_k| \le \eta|\Gamma|^2|Q_k|/4$$

due to the choice of δ. This concludes the proof. □

Remark 13. Note that the proof indeed implies that a set $A\subset\Gamma$ of density α as in the Theorem 3 contains at least $\frac{\eta}{2}|\Gamma|^2\frac{|Q_k|}{N} = \frac{\alpha^3}{96}M(6/\alpha)^{-2}\left(\frac{|\Gamma|}{N}\right)^2 N|Q_k|$ configurations of the form $x, x+d$, $d\in Q_k$. Up to the the factor η this bound is best possible.

7. A restriction theorem - Proof of Theorem 4

In this section we prove Theorem 4. We first introduce some notation. Let $\mathbb{Z}_N$ be endowed with the counting measure μ and its dual $\widehat{\mathbb{Z}}_N$ be endowed with the normalised counting measure ν. Given a function $g:\widehat{\mathbb{Z}}\to\mathbb{C}$ we define the inverse Fourier of g to be $g^\vee$ determined by

$$g^\vee(x) = \int_{\eta\in\widehat{\mathbb{Z}}_N} g(\eta)e(\eta x)d\nu = \frac{1}{N}\sum_{\eta\in\widehat{\mathbb{Z}}_N} g(\eta)e(\eta x). \tag{16}$$

Given a subset $\Lambda \subset \widehat{\mathbb{Z}}_N$ we endow Λ with the induced measure λ, i.e. the normalised counting measure $\lambda(\eta) = \Lambda(\eta)/|\Lambda|$ on Λ. Thus, Λ has total mass 1 and we define the restricted Fourier transform on Λ via

$$(gd\lambda)^\vee(x) = \sum_{\eta \in \widehat{\mathbb{Z}}_N} g(\eta)\lambda(\eta)e(\eta x). \tag{17}$$

Let $B(\mathbb{Z}_N, \mu)$ denote the space of all functions $f : \mathbb{Z}_N \to \mathbb{C}$. We are interested in the linear operator called *restriction map*

$$T^* : B(\mathbb{Z}, \mu) \to B(\Lambda, \lambda) \quad \text{given by} \quad f \mapsto \widehat{f}_{|\Lambda}.$$

It is easy to check that its adjoint operator is

$$T : B(\Lambda, \lambda) \to B(\mathbb{Z}, \mu) \quad \text{given by} \quad g \mapsto (gd\lambda)^\vee.$$

Lastly, let $\|T\|_{r\to q}$ be the infimum of all C such that

$$\|Tf\|_{L^q(\mathbb{Z}_N, d\mu)} \leq C\|f\|_{L^r(\Lambda, d\lambda)}$$

for all $f \in B(\Lambda, \lambda)$. The main objective of this section is to establish the following.

Theorem 14. *Let p and T be defined as above. Then $\|T\|_{2\to p} \leq 2$, i.e. for all $f \in B(\Lambda, \lambda)$ we have*

$$\|Tf\|_{L^p(\mathbb{Z}_N, \mu)} \leq 2\|f\|_{L^2(\Lambda, \lambda)}.$$

With this result Theorem 4 easily follows.

Proof of Theorem 4. Recall that $\mathbb{Z}_N$ is isomorphic to its dual $\widehat{\mathbb{Z}}_N$ and that $g^\vee(x) = \widehat{g}(-x)$. With this in mind let $A \subset \Lambda \subset \widehat{\mathbb{Z}}_N$ be given. Then

$$(Ad\lambda)^\vee(r) = \frac{1}{|\Lambda|}\sum_{\eta \in \widehat{\mathbb{Z}}_N} A(\eta)e(r\eta) = \frac{\widehat{A}(-r)}{|\Lambda|},$$

from which we derive

$$\|(Ad\lambda)^\vee\|^p_{L^p(\mathbb{Z}_N, \mu)} = \frac{1}{|\Lambda|^p}\sum_{r\in\mathbb{Z}} |\widehat{A}(-r)|^p \leq 2^p\|A\|^p_{L^2(\Lambda,\lambda)} = 2^p\left(\frac{|A|}{|\Lambda|}\right)^{p/2}$$

and the theorem follows. □

The proof of Theorem 14 will utilise the following principle

$$\|T\|^2_{2\to p} = \|T^*\|^2_{p'\to 2} = \|TT^*\|_{p'\to p}$$

where p' is the dual index of p, i.e. $p' = (2-2\gamma)/(2-\gamma-\beta)$. Indeed, we will need $\|T\|_{2\to p}^2 \le \|TT^*\|_{p'\to p}$ only. This is easily seen by using Hölder's inequality

$$\begin{aligned}
\|Tf\|_p &= \sup_{\|g\|_{p'}=1} \langle Tf, g\rangle \\
&= \sup_{\|g\|_{p'}=1} \langle f, T^*g\rangle \\
&\le \|f\|_2 \sup_{\|g\|_{p'}=1} \|T^*g\|_2 \\
&= \|f\|_2 \sup_{\|g\|_{p'}=1} \langle g, TT^*g\rangle^{1/2} \\
&\le \|f\|_2 \sup_{\|g\|_{p'}=1} \|g\|_{p'}^{1/2} \|TT^*g\|_p^{1/2} \\
&= \|f\|_2 \|TT^*\|_{p'\to p}^{1/2}
\end{aligned}$$

Further, we will utilise the following interpolation theorem, see [7].

Theorem 15 (Riesz-Thorin interpolation theorem)**.** *Let $L : B(X) \to B(Y)$ be a linear operator and suppose that $p_0, p_1, q_0, q_1 \in [1,\infty]$ satisfy $p_0 < p_1$ and $q_0 < q_1$. For any $t \in [0,1]$ define p_t and q_t by*

$$\frac{1}{p_t} = \frac{1-t}{p_0} + \frac{t}{p_1} \quad \text{and} \quad \frac{1}{q_t} = \frac{1-t}{q_0} + \frac{t}{q_1}.$$

Then

$$\|L\|_{p_t\to q_t} \le \|L\|_{p_0\to q_0}^{1-t} \|L\|_{p_1\to q_1}^{t}.$$

□

We are now in the position to prove Theorem 14.

Proof of Theorem 14. Note that the map

$$TT^* : B(\mathbb{Z}_N, \mu) \to B(\mathbb{Z}_N, \mu) \quad \text{is given by} \quad f \mapsto f * (d\lambda)^\vee$$

As $(d\lambda)^\vee(r)$ expands to

$$(d\lambda)^\vee(r) = \sum_\eta \lambda(\eta) e(r\eta) = \frac{1}{|\Lambda|}\widehat{\Lambda}(-r)$$

we have $(d\lambda)^\vee(0) = 1$ and, by the pseudorandomness assumption, $(d\lambda)^\vee(r) \le N^{\gamma-\beta}$ for $r \neq 0$. We define $K = (d\lambda)^\vee - \delta_0$, which is $(d\lambda)^\vee$ with the origin removed. Then K satisfies

$$\|K\|_\infty \le N^{\gamma-\beta} \quad \text{and} \quad \|\widehat{K}\|_\infty = \max_\eta N d\lambda(\eta) - 1 \le N^{1-\beta}.$$

To show $\|TT^*\|_{p'\to p} \le 2$, i.e.

$$\|f * \delta_0 + f * K\|_{L^p(\mathbb{Z}_N,\mu)} \le 2\|f\|_{L^{p'}(\mathbb{Z}_N,\mu)}$$

we first note that $\|f*\delta_0\|_{L^p(\mathbb{Z}_N,\mu)} \le \|f\|_{L^{p'}(\mathbb{Z}_N,\mu)}$ as $p \ge p'$. To finish the proof we need to establish

$$\|f * K\|_{L^p(\mathbb{Z}_N,\mu)} \le \|f\|_{L^{p'}(\mathbb{Z}_N,\mu)}. \tag{18}$$

To do so, we will use the Riesz-Thorin interpolation theorem, Theorem 15, to interpolate between L^1-L^∞ and L^2-L^2 norm. For the former we obtain the bound

$$\|f * K\|_\infty \le \|K\|_\infty \|f\|_{L^1(\mathbb{Z}_N,\mu)} \le N^{\gamma-\beta}\|f\|_{L^1(\mathbb{Z}_N,\mu)}.$$

A bound for the latter follows from Plancherel and $\|\widehat{K}\|_\infty \leq N^{1-\beta}$:

$$\|f * K\|_{L^2(\mathbb{Z}_N,\mu)} = \|\widehat{f}\widehat{K}\|_{L^2(\widehat{\mathbb{Z}}_N,\nu)} \leq \|\widehat{K}\|_\infty \|\widehat{f}\|_{L^2(\widehat{\mathbb{Z}}_N,\nu)} \leq N^{1-\beta}\|f\|_{L^2(\mathbb{Z}_N,\mu)}.$$

We choose $q_0 = \infty$, $p_0 = 1$, $q_1 = 2$, $p_1 = 2$ and $t = \frac{\beta-\gamma}{1-\gamma} \in [0,1]$ and apply the Riesz-Thorin interpolation theorem with the linear operator $f \mapsto f * K$ to obtain

$$\frac{1}{p}_t = \frac{(1-t)}{p_0} + \frac{t}{p_1} = \frac{1}{p'} \qquad \text{and} \qquad \frac{1}{q_t} = \frac{(1-t)}{q_0} + \frac{t}{q_1} = \frac{1}{p}$$

and

$$\|f * K\|_{L^p(\mathbb{Z}_N,\mu)} \leq N^{(\gamma-\beta)(1-t)} N^{(1-\beta)t} \|f\|_{L^{p'}(\mathbb{Z}_N,\mu)} = \|f\|_{L^{p'}(\mathbb{Z}_N,\mu)}$$

which establish (18) and the theorem follows. □

References

1. A. Balog, J. Pelikán, J. Pintz, and E. Szemerédi, *Difference sets without κth powers*, Acta Math. Hungar. **65** (1994), no. 2, 165–187.
2. J. Bourgain, *On triples in arithmetic progression*, Geom. Funct. Anal. **9** (1999), no. 5, 968–984.
3. D. Conlon and W.T. Gowers, *Combinatorial theorems in sparse random sets*, submitted.
4. David Conlon, Jacob Fox, and Yufei Zhao, *Extremal results in sparse pseudorandom graphs*, submitted.
5. Harry Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. **31** (1977), 204–256.
6. M. Gauy, H. Hàn, and I. Oliveira, *Erdos-Ko-Rado for random hypergraphs: asymptotics and stability*, submitted.
7. Ben Green, *Restriction and Kakeya phenomena*, notes from a course given in Part III of the Cambridge Mathematical Tripos (2002).
8. Ben Green, *On arithmetic structures in dense sets of integers*, Duke Math. J. **114** (2002), no. 2, 215–238.
9. Ben Green, *Roth's theorem in the primes*, Ann. of Math. (2) **161** (2005), no. 3, 1609–1636.
10. M. Hamel, N. Lyall, and A. Rice, *mproved bounds on sarkozy's theorem for quadratic polynomials*, Int. Math. Res. Notices (2013), no. 8, 1761–1782.
11. G. H. Hardy and J. E. Littlewood, *A new solution of Waring's problem*, Q. J. Math. **48** (1919), 272–293.
12. Balogh József, Morris Robert, and Wojciech Samotij, *Independent sets in hypergraphs*, submitted.
13. Yoshiharu Kohayakawa, Vojtěch Rödl, Mathias Schacht, and Jozef Skokan, *On the triangle removal lemma for subgraphs of sparse pseudorandom graphs*, An irregular mind, Bolyai Soc. Math. Stud., vol. 21, János Bolyai Math. Soc., Budapest, 2010, pp. 359–404.
14. I. Łaba and M. Hamel, *Arithmetic structures in random sets*, Integers: Elec. J. of combin. num. th. **8** (2008), 21.
15. Gerd Mockenhaupt and Terence Tao, *Restriction and Kakeya phenomena for finite fields*, Duke Math. J. **121** (2004), no. 1, 35–74.
16. Melvyn B. Nathanson, *Additive number theory*, Graduate Texts in Mathematics, vol. 164, Springer-Verlag, New York, 1996, The classical bases.
17. H. H. Nguyen, *On two-point configurations in random set*, Integers **9** (2009), 41–45.
18. János Pintz, W. L. Steiger, and Endre Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. (2) **37** (1988), no. 2, 219–231.
19. I. Z. Ruzsa, *Difference sets without squares*, Period. Math. Hungar. **15** (1984), no. 3, 205–209.
20. A. Sárkőzy, *On difference sets of sequences of integers. I*, Acta Math. Acad. Sci. Hungar. **31** (1978), no. 1–2, 125–149.
21. David Saxton and Andrew Thomason, *Hypergraphs containers*, submitted.
22. M. Schacht, *Extremal results for random discrete structures*, submitted.
23. T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2010.

24. Terence Tao and Tamar Ziegler, *The primes contain arbitrarily long polynomial progressions*, Acta Math. **201** (2008), no. 2, 213–305.
25. Peter A. Tomas, *A restriction theorem for the Fourier transform*, Bull. Amer. Math. Soc. **81** (1975), 477–478.
26. P. Varnavides, *On certain sets of positive density*, J. London Math. Soc. **34** (1959), 358–360.